UNIVERSIDAD NACIONAL DE CÓRDOBA

FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

SERIE "B"

TRABAJOS DE MATEMÁTICA

N° 63/12

VI Encuentro de Nacional de Álgebra

Notas de Cursos

2 al 4 de agosto de 2012, La Falda, Sierras de Córdoba.

Iván Angiono – Nicolás Botbol – Rodrigo Iglesias
Emilio Lauret – Federico Quallbrunn – Ricardo Toledano

Editores: Jorge G. Adrover – Gastón A. García

CIUDAD UNIVERSITARIA – (5000) CÓRDOBA
REPÚBLICA ARGENTINA

La presente publicación fue financiada por el CIEM con fondos del CONICET, CCT-Cba.

Prefacio

Los Encuentros Nacionales de Álgebra vienen realizándose en las Sierras de Córdoba, periódicamente y con gran éxito, desde que en 2003 tuvo lugar el primero. El segundo Encuentro *elENA II* se realizó en 2004 y a partir de éste se hicieron en forma bianual: *elENA III* (2006), *elENA IV* (2008) y *elENA V* (2010).

El *Sexto Encuentro Nacional de Álgebra elENA VI*, se llevará a cabo durante los días 2 al 4 de agosto de 2012, en el Hotel del Lago, la Falda, Sierras de Córdoba, con la presencia de numerosos matemáticos del país y también del extranjero. En esta ocasión, el encuentro será un congreso satélite del *IV Congreso Latinoamericano de Matemáticos*, *IV CLAM*, que se realizará en la Ciudad de Córdoba del 6 al 10 de agosto de 2012. Además, durante la semana que se desarrollará el IV CLAM, tendrá lugar la Reunión Anual de la Unión Matemática Argentina, la Reunión de Educación Matemática, el Encuentro de Estudiantes y el IV Festival de Matemáticas. Por esta razón, esperamos contar con la grata presencia de representantes y estudiantes de universidades y centros tanto de todo el territorio argentino como del exterior, entre ellos participantes de Bolivia, Brasil, Chile, Colombia, El Salvador, España, Estados Unidos, Guatemala, Mexico, Paraguay, Perú.

En nombre del Comité Organizador nos es grato poner aquí a disposición de los asistentes a dichos cursos, y del ocasional lector, las notas de los cursos dictados en dicho encuentro. Aprovechamos esta oportunidad para agradecer a todos los cursistas por preparar sus cursos y muy especialmente a aquellos que se han tomado el enorme trabajo de escribir estas notas con antelación, para que estén disponibles al momento del encuentro. Éstas representan sin duda una gran ayuda para el seguimiento y mejor aprovechamiento de los cursos por parte de los asistentes.

Gastón A. García Carolina Maldonado Ricardo Podestá

Córdoba, 1 de julio de 2012.

Contenidos

Cursos de Nivel Básico

Cursos de Nivel Intermedio

Cursos de Nivel Avanzado

Cursos de Nivel Básico

GRUPOS DE COXETER Y SU COMBINATORIA

IVÁN ANGIONO

RESUMEN. Estudiaremos los grupos de Coxeter partiendo de sus propiedades asociadas a la función longitud y expresiones reducidas para un conjunto de generadores fijo. Introduciremos dos órdenes parciales entre los elementos del grupo y daremos su relación también con las expresiones reducidas. Finalmente introduciremos el conjunto de raíces asociado a un grupo de Coxeter y parte de su utilidad para obtener resultados sobre el grupo.

ÍNDICE

INTRODUCCIÓN

Una de las cuestiones que más llama la atención de las matemáticas es, a mi juicio, la traducción de un problema de un área en un problema de otro área, a veces completamente diferente, para simplificar notoriamente la obtención de la respuesta que se busca. Un ejemplo claro está relacionado con los grupos de Lie. En primer lugar se traducen varias preguntas sobre su comportamiento a preguntas sobre el álgebra de Lie asociada, y el problema inicialmente geométrico/análitico se traduce en un problema algebraico. En el caso de algunas de esas álgebras podemos considerar un grupo asociado, el grupo de Weyl, generado por elementos de orden 2 y satisfaciendo algunas

2010 *Mathematics Subject Classification.* 20F05, 20F55.

El trabajo del autor está parcialmente financiado por los siguientes organismos: CONICET, FONCyT-ANPCyT, Secyt (UNC).

propiedades especiales, lo cual traduce parte del problema a estudiar en otro problema algebraico, pero referido a la teoría de grupos. Sin embargo, en este contexto aparecen los grupos de Coxeter, que generalizan esta idea y traducen nuestras preguntas al ámbito combinatorio.

Y aquí aparece otra cuestión importante: el desarrollo de una teoría como la de grupos de Coxeter, que vio la luz generalizando los grupos de Weyl, tiene consecuencias fundamentales en otras áreas de la matemática. En este caso, además de su aplicación a la teoría de Lie, los grupos de Coxeter y su rica combinatoria tienen un fuerte impacto en problemas algorítmicos, topológicos y algebraicos de distinta índole, algunos de ellos de gran dificultad como los asociados a los polinomios de Kazhdan-Lusztig, ver [1, 4].

En estas notas descubriremos la teoría básica asociada a estos grupos. En primer lugar daremos su definición y mostraremos algunos ejemplos conocidos que resultan ser grupos de Coxeter. Estudiaremos sus primeras propiedades, tales como la propiedad de Intercambio o la propiedad de Supresión, que caracterizan al grupo. En la segunda parte, introduciremos el orden de Bruhat y conoceremos una caracterización importante del mismo, así como una descripción de sus intervalos y aplicaciones a grupos de Coxeter finitos. También conoceremos otro orden, el débil, y algunas propiedades. En la última parte mostraremos una representación fiel del grupo, que nos permitirá interpretarlo como un grupo generado por reflexiones en algún espacio vectorial $\mathbb{R}^n$, las consecuencias de la existencia de dicha representación y la introducción del sistema de raíces asociado.

Notación. $\mathbb{N}$ denotará el conjunto de números naturales, $\mathbb{N}_0$ el de enteros no negativos y $\mathbb{N}_\infty$ el conjunto $\mathbb{N} \cup \{\infty\}$. Dado $n \in \mathbb{N}$, $\mathbb{I}_n$ denotará el conjunto $\{1, 2, \dots, n\}$.

Dados a, b elementos de un conjunto A, $\delta_{a,b}$ es el símbolo de Kronecker; es decir, $\delta_{a,b} = 0$ si $a \neq b$, $\delta_{a,b} = 1$ si $a = b$.

Dado un producto ordenado $s_1 \cdots s_n$ de elementos s_i de un grupo, denotaremos

$$s_1 \cdots \widehat{s_{i_1}} \cdots \widehat{s_{i_k}} \cdots s_n, \qquad 1 \leq i_1 < \ldots < i_k \leq n,$$

al producto ordenado que resulta de quitar $s_{i_1}, \dots, s_{i_k}$.

1. Grupos de Coxeter: definición, ejemplos, propiedades

Los grupos de Coxeter se definen a partir de una presentación por generadores y relaciones. A continuación presentaremos dicha definición diferentes ejemplos, desde los más conocidos hasta los relacionados con las diferentes aplicaciones; en efecto, explicaremos algunos de los usos de esta familia de grupos. Finalmente consideraremos las propiedades básicas que tienen estos grupos, relacionadas especialmente con la longitud, y describiremos una familia de subgrupos, que resultan ser también grupos de Coxeter. Los resultados fueron extraídos principalmente de [1, 2], recomendamos fuertemente leer estos libros a quien se interese en el tema.

1.1. Definiciones y propiedades básicas.

Consideramos para empezar dos definiciones que nos serán útiles para introducir los grupos de Coxeter.

Definición 1.1. Sea $\mathcal{S}$ un conjunto. $M \in \mathbb{N}_\infty^{\mathcal{S}\times\mathcal{S}}$ es una *matriz de Coxeter* si

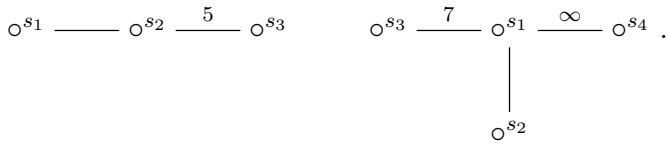
- es simétrica, o sea $m_{ij} = m_{ji}$ para todo par de elementos $i, j \in \mathcal{S}$, y
- $m_{ij} = 1$ si y solamente si $i = j$.

Un *diagrama de Coxeter* es un grafo cuyo conjunto de vértices es $\mathcal{S}$, y cuyas aristas son los conjuntos de dos elementos $\{i, j\}$, con $i \neq j \in \mathcal{S}$ tales que $m_{ij} \geq 3$. Las aristas tales que $m_{ij} \geq 4$ están etiquetadas con $m_{ij} = m_{ji}$.

Ejemplo 1.2. Las siguientes matrices son de Coxeter:

$$\begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 5 \\ 2 & 5 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 3 & 7 & \infty \\ 3 & 1 & 2 & 2 \\ 7 & 2 & 1 & 2 \\ \infty & 2 & 2 & 1 \end{pmatrix}. \tag{1.1}$$

Sus respectivos diagramas de Coxeter son:



Como en [2], consideramos un grupo $\mathbf{W}$ con unidad 1, y $\mathcal{S}$ un conjunto de generadores tal que $\mathcal{S}^{-1} = \mathcal{S}$. La *longitud* de w con respecto a $\mathcal{S}$ se define como

$$\ell_{\mathcal{S}}(w) := \text{mín}\{n \in \mathbb{N}_0 : \exists s_1, \dots, s_k \in \mathcal{S} \text{ tales que } w = s_1 \cdots s_k\}.$$

En general $\mathcal{S}$ estará determinado por el contexto, y denotaremos simplemente $\ell(w)$ a la longitud. Una expresión $w = s_1 \cdots s_k$ se dice *reducida* si $k = \ell(w)$.

Observación 1.3. Algunas de las propiedades básicas de las expresiones reducidas y la función longitud son las siguientes:

- Si $x, w \in \mathbf{W}$, se verifican las siguientes fórmulas:
$$\ell(xw) \leq \ell(x) + \ell(w), \qquad \ell(w) = \ell(w^{-1}), \qquad |\ell(w) - \ell(x)| \leq \ell(wx^{-1}).$$
- Si $w = s_1 \cdots s_p s_{p+1} \cdots s_k$ es una expresión reducida, entonces $w_1 = s_1 \cdots s_p$ y $w_2 = s_{p+1} \cdots s_k$ son expresiones reducidas.
- Si $w_1 = s_1 \cdots s_p$ y $w_2 = s'_1 \cdots s'_q$ son dos expresiones de w_1 y w_2, y $\ell(w_1 w_2) = p+q$, entonces las expresiones anteriores son reducidas.

Ahora asociaremos a cada matriz de Coxeter M sobre $\mathcal{S}$ (o equivalentemente a cada diagrama de Coxeter) un grupo de Coxeter. Fijemos M una matriz de Coxeter. $\mathcal{S}^2_{\text{fin}}$ es el conjunto de pares (s,t), $s,t \in \mathcal{S}$, tales que $m_{st} < \infty$.

Definición 1.4. Decimos que $(\mathbf{W}, \mathcal{S})$ es un *sistema de Coxeter* si $\mathbf{W}$ es el grupo presentado por generadores $\mathcal{S}$, y relaciones $(st)^{m_{st}} = 1$, para cada par $(s,t) \in \mathcal{S}^2_{\text{fin}}$. Esto es, $\mathbf{W}$ es isomorfo al cociente F/N, donde F es el grupo libre generado por $\mathcal{S}$, y N es el subgrupo normal generado por $(st)^{m_{st}}$, $(s,t) \in \mathcal{S}^2_{\text{fin}}$.

En tal caso, $\mathbf{W}$ se dice un *grupo de Coxeter*, y $\mathcal{S}$ es el conjunto de *generadores de Coxeter*. El *rango* de $(\mathbf{W}, \mathcal{S})$ es el cardinal de $\mathbf{W}$. El sistema es *irreducible* si el diagrama de Coxeter es conexo.

Veremos más adelante que existe una correspondencia biyectiva entre matrices de Coxeter y sistemas de Coxeter, salvo isomorfismo.

Observación 1.5. Notar que en particular $s^2 = 1$, para todo $s \in \mathcal{S}$, pues $m_{ss} = 1$. Además, la relación $(st)^{m_{st}} = 1$ es equivalente a:

$$\underbrace{ststs\cdots}_{m_{st} \text{ elementos}} = \underbrace{tstst\cdots}_{m_{st} \text{ elementos}}.$$

Observación 1.6. Sea $\pi : F \twoheadrightarrow \mathbf{W}$ la proyección canónica desde el grupo libre F generado por $\mathcal{S}$. Un morfismo de grupos $\Phi : F \to G$, donde G es un grupo arbitrario, está caracterizado simplemente por una función $\phi : \mathcal{S} \to G$; es decir, Φ es el único

morfismo de grupos tal que $\Phi|_{\mathcal{S}} = \phi$. Luego, Φ induce un morfismo de grupos $\widetilde{\Phi} : \mathbf{W} \to G$ si y sólo si $N \subseteq \ker \Phi$; i.e., existe $\widetilde{\Phi} : \mathbf{W} \to G$ tal que $\widetilde{\Phi} \circ \pi = \Phi$ si y sólo si

$$\Phi(s)^2 = e, \quad (\Phi(s)\Phi(t))^{m_{st}} = \Phi\left((st)^{m_{st}}\right) = 1, \qquad \text{para todo par } s, t \in \mathcal{S}. \tag{1.2}$$

Por ejemplo, $\Phi : F \to \{\pm 1\}$ definido por $\Phi(s) = -1$ para todo $s \in \mathcal{S}$, induce un morfismo $\widetilde{\Phi} : \mathbf{W} \to \{\pm 1\}$. Notar que $\widetilde{\Phi}(w) = (-1)^{\ell(w)}$ para todo $w \in \mathbf{W}$, con lo cual

$$\ell(ww') \equiv \ell(w) + \ell(w') \mod 2 \quad \text{para todo par de elementos } w, w' \in \mathbf{W}. \tag{1.3}$$

Ejemplo 1.7. Para la primer matriz del Ejemplo 1.1, el grupo de Coxeter es el generado por s_i, $i \in \mathbb{I}_3$, y las siguientes relaciones:

$$s_1^2 = s_2^2 = s_3^2 = 1, \qquad s_1 s_2 s_1 = s_2 s_1 s_2,$$
$$s_2 s_3 s_2 s_3 s_2 = s_3 s_2 s_3 s_2 s_3, \qquad s_1 s_3 = s_3 s_1.$$

Para la segunda matriz, el grupo de Coxeter es el generado por s_i, $i \in \mathbb{I}_4$, y las relaciones:

$$s_1^2 = s_2^2 = s_3^2 = s_4^2 = 1, \qquad s_1 s_2 s_1 = s_2 s_1 s_2,$$
$$s_1 s_3 s_1 s_3 s_1 s_3 s_1 = s_3 s_1 s_3 s_1 s_3 s_1 s_3, \qquad s_2 s_3 = s_3 s_2,$$
$$s_3 s_4 = s_4 s_3, \qquad s_2 s_4 = s_4 s_2.$$

1.2. Ejemplos clásicos. A continuación interpretaremos varios grupos *conocidos* como grupos de Coxeter, para algún conjunto de generadores $\mathcal{S}$ adecuado.

Ejemplo 1.8. $(\mathbf{W} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2, \{e_1, \dots, e_n\})$, donde e_i es el generador de la i-ésima copia de $\mathbb{Z}_2$, es un sistema de Coxeter cuyo grupo es de orden 2^n. Su diagrama de Coxeter consta de n vértices desconectados, pues su matriz de Coxeter es $m_{ii} = 1$, $m_{ij} = 2$ si $i \neq j$.

Ejemplo 1.9. El grafo completo de n vértices cuyas aristas están etiquetadas con ∞ corresponde al *grupo de Coxeter universal* U_n de rango n. Es el grupo generado por n elementos de orden 2, sin relaciones extras, cuyos elementos son todas las palabras en n letras que no tienen dos letras iguales repetidas.

El nombre proviene del hecho que, si $(\mathbf{W}, \mathcal{S})$ es otro grupo de Coxeter con n generadores, existe un morfismo suryectivo de grupos $U_n \twoheadrightarrow \mathbf{W}$ para cada biyección $\mathbb{I}_n \to \mathcal{S}$.

Ejemplo 1.10. Recordemos que el *grupo simétrico* $\mathbb{S}_n$, es decir, el grupo de permutaciones de $\mathbb{I}_n$, admite una presentación por generadores s_i, $1 \leq i \leq n-1$ y relaciones:

$$s_i^2 = 1, \quad s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \quad s_i s_j = s_j s_i \text{ si } |i-j| \geq 2,$$

donde $s_i = (i, i+1)$ es la biyección que permuta los elementos i e $i+1$, y por lo tanto tiene orden 2. En consecuencia, su matriz de Coxeter tiene como entradas $m_{ii} = 1$, $m_{i,i\pm 1} = 3$, $m_{ij} = 2$ si $|i-j| \geq 2$, y su diagrama de Coxeter es:

$$\circ^{s_1} \text{——} \circ^{s_2} \text{——} \cdots \text{——} \circ^{s_{n-1}}.$$

Ejemplo 1.11. Si consideramos el diagrama de Coxeter infinito:

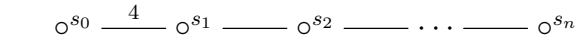
$$\circ^{s_1} \text{——} \circ^{s_2} \text{——} \circ^{s_3} \text{——} \circ^{s_4} \text{——} \cdots$$

el grupo correspondiente es el de biyecciones de $\mathbb{N}$ que mueven a lo sumo una cantidad finita de elementos. Es decir, el conjunto de biyecciones $\sigma : \mathbb{N} \to \mathbb{N}$ tales que el conjunto $\{n \in \mathbb{N} : \sigma(n) \neq n\}$ es finito. El mismo admite una presentación por generadores s_i, $i \geq 1$ y relaciones como en el caso de $\mathbb{S}_n$.

Ejemplo 1.12. Supongamos ahora que tenemos un conjunto de cartas numeradas de 1 a n, donde en la parte superior de la j-ésima carta se escribe $+j$, y en la parte inferior $-j$. Nuestro nuevo grupo $\mathbb{S}_n^B$ consta de todas las formas de ordenar las cartas, pudiendo poner hacia arriba $+j$ o $-j$ para cada carta. Así, un elemento del grupo es una permutación de $\mathbb{I}_n$ junto con la información de los signos, es decir una función $\mathbb{I}_n \to \{+,-\}$; luego, $|\mathbb{S}_n^B| = 2^n \cdot n!$. Podemos probar que el grupo $\mathbb{S}_n^B$ está generado por las mismas s_i, $1 \leq i \leq n-1$ (las biyecciones que cambian de lugar las cartas de las posiciones i e $i+1$, sin modificar la cara que está hacia arriba) y s_0, el elemento que voltea la carta que está en la parte superior de la pila. Es claro que $s_0 s_i = s_i s_0$ para cada $i > 1$, mientras que $s_0 s_1 s_0 s_1 = s_1 s_0 s_1 s_0$, pues ambas operaciones son:

$$(+1, +2, +3, \cdots, +n) \mapsto (-1, -2, +3, \cdots, +n).$$

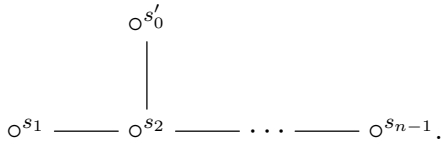
En consecuencia, el diagrama de Coxeter de $\mathbb{S}_n^B$ es:



Este grupo admite un subgrupo $\mathbb{S}_n^D$ que consiste de todos los movimientos de la pila que rotan un número par de cartas. Ahora, $s_0' = s_0 s_1 s_0$ es la simetría

$$(+1, +2, +3, \cdots, +n) \mapsto (-2, -1, +3, \cdots, +n),$$

que toma las dos primeras cartas como un bloque y las voltea. Notar que $s_0' s_2 s_0' = s_2 s_0' s_2$, $s_0' s_1 = s_1 s_0'$, por lo cual el diagrama de Coxeter de $\mathbb{S}_n^D$ es:



Ejemplo 1.13. Consideremos dos rectas ℓ_1 y ℓ_2 en $\mathbb{R}^2$ que pasan por el origen tal que el ángulo entre ellas es π/m, con $m \geq 2$. Denotamos por r_1 y r_2 a las reflexiones ortogonales por ℓ_1 y ℓ_2, respectivamente, de modo que $r_1 r_2$ es la rotación de $\mathbb{R}^2$ por un ángulo $2\pi/m$. Luego, $(r_1 r_2)^m = \mathrm{id}$. Sea D_m el grupo generado por r_1 y r_2. Podemos identificarlo con el grupo de simetrías de un m-ágono regular, de modo que es un grupo finito, conocido como *grupo diedral*. Dicho grupo tiene orden $2m$, pues consta de todas las rotaciones del plano por un ángulo de $2\pi k/m$, $0 \leq k < m$, seguido o no de la rotación r_1.

Si consideramos el diagrama de Coxeter 

, el correspondiente grupo de Coxeter $I_2(m)$ está presentado por generadores s_1, s_2, y relaciones $s_1^2 = s_2^2 = e$, $(s_1 s_2)^m = e$, de modo que existe un morfismo suryectivo $\phi : I_2(m) \twoheadrightarrow D_m$ determinado por $s_i \mapsto r_i$. Ahora, de acuerdo a la Observación 1.5, todo elemento de $I_2(m)$ puede expresarse como una palabra $s_1 s_2 s_1 \cdots$ o $s_2 s_1 s_2 \cdots$, de longitud a lo sumo m, de modo que $|I_2(m)| \leq 2m = |D_m|$. Por lo tanto, ϕ es un isomorfismo, y cada grupo diedral es un grupo de Coxeter.

Notar que si el ángulo entre ℓ_1 y ℓ_2 no es de la forma $q\pi$, $q \in \mathbb{Q}$, entonces $r_1 r_2$ tiene orden infinito, y así obtenemos el grupo de Coxeter $I_2(\infty)$ asociado al diagrama de Coxeter

.

Podemos obtener de modo análogo los grupos de simetría de los poliedros regulares, o más generalmente (es decir, en dimensiones más grandes) de los polítopos regulares en $\mathbb{R}^d$, $d \geq 3$. En $\mathbb{R}^3$ los poliedros regulares y sus correspondientes grupos de simetría

son: tetraedro, con grupo de tipo A_3, es decir $\mathbb{S}_4$; cubo y octaedro, con grupo B_3, es decir $\mathbb{S}_3^B$; dodecaedro e icosaedro, con grupo H_3, que es el correspondiente al diagrama

$$\circ \overset{5}{\text{———}} \circ \text{———} \circ .$$

1.3. Propiedades de intercambio y de supresión. Fijemos $(\mathbf{W}, \mathcal{S})$ un sistema de Coxeter. Sean:

$$\mathcal{T} := \{wsw^{-1} : s \in \mathcal{S}, w \in \mathbf{W}\}, \qquad \mathcal{R} := \{1, -1\} \times \mathcal{T}. \tag{1.4}$$

Dada $\mathbf{s} = (s_1, \dots, s_n)$ una sucesión finita de elementos de $\mathcal{S}$, definimos

$$\Xi(\mathbf{s}) := (t_1, \dots, t_n), \qquad \text{donde } t_j = (s_1 \cdots s_{j-1}) s_j (s_{j-1} \cdots s_1) \in \mathcal{T},\ j \in \mathbb{I}_n. \tag{1.5}$$

Notar que $t_1 = s_1$, y además $s_1 \cdots s_n = t_n \cdots t_1$. Para cada $t \in \mathcal{T}$, denotaremos $n(\mathbf{s}, t)$ al número de enteros $j \in \mathbb{I}_n$ tales que $t_j = t$.

Lema 1.14. (i) *Para cada $w \in \mathbf{W}$ y $t \in \mathcal{T}$, la paridad de $n(\mathbf{s}, t)$ no depende de la sucesión de elementos $\mathbf{s}$ tal que $w = s_1 \cdots s_n$.*

Así, denotaremos $\eta(w, t) := (-1)^{n(\mathbf{s},t)}$, para cualquier sucesión $\mathbf{s}$ como antes.

(ii) *Sea $\mathbb{S}(\mathcal{R})$ el grupo de permutaciones de $\mathcal{R}$. Para cada $w \in \mathbf{W}$, sea $\mathbf{U}_w : \mathcal{R} \to \mathcal{R}$ la función definida por*

$$\mathbf{U}_w(\epsilon, t) := \left(\epsilon \eta(w^{-1}, t), wtw^{-1}\right), \qquad \epsilon = \pm 1, t \in \mathcal{T}. \tag{1.6}$$

Luego, $\mathbf{U} : \mathbf{W} \to \mathbb{S}(\mathcal{R})$, $w \mapsto \mathbf{U}_w$ es un morfismo de grupos.

Demostración. Sea F el grupo libre generado por $\mathcal{S}$ como en la Observación 1.6. Definimos $U : F \to \mathbb{S}(\mathcal{R})$ como el morfismo de grupos determinado por $s \mapsto U_s$, $s \in \mathcal{S}$,

$$U_s(\epsilon, t) = (\epsilon(-1)^{\delta_{s,t}}, sts), \qquad \epsilon = \pm 1,\ t \in \mathcal{T}.$$

Se deduce fácilmente que $U_s^2 = \mathrm{id}_{\mathcal{R}}$, de modo que el morfismo está bien definido; es decir, en principio U_s define una función de $\mathcal{R}$ en sí mismo, la cual resulta ser una biyección por la relación anterior.

Dada $\mathbf{s} = (s_1, \dots, s_n)$, sean $w = s_n \cdots s_1$, con lo cual $U_{\mathbf{s}} = U_{s_n} \circ \cdots \circ U_{s_1}$. Probaremos por inducción en n que $U_{\mathbf{s}}(\epsilon, t) = (\epsilon(-1)^{n(\mathbf{s},t)}, wtw^{-1})$.

Si $n = 0, 1$, la prueba es directa. Si $n \geq 2$, sean $\widehat{\mathbf{s}} = (s_1, \dots, s_{n-1})$, $\widehat{w} = s_{n-1} \cdots s_1$; así, $w = s_n \widehat{w}$. Por hipótesis inductiva,

$$U_{\mathbf{s}}(\epsilon, t) = U_{s_n} \circ U_{\widehat{\mathbf{s}}}(\epsilon, t) = U_{s_n}\left(\epsilon(-1)^{n(\widehat{\mathbf{s}},t)}, \widehat{w}t\widehat{w}^{-1}\right) = \left(\epsilon(-1)^{n(\widehat{\mathbf{s}},t)+\delta_{s_n,\widehat{w}t\widehat{w}^{-1}}}, wtw^{-1}\right).$$

Así, basta probar que $n(\mathbf{s}, t) = n(\widehat{\mathbf{s}}, t) + \delta_{s_n,\widehat{w}t\widehat{w}^{-1}}$, que sigue de $\Xi(\mathbf{s}) = (\Xi(\widehat{\mathbf{s}}), \widehat{w}^{-1} s_n \widehat{w})$.

Consideremos $s, t \in \mathcal{S}$ tales que $m_{st} < \infty$. Denotamos $\widetilde{p} = st \in F$, y p a su imagen en $\mathbf{W}$. Sea $\mathbf{s} = \{s, t, s, t, \dots, s, t\}$, sucesión de longitud $2m_{st}$. Notar que p tiene orden m_{st} y los elementos t_j asociados son $t_j = p^{j-1}s$. Luego, $t_1, \dots, t_{m_{st}}$ son todos distintos, y $t_{m_{st}+j} = t_j$, para todo $1 \leq j \leq m_{st}$. Así, $n(\mathbf{s}, t) \in \{0, 2\}$, de donde $U_{\widetilde{p}^{m_{st}}} = (U_s \circ U_t)^{m_{st}} = \mathrm{id}_{\mathcal{R}}$. De acuerdo a la Observación 1.6, U induce un morfismo $\mathbf{U} : \mathbf{W} \to \mathbb{S}(\mathcal{R})$ tal que $\mathbf{U} \circ \pi = U$. Es decir, si $w \in \mathbf{W}$ se expresa como $w = s_1 \cdots s_n$, entonces $U_w(\epsilon, t) = (\epsilon(-1)^{n(\mathbf{s},t)}, wtw^{-1})$, de modo que $(-1)^{n(\mathbf{s},t)}$ no depende de la expresión elegida, y probamos (i) y (ii) simultáneamente. □

Podemos ahora caracterizar las expresiones reducidas a partir de los conjuntos $\Xi(\mathbf{s})$.

Lema 1.15. *$w = s_1 \cdots s_n$ es una expresión reducida de w si y sólo si $t_i \neq t_j$, para todo par $i \neq j \in \mathbb{I}_n$.*

Demostración. Dados $\mathbf{s}$, $\Xi(\mathbf{s})$, w como antes, sea $\mathcal{T}_w := \{t \in \mathcal{T} : \eta(w,t) = -1\}$. Notar que $\mathcal{T}_w \subseteq \{t_1, \dots, t_n\}$ para cualquier expresión de w, con lo cual se deduce que $|\mathcal{T}_w| \leq \ell(w)$, al considerar una expresión reducida.

Ahora, si todos los t_i's son diferentes, entonces $n(\mathbf{s}, t)$ vale 1 si $t = t_i$, y 0 si $t \notin \{t_1, \dots, t_n\}$. Así, $\mathcal{T}_w = \{t_1, \dots, t_n\}$, con lo cual $n = |\mathcal{T}_w| \geq \ell(w)$. Luego, $n = \ell(w)$; es decir, la expresión es reducida.

Ahora si $t_i = t_j$ para $i < j$, se tiene que $s_i = us_ju^{-1}$, donde $u = s_{i+1} \cdots s_{j-1}$, y así

$$w = s_1 \cdots s_{i-1} s_i u s_j s_{j+1} \cdots s_n = s_1 \cdots s_{i-1}(s_i^2 u) s_{j+1} \cdots s_n = s_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_n;$$

es decir, $\mathbf{s}$ no da lugar a una expresión reducida de w. □

Definición 1.16. Dados un grupo $\mathbf{W}$ y un conjunto de generadores $\mathcal{S}$, se dice que $(\mathbf{W}, \mathcal{S})$ satisface la *propiedad de intercambio fuerte* si vale la siguiente afirmación.

PIF: Sean $w \in \mathbf{W}$ y $t \in \mathcal{T}$ tales que $\ell(tw) \leq \ell(w)$. Para cada sucesión $\mathbf{s} = \{s_1, \dots, s_n\}$ de elementos de $\mathcal{S}$ tales que $w = s_1 \dots s_n$, existe $j \in \mathbb{I}_n$ tal que

$$ts_1 \cdots s_{j-1} = s_1 \cdots s_{j-1} s_j.$$

Se dice que $(\mathbf{W}, \mathcal{S})$ satisface la *propiedad de intercambio* si vale lo siguiente.

PI: Sean $w \in \mathbf{W}$ y $s \in \mathcal{S}$ tales que $\ell(sw) \leq \ell(w) = n$. Para cada expresión reducida $w = s_1 \cdots s_n$, existe $j \in \mathbb{I}_n$ tal que $ss_1 \cdots s_{j-1} = s_1 \cdots s_{j-1} s_j$.

Se dice que $(\mathbf{W}, \mathcal{S})$ satisface la *propiedad de supresión* si vale lo siguiente.

PS: Sean $w \in \mathbf{W}$ y $\mathbf{s} = \{s_1, \dots, s_n\}$ una sucesión de elementos de $\mathcal{S}$ tales que $w = s_1 \cdots s_n$, $\ell(w) < n$. Existen $1 \leq i < j \leq n$ tales que

$$w = s_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_n.$$

Notar que, tal como lo indican sus nombres, **PIF** $\Rightarrow$ **PI**. Veremos ahora que los sistemas de Coxeter satisfacen ambas propiedades.

Teorema 1.17. *Todo sistema de Coxeter $(\mathbf{W}, \mathcal{S})$ satisface la **PIF**.*

Demostración. Dados $w \in \mathbf{W}$ y $t \in \mathcal{T}$, probaremos en primer lugar que:

Afirmación 1.1. *$\ell(tw) < \ell(w)$ si y sólo si $\eta(w,t) = -1$.*

Asumimos primero que $\eta(w,t) = -1$, y fijemos $w = s_1 \cdots s_m$ una expresión reducida. Luego, $t \in \Xi(s_1, \cdots, s_m)$, pues t aparece un número impar de veces, o lo que es equivalente, $t = (s_1 \cdots s_{j-1}) s_j (s_{j-1} \cdots s_1)$ para algún j. Luego,

$$\ell(tw) = \ell(s_1 \cdots s_{j-1} s_{j+1} \cdots s_m) < \ell(w) = m.$$

Ahora, si $\eta(w,t) = 1$, el Lema 1.14 nos dice que:

$$\mathbf{U}_{(tw)^{-1}}\big(\epsilon, t\big) = \mathbf{U}_{w^{-1}} \mathbf{U}_t\big(\epsilon, t\big) = \mathbf{U}_{w^{-1}}\big(-\epsilon, t\big) = \big(-\epsilon\eta(w,t), wtw^{-1}\big) = \big(-\epsilon, wtw^{-1}\big).$$

Así $\eta(tw, t) = -1$, con lo cual la prueba anterior dice que $\ell(w) = \ell(t(tw)) < \ell(tw)$.

Si $\ell(tw) < \ell(w)$, se tiene que $\eta(w,t) = -1$; si $w = s_1 \cdots s_n$ es una expresión cualquiera, se tiene que $t = (s_1 \cdots s_{j-1}) s_j (s_{j-1} \cdots s_1)$ para algún j, y se satisface la **PIF**. □

Corolario 1.18. *Sean $w = s_1 \cdots s_n$ una expresión reducida y $t \in \mathcal{T}$. Son equivalentes:*

1. *$\ell(tw) < \ell(w)$,*
2. *$tw = s_1 \cdots s_{j-1} s_{j+1} \cdots s_n$, para algún $j \in \mathbb{I}_m$,*
3. *$t = s_1 \cdots s_{j-1} s_j s_{j-1} \cdots s_1$ para algún $j \in \mathbb{I}_m$.*

Más aún, j está unívocamente determinado en los ítems anteriores.

Demostración. La equivalencia entre 1. y 2. se sigue del Teorema 1.17. Además, se deduce fácilmente que 2. vale sii vale 3. y la unicidad se deduce del Lema 1.15. □

Definición 1.19. Sea $w \in \mathbf{W}$. Consideremos los siguientes conjuntos:

$$\mathcal{T}_L(w) := \{t \in \mathcal{T} : \ell(tw) < \ell(w)\}, \qquad \mathcal{D}_L(w) := \mathcal{T}_L(w) \cap \mathcal{S},$$
$$\mathcal{T}_R(w) := \{t \in \mathcal{T} : \ell(wt) < \ell(w)\}, \qquad \mathcal{D}_R(w) := \mathcal{T}_R(w) \cap \mathcal{S}.$$

$\mathcal{T}_L(w)$ (resp. $\mathcal{T}_R(w)$) es el conjunto de *reflexiones asociadas a izquierda* (resp. *a derecha*), y $\mathcal{D}_L(w)$ (resp. $\mathcal{D}_R(w)$) es el conjunto *descendente a izquierda* (resp. *a derecha*).

Sea $w = s_1 \cdots s_n$ una expresión reducida. Notar que, de acuerdo al Corolario 1.18,

$$\mathcal{T}_L(w) = \{s_1 \cdots s_{j-1} s_j s_{j-1} \cdots s_1 | j \in \mathbb{I}_n\}$$

y como el Lema 1.15 nos dice que todos estos elementos son diferentes, se tiene que

$$|\mathcal{T}_L(w)| = \ell(w). \tag{1.7}$$

Además, se verifica que

$$\mathcal{T}_R(w) = \mathcal{T}_L(w^{-1}), \qquad \mathcal{D}_R(w) = \mathcal{D}_L(w^{-1}). \tag{1.8}$$

Daremos a continuación otras consecuencias del Teorema 1.17.

Corolario 1.20. *Sean $s \in \mathcal{S}$, $w \in \mathbf{W}$. Se verifican:*

1. *$s \in \mathcal{D}_L(w)$ sii existe una expresión reducida de w comenzando en s,*
2. *$s \in \mathcal{D}_R(w)$ sii existe una expresión reducida de w finalizando en s.*

Demostración. Basta con probar 1., pues 2. se deduce de este ítem y (1.8).

Para probar 1., si $s \in \mathcal{D}_L(w)$, el Corolario 1.18 dice que $sw = s_1 \cdots s_{j-1} s_{j+1} \cdots s_n$ para algún j y una expresión reducida de w, de donde $w = ss_1 \cdots s_{j-1} s_{j+1} \cdots s_n$ es una expresión reducida. La definición del conjunto $\mathcal{D}_L(w)$ implica la recíproca. □

Proposición 1.21. $(\mathbf{W}, \mathcal{S})$ *satisface la* ***PS****.*

Demostración. Sea $w = s_1 \cdots s_m$, $\ell(w) < m$. Elegimos el mayor i tal que $s_i s_{i+1} \cdots s_m$ no es reducida. Así, $\ell(s_i s_{i+1} \cdots s_m) < \ell(s_{i+1} \cdots s_m)$, de modo que, por el Teorema 1.17, existe $j > i$ tal que $s_i s_{i+1} \cdots s_m = s_{i+1} \cdots \widehat{s_j} \cdots s_m$, con lo cual $w = s_1 \cdots s_m = s_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_m$. □

De esta propiedad se derivan las siguientes consecuencias:

Corolario 1.22.
1. *Cada expresión $w = s_1 \cdots s_m$ contiene una expresión reducida que se obtiene quitando una cantidad par de letras.*
2. *Si $w = s_1 \cdots s_m = s'_1 \cdots s'_m$ son dos expresiones reducidas, entonces*
$$\{s_1, \dots, s_m\} = \{s'_1, \dots, s'_m\}.$$
3. *Ningún generador de Coxeter $s \in \mathcal{S}$ puede expresarse en términos de los restantes generadores; luego, $\mathcal{S}$ es un conjunto minimal de generadores para $\mathbf{W}$.*

Demostración. La primer afirmación sigue de modo inmediato de la Proposición anterior, mientras que la última sigue de la segunda afirmación.

Probaremos la segunda afirmación por inducción en $\ell(w)$. Para ello, el caso $\ell(w) = 1$ es trivial. Supongamos ahora que vale para $m-1 \geq 1$, y sea w elemento de longitud m, para el cual consideramos dos expresiones reducidas distintas $w = s_1 \cdots s_m = s'_1 \cdots s'_m$. Como $\ell(s'_1 w) = m - 1 < \ell(w)$, existe $j \in \mathbb{I}_m$ tal que $s'_1 s_1 \cdots s_{j-1} = s_1 \cdots s_j$, de acuerdo al Teorema 1.17, con lo cual $s'_1 = s_1 \cdots s_{j-1} s_j s_{j-1} \cdots s_1$. De acuerdo a la

primer afirmación de este corolario, podemos obtener una expresión reducida de s_1' a partir de $s_1 \cdots s_{j-1} s_j s_{j-1} \cdots s_1$ borrando una cantidad par de elementos, de modo que nos quedaremos finalmente con un único elemento: $s_1' = s_l$ para algún $l \in \mathbb{I}_m$. Además,

$$w' = s_2' \cdots s_m' = s_1' s_1 \cdots s_m = s_1 \cdots s_{j-1} s_{j+1} \cdots s_m$$

tiene longitud $m-1$, y se aplica hipótesis inductiva para ver que $\{s_2', \ldots, s_m'\} \subseteq \{s_1, \ldots, s_m\}$. Luego, $\{s_1, \ldots, s_m\} \supseteq \{s_1', \ldots, s_m'\}$, y el resultado se completa intercambiando los roles de las expresiones reducidas. □

1.4. Caracterización de los grupos de Coxeter. Luego de verificar que todo grupo de Coxeter satisface las **PS** y **PI**, veremos la fortaleza de estos enunciados, pues caracterizan los grupos de Coxeter. Más exactamente, se tiene el siguiente resultado.

Teorema 1.23. *Sea* $\mathbf{W}$ *un grupo y* $\mathcal{S}$ *un conjunto de generadores de orden 2. Son equivalentes:*

(i) $(\mathbf{W}, \mathcal{S})$ *es un* sistema de Coxeter*,*

(ii) $(\mathbf{W}, \mathcal{S})$ *satisface la* Propiedad de Intercambio*,*

(iii) $(\mathbf{W}, \mathcal{S})$ *satisface la* Propiedad de Supresión*.*

Demostración. (ii) $\Rightarrow$ (iii) La prueba de la Proposición 1.21 no utiliza la hipótesis de tener un sistema de Coxeter sino simplemente que satisface la **PI**.

(iii) $\Rightarrow$ (ii) Sea $w = s_1 \cdots s_n$ una expresión reducida, y $s \in \mathcal{S}$ tal que $\ell(sw) < n = \ell(w)$. Como asumimos que vale la **PS**, podemos quitar dos letras de $ss_1 \cdots s_n$ y obtener una nueva expresión de sw. Si ninguna de esas letras es s, entonces $sw = ss_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_n$ para algunos $i < j \in \mathbb{I}_n$, con lo cual $w = s_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_n$ tiene longitud menor o igual que $n-2$, que es un absurdo. Así, una de las dos letras a quitar es s, con lo cual $sw = ss_1 \cdots \widehat{s_i} \cdots s_n$ para algún $i \in \mathbb{I}_n$, y $(\mathbf{W}, \mathcal{S})$ satisface la **PI**.

(i) $\Rightarrow$ (ii) Sigue del Teorema 1.17.

(ii) $\Rightarrow$ (i) Sea $s_1 \cdots s_n = e$ una relación en $(\mathbf{W}, \mathcal{S})$, un grupo generado por elementos de orden 2 que satisfacen la **PI**; es decir, si consideramos el morfismo de grupos $\phi : F \to \mathbf{W}$, donde F es el grupo libre generado por $\mathcal{S}$, consideramos $s_1 \cdots s_n \in \ker \phi$.

Notar que $r = 2k$ para algún k, dado que ya vimos que vale **PI** $\Leftrightarrow$ **PS**. Así escribimos la relación como $s_1 \cdots s_k = s_1' \cdots s_k'$. Probaremos por inducción en k que esta relación se deriva de relaciones del tipo $(ss')^{m_{ss'}} = e$; o sea, $\ker \phi$ está generado por $(ss')^{m_{ss'}}$ y s^2. Si $k = 1$, entonces $s_1 = s_1'$. Asumimos ahora que todo elemento de $\ker \phi$ expresado por menos de $2k$ elementos pertenece al subgrupo N generado por $(ss')^{m_{ss'}}$ y s^2.

- Si $s_1 \cdots s_k$ no es reducida, existe $i \in \mathbb{I}_k$ tal que $s_{i+1} \cdots s_k$ es reducida, pero $s_i \cdots s_k$ no lo es. Aplicando la **PI**, existe $j > i$ tal que $s_{i+1} \cdots s_k = s_i s_{i+1} \cdots \widehat{s_j} \cdots s_k$. Como esta relación tiene longitud menor que $2k$, está en N, lo cual nos lleva a la relación
$$s_1 \cdots s_i s_i s_{i+1} \cdots \widehat{s_j} \cdots s_k = s_1' \cdots s_k',$$
de la cual podemos quitar s_i^2, y por lo tanto está en N por hipótesis inductiva, y por lo tanto la relación inicial también lo está.
- Si $s_1 \cdots s_k$ es reducida, asumimos que $s_1 \neq s_1'$, pues en tal caso las quitamos y obtenemos una relación de longitud menor. En otro caso, existe $i \in \mathbb{I}_k$ tal que $s_1 \cdots s_i = s_1' s_1 \cdots s_{i-1}$, a partir de la cual obtenemos $s_1 \cdots \widehat{s_i} \cdots s_k = s_2' \cdots s_k'$, que por hipótesis inductiva pertenece a N. Si $i < k$ la prueba está completa, pues la relación está en N a partir de reemplazar la igualdad anterior en la original.

Si $i = k$, se tiene $s'_1 s_1 \cdots s_{k-1} = s'_1 s'_2 \cdots s'_k$, con lo cual basta probar que

$$s'_1 s_1 \cdots s_{k-1} = s_1 s_2 \cdots s_k$$

es una relación en N. Repitiendo el argumento, basta probar que

$$s'_1 s_1 \cdots s_{k-1} = s_1 s'_1 s_1 s_2 \cdots s_{k-2}$$

es una relación en N. Iterando este proceso, lo anterior se reduce a probar que

$$s_1 s'_1 s_1 s'_1 \cdots = s'_1 s_1 s'_1 s_1 \cdots ,$$

la cual se sigue que pertenece a N a partir de $(s_1 s'_1)^{m_{s_1,s'_1}} = e$.

Luego, $(\mathbf{W}, \mathcal{S})$ es un sistema de Coxeter. □

Veremos aplicaciones de este Teorema en los ejercicios para probar que algunos grupos generados por elementos de orden 2 son efectivamente sistemas de Coxeter.

1.5. Subgrupos parabólicos. A lo largo de esta sección, fijemos $\mathcal{X}$ un subconjunto de $\mathcal{S}$. Denotaremos $\mathbf{W}_\mathcal{X}$ al subgrupo de $\mathbf{W}$ generado por los elementos $s \in \mathcal{X}$. Subgrupos de este tipo se dicen *parabólicos*.

Para cada $w \in \mathbf{W}$, llamamos $\mathcal{X}(w)$ al conjunto de elementos $s \in \mathcal{S}$ que aparecen en una expresión reducida de w; notar que dicho conjunto no depende de la expresión elegida, de acuerdo al Corolario 1.22.

Proposición 1.24. *Para cada $\mathcal{X} \subset \mathcal{S}$, se tiene $\mathbf{W}_\mathcal{X} = \{w \in \mathbf{W} : \mathcal{X}(w) \subset \mathcal{X}\}$.*

Demostración. Sea $S_\mathcal{X} := \{w \in \mathbf{W} : \mathcal{X}(w) \subset \mathcal{X}\}$. De la definición de este conjunto se sigue que $S_\mathcal{X} \subseteq \mathbf{W}_\mathcal{X}$, con lo cual basta con probar que $S_\mathcal{X}$ es un subgrupo. En primer lugar, $\mathcal{X}(w) = \mathcal{X}(w^{-1})$, pues si $w = s_1 \cdots s_n$, entonces $w^{-1} = s_n \cdots s_1$. Luego,

$$w \in S_\mathcal{X} \Leftrightarrow \mathcal{X}(w) = \mathcal{X}(w^{-1}) \subseteq \mathcal{X} \Leftrightarrow w^{-1} \in S_\mathcal{X}.$$

Por otro lado, sean $w, w' \in S_\mathcal{X}$, y $w = s_1 \cdots s_n$, $w' = s'_1 \cdots s'_m$ dos expresiones reducidas. Luego, $ww' = s_1 \cdots s_n s'_1 \cdots s'_m$ es una expresión de ww', de la cual podemos obtener una expresión reducida quitando algunos elementos (posiblemente ninguno), de acuerdo al Corolario 1.22. Así, $\mathcal{X}(ww') \subseteq \{s_1, \dots, s_n, s'_1, \dots, s'_m\} = \mathcal{X}(w) \cup \mathcal{X}(w') \subseteq \mathcal{X}$, con lo cual $ww' \in S_\mathcal{X}$. Por lo tanto, $S_\mathcal{X}$ es un subgrupo. □

Corolario 1.25. $\mathbf{W}_\mathcal{X} \cap \mathcal{S} = \mathcal{X}$.

Demostración. Inmediato de la Proposición anterior, pues $\mathcal{X}(s) = \{s\}$. □

Para cada $w \in \mathbf{W}_\mathcal{X}$, denotaremos $\ell_\mathcal{X}(w)$ a la longitud de w como elemento de $\mathbf{W}_\mathcal{X}$, considerando el conjunto de generadores $\mathcal{X}$.

Corolario 1.26. *Para cada $w \in \mathbf{W}_\mathcal{X}$, $\ell_\mathcal{X}(w) = \ell(w)$.*

Demostración. Se sigue de la Proposición 1.24 y la independencia de la expresión reducida para obtener $\mathcal{X}_w$. □

A continuación caracterizaremos los subgrupos $\mathbf{W}_\mathcal{X}$. La propiedad más importante es que $\mathbf{W}_\mathcal{X}$ es un grupo de Coxeter.

Teorema 1.27. (i) $(\mathbf{W}_\mathcal{X}, \mathcal{X})$ *es un sistema de Coxeter.*
(ii) *Si $\mathcal{X}$, $\mathcal{X}'$ son dos subconjuntos de $\mathcal{S}$, entonces $\mathbf{W}_\mathcal{X} \subset \mathbf{W}_{\mathcal{X}'}$ si y sólo si $\mathcal{X} \subseteq \mathcal{X}'$.*
(iii) *Sea $(\mathcal{X}_i)_{i\in I}$ una familia de subconjuntos de $\mathcal{S}$, y $\mathcal{X} = \cap_{i\in I}\mathcal{X}_i$. Entonces,*

$$\mathbf{W}_\mathcal{X} = \cap_{i\in I}\mathbf{W}_{\mathcal{X}_i}.$$

Demostración. (i) $\mathbf{W}_{\mathcal{X}}$ es un grupo generado por elementos de orden 2, con lo cual basta con probar que satisface la **PI**, de acuerdo con el Teorema 1.23. Si $x \in \mathcal{X}$ y $w \in \mathbf{W}_{\mathcal{X}}$ son tales que $\ell_{\mathcal{X}}(xw) \leq \ell_{\mathcal{X}}(w) = n$. A partir del corolario anterior, $\ell(xw) \leq \ell(w) = n$. Si $w = s_1 \cdots s_n$ es una expresión reducida, entonces $s_i \in \mathcal{X}(w) \subseteq \mathcal{X}$ de acuerdo con la Proposición 1.24. Utilizando que $\mathbf{W}$ satisface la **PI**, existe $i \in \mathbb{I}_n$ tal que $xs_1 \cdots s_{i-1} = s_1 \cdots s_i$; así, $(\mathbf{W}_{\mathcal{X}}, \mathcal{X})$ satisface la **PI**.

(ii) Sigue de la Proposición 1.24 y el Corolario 1.25.

(iii) Es inmediato a partir del inciso anterior. □

A partir del Teorema anterior comprenderemos la relación entre las componentes conexas del diagrama de Coxeter y los correspondientes subgrupos $\mathbf{W}_{\mathcal{X}}$, de acuerdo con el resultado que presentaremos a continuación. Esta relación nos permitirá reducirnos al estudio de grupos de Coxeter con diagrama conexo.

Proposición 1.28. *Sea $(\mathcal{S}_i)_{i\in I}$ una partición de $\mathcal{S}$ tal que $m_{st} = 2$ (es decir, $st = ts$) para cada $s \in \mathcal{S}_i$, $t \in \mathcal{S}_j$, $i \neq j$. Entonces, $\mathbf{W} = \prod_{i\in I} \mathbf{W}_{\mathcal{S}_i}$.*

Demostración. Para cada $i \in I$, sea $\mathbf{W}'_i$ el subgrupo generado por todos los $\mathbf{W}_{\mathcal{S}_j}$, $j \neq i$. Notar que $\mathbf{W}'_i$ es exactamente el grupo generado por $\mathcal{S} \setminus \mathcal{S}_i$. El Teorema 1.27 nos dice que $\mathbf{W}_{\mathcal{S}_i} \cap \mathbf{W}'_i = \mathbf{W}_\emptyset = \{e\}$. Además, $\mathbf{W}$ está generado por la unión de los $\mathbf{W}_{\mathcal{S}_i}$'s, con lo cual el resultado está probado. □

Ejercicios.

1. Completar los detalles de los Ejemplos; es decir, probar efectivamente que los ejemplos son grupos de Coxeter y que se satisfacen las relaciones indicadas.
2. Consideramos los siguientes elementos de $\mathbb{S}_5$: $a_1 = (12)(34)$, $a_2 = (12)(45)$, $a_3 = (14)(23)$. Probar que $a_i^2 = \mathrm{id}$ y calcular el orden de los 3 productos $a_i a_j$, $i < j$. Probar que existe un isomorfismo de grupos entre H_3 y $\mathbb{S}_5$.
3. El ejercicio anterior muestra que un mismo grupo puede tener más de una estructura como sistema de Coxeter, simplemente eligiendo diferentes conjuntos de generadores. Veremos otro ejemplo. Consideremos el grupo diedral D_6 que tiene 12 elementos, ver el Ejemplo 1.13. Si $\mathcal{S}' = \{r_2, (r_1r_2)^3, r_2(r_1r_2)^3\}$, probar que $(\mathbf{W}, \mathcal{S}')$ es un sistema de Coxeter reducible.
4. Probar que para todo par de elementos $u \neq w \in \mathbf{W}$, se tiene $\mathcal{T}_L(u) \neq \mathcal{T}_L(w)$.
5. Caracterizar $\mathcal{T}$ para cada grupo diedral D_m.
6. Probar que $\mathcal{T}_R(uw) = \mathcal{T}_R(w) \triangle w^{-1}\mathcal{T}_R(u)w$ para todo par de elementos $u, w \in \mathbf{W}$ (donde $\triangle$ denota la diferencia simétrica entre los conjuntos).
7. Dados $u, w \in \mathbf{W}$, probar que las siguientes afirmaciones son equivalentes:
   a) $\ell(uw) = \ell(u) + \ell(w)$,
   b) $\mathcal{T}_R(w) \bigcap \mathcal{T}_R(u) = \emptyset$,
   c) $\mathcal{T}_R(uw) = \mathcal{T}_R(w) \bigcup w^{-1}\mathcal{T}_R(u)w$,
   d) $\mathcal{T}_R(uw) = \mathcal{T}_R(w) \biguplus w^{-1}\mathcal{T}_R(u)w$ (es decir, la unión es disjunta).
8. Dado $x \in \mathbb{S}_n$, definimos el número de inversión de x como:
$$\mathrm{inv}(x) := |\{(i,j) : 1 \leq i < j \leq n, x(i) > x(j)\}|.$$
   a) Probar que $\mathrm{inv}(xs_i) = \begin{cases} \mathrm{inv}(x) - 1, & \mathrm{x(i)>x(i+1)}; \\ \mathrm{inv}(x) + 1, & \mathrm{x(i)<x(i+1)}. \end{cases}$
   b) Usar el hecho anterior para concluir que $\ell(x) = \mathrm{inv}(x)$ (definimos ℓ para el conjunto de generadores $\mathcal{S} = \{s_1, \ldots, s_{n-1}\}$).
   c) Probar que $\mathcal{D}_R(x) = \{s_i \in \mathcal{S} : x(i) > x(i+1)\}$.

d) Concluir que $(\mathbb{S}_n, \mathcal{S})$ satisface la propiedad del intercambio, y por lo tanto es un sistema de Coxeter.

9. Dado $\mathcal{X} \subseteq \mathcal{S}$, sea $\mathcal{T}_{\mathcal{X}} := \{wsw^{-1} : w \in \mathbf{W}_{\mathcal{X}}, s \in \mathcal{X}\}$. Probar que $\mathcal{T}_{\mathcal{X}} = \mathcal{T} \cap \mathbf{W}_{\mathcal{X}}$.

2. Orden de Bruhat, orden débil y expresiones reducidas

Introduciremos a continuación un orden parcial muy importante en el conjunto de elementos de un grupo de Coxeter, llamado orden de Bruhat. También mencionaremos algunas propiedades relacionadas con el orden débil. Veremos que el orden de Bruhat está relacionado con todas las subpalabras de las expresiones reducidas, mientras que el orden débil está relacionado con los comienzos de las mismas. Nuestra principal referencia para esta sección será [1].

2.1. Orden de Bruhat: propiedades básicas.

Definición 2.1. Sean $(\mathbf{W}, \mathcal{S})$ un sistema de Coxeter, y $u, w \in \mathbf{W}$.

(i) Escribiremos $u \xrightarrow{t} v$ si $t = u^{-1}v \in \mathcal{T}$ y $\ell(u) < \ell(v)$.

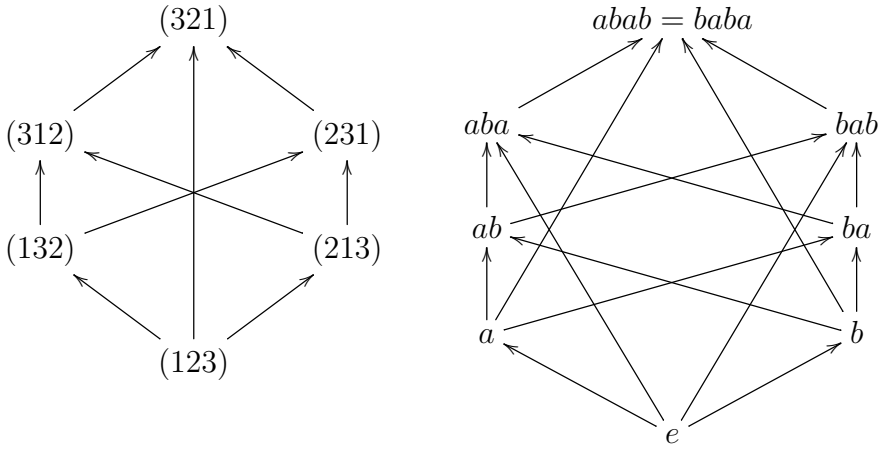
(ii) Escribiremos $u \longrightarrow v$ si existe $t \in \mathcal{T}$ tal que $u \xrightarrow{t} v$.

(iii) Escribiremos $u \leq v$ si existen $w_i \in \mathbf{W}$ tales que

$$u \longrightarrow w_1 \longrightarrow w_2 \longrightarrow \cdots \longrightarrow w_n \longrightarrow v.$$

El *orden de Bruhat* es el orden parcial en $\mathbf{W}$ definido por (iii) . El *gráfico de Bruhat* es el grafo dirigido cuyos vértices son los elementos de $\mathbf{W}$ y cuyas flechas son las de (ii) .

Ejemplo 2.2. A continuación, los gráficos de Bruhat para $\mathbb{S}_3$ e $I_2(4)$.



Lo anterior se deduce a partir de:

$$\mathcal{T}_{\mathbb{S}_3} = \{(213), (132), (321)\}, \qquad \mathcal{T}_{I_2(4)} = \{a, b, aba, bab\}.$$

Comenzaremos a descubrir cuáles son las propiedades de este orden. La primera será la Propiedad de subpalabra, donde por una *subpalabra* de una palabra $s_1 s_2 \cdots s_n$ entendemos una palabra $s_{i_1} \cdots s_{i_j}$, donde $1 \leq i_1 < \cdots < i_j \leq n$.

Teorema 2.3. *Sea $v = s_1 \cdots s_n$ una expresión reducida, y $u \in \mathbf{W}$. Entonces, $u \leq v$ sii u admite una expresión reducida que es una subpalabra de $s_1 \cdots s_n$.*

Demostración. ($\Rightarrow$) Sea $u \leq v$, con lo cual existen $t_i \in \mathcal{T}$ tales que

$$u \xrightarrow{t_0} w_1 \xrightarrow{t_1} w_2 \xrightarrow{t_2} \cdots \xrightarrow{t_{m-1}} w_m \xrightarrow{t_m} v.$$

Como $v^{-1} = s_n \cdots s_1$ es una expresión reducida y $x_m^{-1} = t_m v^{-1}$, $\ell(x_m^{-1}) < \ell(w^{-1})$, la **PIF** nos dice que $x_m^{-1} = s_n \cdots \widehat{s_i} \cdots s_1$ para algún $i \in \mathbb{I}_n$, con lo cual $x_m = s_1 \cdots \widehat{s_i} \cdots s_m$. Siguiendo, cada x_{m-k} se obtiene quitando $k+1$ de las s_i's de la expresión reducida de v, por lo cual u admite una expresión que es una subpalabra de v. Por la **PS**, u admite una expresión reducida que es una subpalabra de esta expresión de u, y por lo tanto es una subpalabra de la expresión reducida de v.

($\Leftarrow$) Comencemos por probar el siguiente resultado.

Afirmación 2.1. *Sean $u \neq v \in \mathbf{W}$ y $v = s_1 \cdots s_n$ una expresión reducida. Asumimos que u admite una expresión reducida que es subpalabra de $v = s_1 \cdots s_n$. Entonces existe $w \in \mathbf{W}$ tal que $u \leq w$, $\ell(w) = \ell(u) + 1$ y w admite una expresión reducida que es subpalabra de $v = s_1 \cdots s_n$.*

Demostración. Dado que la cantidad de expresiones reducidas de u es finita, podemos elegir aquélla que sea subpalabra de $v = s_1 \cdots s_n$, es decir de la forma $u = s_1 \cdots \widehat{s_{i_1}} \cdots \widehat{s_{i_k}} \cdots s_n$, $k = \ell(v) - \ell(u)$, con i_k mínimo. Sea $t = s_n s_{n-1} \cdots s_{i_k} \cdots s_{n-1} s_n \in \mathcal{T}$, de modo que

$$ut = s_1 \cdots \widehat{s_{i_1}} \cdots \widehat{s_{i_{k-1}}} \cdots s_{i_k} \cdots s_n.$$

Así, $\ell(ut) \leq \ell(u) + 1$. Supongamos que $\ell(ut) < \ell(u)$, de modo que la **PIF** nos dice que

- $t = s_n s_{n-1} \cdots s_p \cdots s_{n-1} s_n$ para algún $p > i_k$, o
- $t = s_n s_{n-1} \cdots \widehat{s_{i_k}} \cdots \widehat{s_{i_d}} \cdots s_p \cdots \widehat{s_{i_d}} \cdots \widehat{s_{i_k}} \cdots s_{n-1} s_n$ para algún $i_k \geq i_d > p$.

En el primer caso, las dos expresiones distintas de t nos dicen que

$$\begin{aligned} v = vt^2 &= (s_1 \cdot s_n)(s_n s_{n-1} \cdots s_{i_k} \cdots s_{n-1} s_n)(s_n s_{n-1} \cdots s_p \cdots s_{n-1} s_n) \\ &= s_1 \cdots \widehat{s_{i_k}} \cdots \widehat{s_p} \cdots s_n, \end{aligned}$$

que contradice la hipótesis de que $\ell(v) = n$. En el segundo caso,

$$\begin{aligned} u = ut^2 = (s_1 \cdots \widehat{s_{i_1}} \cdots \widehat{s_{i_k}} \cdots s_n)(s_n \cdots \widehat{s_{i_k}} \cdots \widehat{s_{i_d}} \cdots s_p \cdots \widehat{s_{i_d}} \cdots \widehat{s_{i_k}} \cdots s_n) \\ (s_n s_{n-1} \cdots s_{i_k} \cdots s_{n-1} s_n) = s_1 \cdots \widehat{s_{i_1}} \cdots \widehat{s_p} \cdots s_n, \end{aligned}$$

que contradice la minimalidad de i_k. Así, $\ell(ut) = \ell(u) + 1$, con lo cual $w = ut$ es el elemento buscado. □

Luego, la prueba es inmediata por inducción en $\ell(v) - \ell(u)$ a partir del Lema. □

Corolario 2.4. *Los intervalos de Bruhat $[u, v] := \{w \in \mathbf{W} : u \leq w \leq v\}$ son finitos. Más aún, se tiene $\big|[u, v]\big| \leq 2^{\ell(v)}$.*

Demostración. Sean $v = s_1 \cdots s_n$ una expresión reducida, y $\zeta(s_1, \ldots, s_n)$ el conjunto de subpalabras de $s_1 \cdots s_n$. De acuerdo al Teorema anterior, existe una función inyectiva $f : [u, v] \to \zeta(s_1, \ldots, s_n)$, de modo que $\big|[u, v]\big| \leq \big|\zeta(s_1, \ldots, s_n)\big| = 2^n$. □

Corolario 2.5. *La aplicación $\mathbf{W} \to \mathbf{W}$, $w \mapsto w^{-1}$, es un automorfismo para el orden de Bruhat. Esto es, $u \leq v$ sii $u^{-1} \leq v^{-1}$.*

Demostración. Es inmediato a partir del Teorema anterior. □

A continuación, probaremos que se satisface la Propiedad de Cadena.

Teorema 2.6. *Si $u < v$, entonces existe una cadena $u < w_1 < \cdots < w_n = v$ tal que $\ell(w_i) = \ell(u) + i$ para todo $i \in \mathbb{I}_n$.*

Demostración. Es consecuencia de la Afirmación 2.1. □

Observación 2.7. $u \lhd v$ denota un *cubrimiento* para el orden de Bruhat; esto es, $u \leq_R v$ y no existe $z \in \mathbf{W}$ tal que $u < z < v$. De acuerdo al Teorema anterior, $u \lhd v$ sii $u < v$ y $\ell(v) = \ell(u) + 1$.

Probaremos que también se satisface la PROPIEDAD DEL LEVANTAMIENTO.

Teorema 2.8. *Si $u < v$ y $s \in \mathcal{D}_L(v) - \mathcal{D}_L(u)$, entonces $u \leq sv$ y $su \leq v$.*

Demostración. Aplicaremos varias veces el Teorema 2.3

Sea $sv = s_1 \cdots s_n$ una expresión reducida; luego, $v = ss_1 \cdots s_n$ también es reducida, pues $s \in \mathcal{D}_L(w)$. Así, u admite una expresión reducida $u = s_{i_1} \cdots s_{i_k}$, que es una subpalabra de $v = ss_1 \cdots s_n$. Como $su > u$, pues $s \notin \mathcal{D}_L(u)$, se tiene que $s_{i_1} \neq s$, con lo cual $u = s_{i_1} \cdots s_{i_k}$ es una subpalabra de $sv = s_1 \cdots s_n$ y por lo tanto $u \leq sv$. También, $su = ss_{i_1} \cdots s_{i_k}$ es una expresión reducida y es a la vez una subpalabra de $v = ss_1 \cdots s_n$, por lo tanto $su \leq v$. □

Corolario 2.9. (i) *Sean $s, s' \in \mathcal{S}$ tales que $w \lhd sw, s'w$. Entonces, o bien $sw, ws' \lhd sws'$, o $w = sws'$.*

(ii) *Si $s \in \mathcal{S}$, $t \in \mathcal{T}$, $s \neq t$, son tales que $w \lhd sw, tw$, entonces $sw, tw \lhd stw$.*

Demostración. Inmediata a partir de la Proposición anterior. □

Finalizamos esta subsección con el siguiente resultado.

Proposición 2.10. *El orden de Bruhat en $\mathbf{W}$ es* dirigido*: esto es, para cada par de elementos $u, v \in \mathbf{W}$ existe $w \in \mathbf{W}$ tal que $u \leq w$, $v \leq w$.*

Demostración. Lo probaremos por inducción en $\ell(u)+\ell(v)$. Si $\ell(u)+\ell(v) = 0$, entonces $u = v = e$, y $w = e$ es un candidato. Asumimos ahora que $\ell(u) + \ell(v) \geq 1$, y que vale la hipótesis inductiva. Podemos considerar $u, v \neq e$, pues $w \geq e$ para todo $w \in \mathbf{W}$. Sea $s \in \mathcal{D}_L(u)$, de modo que $\ell(su) = \ell(u) - 1$. Por inducción, existe $w' \in \mathbf{W}$ tal que $su \leq w'$, $v \leq w'$. Usando el Teorema 2.8, se tiene que $sw' < w'$, en cuyo caso $u \leq w'$, o $sw' > w'$, en cuyo caso $u \leq sw'$. Así, el w buscado es en el primer caso $w = w'$, y en el segundo, $w = sw'$. □

2.2. Grupos finitos: algunas propiedades. A continuación estudiaremos algunas particularidades que presenta el orden de Bruhat cuando nos restringimos a grupos de Coxeter finitos. En esta Subsección, $\mathbf{W}$ será siempre un grupo de Coxeter finito.

Proposición 2.11. *Existe un único elemento de longitud máxima w_0, que es máximo para el orden de Bruhat.*

Recíprocamente, si $(\mathbf{W}, \mathcal{S})$ es un sistema de Coxeter que admite un elemento u tal que $\mathcal{D}_L(u) = \mathcal{S}$, entonces $\mathbf{W}$ es finito y $u = w_0$.

Demostración. Existe algún elemento de longitud máxima w_0. Para cualquier otro elemento $w \in \mathbf{W}$, la Proposición 2.10 dice que existe una cota superior x de estos dos elementos, la cual satisface $\ell(w_0) \leq \ell(x)$. La maximalidad de $\ell(w_0)$ nos dice que $w_0 = x$ por el Teorema 2.3 (w_0 debe ser una subpalabra de x de la misma longitud) y así $w_0 \geq w$.

Para la segunda afirmación, probemos que $v < u$ para todo $v \in \mathbf{W}$ por inducción en $\ell(v)$ (el caso $\ell(v) = 0$ es trivial). Si $v \neq e$, existe $s \in \mathcal{S}$ tal que $sv < v$, de modo que $s \notin \mathcal{D}_L(sv)$. Por hipótesis inductiva, $sv < u$, y por el Teorema 2.8, $s(sv) = v \leq u$. Luego, $\mathbf{W} = [e, u]$ es finito, y u es el elemento máximo. □

Proposición 2.12. *El elemento w_0 tiene las siguientes propiedades:*
(i) $w_0^2 = e$.
(ii) $\ell(ww_0) = \ell(w_0) - \ell(w)$ *para todo* $w \in \mathbf{W}$.
(iii) $\mathcal{T}_L(ww_0) = \mathcal{T} \setminus \mathcal{T}(w)$ *para todo* $w \in \mathbf{W}$.
(iv) $\ell(w_0) = |\mathcal{T}|$.
(v) $\ell(w_0 w) = \ell(w_0) - \ell(w)$, $\ell(w_0 w w_0) = \ell(w)$ *para todo* $w \in \mathbf{W}$.

Demostración. (i) Como $\ell(w_0^{-1}) = \ell(w_0)$, la unicidad del elemento de longitud máxima nos dice que $w_0^{-1} = w_0$.
(ii) En primer lugar, $\ell(w) + \ell(ww_0) = \ell(w^{-1}) + \ell(ww_0) \geq \ell(w_0)$. Ahora, probaremos que $\ell(w)+\ell(ww_0) \leq \ell(w_0)$ por inducción en $\ell(w_0)-\ell(w)$. Si $\ell(w_0)-\ell(w) = 0$, entonces $w = w_0$ y la igualdad es trivial. Asumimos ahora que vale para $\ell(w_0) - \ell(w) = k > 0$, con lo cual existe $s \in \mathcal{S}$ tal que $w < sw$ (ver Proposición 2.11). Luego,

$$\begin{aligned}\ell(ww_0) \leq & \ell(sww_0) + 1 \leq (\ell(w_0) - \ell(sw)) + 1 \\ & = \ell(w_0) - (\ell(w) + 1) + 1 = \ell(w_0) - \ell(w),\end{aligned}$$

lo cual concluye la prueba.
(iii) Notar que (ii) implica que $tw < w$ sii $tww_0 > w$ para todo $t \in \mathcal{T}$, con lo cual cada $t \in \mathcal{T}$ pertenece a uno y sólo uno de los conjuntos $\mathcal{T}_L(w)$, $\mathcal{T}_L(ww_0)$.
(iv) Si $w = e$ en (iii) , $\mathcal{T} = \mathcal{T}_L(w_0)$, y el resultado sigue de (1.7).
(v) Notar que $\ell(w_0 w) = \ell(w^{-1}w_0) = \ell(w_0) - \ell(w^{-1}) = \ell(w_0) - \ell(w)$. □

2.3. Orden débil. Nuevamente $(\mathbf{W}, \mathcal{S})$ denotará un sistema de Coxeter.

Definición 2.13. El *orden débil a derecha* $\leq_R$ está definido por la siguiente condición:

> $u \leq_R w$ sii existen $s_i \in \mathcal{S}$ tales que $w = us_1 \cdots s_k$ y $\ell(us_1 \cdots s_i) = \ell(u) + i$ para todo $i \in \mathbb{I}_k$.

El *orden débil a izquierda* $\leq_L$ está definido por la siguiente condición:

> $u \leq_L w$ sii existen $s_i \in \mathcal{S}$ tales que $w = s_k \cdots s_1 u$ y $\ell(s_i \cdots s_1 u) = \ell(u) + i$ para todo $i \in \mathbb{I}_k$.

Observación 2.14. Estos dos órdenes son diferentes; sin embargo están relacionados por la condición:

$$u \leq_R w \quad \Leftrightarrow \quad u^{-1} \leq_L w^{-1}.$$

Además, justamente son órdenes más débiles que el de Bruhat: si $u \leq_R v$ o $u \leq_L v$, entonces $u \leq v$.

Usaremos la siguiente notación, análoga a la relacionada con el orden de Bruhat:

- $u \lhd_R v$ denota un *cubrimiento* para el orden a derecha; esto es, $u \leq_R v$ y no existe $z \in \mathbf{W}$ tal que $u \leq_R z \leq_R v$.
- $[u, v]_R := \{w \in \mathbf{W} : u \leq_R w \leq_R v\}$.
- De modo análogo se definen $u \lhd_L v$ y $[u, v]_L$ para el orden a izquierda.

Algunas propiedades del orden débil son las siguientes:

Proposición 2.15. (i) *Existe una correspondencia biyectiva entre expresiones reducidas de* $w \in \mathbf{W}$ *y cadenas maximales de* $[e, w]_R$.
(ii) $u \leq_R w$ *sii* $\ell(w) = \ell(u) + \ell(u^{-1}w)$.
(iii) *El orden débil satisface la* propiedad del prefijo*:*

$u \leq_R w$ sii existe una expresión reducida $w = s_1 \cdots s_m$ tal que $u = s_1 \cdots s_n$, $n = \ell(u) \leq m = \ell(w)$.

(iv) *El orden débil satisface la* propiedad de la cadena*:*

Si $u \leq_R w$, entonces existe una cadena $u \leq_R v_1 \leq_R \cdots \leq_R v_n = w$ tal que $\ell(v_i) = \ell(u) + i$ para todo $i \in \mathbb{I}_n$.

(v) *Si $s \in \mathcal{D}_L(u) \cap \mathcal{D}_L(w)$, entonces $u \leq_R w$ si y sólo si $su \leq_R sw$.*

(vi) *Si $\mathbf{W}$ es finito, entonces $w \leq_R w_0$ para todo $w \in \mathbf{W}$.*

(vii) *Si $r(w)$ denota el número de expresiones reducidas de $w \in \mathbf{W}$, entonces*

$$r(w) = \sum_{u \in \mathbf{W}:\, u \lhd_R w} r(u). \tag{2.1}$$

Demostración. Todos los ítems son fáciles de probar, y quedan como ejercicio para el lector. □

Existe una buena caracterización para el orden débil, que damos a continuación.

Proposición 2.16. *$u \leq_R w$ sii $\mathcal{T}_L(u) \subseteq \mathcal{T}_L(w)$.*

Demostración. ($\Rightarrow$) Existe una expresión reducida $w = s_1 \cdots s_n$ tal que $u = s_1 \cdots s_k$, $k \leq n$. De la definición de los conjuntos se sigue que $\mathcal{T}_L(u) \subseteq \mathcal{T}_L(w)$.

($\Leftarrow$) Asumimos que $\mathcal{T}_L(u) \subseteq \mathcal{T}_L(w)$, y fijamos $u = s_1 \cdots s_k$ una expresión reducida. Sea $t_i = s_1 s_2 \cdots s_i \cdots s_2 s_1$, para cada $i \in \mathbb{I}_k$. Notar que $n = \ell(w) \geq k$ por (1.7). Probaremos por inducción en i que existe una expresión reducida $w = s_1 \cdots s_i s'_1 \cdots s'_{n-i}$, para $i \in \mathbb{I}_k$. El caso $i = 1$ sigue del Corolario 1.20. Asumimos que vale para i: $w = s_1 \cdots s_i s'_1 \cdots s'_{n-i}$. El Lema 1.15 nos dice que existe $m \in \mathbb{I}_{n-i}$ tal que

$$t_{i+1} = s_1 \cdots s_i s'_1 \cdots s'_m \cdots s'_1 s_i \cdots s_1,$$

pues $t_{i+1} \neq t_j$ para todo $j \in \mathbb{I}_i$, con lo cual

$$\begin{aligned} w = t_{i+1}^2 w &= (s_1 s_2 \cdots s_{i+1} \cdots s_2 s_1)(s_1 \cdots s_i s'_1 \cdots s'_m \cdots s'_1 s_i \cdots s_1) s_1 \cdots s_i s'_1 \cdots s'_{n-i} \\ &= s_1 \cdots s_{i+1} s'_1 \cdots \widehat{s'_m} \cdots s'_{n-i}. \end{aligned}$$

Luego, como vale para $i = k$, se tiene $u \leq_R w$. □

Ejercicios.

1. Hallar el diagrama de Bruhat correspondiente al grupo diedral D_m. Probar que dos elementos cualesquiera de distinta longitud son comparables; más aún, vale que $\ell(u) < \ell(v)$ sii $u < v$.
2. Definimos el *orden de Bruhat a izquierda* cambiando la condición $t = u^{-1}v$ por $t = vu^{-1}$ en la definición del orden de Bruhat. Probar que dicho orden coincide con el de Bruhat (es por eso que no se definen órdenes de Bruhat a derecha e izquierda, sino un único orden de Bruhat).
3. Probar que el elemento de longitud máxima de $\mathbb{S}_n$ es w_0, la permutación que invierte el orden: $i \leftrightarrow n - i$. Hallar una expresión reducida de dicho elemento.
4. Dado $\mathcal{X} \subset \mathcal{S}$ y $u, v \in \mathbf{W}_\mathcal{X}$, probar que $u \leq v$ para el orden de Bruhat en $\mathbf{W}_\mathcal{X}$ sii $u \leq v$ para el orden de Bruhat en $\mathbf{W}$.
5. Sea $\mathbf{W}$ un grupo de Coxeter finito, y $w \in \mathbf{W}$. Probar que:
   a) $\mathcal{D}_L(ww_0) = \mathcal{S} \setminus \mathcal{D}_L(w)$.
   b) $\mathcal{D}_L(w_0 w) = w_0\big(\mathcal{S} \setminus \mathcal{D}_L(w)\big)w_0 = \mathcal{S} \setminus w_0 \mathcal{D}_L(w) w_0$.
   c) $\mathcal{D}_L(w_0 w w_0) = w_0 \mathcal{D}_L(w) w_0$.

d) $\mathcal{T}_L(w_0ww_0) = w_0\mathcal{T}_L(w)w_0$.

6. Probar la Proposición 2.15.

3. Representaciones lineales y raíces

En la última parte de estas notas descubriremos un punto de vista geométrico que presentan los grupos de Coxeter. En primer lugar, los realizaremos como grupos lineales, es decir como subgrupos de $\mathrm{GL}(V)$, el grupo de automorfismos sobre un espacio $\mathbb{R}$-lineal V. Luego, daremos la definición y algunas propiedades de los sistemas de raíces asociados a dichos grupos.

3.1. Representación lineal y matriz de Coxeter. Mostraremos a continuación una representación lineal canónicamente asociada a un grupo de Coxeter y algunas consecuencias de su existencia. Entre otras, probaremos que existe una biyección entre las matrices de Coxeter y los sistemas de Coxeter salvo isomorfismos (notar que no dijimos simplemente grupos, sino que debemos fijar el conjunto de generadores).

En lo que resta de estas notas, $\mathcal{S}$ será un conjunto finito. Recordar que una *representación lineal* es un morfismo de grupos $\phi : \mathbf{W} \to \mathrm{GL}(V)$, donde $\mathrm{GL}(V)$ denota el grupo de automorfismos lineales de V (consideraremos $\mathbb{R}$-espacios vectoriales).

Fijemos un entero $m \geq 3$, y reales $k_1, k_2 > 0$ tales que $k_1k_2 = 4\cos^2(\pi/m)$. Fijemos una base $\{v_1, v_2\}$ de $\mathbb{R}^2$ tal que el ángulo entre v_1 y v_2 es π/m, y sus normas satisfacen

$$\|v_2\| = \frac{2\cos(\pi/m)}{-k_1}\|v_1\|, \qquad \|v_1\| = \frac{2\cos(\pi/m)}{-k_2}\|v_2\|.$$

Sea r_i la reflexión ortogonal con respecto a v_i, $i = 1, 2$.

Lema 3.1. *r_i está determinada por:*

$$r_i(v_i) = -v_i, \qquad r_i(v_j) = v_j + k_jv_i, j \neq i.$$

Demostración. Es un cálculo directo, que dejamos como ejercicio para el lector. □

Sea $a : \mathcal{S} \times \mathcal{S} \to \mathbb{R}$ la función dada por

$$a_{ss} = 2, \qquad a_{st} = a_{ts} = -2\cos\frac{\pi}{m_{st}}, \quad \text{si } 3 \leq m_{st} < \infty,$$
$$a_{st} = 0, \quad \text{si } m_{st} = 2, \qquad a_{st} = a_{ts} = -2, \quad \text{si } m_{st} = \infty.$$

Ahora, sea $\{\alpha_s\}_{s\in\mathcal{S}}$ la base canónica de $\mathbb{R}^{\mathcal{S}}$, el espacio vectorial de funciones de $\mathcal{S}$ a valores en $\mathbb{R}$; ésto es, $\alpha_s(t) = \delta_{st}$ para cada par $s, t \in \mathcal{S}$. Definimos la transformación lineal $\sigma_s : \mathbb{R}^{\mathcal{S}} \to \mathbb{R}^{\mathcal{S}}$, $\sigma_s(\alpha_t) = \alpha_t - a_{st}\alpha_s$. Definimos una forma bilineal $B : V \times V \to \mathbb{R}$, $B(\alpha_s, \alpha_t) = a_{st}/2$. Dicha forma es simétrica, y $B(\alpha_s, \alpha_s) = 1$, $B(\alpha_s, \alpha_t) \leq 0$ para todo par $s \neq t \in \mathcal{S}$. Si H_s es el hiperplano ortogonal a α_s con respecto a B, entonces $\sigma_s(H_s) = H_s$ y H_s es un complemento lineal de $\mathbb{R}\alpha_s$, pues $B(\alpha_s, \alpha_s) \neq 0$. También $\sigma_s(\alpha_s) = -\alpha_s$. Además, para cada $s \in \mathcal{S}$,

$$B\left(\sigma_s(v), \sigma_s(w)\right) = B(v, w), \qquad \text{para todo } v, w \in V. \tag{3.1}$$

Teorema 3.2. *Sea $(\mathbf{W}, \mathcal{S})$ un sistema de Coxeter. Entonces, existe un único morfismo de grupos $\sigma : \mathbf{W} \to \mathrm{GL}(\mathbb{R}^{\mathcal{S}})$, $s \mapsto \sigma_s$.*

Demostración. Lo probaremos en una serie de pasos; el primero es fácil de probar.

Afirmación 3.1. *$\sigma_s^2 = \mathrm{id}$ para todo $s \in \mathcal{S}$, y $\sigma_s\sigma_t = \sigma_t\sigma_s$ si $m_{st} = 2$.*

Afirmación 3.2. *$\sigma_s\sigma_t$ tiene orden m_{st} si $3 \leq m_{st} < \infty$.*

Sea V el subespacio generado por α_s y α_t, de dimensión 2. Notar que $\sigma_s\sigma_t(V) \subseteq V$, pues ambas reflexiones dejan invariante a V (basta con aplicarlas a α_s y α_t). Luego, podemos pensar a V como $\mathbb{R}^2$, y considerar $\sigma_s\sigma_t : \mathbb{R}^2 \to \mathbb{R}^2$. Dadas dos reflexiones ortogonales con respecto a planos que se diferencian en un ángulo γ, su composición es una rotación de ángulo 2γ. En nuestro caso, a partir de la fórmula de σ_s y σ_t, y del Lema 3.1, σ_s y σ_t son las reflexiones con respecto a α_s y α_t. Luego, $\sigma_s\sigma_t$ tiene orden m_{st}, pues es la rotación en un ángulo de amplitud $2\pi/m_{st}$; los conjuntos $\{(\sigma_s\sigma_t)^m(\alpha_s) : 0 \leq m < m_{st}\}$, $\{(\sigma_s\sigma_t)^m(\alpha_t) : 0 \leq m < m_{st}\}$ tienen m_{st} elementos cada uno de ellos. Ahora, $\sigma_s\sigma_t$ deja estable $H_s \cap H_t$, y como $(H_s \cap H_t) \cup \{\alpha_s, \alpha_t\}$ generan V, se sigue que $\sigma_s\sigma_t$ tiene orden m_{st}.

Afirmación 3.3. *$\sigma_s\sigma_t$ tiene orden ∞ si $m_{st} = \infty$.*

Por inducción podemos probar que

$$(st)^n(\alpha_s) = (2m+1)\alpha_s + 2m\alpha_t, \qquad t(st)^n(\alpha_s) = (2m+1)\alpha_s + 2(m+1)\alpha_t.$$

En particular, $(st)^n \neq \mathrm{id}$ para todo $n \in \mathbb{N}$.

Luego, el resultado sigue de las Afirmaciones y la Observación 1.6. □

Observación 3.3. En general usaremos la notación $\sigma_w := \sigma(w)$, para cada $w \in \mathbf{W}$. Además, escribiremos $w(\alpha) := \sigma_w(\alpha)$.

Teorema 3.4. *Existe una biyección entre matrices de Coxeter y clases de equivalencia de sistemas de Coxeter.*

Demostración. Simplemente, si m_{st} es finito, entonces el orden de st divide a m_{st}, pues se tiene la relación $(st)^{m_{st}} = e$, pero por otro lado es al menos m_{st}, pues $\sigma\big((st)^m\big) \neq e$ si $a < m_{st}$ (ver las Afirmaciones de la prueba anterior). Si $m_{st} = \infty$, el Teorema anterior también nos dice que $(st)^m \neq e$ para todo $m \in \mathbb{N}$. Luego, cada matriz de Coxeter determina un único sistema de Coxeter, del cual obtenemos la matriz de Coxeter asociada (única) como la matriz de los órdenes de st, $s, t \in \mathcal{S}$. □

3.2. Raíces. Reflexiones. En esta última parte introduciremos el sistema de raíces asociado a un grupo de Coxeter y obtendremos una relación con la longitud de cada elemento de $\mathbf{W}$. Además probaremos la inyectividad de la representación σ.

Definición 3.5. El *sistema de raíces* de $(\mathbf{W}, \mathcal{S})$ es el conjunto

$$\Delta := \{w(\alpha_s) | s \in \mathcal{S}, w \in \mathbf{W}\}.$$

Dado $\alpha \in \Delta$, escribimos $\alpha = \sum_{s\in\mathcal{S}} c_s\alpha_s$, donde los c_s están unívocamente determinados. Decimos que α es *positiva* (respectivamente, *negativa*) si $c_s \geq 0$ (respectivamente, $c_s \leq 0$) para todo $s \in \mathcal{S}$. Usaremos la notación $\alpha > 0$ (respectivamente, $\alpha < 0$) para indicar que α es positiva (respectivamente, negativa). Además,

$$\Delta_+ := \{\alpha \in \Delta : \alpha > 0\}, \qquad \Delta_- := \{\alpha \in \Delta : \alpha < 0\}.$$

Observación 3.6. Notar que $B(\alpha, \alpha) = 1$ para cada $\alpha \in \Delta$, pues $\mathbf{W}$ preserva B. Además, $\Delta = -\Delta$, pues $s(\alpha_s) = -\alpha_s$.

Teorema 3.7. *Sean $w \in \mathbf{W}$, $s \in \mathcal{S}$. Si $\ell(ws) > \ell(w)$, entonces $w(\alpha_s) > 0$. Si $\ell(ws) < \ell(w)$, entonces $w(\alpha_s) < 0$.*

Demostración. Lo probaremos por inducción en $\ell(w)$, siendo trivial el caso inicial $\ell(w) = 0$. Asumimos que $w'(\alpha_s) > 0$ para cada $w' \in \mathbf{W}$ tal que $\ell(w') < k$, $\ell(w's) > \ell(w')$, y sea $w \in \mathbf{W}$ tal que $\ell(w) = k$. Fijemos una expresión reducida de w, la cual termina en t, de modo que $\ell(wt) = k - 1$; luego, $s \neq t$. Sea $\mathcal{X} = \{s, t\}$, de modo que $\mathbf{W}_\mathcal{X}$ es isomorfo al grupo diedral $I_2(m)$, donde $m = m_{st}$. Consideramos

$$A := \{v \in \mathbf{W} : \, v^{-1}w \in \mathbf{W}_\mathcal{X}, \, \ell(v) + \ell(v^{-1}w) = \ell(w)\}.$$

Notar que $A \neq \emptyset$, pues $w \in A$. Fijemos entonces $v \in A$ de longitud mínima, y $v_\mathcal{X} := v^{-1}w$. Así, $\ell(v) + \ell(v_\mathcal{X}) = \ell(w)$. Por otro lado, $wt \in A$, pues $(tw^{-1})w = t \in \mathbf{W}_\mathcal{X}$ y $\ell(wt) = \ell(w) - 1$, de modo que $\ell(v) \leq \ell(wt) = k - 1$. Supongamos que $\ell(vs) < \ell(v)$; es decir, $\ell(vs) = \ell(v) - 1$. Entonces,

$$\ell(w) \leq \ell(vs) + \ell(sv^{-1}w) = \ell(v) - 1 + \ell(sv^{-1}w) \leq \ell(v) - 1 + \ell(v^{-1}w) + 1 = \ell(w).$$

Así, $\ell(w) = \ell(vs) + \ell(sv^{-1}w)$, y $sv^{-1}w \in \mathbf{W}_\mathcal{X}$, con lo cual $vs \in A$. Este hecho contradice la elección de v, con lo cual $\ell(vs) > \ell(v)$, y por hipótesis inductiva $v(\alpha_s) > 0$. De modo análogo probamos que $\ell(vt) > \ell(v)$, y así $v(\alpha_t) > 0$. Dado que $w = vv_\mathcal{X}$, basta con probar que $v_\mathcal{X}(\alpha_s) > 0$, pues en tal caso es una combinación lineal con coeficientes no negativos de α_s y α_t, a la cual le aplicamos v, y obtenemos una combinación lineal con coeficientes no negativos.

Supongamos que $\ell(v_\mathcal{X}s) < \ell(v_\mathcal{X})$. Entonces,

$$\ell(ws) = \ell(vv^{-1}ws) \leq \ell(v) + \ell(v^{-1}ws) = \ell(v) + \ell(v_\mathcal{X}s) < \ell(v) + \ell(v_\mathcal{X}) = \ell(w),$$

lo cual es un absurdo. Así, $\ell(v_\mathcal{X}s) > \ell(v_\mathcal{X})$. Luego, toda expresión reducida de $v_\mathcal{X}$ termina en t, y así $v_\mathcal{X} = (st)^n$ o $v_\mathcal{X} = t(st)^n$, para algún $m \in \mathbb{N}$.

- Si $m < \infty$, entonces $\ell(v_\mathcal{X}) < m$, pues $v_\mathcal{X}$ no puede ser el elemento de longitud máxima w_0 (w_0 tiene una escritura que termina en s). Calculando directamente, donde interpretamos a α_s, α_t como dos vectores de longitud 1 en $\mathbb{R}_2$ que forman un ángulo de $\pi - \pi/m$, vemos que $v_\mathcal{X}(\alpha_s) > 0$.
- Si $m = \infty$, entonces $v_\mathcal{X}(\alpha_s) > 0$, ver la prueba de la Afirmación 3.3.

En cualquier caso tenemos que $v_\mathcal{X}(\alpha_s) > 0$, lo que concluye la prueba.

Una vez probada la primer afirmación, la segunda se obtiene a partir de ella, pues si $w' = ws$, entonces $\ell(w') < \ell(w's)$, y por lo tanto $w'(\alpha_s) = -w(\alpha_s) > 0$. □

Corolario 3.8. *La representación $\sigma : \mathbf{W} \to \mathrm{GL}(\mathbb{R}^\mathcal{S})$ es inyectiva.*

Demostración. Si $w \neq e$, existe $s \in \mathcal{S}$ tal que $\ell(ws) < \ell(w)$ (como dijimos antes, un final de una expresión reducida), con lo cual $w(\alpha_s) < 0$, y por lo tanto $w(\alpha_s) \neq \alpha_s$. Así, $w \notin \ker \sigma$. □

Corolario 3.9. $\Delta = \Delta_+ \cup \Delta_-$. □

Para cada $w \in \mathbf{W}$ definimos $L_w := \{\alpha \in \Delta_+ : w(\alpha) < 0\}$.

Proposición 3.10. (i) *Para cada $s \in \mathcal{S}$, $s\big(\Delta_+ \setminus \{\alpha_s\}\big) = \Delta_+ \setminus \{\alpha_s\}$.*
(ii) *Para cada $w \in \mathbf{W}$, $\ell(w) = |L_w|$.*

Demostración. (i) Sea $\alpha = \sum_{t \in \mathcal{S}} c_t \alpha_t \in \Delta_+$, $\alpha \neq \alpha_s$. Entonces, existe $t_0 \neq s$ tal que $c_{t_0} > 0$, pues α no es un múltiplo de α_s (todas las raíces son unitarias). Dado que

$$s(\alpha) = s\left(\sum_{t \in \mathcal{S}} c_t \alpha_t\right) = \sum_{t \neq s} c_t \alpha_t + (-c_s + \sum_{t \neq s} c_t a_{st})\alpha_s,$$

s no modifica el coeficiente de α_{t_0}, que sigue siendo positivo, y por el Corolario 3.9, $s(\alpha) \in \Delta_+$. Luego, $s\big(\Delta_+ \setminus \{\alpha_s\}\big) \subseteq \Delta_+ \setminus \{\alpha_s\}$, y aplicando s obtenemos la otra inclusión.

(ii) El enunciado es claro para $\ell(w) = 0$ (es decir, $w = e$), y $\ell(w) = 1$ a partir de (i) . Procederemos entonces por inducción, para lo cual, a partir del Teorema 3.7 basta con probar lo siguiente:

Afirmación 3.4. *Sean $w \in \mathbf{W}$, $s \in \mathcal{S}$. Si $w(\alpha_s) > 0$, entonces $|L_{ws}| = |L_w| + 1$. Si $w(\alpha_s) < 0$, entonces $|L_{ws}| = |L_w| - 1$.*

Tenemos que $L_w = \Delta_+ \cap w^{-1}(\Delta_-)$. Si $w(\alpha_s) > 0$, (i) nos dice que

$$L_{ws} = \Delta_+ \cap sw^{-1}(\Delta_-) = s(L_w) \cup \{\alpha_s\},$$

y $\alpha_s \notin s(L_w)$, con lo cual $|L_{ws}| = |L_w| + 1$. De modo análogo, si $w(\alpha_s) > 0$,

$$L_{ws} = \Delta_+ \cap sw^{-1}(\Delta_-) = s(L_w) \setminus \{\alpha_s\},$$

con lo cual $|L_{ws}| = |L_w| - 1$, y la Afirmación queda probada. □

Sea $\alpha \in \Delta$; así, existen $w \in \mathbf{W}$, $s \in \mathcal{S}$ tales que $\alpha = w(\alpha_s)$. Notar que

$$wsw^{-1}(v) = w\left(w^{-1}(v) - 2B\big(w^{-1}(v), \alpha_s\big)\alpha_s\right) = v - 2B\big(w^{-1}(v), \alpha_s\big)w(\alpha_s)$$
$$v - 2B\big(v, w(\alpha_s)\big)w(\alpha_s) = v - 2B(v, \alpha)\alpha,$$

para todo $v \in V$, con lo cual $wsw^{-1} \in \mathcal{T}$ no depende de w, s sino solamente de α. Llamaremos s_α a este elemento, que resulta ser la reflexión ortogonal con respecto a α, que envía α en $-\alpha$ y deja fijo el hiperplano H_α ortogonal a α; además $s_\alpha = s_{-\alpha}$.

Lema 3.11. (i) *La función $\Delta_+ \to \mathcal{T}$, $\alpha \mapsto s_\alpha$ es biyectiva.*
(ii) *Dados $\alpha, \beta \in \Delta$ tales que $w(\alpha) = \beta$ para algún $w \in \mathbf{W}$, entonces $ws_\alpha w^{-1} = s_\beta$.*

Demostración. (i) La definición de $\mathcal{T}$ dice que la aplicación es suryectiva. Si $s_\alpha = s_\beta$,

$$-\beta = s_\beta(\beta) = s_\alpha(\beta) = \beta - 2B(\beta, \alpha)\alpha,$$

con lo cual $\beta = B(\beta, \alpha)\alpha$, y por lo tanto $\alpha = \beta$, pues ambas raíces son positivas y son vectores unitarios. Así la aplicación es inyectiva.
(ii) Es inmediato de la definición de s_β y el hecho que B es $\mathbf{W}$-invariante. □

Ahora podemos generalizar el Teorema 3.7.

Teorema 3.12. *Dados $w \in \mathbf{W}$, $\alpha \in \Delta_+$, $\ell(ws_\alpha) > \ell(w)$ sii $w(\alpha) > 0$.*

Demostración. ($\Rightarrow$) Aplicaremos inducción en $\ell(w)$, siendo trivial el caso $\ell(w) = 0$. Asumimos que $u(\alpha) > 0$ para cada $u \in \mathbf{W}$ tal que $\ell(u) < k$, $\ell(u) < \ell(us_\alpha)$. Sea $w \in \mathbf{W}$ tal que $\ell(w) = k$, $\ell(w) < \ell(ws_\alpha)$. Sea $s \in \mathcal{S}$ tal que $\ell(sw) = \ell(w) - 1$. Notar que

$$\ell(sws_\alpha) \geq \ell(ws_\alpha) - 1 > \ell(w) - 1 = \ell(sw).$$

Por hipótesis inductiva, $sw(\alpha) > 0$. Supongamos que $w(\alpha) < 0$. La Proposición 3.10 nos dice que $w(\alpha) = -\alpha_s$, a partir de lo cual $sw(\alpha) = \alpha_s$ y $s = (sw)s_\alpha(sw)^{-1}$, por el Lema 3.11. Así, $ws_\alpha = sw$. Como $\ell(ws_\alpha) > \ell(w) > \ell(sw)$, obtenemos un absurdo, de donde $w(\alpha) > 0$.
($\Leftarrow$) Como en la prueba del Teorema 3.7, se deduce de la prueba anterior. □

Ejercicios.

1. Probar que $L_{w^{-1}} = -wL_w$ para todo $w \in \mathbf{W}$.
2. Probar que para todo par de elementos $v, w \in \mathbf{W}$, $\ell(vw) = \ell(v) + \ell(w)$ si y sólo si $L_w \subseteq L_{vw}$. En tal caso, probar que $L_{vw} = L_w \cup w^{-1}L_v$.
3. Sea $w = s_1 \cdots s_r$ una expresión reducida. Consideremos
$$\beta_r := \alpha_{s_r}, \qquad \beta_j := s_r s_{r-1} \cdots s_{j-1}(\alpha_{s_j}).$$
Probar que $\beta_1, \ldots, \beta_r$ son r raíces positivas distintas.
4. Si $\mathbf{W}$ es infinito, probar que ℓ toma valores arbitrariamente grandes, y por lo tanto Δ es infinito. Si $\mathbf{W}$ es finito, probar que $w_0(\Delta_+) = \Delta_-$.
5. Sean $\mathcal{R}$, $\mathbf{U}_w$ como en (1.4), (1.6). Definimos $\phi : \mathcal{R} \to \Delta$ como sigue:
$$(t, \pm 1) \mapsto \gamma \in \Delta_\pm, \quad \text{si } t_\gamma = t.$$
   a) Probar que ϕ es biyectiva.
   b) Probar que $\phi \circ \pi_w = w \circ \phi$ para todo $w \in \mathbf{W}$.
   c) Probar que la Proposición 3.10 y el Teorema 3.12 se pueden probar a partir del ítem anterior.
6. Consideremos la forma bilineal $B(\cdot, \cdot)$.
   a) Si $|\mathcal{S}| = 2$, probar que $B(\cdot, \cdot)$ es definida positiva o semidefinida positiva.
   b) Consideremos $\mathcal{S} = \{s_1, s_2, s_3\}$, $(p, q, r) = (m_{s_1,s_2}, m_{s_1,s_3}, m_{s_2,s_3})$ y
$$d := \frac{1}{p} + \frac{1}{q} + \frac{1}{r}.$$
   Probar que $B(\cdot, \cdot)$ es
   - definida positiva si y sólo si $d > 1$
   - semidefinida positiva degenerada sii $d = 1$.
   - de signo (2,1), es decir tiene dos autovalores positivos y uno negativo, sii $d < 1$.

   Ayuda: dividir el estudio en dos casos: cuando el diagrama es un triángulo, o cuando no lo es (es decir, uno de las entradas de M es 2).
   c) Hallar todas las ternas (p, q, r) para los cuales la forma bilineal es definida positiva o semidefinida positiva.

Referencias

[1] A. Björner y F. Brenti, *Combinatorics of Coxeter groups*. Graduate Texts in Mathematics, **231**. Springer, New York, xiv+363 pp. (2005).

[2] N. Bourbaki, *Groupes et algèbres de Lie*, Ch. **4, 5 et 6**. Éléments de mathematique. Hermann, Paris, 300 pp. (1968).

[3] A. Cohen, *Coxeter groups*. Notes of a MasterMath course, Fall 2007. Disponible en `http://www.win.tue.nl/~jpanhuis /coxeter/notes/notes.pdf`

[4] J. Humphreys, *Reflection groups and Coxeter groups*. Cambridge Studies in Advanced Mathematics, **29**. Cambridge University Press, Cambridge, xii+204 pp. (1990)

FaMAF-CIEM (CONICET), Universidad Nacional de Córdoba, Medina Allende s/n, Ciudad Universitaria, 5000 Córdoba, República Argentina.

E-mail address: `angiono@famaf.unc.edu.ar`

ANILLOS DE ENTEROS DE CUERPOS CUADRÁTICOS

EMILIO LAURET

RESUMEN. En este breve curso introduciremos una simple generalización del anillo de los números enteros llamado *anillo de enteros cuadráticos*. Veremos cómo se comporta su aritmética estudiando sus semejanzas y diferencias con los enteros racionales. Finalizaremos con el concepto de *número de clase* de un dominio de integridad el cual mide cuán lejos está de ser dominio de factorización única.

ÍNDICE

INTRODUCCIÓN

Como todos sabemos, el cuerpo de cocientes del anillo de números enteros $\mathbb{Z}$ es el cuerpo de los números racionales $\mathbb{Q}$. En este curso consideraremos extensiones cuadráticas de $\mathbb{Q}$, es decir, subcuerpos K de $\mathbb{C}$ de dimensión dos como espacios vectoriales sobre $\mathbb{Q}$. Dentro de cada uno de ellos definiremos su anillo de enteros $\mathcal{O}_K$, que resultará ser un $\mathbb{Z}$-módulo libre de rango dos.

Los anillos $\mathcal{O}_K$ conservan algunas propiedades de $\mathbb{Z}$, como por ejemplo que todo elemento no nulo y no inversible se factoriza como producto de irreducibles, aunque tal factorización no es única en general.

Los ejemplos más conocidos son los *enteros de Gauss*

$$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$$

2010 *Mathematics Subject Classification.* 11R11.

y los *enteros de Eisenstein*

$$\mathbb{Z}[\tfrac{1+\sqrt{-3}}{2}] = \mathbb{Z} + \mathbb{Z}\,\tfrac{1+\sqrt{-3}}{2},$$

en los cuales existe un algoritmo de división (dominios Euclídeos) tal como en $\mathbb{Z}$. En general éste no será el caso, ya que por ejemplo en el anillo

$$\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$$

ni siquiera se puede factorizar de manera única. También son enteros cuadráticos los anillos $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{5}]$, los cuales contienen infinitas unidades (elementos inversibles) a diferencia de $\mathbb{Z}$.

La principal similitud entre $\mathbb{Z}$ y $\mathcal{O}_K$ es que en ambos todo ideal se factoriza de manera única (salvo orden) como producto de ideales primos. Sin embargo, $\mathcal{O}_K$ no necesariamente es un dominio de ideales principales, por lo tanto esta propiedad no asegura la factorización única de elementos.

Finalizaremos con el difícil concepto de *número de clase* de un anillo $\mathcal{O}_K$, tema en el que existen diversos problemas abiertos de enunciado entendible. Este número mide por cuánto el anillo $\mathcal{O}_K$ no es un dominio de factorización única.

Estos cuerpos K de grado dos sobre $\mathbb{Q}$ son un caso particular de los *cuerpos de números* (subcuerpos de $\mathbb{C}$ de dimensión finita con respecto a $\mathbb{Q}$). Además, sus respectivos anillos de enteros $\mathcal{O}_K$ son en particular lo que se llama *Dominios de Dedekind*, principal objeto de estudio en cualquier curso de *teoría algebraica de números*. Existe una vasta bibliografía que trata sobre ellos. Recomendamos los textos de Narasimhan [4] y Alaca-Williams [1]. Diversos ejemplos y pruebas fueron extraídos de las notas de Pacharoni [5] y Conrad [2].

Le agradezco a Fiorela Rossi Bertone por revisar las notas y al Comité Organizador del *VI Encuentro Nacional de Álgebra* por la invitación para dar el curso.

1. Aritmética en cuerpos cuadráticos

1.1. Cuerpos cuadráticos. Todo subcuerpo K de los números complejos $\mathbb{C}$ contiene al cuerpo de los números racionales $\mathbb{Q}$. Esto vale pues como el elemento 1 está en K, entonces

$$\pm m = \pm(\underbrace{1 + \cdots + 1}_{m \text{ veces}}) \in K,$$

es decir, los números enteros están contenidos en K, por lo tanto su cuerpo de cocientes —el cual es precisamente $\mathbb{Q}$— también lo está. Luego todo subcuerpo de $\mathbb{C}$ se puede ver como un espacio vectorial sobre $\mathbb{Q}$, lo que permite la siguiente definición con la que trabajaremos de aquí en más.

Definición 1.1. Llamaremos —en este curso— un *cuerpo cuadrático* a un subcuerpo de $\mathbb{C}$ de dimensión dos como $\mathbb{Q}$-espacio vectorial.

Para $\alpha \in \mathbb{C}$ denotaremos $\mathbb{Q}[\alpha] = \{g(\alpha) \in \mathbb{C} : g(x) \in \mathbb{Q}[x]\}$ y diremos que $f(x) \in \mathbb{Q}[x]$ es su *polinomio minimal* si es mónico, anula a α y es de grado mínimo con esta propiedad. Dicho polinomio es único e irreducible sobre $\mathbb{Q}$ (Ejercicio 1).

Sea K un cuerpo cuadrático. Si $\alpha \in \mathbb{Q} \subset K$ entonces su polinomio minimal es $x - \alpha$. Tomemos $\alpha \in K \smallsetminus \mathbb{Q}$, entonces $\{1, \alpha\}$ es una $\mathbb{Q}$-base de K, en particular $K = \mathbb{Q}[\alpha]$. Como $\alpha^2 \in K$ existen coeficientes $q, r \in \mathbb{Q}$ tales que

$$\alpha^2 = q \cdot \alpha + r \cdot 1,$$

o equivalentemente

$$f(x) = x^2 - qx - r \tag{1.1}$$

es el polinomio minimal de α (Ejercicio 2).

Proposición 1.2. *Todos los cuerpos cuadráticos son de la forma*

$$\mathbb{Q}[\sqrt{m}] = \mathbb{Q} + \mathbb{Q}\sqrt{m},$$

con $m \in \mathbb{Z}$ libre de cuadrados. Más aún, todos ellos son no isomorfos dos a dos.

Demostración. Dado $m \in \mathbb{Z}$ libre de cuadrados, fácilmente podemos ver que $\mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático y que son no isomorfos de a pares (Ejercicio 3). Veamos ahora que son todos. Sean K un cuerpo cuadrático y $\alpha \in K \setminus \mathbb{Q}$, entonces $K = \mathbb{Q}[\alpha]$. Como $\dim_{\mathbb{Q}}(K) = 2$ tenemos que $1, \alpha, \alpha^2$ son linealmente dependientes, por lo tanto existen $a, b, c \in \mathbb{Q}$ tales que $a \neq 0$ y

$$a\alpha^2 + b\alpha + c = 0.$$

Sin pérdida de la generalidad, podemos suponer que $a, b, c \in \mathbb{Z}$. Multiplicando por $4a$ tenemos que

$$(2a\alpha + b)^2 = b^2 - 4ac.$$

Denotemos $\beta = 2a\alpha + b$ y $n = b^2 - 4ac \in \mathbb{Z}$. Luego $\mathbb{Q}[\sqrt{n}] \subset \mathbb{Q}[\beta]$ y $\mathbb{Q}[\beta] = K$. Además $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{n}] = 2$ por lo que $K = \mathbb{Q}[\sqrt{n}]$. Finalmente, $K = \mathbb{Q}[\sqrt{m}]$ donde $n = k^2 m$ con $m \in \mathbb{Z}$ libre de cuadrados. □

A partir de ahora, a menos que aclaremos lo contrario, cuando escribamos $\mathbb{Q}[\sqrt{m}]$ estaremos asumiendo que m es un entero libre de cuadrados, por lo tanto $\mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático.

Definición 1.3. Un cuerpo cuadrático $K = \mathbb{Q}[\sqrt{m}]$ es llamado *real* si $K \subset \mathbb{R}$ ($\iff$ $m > 0$) e *imaginario* si $K \nsubseteq \mathbb{R}$ ($\iff$ $m < 0$).

Sea $\sigma : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{m}]$ definido por $\sigma(1) = 1$ y $\sigma(\sqrt{m}) = -\sqrt{m}$ extendiendo de manera $\mathbb{Q}$-lineal. Se ve que σ es un morfismos de cuerpos (Ejercicio 4). Si $\alpha \in \mathbb{Q}[\sqrt{m}]$ llamaremos a $\sigma(\alpha)$ el *conjugado* de α y lo denotaremos por α'. Observemos que si $m < 0$ entonces el conjugado coincide con el conjugado complejo (Ejercicio 4) y que el mapeo identidad y σ son los únicos morfismos de cuerpos de $\mathbb{Q}[\sqrt{m}]$ a $\mathbb{C}$. En otras palabras, σ es el elemento no trivial del grupo de Galois de la extensión $\mathbb{Q} \subset \mathbb{Q}[\sqrt{m}]$.

Si $\alpha = r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ denotamos

$$\mathrm{Tr}_K(\alpha) = \alpha + \alpha' = 2r \qquad \text{y} \qquad \mathrm{N}_K(\alpha) = \alpha\alpha' = p^2 - mr^2.$$

Abreviaremos por $\mathrm{Tr}(\alpha)$ y $\mathrm{N}(\alpha)$ cuando no quepa lugar a dudas. El operador Tr resulta aditivo y N multiplicativo (Ejercicio 5). Notemos que

$$\begin{aligned} \alpha^2 = (r + s\sqrt{m})^2 &= r^2 + ms^2 + 2rs\sqrt{m} \\ &= -r^2 + ms^2 + 2r(r + s\sqrt{m}) \\ &= 2r\alpha - (r^2 - ms^2), \end{aligned}$$

por lo tanto

$$f(x) := x^2 + \mathrm{Tr}(\alpha)\, x - \mathrm{N}(\alpha) \tag{1.2}$$

anula a α, es mónico y de grado dos. Esto nos asegura que si $\alpha \notin \mathbb{Q}$ entonces $f(x)$ es su polinomio minimal.

Se puede definir la traza y la norma como sigue. Para $\alpha \in K$, el mapeo $L_\alpha : K \to K$ de multiplicar por izquierda, i. e. $L_\alpha(\beta) = \alpha\beta$, es una transformación lineal del $\mathbb{Q}$-espacio vectorial K. Entonces (Ejercicio 6)

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(L_\alpha) \quad \text{y} \quad \mathrm{N}(\alpha) = \mathrm{Tr}(L_\alpha). \tag{1.3}$$

1.2. Enteros cuadráticos.

Definición 1.4. Un número complejo α se dice un *entero algebraico* si es raíz de un polinomio mónico en $\mathbb{Z}[x]$.

Se puede ver que los enteros algebraicos forman un anillo (Ejercicio 7). Luego también lo hace el conjunto de *enteros cuadráticos* $\mathcal{O}_K$ formado por los enteros algebraicos en un cuerpo cuadrático K. Más aún, $\mathcal{O}_K$ es un *dominio de integridad*, es decir, un anillo conmutativo con unidad sin divisores de cero.

Nuestro siguiente paso es determinar $\mathcal{O}_K$ para cuerpos cuadráticos K. Es claro que $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ (Ejercicio 8). Para $\alpha \in \mathbb{C}$ denotemos $\mathbb{Z}[\alpha] = \{g(\alpha) \in \mathbb{C} : g(x) \in \mathbb{Z}[x]\}$. Se prueba que $\mathbb{Z}[\sqrt{m}] \subset \mathcal{O}_K$ (Ejercicio 8). El siguiente resultado determina completamente a $\mathcal{O}_K$.

Proposición 1.5. *Sea $K = \mathbb{Q}[\sqrt{m}]$. Entonces*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{si } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Observación 1.6. Notemos que

$$\mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \sqrt{m}\,\mathbb{Z} = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\},$$
$$\mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] = \mathbb{Z} + \tfrac{1+\sqrt{m}}{2}\,\mathbb{Z} = \left\{ \tfrac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$$

con $m \equiv 1 \pmod 4$ en el segundo caso.

Demostración. Un número complejo es algebraico si y sólo si su polinomio minimal tiene coeficientes enteros (Ejercicio 9). Si $\alpha \in K \setminus \mathbb{Q}$, hemos visto que su polinomio minimal está dado por (1.2). Luego, si $m \equiv 2, 3 \pmod 4$ y $\alpha = r + s\sqrt{m} \in K$, entonces $\alpha \in \mathcal{O}_K$ si y sólo si $\mathrm{Tr}(\alpha) = 2r \in \mathbb{Z}$ y $\mathrm{N}(\alpha) = r^2 - ms^2 \in \mathbb{Z}$. Supongamos que $r \notin \mathbb{Z}$, entonces $s \notin \mathbb{Z}$. Escribimos $r = r_1/2$ y $s = s_1/2$ con r_1 y s_1 impares, entonces $(r_1^2 - ms_1^2)/4 \in \mathbb{Z}$ o equivalentemente $r_1^2 \equiv ms_1^2 \pmod 4$. Como r_1 y s_1 son impares, $r_1^2 \equiv s_1^2 \equiv 1 \pmod 4$, lo cual nos lleva a una contradicción ya que $m \not\equiv 1 \pmod 4$. Luego r y s son enteros racionales y queda probado el primer caso.

Ahora supongamos $m \equiv 1 \pmod 4$ y tomemos $\alpha = r + s\sqrt{m} \in K$. Como antes, $\alpha \in \mathcal{O}_K$ si y sólo si $2r \in \mathbb{Z}$ y $r^2 - ms^2 \in \mathbb{Z}$. Esto último resulta equivalente a $r, s \in \mathbb{Z}$ o $r, s \in \mathbb{Z} + \frac{1}{2} := \{a + \frac{1}{2} : a \in \mathbb{Z}\}$. Finalmente notemos que

$$\begin{aligned} \alpha = r + s\sqrt{m} &= r + s\left(2\,\frac{1+\sqrt{m}}{2} - 1\right) \\ &= (r - s) + (2s)\,\frac{1+\sqrt{m}}{2}, \end{aligned}$$

por lo que $\alpha \in \mathcal{O}_K$ si y sólo si $r - s, 2s \in \mathbb{Z}$. □

Los enteros algebraicos $\mathbb{Z}[\sqrt{-1}]$ son comúnmente llamados *enteros de Gauss* y *enteros de Eisenstein* los de $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Por comodidad denotaremos para $K=\mathbb{Q}[\sqrt{m}]$,

$$\omega_K = \begin{cases} \sqrt{m} & \text{si } m \equiv 2,3 \pmod 4, \\ \dfrac{1+\sqrt{m}}{2} & \text{si } m \equiv 1 \pmod 4, \end{cases} \tag{1.4}$$

por lo tanto tenemos que

$$\mathcal{O}_K = \mathbb{Z} + \omega_K \mathbb{Z}. \tag{1.5}$$

Se puede ver que $\mathrm{Tr}(\alpha)$ y $\mathrm{N}(\alpha)$ son enteros racionales si α es entero algebraico (Ejercicio 10).

1.3. Elementos destacados en $\mathcal{O}_K$. A continuación estudiaremos los conceptos de elementos inversibles, irreducibles y primos en los enteros cuadráticos $\mathcal{O}_K$, comparándolos con los propios de $\mathbb{Z}$.

Recordemos las siguientes definiciones en un dominio de integridad A:

- ε se llama *unidad* si existe $v \in A$ tal que $\varepsilon v = 1_A$ (se denota $v = \varepsilon^{-1}$);
- γ se llama *irreducible* si es no nulo, no es unidad y $\gamma = \alpha\beta$ implica que α o β es una unidad;
- π se llama *primo* si es no nulo, no es unidad y si $\pi \mid \alpha\beta$ entonces $\pi \mid \alpha$ o $\pi \mid \beta$.

Comencemos estudiando el conjunto $\mathcal{O}_K^\times$ de unidades de $\mathcal{O}_K$ para $K=\mathbb{Q}[\sqrt{m}]$. Supongamos que ε es una unidad, entonces

$$1 = \mathrm{N}(1) = \mathrm{N}(\varepsilon\varepsilon^{-1}) = \mathrm{N}(\varepsilon)\mathrm{N}(\varepsilon^{-1})$$

por lo tanto $\mathrm{N}(\varepsilon)$ es una unidad en $\mathbb{Z}$, es decir $\mathrm{N}(\varepsilon) = \pm 1$. Más aún, la recíproca es cierta ya que si $\pm 1 = \mathrm{N}(\varepsilon) = \varepsilon\varepsilon'$ entonces $\varepsilon^{-1} = \pm\varepsilon' \in \mathcal{O}_K$. Podemos enunciar lo siguiente:

(♣) *si $\varepsilon \in \mathcal{O}_K$, ε es unidad si y sólo si* $\mathrm{N}(\varepsilon) = \pm 1$.

Ejemplo 1.7. Con esta equivalencia calcularemos $\mathcal{O}_K^\times$ para cuerpos cuadráticos imaginarios $K=\mathbb{Q}[\sqrt{m}]$ $(m<0)$. Supongamos $m \equiv 2,3 \pmod 4$, por lo tanto $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. Entonces $\varepsilon = a + b\sqrt{m} \in \mathcal{O}_K^\times$ $(a,b \in \mathbb{Z})$ si y sólo si

$$\mathrm{N}(\varepsilon) = a^2 - mb^2 = \pm 1.$$

Esto nos dice que $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$ y $\mathbb{Z}[\sqrt{m}]^\times = \{\pm 1\}$ para $m \neq -1$.

Ahora tomemos $m \equiv 1 \pmod 4$, por lo tanto $\varepsilon = \frac{a+b\sqrt{m}}{2} \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]^\times$ $(a,b \in \mathbb{Z},\ a \equiv b \pmod 2)$ si y sólo si

$$\mathrm{N}(\varepsilon) = \frac{a^2 - mb^2}{4} = \pm 1.$$

Luego $\mathbb{Z}[m]^\times = \{\pm 1\}$ para $m \neq -3$ y $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \left\{\pm 1,\ \pm\frac{1+\sqrt{-3}}{2},\ \pm\frac{1-\sqrt{-3}}{2}\right\}$.

El caso de cuerpos cuadráticos reales $K=\mathbb{Q}[\sqrt{m}]$ $(m>0)$ es muy diferente. Por ejemplo, notemos que $1+\sqrt{2}$ es una unidad de $\mathbb{Z}[\sqrt{2}]$ al igual que todas sus potencias, las cuales son distintas (Ejercicio 11), es decir, $\mathbb{Z}[\sqrt{2}]$ tiene infinitas unidades. Es notable esta diferencia con el caso imaginario en el que, como acabamos de ver, siempre existe una cantidad finita de unidades.

Supongamos que $m \equiv 2, 3 \pmod 4$. Notemos que si $\varepsilon = x + y\sqrt{m} \in \mathcal{O}_K$ $(x, y \in \mathbb{Z})$, entonces $\mathrm{N}(\varepsilon) = (x + y\sqrt{m})(x - y\sqrt{m}) = 1$ si y sólo si (x, y) es una solución de la *ecuación de Pell*

$$x^2 - my^2 = 1. \tag{1.6}$$

Luego, las soluciones de la ecuación de Pell están en correspondencia con las unidades en $\mathcal{O}_K$ de norma 1. En varios casos no existen unidades de norma -1, e. g. $m = 3$ (Ejercicio 12), por lo que la correspondencia llegaría a todas las unidades de $\mathcal{O}_K$.

Para cerrar el tema de las unidades en $\mathcal{O}_K$ para cuerpos cuadráticos reales K, enunciaremos el teorema que las caracteriza. Para la demostración de este teorema y un amplio estudio del tema, sugerimos ver el Capítulo 11 de [1].

Teorema 1.8. *Sea K un cuerpo cuadrático real y sea ε la menor unidad de $\mathcal{O}_K$ mayor a 1* (unidad fundamental)*. Entonces*

$$\mathcal{O}_K^\times \;=\; \{\pm\varepsilon^n : n \in \mathbb{Z}\}.$$

Ahora estudiemos los elementos irreducibles en $\mathcal{O}_K$. Supongamos que $\gamma \in \mathcal{O}_K$ es tal que $\mathrm{N}(\gamma) = p$ es un primo racional no necesariamente positivo. Si escribimos $\gamma = \alpha\beta$, entonces $p = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ lo que implica que $\mathrm{N}(\alpha)$ o $\mathrm{N}(\beta)$ es ± 1, o equivalentemente α o β es unidad por (♣). Esto nos permite enunciar lo siguiente:

(♠) *si $\gamma \in \mathcal{O}_K$ satisface que $\mathrm{N}(\gamma) = p$ es primo en $\mathbb{Z}$, entonces γ es irreducible.*

Sin embargo la recíproca no es verdadera tal como lo muestra el siguiente ejemplo.

Ejemplo 1.9. El elemento 3 es irreducible en $\mathbb{Z}[\sqrt{-1}]$ mas $\mathrm{N}(3) = 9$. En efecto, si $3 = \alpha\beta$, tomando norma en ambos miembros obtenemos que $9 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, lo cual implica que $\mathrm{N}(\alpha) \in \{\pm 1, \pm 3, \pm 9\}$. Pero $\mathrm{N}(\alpha) \geq 0$, si $\mathrm{N}(\alpha) = 1$ entonces α es unidad, si $\mathrm{N}(\alpha) = \pm 9$ entonces β es unidad, y $\mathrm{N}(\alpha)$ no puede valer 3 (Ejercicio 13), por lo tanto 3 es irreducible.

Es sabido que en un dominio de integridad, todo elemento primo es irreducible. Además, la recíproca es cierta en $\mathbb{Z}$ (más generalmente en todo dominio de ideales principales), pero no lo es en general en $\mathcal{O}_K$.

Ejemplo 1.10. El número 3 es un elemento irreducible en $\mathbb{Z}[\sqrt{-14}]$ (Ejercicio 14) que divide a $15 = (1 + \sqrt{-14})(1 - \sqrt{-14})$ pero no a $1 \pm \sqrt{-14}$. En general, un entero racional $c \in \mathbb{Z}$ divide un entero cuadrático $\alpha = a + b\omega_K$ $(a, b \in \mathbb{Z})$ si y sólo si c divide a a y b en $\mathbb{Z}$. Luego 3 no es primo en $\mathbb{Z}[\sqrt{-14}]$.

1.4. Factorización en $\mathcal{O}_K$. Recordemos las diferentes definiciones relacionadas con la factorización en un dominio de integridad A.

- A se dice de *factorización* si todo elemento α no nulo, no unidad, puede escribirse como $\alpha = \gamma_1 \dots \gamma_n$ con $\gamma_1, \dots, \gamma_n$ elementos irreducibles.
- A se dice *dominio de factorización única* (DFU) si es de factorización y además si $\alpha = \gamma_1 \dots \gamma_n = \delta_1 \dots \delta_m$ (γ_i, δ_i irreducibles) entonces $n = m$ y existe una permutación s de n elementos tal que γ_i es asociado a $\delta_{s(i)}$ para todo i (i. e. existe ε_i unidad tal que $\varepsilon_i\gamma_i = \delta_{s(i)}$).
- A se dice *dominio de ideales principales* (DIP) si todo ideal de A es principal, es decir, generado por un elemento.
- A se dice *dominio Euclídeo* (DE) si existe $\varphi : A \smallsetminus \{0\} \to \mathbb{N}$ tal que
  (i) si $\alpha, \beta \in A \smallsetminus \{0\}$ entonces $\varphi(\alpha) \leq \varphi(\alpha\beta)$;

(ii) si $\alpha, \beta \in A$ y $\beta \neq 0$ entonces existen $q, r \in A$ tales que $\alpha = \beta q + r$ donde $r = 0$, o $r \neq 0$ y $\varphi(r) < \varphi(\alpha)$.

Probemos primero que el anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático K es de factorización a partir del siguiente enunciado:

($\heartsuit$) *todo $0 \neq \alpha \in \mathcal{O}_K$ no unidad se factoriza como producto de irreducibles en $\mathcal{O}_K$.*

Demostración. Si $\alpha \in \mathcal{O}_K$ no es nulo ni unidad, tiene un divisor irreducible γ_1 (Ejercicio 15), entonces $\alpha = \gamma_1\alpha_1$ con $1 \leq \mathrm{N}(\alpha_1) < \mathrm{N}(\alpha)$. Si α_1 no es irreducible y no es unidad —i.e. $\mathrm{N}(\alpha_1) \neq 1$— entonces $\alpha_1 = \gamma_2\alpha_2$, con γ_2 irreducible, obteniendo así una sucesión decreciente de números naturales $\mathrm{N}(\alpha)$, $\mathrm{N}(\alpha_1)$, $\mathrm{N}(\alpha_2), \ldots$, la cual en algún momento debe estabilizarse en 1, digamos $\mathrm{N}(\alpha_j) = 1$. Por lo tanto $\alpha = \gamma_1 \ldots \gamma_j\alpha_j$ con $\gamma_1, \ldots, \gamma_{j-1}, \gamma_j\alpha_j$ elementos irreducibles. □

Sin embargo, dicha factorización en $\mathcal{O}_K$ puede no ser única (salvo orden y unidades). En general, $\mathcal{O}_K$ no es DFU, más aún, la cantidad de elementos irreducibles en una factorización de un entero puede no ser siempre la misma.

Ejemplo 1.11. Notemos que

$$3^4 = 81 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

Ya vimos que 3 es irreducible en $\mathbb{Z}[\sqrt{-14}]$ (Ejercicio 14). Veamos que $5 \pm 2\sqrt{-14}$ también lo son. Ambos tienen norma igual a 81, por lo tanto si suponemos que $5 \pm 2\sqrt{-14} = \alpha\beta$ entonces $\mathrm{N}(\alpha) \in \{1, 3, 9, 27, 81\}$. Si escribimos $\alpha = a+b\sqrt{-14} \in \mathbb{Z}[\sqrt{-14}]$ tenemos

$$\mathrm{N}(\alpha) = a^2 + 14b^2.$$

Claramente $\mathrm{N}(\alpha) \neq 3, 27$. Además, los únicos elementos en $\mathbb{Z}[\sqrt{-14}]$ con norma igual a 9 son ± 3, los cuales no dividen a $5 \pm 2\sqrt{-14}$. Finalmente obtenemos que $\mathrm{N}(\alpha) = 1$ o $\mathrm{N}(\alpha) = 81$, es decir, α o β es unidad, por lo tanto $5 \pm 2\sqrt{-14}$ es irreducible.

Sabemos que todo dominio de ideales principales es un dominio de factorización única. Para nuestros anillos $\mathcal{O}_K$ con K un cuerpo cuadrático, la recíproca es cierta, lo cual demostraremos más adelante (Teorema 2.13). En particular $\mathbb{Z}[\sqrt{-14}]$ no es un dominio de ideales principales por Ejemplo 1.11.

Ejemplo 1.12. Veamos que el ideal $\mathfrak{a} = 2\mathcal{O}_K + \sqrt{-14}\mathcal{O}_K$ no es principal en $\mathbb{Z}[\sqrt{-14}]$. Supongamos que $\mathfrak{a} = \alpha\mathcal{O}_K$ para algún $\alpha \in \mathcal{O}_K$. Tenemos que $\alpha \mid 2$ entonces existe $\beta \in \mathcal{O}_K$ tal que $2 = \alpha\beta$. Tomando norma a ambos lados obtenemos que $4 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. De la misma manera, como $\alpha \mid \sqrt{-14}$ resulta que $\mathrm{N}(\alpha)$ divide a $\mathrm{N}(\sqrt{-14}) = 14$, por lo tanto $\mathrm{N}(\alpha)$ es 1 o 2. Escribiendo $\alpha = a + b\sqrt{-14}$ tenemos que $\mathrm{N}(\alpha) = a^2 + 14b^2 \neq 2$, entonces $\mathrm{N}(\alpha) = 1$. Así $\mathfrak{a} = \alpha\mathcal{O}_K = \mathcal{O}_K$ lo cual no es cierto.

Finalizaremos esta sección considerando los dominios Euclídeos. Supongamos que K es un cuerpo cuadrático imaginario, entonces es posible probar que $\mathcal{O}_K$ es dominio Euclídeo con respecto a una función $\varphi(\cdot)$ si y sólo si lo es con respecto a $\mathrm{N}(\cdot)$. Esto nos permite usar la siguiente propiedad

($\diamondsuit$) $\mathcal{O}_K$ *es DE con* $|\mathrm{N}(\cdot)|$ *si y sólo si* $\forall\, x \in K\ \exists \alpha \in \mathcal{O}_K$ *tal que* $\mathrm{N}(x - \alpha) < 1$.

La siguiente demostración, al igual que muchas otras, se encuentra en [5]. Además [1] recorre el tema exhaustivamente.

Demostración. Supongamos que $\mathcal{O}_K$ es dominio Euclídeo. Si $x \in K$ existe $c \in \mathbb{N}$ tal que $cx \in \mathcal{O}_K$, por lo tanto existen $\alpha, \gamma \in \mathcal{O}_K$ tales que $cx = c\alpha + \gamma$ con $|\mathrm{N}(\gamma)| < |\mathrm{N}(c)|$. Esto implica $|\mathrm{N}(x - \alpha)| = |\mathbb{N}(\gamma)|/|\mathrm{N}(c)| < 1$.

Recíprocamente, dados $\alpha \neq 0$ y β en $\mathcal{O}_K$, existe $x \in K$ tal que $|\mathrm{N}(\beta/\alpha - x)| < 1$, entonces $\beta = x\alpha + (\beta - x\alpha)$ y $|\mathrm{N}(\beta - x\alpha)| < |\mathrm{N}(\alpha)|$. □

Ejemplo 1.13. Usando ($\diamondsuit$) se puede probar (Ejercicio 16) que el anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático imaginario $K = \mathbb{Q}[\sqrt{m}]$ ($m < 0$) es dominio Euclídeo si y sólo si

$$m = -1, -2, -3, -7, -11.$$

Ejemplo 1.14. Similarmente, el anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático real $K = \mathbb{Q}[\sqrt{m}]$ ($m > 0$) es dominio Euclídeo con respecto a $|N(\cdot)|$ si y sólo si

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Sin embargo no podemos afirmar que los enteros positivos libres de cuadrados m que no están en esta lista no sean dominio Euclídeos para alguna función $\varphi(\cdot)$. Por ejemplo para $m = 69$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ es dominio Euclídeo con respecto a la función

$$\varphi(a + b\omega_K) = \begin{cases} |a^2 + ab - 17b^2| & \text{si } (a,b) \neq (10,3), \\ 26 & \text{si } (a,b) = (10,3). \end{cases}$$

Más aún, el número 26 puede ser reemplazado por cualquier entero mayor o igual a 26, por lo que $\mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ es dominio Euclídeo con respecto a infinitas funciones distintas. El anillo $\mathbb{Z}[\sqrt{14}]$ también resulta dominio Euclídeo con respecto a una función distinta de $|\mathrm{N}(\cdot)|$.

Recomendamos [1] para ampliar el tema, en particular su *suggested reading* al final de Capítulo 2.

1.5. Ejercicios.

1. Sea $\alpha \in \mathbb{C}$ y $f(x)$ su polinomio minimal.
   a) Probar que $f(x)$ es irreducible en $\mathbb{Q}[x]$, es decir, si $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Q}[x]$, entonces $g(x)$ o $h(x)$ es constante.
   b) Probar que el conjunto de polinomios en $\mathbb{Q}[x]$ que anulan a α es el ideal generado por $f(x)$.
2. Sea $f(x) \in \mathbb{Q}[x]$ de grado dos. Probar que $f(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si no tiene raíces racionales.
3. Sean m y n enteros libres de cuadrados distintos.
   a) Probar que $\mathbb{Q}[\sqrt{m}]$ es un cuerpo.
   b) Probar que 1 y $\sqrt{m}$ son linealmente independientes sobre $\mathbb{Q}$. Concluir que $\mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático.
   c) Probar que $\mathbb{Q}[\sqrt{m}]$ y $\mathbb{Q}[\sqrt{n}]$ son no isomorfos. Ayuda: considerar la ecuación $\sqrt{m} = a + b\sqrt{n}$ con $a, b \in \mathbb{Q}$.
4. Sea $\sigma : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{m}]$ dado por $\sigma(1) = 1$ y $\sigma(\sqrt{m}) = -\sqrt{m}$.
   a) Probar que σ es un isomorfismo de cuerpos.
   b) Probar que todos los morfismos de $\mathbb{Q}[\sqrt{m}]$ a $\mathbb{C}$ son Id y σ.
   c) Probar que si $m < 0$ entonces $\sigma(\alpha) = \overline{\alpha}$, donde la barra denota el conjugado complejo.
5. Probar que $\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$ y $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ para $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$.
6. Probar (1.3).

7. Probar los siguientes hechos.
   a) α es entero algebraico si y sólo si $\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo.
   b) Si α y β son enteros algebraicos entonces también lo son $\alpha+\beta$ y $\alpha\beta$. Concluir que el conjunto de enteros algebraicos forman un subanillo de $\mathbb{C}$.
   c) Para todo $\alpha \in \mathbb{C}$ que es anulado por algún polinomio en $\mathbb{Q}[x]$ (*número algebraico*) existe $m \in \mathbb{Z}$ tal que $m\alpha$ es entero algebraico.
8. Probar las siguientes afirmaciones.
   a) Todo entero racional es entero algebraico.
   b) Los únicos números racionales que son enteros algebraicos son los enteros racionales.
   c) Los elementos en $\mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \sqrt{m}\mathbb{Z}$ son enteros algebraicos.
9. Un polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ se dice *primitivo* si el máximo común divisor de $\{a_0, \ldots, a_n\}$ es 1. Probar los siguientes hechos.
   a) (*Lema de Gauss*) El producto de dos polinomios primitivos es primitivo.
   b) α es entero algebraico si y sólo si su polinomio minimal vive en $\mathbb{Z}[x]$.
10. Probar que $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$ para todo $\alpha \in \mathcal{O}_K$.
11. Probar que $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ y $(1+\sqrt{2})^n \neq 1$ para todo $n \neq 0$.
12. Probar que todas las unidades de $\mathbb{Z}[\sqrt{3}]$ tienen norma 1.
13. Probar que $\mathrm{N}(\alpha) \neq 3$ para todo $\alpha \in \mathbb{Z}[\sqrt{-1}]$.
14. Probar que 3 es un elemento irreducible en $\mathbb{Z}[\sqrt{-14}]$.
15. Probar que todo elemento no nulo y no unidad en $\mathcal{O}_K$ es divisible por un elemento irreducible en $\mathcal{O}_K$. [Ayuda: si $\gamma = \alpha\beta$ con $1 < \mathrm{N}(\alpha) < \mathrm{N}(\gamma)$, y α no es irreducible, entonces repitiendo el procedimiento, probar que en algún momento debe estabilizarse].
16. Probar la afirmación de Ejemplo 1.13. [Ayuda: ver [1, Thm. 2.2.3 y 2.2.5]]
17. Probar la afirmación de Ejemplo 1.14 únicamente para $m = 2, 3, 6$. [Ayuda: ver [1, Thm. 2.2.8]]

2. Teorema de factorización única de ideales

2.1. Ideales. Tomemos $\mathfrak{a}$ un ideal no nulo en $\mathcal{O}_K$, donde K como siempre denota un cuerpo cuadrático. Primero veamos que siempre contiene un entero racional no nulo. Sean $\alpha \in \mathfrak{a} \smallsetminus \{0\}$ y $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ su polinomio minimal. Notemos que $c \neq 0$ pues $f(x)$ es irreducible en $\mathbb{Q}[x]$. Como $f(\alpha) = 0$, tenemos

$$c = -\alpha\,(\alpha + b) \in \mathfrak{a},$$

por lo tanto $c \in \mathfrak{a} \cap \mathbb{Z}$. Además $\mathfrak{a} \cap \mathbb{Z}$ es un ideal de $\mathbb{Z}$, entonces $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ para algún $a \in \mathbb{Z}$.

Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. Veamos que $\mathfrak{p}$ contiene exactamente un primo racional. Sea $a \in \mathfrak{p} \cap \mathbb{Z}$ y $a = p_1 \ldots p_k \in \mathbb{Z}$ su descomposición en primos (racionales), entonces como $\mathfrak{p}$ es un ideal primo tenemos que $p_i \in \mathfrak{p}$ para algún i. Ahora supongamos que p y q son dos primos distintos en $\mathfrak{p}$. Por ser coprimos existen $r, s \in \mathbb{Z}$ tales que $1 = pr + qs \in \mathfrak{p}$, por lo tanto $\mathcal{O}_K = \mathfrak{p}$, lo que contradice la hipótesis. Luego $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para exactamente un primo racional $p \in \mathbb{Z}$.

Denotaremos $\langle \alpha_1, \ldots, \alpha_m \rangle$ al ideal generado por $\alpha_1, \ldots, \alpha_m$ en $\mathcal{O}_K$, es decir,

$$\langle \alpha_1, \ldots, \alpha_m \rangle = \alpha_1 \mathcal{O}_K + \cdots + \alpha_m \mathcal{O}_K.$$

Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Recordemos que $\mathcal{O}_K = \mathbb{Z} + \omega_K \mathbb{Z}$ por Proposición 1.2, donde ω_K está dado por (1.4). En particular, $\mathfrak{a}$ es un $\mathbb{Z}$-submódulo de $\mathcal{O}_K$ de rango dos

(Ejercicio 1). Luego, por el teorema de subgrupos de grupos abelianos libres, existen $a, b, c \in \mathbb{Z}$, $a, c > 0$, tales que

$$\mathfrak{a} = a\mathbb{Z} + (b + c\,\omega_K)\mathbb{Z}. \tag{2.1}$$

En particular $\mathfrak{a} = \langle a, \alpha \rangle$ con $\alpha := b + c\,\omega_K$, es decir, todo ideal no nulo en $\mathcal{O}_K$ es generado por a lo sumo dos elementos.

Definición 2.1. Dado $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$, el cardinal del conjunto de coclases de $\mathcal{O}_K/\mathfrak{a}$ es llamado *norma* de $\mathfrak{a}$ y se denota $\mathrm{N}(\mathfrak{a})$ o simplemente $\mathrm{N}\mathfrak{a}$. Si $\mathfrak{a} = \{0\}$ entonces $\mathrm{N}\mathfrak{a} := 0$.

Se puede mostrar que $\mathrm{N}(\mathfrak{a}) = ac$ si $\mathfrak{a}$ es como en (2.1) (Ejercicio 2).

Proposición 2.2. *Para $\beta \in \mathcal{O}_K$ no nulo,* $\mathrm{N}\langle\beta\rangle = |\mathrm{N}(\beta)|$.

Demostración. Por un lado sabemos que $\langle\beta\rangle = a\mathbb{Z} + \alpha\mathbb{Z}$ por (2.1) donde $a, c \in \mathbb{N}$, $b \in \mathbb{Z}$ y $\alpha = b + c\,\omega_K$. Por (1.5) tenemos que $\langle\beta\rangle = \beta\mathbb{Z} + \beta\,\omega_K\mathbb{Z}$. Sea $R = (r_{ij}) \in \mathrm{GL}_2(\mathbb{Z})$ la matriz de cambio de bases entre $\{a, \alpha\}$ y $\{\beta, \beta\omega_K\}$ del $\mathbb{Z}$-módulo $\langle\beta\rangle$, más precisamente

$$\begin{pmatrix} \beta \\ \beta\omega_K \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \begin{pmatrix} a \\ \alpha \end{pmatrix}.$$

Sea $Q = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$, entonces $S := RQ$ es la matriz de la transformación lineal L_β (ver (1.3)) con respecto a la base $\{1, \omega\}$, pues

$$S \begin{pmatrix} 1 \\ \omega_K \end{pmatrix} = RQ \begin{pmatrix} 1 \\ \omega_K \end{pmatrix} = R \begin{pmatrix} a \\ \alpha \end{pmatrix} = \begin{pmatrix} \beta \\ \beta\omega_K \end{pmatrix}.$$

Finalmente por (1.3) tenemos que

$$\mathrm{N}\langle\beta\rangle = \det(Q) = |\det(R)|\,\det(Q) = |\det(S)| = |\mathrm{N}(\beta)|$$

pues $\det(R) = \pm 1$. □

Dados $\mathfrak{a}$ y $\mathfrak{b}$ ideales de $\mathcal{O}_K$, recordemos la definición de *suma*, *producto* y *conjugado* de ideales:

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \{\alpha + \beta : \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}, \\ \mathfrak{a}\mathfrak{b} &= \left\{ \sum_{i=1}^{m} \alpha_i\beta_i : \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b} \text{ para todo } i \right\}, \\ \mathfrak{a}' &= \{\alpha' : \alpha \in \mathfrak{a}\}. \end{aligned}$$

Se puede ver (Ejercicio 3) que si $\mathfrak{a} = \langle\alpha_1, \ldots, \alpha_r\rangle$ y $\mathfrak{b} = \langle\beta_1, \ldots, \beta_s\rangle$ entonces $\mathfrak{a} + \mathfrak{b} = \langle\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\rangle$, $\mathfrak{a}\mathfrak{b} = \langle\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_r\beta_s\rangle$ y $\mathfrak{a}' = \langle\alpha_1', \ldots, \alpha_r'\rangle$.

Ejemplo 2.3. En el anillo $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ tenemos

$$\begin{aligned} \langle 3, 2 + \sqrt{-5}\rangle\langle 3, 2 - \sqrt{-5}\rangle &= \langle 9, 6 + 3\sqrt{-5}, 6 - 3\sqrt{-5}, 9\rangle \\ &= \langle 3\rangle\langle 3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\rangle \\ &= \langle 3\rangle \end{aligned}$$

pues $1 = (2 + \sqrt{-5}) + (2 - \sqrt{-5}) - 3 \in \langle 3, 2 + \sqrt{-5}, 2 - \sqrt{-5}\rangle$.

Se dice que $\mathfrak{a}$ *divide a* $\mathfrak{b}$ (se denota $\mathfrak{a} \mid \mathfrak{b}$) si existe un ideal $\mathfrak{c}$ de $\mathcal{O}_K$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Notemos que si $\mathfrak{a} \mid \mathfrak{b}$ entonces $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$. Veremos que la recíproca es cierta, (i. e. $\mathfrak{b} \subset \mathfrak{a} \Rightarrow \mathfrak{a} \mid \mathfrak{b}$) como consecuencia del teorema de factorización única de ideales.

Definición 2.4. Se llama *ideal fraccionario* de K a un $\mathcal{O}_K$-submódulo $\mathfrak{a}$ de K que satisface $b\mathfrak{a} \subset \mathcal{O}_K$ para algún $b \in \mathbb{N}$.

Un ideal de $\mathcal{O}_K$ es trivialmente un ideal fraccionario. A partir de ahora, a éstos los llamaremos *ideales enteros*. Es posible probar que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales fraccionarios, entonces también lo son su suma y producto (Ejercicio 4).

Como corolario del teorema de factorización única de ideales veremos que todo ideal fraccionario no nulo tiene inverso (i. e. existe $\mathfrak{a}^{-1}$ ideal fraccionario tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$). Por ahora sólo lo probaremos para ideales enteros primos.

Lema 2.5. *Todo ideal primo $\mathfrak{p}$ no nulo de $\mathcal{O}_K$ es inversible.*

Demostración. Sea $\mathfrak{q} = \{x \in K : x\mathfrak{p} \subset \mathcal{O}_K\}$. Claramente $\mathfrak{q}$ es un $\mathcal{O}_K$-módulo que contiene a $\mathcal{O}_K$. Si $a \in \mathfrak{p} \cap \mathbb{Z}$, entonces $a\mathfrak{q} \subset \mathfrak{q}\mathfrak{p} \subset \mathcal{O}_K$, por lo que $\mathfrak{q}$ es un ideal fraccionario. Por otro lado tenemos que $\mathfrak{p} \subset \mathfrak{p}\mathfrak{q} \subset \mathcal{O}_K$, pero como $\mathfrak{p}$ es un ideal maximal (Ejercicio 5) entonces $\mathfrak{p}\mathfrak{q} = \mathcal{O}_K$ o $\mathfrak{p}\mathfrak{q} = \mathfrak{p}$. El caso $\mathfrak{p}\mathfrak{q} = \mathfrak{p}$ no es posible (Ejercicio 6), lo cual completa la demostración. □

Teorema 2.6. *Todo ideal $\mathfrak{a}$ no nulo de $\mathcal{O}_K$ se descompone de manera única —salvo orden— como producto de ideales primos de $\mathcal{O}_K$.*

Demostración. Probemos primero la existencia de la factorización. Sea $\mathcal{T}$ el conjunto de ideales propios de $\mathcal{O}_K$ que no se factorizan como producto de ideales primos. Queremos ver que $\mathcal{T}$ es vacío. Supongamos $\mathcal{T} \neq \emptyset$. Puesto que $\mathcal{O}_K$ es Noetheriano (Ejercicio 7), $\mathcal{T}$ contiene un elemento maximal $\mathfrak{a}$ (Ejercicio 8). Como $\mathfrak{a}$ no es primo, está contenido en un ideal maximal $\mathfrak{p}$ (Ejercicio 8), que resulta primo (Ejercicio 5). Por Lema 2.5 existe $\mathfrak{p}^{-1}$ ideal fraccionario tal que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. Luego $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal propio de $\mathcal{O}_K$ que contiene propiamente a $\mathfrak{a}$ pues $\mathcal{O}_K \subsetneq \mathfrak{p}^{-1}$, por lo tanto $\mathfrak{a}\mathfrak{p}^{-1} \in \mathcal{T}$. Entonces $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ para ciertos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideales primos, lo que implica $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_k \notin \mathcal{T}$ contradiciendo la hipótesis. Así $\mathcal{T} = \emptyset$.

Ahora veamos la unicidad. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ tal que $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$, con $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ ideales primos de $\mathcal{O}_K$. Veamos que $\mathfrak{q}_1$ divide a $\mathfrak{p}_1 \dots \mathfrak{p}_r$, por lo tanto divide a alguno de ellos (Ejercicio 9), digamos $\mathfrak{p}_1$. Como todo ideal primo es maximal (Ejercicio 5), $\mathfrak{p}_1 = \mathfrak{q}_1$. Por Lema 2.5 tenemos que

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{q}_1^{-1}\mathfrak{a} = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

Repitiendo este argumento se prueba que $r = s$ y que $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ coinciden con $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ salvo el orden. □

2.2. Consecuencias del teorema de factorización única. Ahora sí estamos en condiciones de demostrar que todo ideal fraccionario no nulo tiene inverso. En efecto, por Teorema 2.6 sabemos que $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, y por Lema 2.5 se tiene que $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$ es un ideal fraccionario. Más aún, Teorema 2.6 asegura que todo ideal fraccionario se descompone de manera única salvo orden como

$$\frac{\mathfrak{q}_1 \dots \mathfrak{q}_s}{\mathfrak{p}_1 \dots \mathfrak{p}_s},$$

donde escribimos $\dfrac{1}{\mathfrak{p}_i}$ en lugar de $\mathfrak{p}_i^{-1}$.

A continuación demostraremos que en el contexto de los ideales, contener es sinónimo de dividir.

Proposición 2.7. *Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales en $\mathcal{O}_K$, entonces $\mathfrak{a} \mid \mathfrak{b}$ si y sólo si $\mathfrak{b} \subset \mathfrak{a}$.*

Demostración. La ida es clara. Supongamos que $\mathfrak{b} \subset \mathfrak{a}$. El caso $\mathfrak{a} = \mathcal{O}_K$ es trivial. Si $\mathfrak{a} = \langle 0 \rangle$ tenemos que $\mathfrak{b} = \langle 0 \rangle$ y por lo tanto $\mathfrak{a} \mid \mathfrak{b}$. Asumamos entonces $\mathfrak{a}$ ideal entero propio. Por Teorema 2.6 podemos descomponer a $\mathfrak{a}$ y $\mathfrak{b}$ como

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}, \qquad \mathfrak{b} = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_r^{b_r},$$

donde $a_1, b_1, \dots, a_r, b_r$ son enteros no negativos y $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ son ideales primos distintos.

Sólo resta probar que $b_j \leq a_j$ para todo j. Supongamos que esto no es cierto, digamos $b_1 > a_1$. Como $\mathfrak{b} \subset \mathfrak{a}$ se tiene

$$\mathfrak{p}_2^{a_2} \dots \mathfrak{p}_r^{a_r} \subset \mathfrak{p}_1^{-a_1}\mathfrak{a} \subset \mathfrak{p}_1^{-a_1}\mathfrak{b} \subset \mathfrak{p}_1^{b_1-a_1}\mathfrak{p}_2^{a_2} \dots \mathfrak{p}_r^{a_r}.$$

Sin embargo, el lado derecho es divisible por $\mathfrak{p}_1$ pues $b_1 - a_1 > 0$, mientras que el lado izquierdo no lo es por la unicidad de la factorización, lo cual es absurdo. Por lo tanto $b_1 \leq a_1$. □

A partir de la descomposición única de ideales se puede definir el *máximo común divisor* y el *mínimo común múltiplo* de dos ideales $\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}$ y $\mathfrak{b} = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_r^{b_r}$ $(a_i, b_i \geq 0)$ como

$$\operatorname{mcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{c_1} \dots \mathfrak{p}_r^{c_r} \quad \text{y} \quad \operatorname{mcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{d_1} \dots \mathfrak{p}_r^{d_r},$$

donde $c_i := \min(a_i, b_i)$ y $d_i := \max(a_i, b_i)$ para cada i. Se puede mostrar que $\operatorname{mcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ y $\operatorname{mcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$ (Ejercicio 10).

Otra consecuencia es

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\,\mathrm{N}\mathfrak{b} \tag{2.2}$$

para ideales enteros $\mathfrak{a}$ y $\mathfrak{b}$. Recordemos que por Proposición 2.2 sabemos que $|\mathbb{N}(\alpha)| = \mathbb{N}\langle\alpha\rangle$ para cualquier $\alpha \in \mathcal{O}_K$, por lo tanto (2.2) vale para ideales principales. El caso general requiere algo más de trabajo (Ejercicio 11).

La propiedad (2.2) nos permite enunciar, de manera análoga a (♠), la siguiente condición para que un ideal sea primo.

Proposición 2.8. *Si $\mathfrak{p}$ es un ideal entero tal que $\mathrm{N}\mathfrak{p} = p$ es un primo racional entonces $\mathfrak{p}$ es un ideal primo.*

Demostración. (Ejercicio 12). □

Consideremos un ideal primo $\mathfrak{p}$ no nulo de $\mathcal{O}_K$. Sabemos que existe un único primo racional p en $\mathfrak{p}$, por lo tanto $\langle p \rangle \subset \mathfrak{p}$, o equivalentemente $\mathfrak{p}$ ocurre en la factorización de $\langle p \rangle = \mathfrak{p}_1 \dots \mathfrak{p}_r$ por Proposición 2.7. Aplicando norma a ambos lados obtenemos $p^2 = \mathrm{N}\mathfrak{p}_1 \dots \mathrm{N}\mathfrak{p}_r$, lo cual nos asegura que $r \leq 2$. Más aún, si $r = 2$ entonces $\mathrm{N}(\mathfrak{p}_i) = p$ para $i = 1, 2$. Esto implica que $\langle p \rangle = \mathfrak{p}$ $(r = 1)$ o $\langle p \rangle = \mathfrak{p}\mathfrak{p}'$ $(r = 2)$ pues si $\mathfrak{p}$ divide a $\langle p \rangle$ también lo hace $\mathfrak{p}'$. Luego, el ideal $\langle p \rangle$ se factoriza de una de las siguientes maneras (y p se denomina con respecto a K como sigue):

$$\langle p \rangle = \begin{cases} \mathfrak{p}\mathfrak{p}' & \text{con } \mathfrak{p} \neq \mathfrak{p}' \quad (p \textit{ se parte en } K), \\ \mathfrak{p} & \text{con } \mathfrak{p} = \mathfrak{p}' \quad (p \textit{ permanece primo en } K), \\ \mathfrak{p}^2 & \text{con } \mathfrak{p} = \mathfrak{p}' \quad (p \textit{ ramifica en } K). \end{cases} \tag{2.3}$$

Notemos que en todos los casos tenemos $\mathfrak{p}\mathfrak{p}' = \langle \mathrm{N}\mathfrak{p} \rangle$. Así, para cualquier ideal entero $\mathfrak{a}$, por (2.2) obtenemos

$$\mathfrak{a}\mathfrak{a}' = \langle \mathrm{N}(\mathfrak{a}) \rangle. \tag{2.4}$$

Con estas nuevas herramientas podemos trabajar con ejemplos explícitos.

Ejemplo 2.9. En Ejemplo 2.3 vimos que si $\mathfrak{p} = \langle 3, 2+\sqrt{-5}\rangle \subset \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, entonces $\mathfrak{p}\mathfrak{p}' = \langle 3\rangle$. Luego, $\mathrm{N}\mathfrak{p} = 3$ por (2.4) y $\mathfrak{p}$ es primo por Proposición 2.8. Más aún, $\mathfrak{p}$ no es principal pues si $\mathfrak{p} = \langle\alpha\rangle$ con $\alpha \in \mathcal{O}_K$, entonces $3 = \mathrm{N}\mathfrak{p} = |\mathrm{N}(\alpha)|$ lo cual no puede suceder pues $\mathrm{N}(a+b\sqrt{-5}) = a^2+5b^2 \neq 3$ para todo $a, b \in \mathbb{Z}$. Así, $\mathcal{O}_K$ no es un dominio de ideales principales.

Ejemplo 2.10. En Ejemplo 1.11 vimos que $3^4 = (5+2\sqrt{-14})(5-2\sqrt{-14})$ con 3, $\alpha := 5+2\sqrt{-14}$ y $\alpha' = 5-2\sqrt{-14}$ elementos irreducibles en $\mathbb{Z}[\sqrt{-14}]$. Si $\mathfrak{a} = \langle 3^4\rangle$, entonces tenemos dos factorizaciones distintas $\mathfrak{a} = \langle 3\rangle^4 = \langle\alpha\rangle\langle\alpha'\rangle$, pero no de ideales primos.

Sea $\mathfrak{p} = \langle 3, 1+\sqrt{-14}\rangle$, entonces

$$\mathfrak{p}\mathfrak{p}' = \langle 9, 3+\sqrt{-14}, 3-3\sqrt{-14}, 15\rangle = \langle 3\rangle.$$

En efecto, en la última igualdad claramente vale $\subset$ pues todos los elementos de $\mathfrak{p}\mathfrak{p}'$ son divisibles por 3. Además $3 = 2\cdot 9 - 15 \in \mathfrak{p}\mathfrak{p}'$ lo que asegura $\supset$. En particular $\mathrm{N}\mathfrak{p} = 3$ y $\mathfrak{p}$ es un ideal primo. Luego $\mathfrak{a} = \mathfrak{p}^4\mathfrak{p}'^4$ es su descomposición en ideales primos. Es posible comprobar que $\langle\alpha\rangle = \mathfrak{p}^4$ y $\langle\alpha'\rangle = \mathfrak{p}'^4$ (Ejercicio 13).

Para un cuerpo cuadrático $K = \mathbb{Q}[\sqrt{m}]$, llamaremos *discriminante* de K a

$$d_K = \begin{cases} 4m & \text{si } m \equiv 2,3 \pmod 4, \\ m & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

Claramente se tiene que $K = \mathbb{Q}[\sqrt{d_K}]$. Más aún, $\{1, \frac{d_k+\sqrt{d_K}}{2}\}$ es una base del $\mathbb{Z}$-módulo $\mathcal{O}_K$ (Ejercicio 14). También haremos uso del conocido *símbolo de Legendre* el cual para un primo racional p impar y $a \in \mathbb{Z}$ se define por

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod p \text{ tiene solución en } \mathbb{Z}, \\ -1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod p \text{ no tiene solución en } \mathbb{Z}, \\ 0 & \text{si } p \mid a. \end{cases}$$

Se puede ver que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ para todo $a, b \in \mathbb{Z}$ (Ejercicio 15).

El siguiente resultado da simples condiciones para que saber cómo se factoriza $\langle p\rangle$, para un número primo racional $p > 2$.

Teorema 2.11. *Sean p un primo racional impar y $K = \mathbb{Q}[\sqrt{m}]$ un cuerpo cuadrático con discriminante d_K. Entonces se tienen las siguientes equivalencias.*

(i) $\langle p\rangle = \mathfrak{p}^2$ *si y sólo si* $\left(\dfrac{d_K}{p}\right) = 0$.

(ii) $\langle p\rangle = \mathfrak{p}\mathfrak{p}'$ *con* $\mathfrak{p} \neq \mathfrak{p}'$ *si y sólo si* $\left(\dfrac{d_K}{p}\right) = +1$.

(iii) $\langle p\rangle = \mathfrak{p}$ *si y sólo si* $\left(\dfrac{d_K}{p}\right) = -1$.

Demostración. Comencemos suponiendo que $\langle p\rangle = \mathfrak{p}^2$. Entonces existe $\pi = a+b\,\frac{d_K+\sqrt{d_K}}{2} \in \mathfrak{p} \setminus \langle p\rangle$ con $a, b \in \mathbb{Z}$. Sin embargo,

$$\begin{aligned} \pi^2 &= \left(\frac{2a+bd_K}{2} + \frac{b}{2}\sqrt{d_K}\right)^2 \\ &= \tfrac{1}{4}\Big((2a+bd_K)^2 + d_K b^2\Big) + \tfrac{1}{2}(a+bd_K)b\sqrt{d_K} \in \langle p\rangle \end{aligned}$$

por lo tanto p divide (en $\mathbb{Z}$) a $(2a+bd_K)^2+d_Kb^2$ y a $(a+bd_K)b$. Si $p \mid b$ entonces $p \mid a$ y en consecuencia $p \mid \pi$ lo cual contradice la hipótesis. Esto implica que $p \mid a+bd_K$ y $p \nmid b$, sumado a que $p \mid (2a+bd_K)^2+d_Kb^2$, resulta $p \mid d_K$, es decir, $\left(\frac{d_K}{p}\right)=0$.

Ahora supongamos $p \mid d_K$. Consideremos $\mathfrak{p}=\langle p\rangle+\langle\sqrt{d_K}\rangle$, entonces (Ejercicio 16)

$$\mathfrak{p}^2=\langle p^2, p\sqrt{d_K}, d_K\rangle=\langle p\rangle, \tag{2.5}$$

con $\mathfrak{p}$ ideal primo por (2.4) y Proposición 2.8.

Supongamos que $\left(\frac{d_K}{p}\right)=1$, es decir, existe $a\in\mathbb{Z}$ tal que $a^2\equiv d_K \pmod p$. Si $\mathfrak{p}=\langle p, a+\sqrt{d}\rangle$ entonces (Ejercicio 16)

$$\mathfrak{p}\mathfrak{p}'=\langle p^2, p(a+\sqrt{d_K}), p(a-\sqrt{d_K}), a^2-d_K\rangle=\langle p\rangle \tag{2.6}$$

con $\mathfrak{p}$ y $\mathfrak{p}'$ ideales primos. Además $\mathfrak{p}\neq\mathfrak{p}'$ pues $\mathfrak{p}+\mathfrak{p}'=\mathcal{O}_K$.

Recíprocamente, si $\langle p\rangle=\mathfrak{p}\mathfrak{p}'$ con $\mathfrak{p}\neq\mathfrak{p}'$, entonces $\mathrm{N}(\mathfrak{p})=\mathrm{N}(\mathfrak{p}')=p$. Tomemos $\alpha=a+b\frac{d_K+\sqrt{d_K}}{2}\in\mathfrak{p}\smallsetminus\langle p\rangle$ donde $a,b\in\mathbb{Z}$ satisfacen que $p\nmid \mathrm{mcd}(a,b)$. Como $\langle\alpha\rangle\subset\mathfrak{p}$ se tiene $\mathfrak{p}\mid\langle\alpha\rangle$ por Proposición 2.7, por lo tanto $p=\mathrm{N}\mathfrak{p}$ divide a

$$\mathrm{N}\langle\alpha\rangle=|\mathrm{N}(\alpha)|=\left|\mathrm{N}\left(\tfrac{2a+bd_K}{2}+\tfrac{bd_K}{2}\sqrt{d_K}\right)\right|=\tfrac{1}{4}\left|(2a+bd_K)^2-b^2d_K\right|,$$

en particular $(2a+bd_K)^2\equiv b^2d_K \pmod p$. Si $p\mid b$ entonces $p\mid a$ lo cual contradice la hipótesis. Luego $p\nmid b$, entonces existe $c\in\mathbb{Z}$ tal que $bc\equiv 1 \pmod p$ (i. e. c es el inverso de b módulo p), por lo tanto $x^2\equiv d_K \pmod p$ tiene solución $x=(2a+bd_K)c$.

El último caso es inmediato a partir de los dos ítems anteriores. □

Existe una teoría similar para $p=2$ que utiliza el *símbolo de Kronecker*, la cual no abordaremos para no abultar el texto (ver [4]).

Para finalizar esta sección, veamos que en estos anillos todo DFU es necesariamente DIP. Necesitaremos el siguiente lema que tiene valor por sí mismo para entender los ideales primos en un DFU.

Lema 2.12. *Si $\mathcal{O}_K$ es un dominio de factorización única, entonces todo ideal primo en $\mathcal{O}_K$ es principal.*

Demostración. Primero veamos que dado π elemento irreducible en $\mathcal{O}_K$, el ideal $\langle\pi\rangle$ es maximal. Supongamos que $\langle\pi\rangle\subset\mathfrak{a}\subset\mathcal{O}_K$ y $\langle\pi\rangle\neq\mathfrak{a}$ para algún ideal entero $\mathfrak{a}$. Sea $\alpha\in\mathfrak{a}\smallsetminus\langle\pi\rangle$, escribimos $\langle\pi\rangle=\mathfrak{a}\mathfrak{b}$ por Proposición 2.7. Para todo $\beta\in\mathfrak{b}$ se tiene $\alpha\beta\in\langle\pi\rangle$, entonces $\pi\mid\alpha\beta$ y por lo tanto $\pi\mid\beta$ pues $\alpha\notin\langle\pi\rangle$. Esto nos dice que $\langle\pi\rangle=\mathfrak{b}$, de esta forma $\langle\pi\rangle=\langle\pi\rangle\mathfrak{a}$ lo que significa que $\mathfrak{a}=\mathcal{O}_K$ y $\langle\pi\rangle$ es maximal.

Tomemos $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y $\alpha\in\mathfrak{p}$ no nulo. Como $\mathcal{O}_K$ es dominio de factorización única, existen $\pi_1,\dots,\pi_r$ elementos irreducibles tales que $\alpha=\pi_1\dots\pi_r$. Esto nos dice que $\mathfrak{p}$ divide a $\langle\pi_1\rangle\dots\langle\pi_r\rangle$, por lo tanto divide a algún $\langle\pi_i\rangle$, i. e. $\langle\pi_i\rangle\subset\mathfrak{p}$. Por lo anterior $\langle\pi\rangle$ es maximal y en consecuencia vale la igualdad. □

Teorema 2.13. *El anillo de enteros $\mathcal{O}_K$ de un cuerpo cuadrático K es dominio de ideales principales si y sólo si es dominio de factorización única.*

Demostración. La ida vale en general. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$, veamos que es principal. Claramente podemos suponer que $\mathfrak{a}$ es propio. Descomponemos $\mathfrak{a}=\mathfrak{p}_1\dots\mathfrak{p}_r$ como producto de ideales primos $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ por Teorema 2.6. Por Lema 2.12, $\mathfrak{p}_i=\langle\pi_i\rangle$ para algún $\pi_i\in\mathcal{O}_K$, por lo tanto $\mathfrak{a}=\langle\pi_1\dots\pi_r\rangle$. □

Como consecuencia tenemos que $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única ya que en Ejemplo 2.9 vimos que no es dominio de ideales principales.

2.3. Ejercicios.

1. Probar que todo ideal $\mathfrak{a}$ de $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango 2.
2. Probar que si $\mathfrak{a}$ es un ideal de $\mathcal{O}_K$ como en (2.1) entonces $\mathrm{N}\mathfrak{a} = ac$. [Ayuda: mostrar que un conjunto de representantes de $\mathcal{O}_K/\mathfrak{a}$ es $\{r + s\omega_K : 0 \leq r < a,\ 0 \leq s < c\}$.]
3. Probar que si $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_r \rangle$ y $\mathfrak{b} = \langle \beta_1, \ldots, \beta_s \rangle$ entonces:
   a) $\mathfrak{a} + \mathfrak{b} = \langle \alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \rangle$.
   b) $\mathfrak{a}\mathfrak{b} = \langle \alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_r\beta_s \rangle$.
   c) $\mathfrak{a}' = \langle \alpha_1', \ldots, \alpha_r' \rangle$.
4. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales fraccionarios. Probar que también lo son $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a}'$ y $c\,\mathfrak{a}$ para $c \in \mathbb{Q}$.
5. Probar que todo ideal primo es maximal. [Ayuda: todo dominio de integridad finito es un cuerpo.]
6. Probar que si $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos entonces $\mathfrak{p}\mathfrak{q} \neq \mathfrak{p}$.
7. Probar que $\mathcal{O}_K$ es Noetheriano, es decir, toda cadena ascendente $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ de ideales en $\mathcal{O}_K$ debe estabilizarse en algún momento.
8. Probar las siguientes equivalencias para un anillo A.
   (i) A es Noetheriano.
   (ii) Todo subconjunto no vacío $\mathcal{T}$ de ideales en A contiene un elemento maximal, es decir, existe $\mathfrak{a} \in \mathcal{T}$ tal que $\mathfrak{a} \not\subset \mathfrak{b}$ para todo $\mathfrak{b} \in \mathcal{T}$ distinto de $\mathfrak{a}$.
   (iii) Todo ideal en A está contenido en un ideal maximal.
   (iv) Todo ideal en A es finitamente generado.
9. Probar que si un ideal primo $\mathfrak{p}$ divide a un producto de ideales $\mathfrak{a}\mathfrak{b}$, entonces $\mathfrak{p}$ divide a uno de ellos.
10. Probar que $\mathrm{mcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ y $\mathrm{mcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$. Generalizarlo para una cantidad finita de ideales.
11. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales enteros en $\mathcal{O}_K$ de norma m y n respectivamente. Denotemos $\xi_1, \ldots, \xi_m$ y $\eta_1, \ldots, \eta_n$ los conjuntos de representantes de $\mathcal{O}_K/\mathfrak{a}$ y $\mathcal{O}_K/\mathfrak{b}$ respectivamente.
    a) Probar que existe $\gamma \in \mathcal{O}_K$ tal que $\mathrm{mcd}(\mathfrak{a}\mathfrak{b}, \langle\gamma\rangle) = \mathfrak{a}$.
    b) Probar que los elementos $\xi_i + \gamma\eta_j$ para $1 \leq i \leq m$ y $1 \leq j \leq n$ viven en clases distintas de $\mathcal{O}_K/\mathfrak{a}\mathfrak{b}$.
    c) Probar que los mn elementos del ítem anterior forman un conjunto completo de representantes de $\mathcal{O}_K/\mathfrak{a}\mathfrak{b}$.
12. Probar Proposición 2.8
13. Probar que $\langle 5 + 2\sqrt{-14} \rangle = \langle 3, 1 + \sqrt{-14} \rangle^4$ en $\mathbb{Z}[\sqrt{-14}]$.
14. Probar que $\mathcal{O}_K = \mathbb{Z} + \frac{d_K + \sqrt{d_K}}{2}\mathbb{Z}$.
15. Probar que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ para todo $a, b \in \mathbb{Z}$.
16. Probar (2.5) y (2.6)

3. Grupo de clases

3.1. Finitud del número de clases. Sea K un cuerpo cuadrático con anillo de enteros $\mathcal{O}_K$. Vimos al comenzar Subsección 2.2 que todo ideal fraccionario no nulo tiene inverso, lo que nos asegura que el conjunto de ideales fraccionarios no nulos forman un grupo multiplicativo (abeliano). Este grupo será denotado por Δ_K.

Notemos que si $\alpha \in K$ entonces $\langle\alpha\rangle := \{\alpha\beta : \beta \in \mathcal{O}_K\}$ es un ideal fraccionario en K. Los ideales fraccionarios de esta forma serán llamados naturalmente *principales*.

Claramente los ideales fraccionarios principales no nulos forman un subgrupo Π_K de Δ_K.

Definición 3.1. El grupo cociente $\mathfrak{I}_K = \Delta_K/\Pi_K$ es llamado el *grupo de clases de ideales* de K, o simplemente *grupo de clases*.

La intención es probar que el grupo $\mathfrak{I}_K$ es finito. El orden de tal grupo lo denotaremos por h_K y es llamado *número de clase* de K. Se puede ver que (Ejercicio 1)

$$h_K = 1 \iff \mathcal{O}_K \text{ es DFU.} \tag{3.1}$$

En general, el número h_K mide por cuánto $\mathcal{O}_K$ no es dominio de factorización única.

Dado $\mathfrak{a}$ un ideal fraccionario no nulo de K, denotaremos $[\mathfrak{a}]$ su clase en $\mathfrak{I}_K$. Notemos que $[\mathfrak{a}] = [\mathfrak{b}]$ equivale a $\mathfrak{a} = \langle\alpha\rangle\mathfrak{b}$ para algún $\alpha \in K$.

Lema 3.2. *Para todo entero $t > 0$ existe una cantidad finita de ideales enteros $\mathfrak{a}$ de $\mathcal{O}_K$ tales que $\mathrm{N}\mathfrak{a} < t$.*

Demostración. (Ejercicio 2). □

Lema 3.3. *Todo ideal entero no nulo $\mathfrak{a}$ contiene un elemento $\alpha \neq 0$ tal que*

$$|\mathrm{N}(\alpha)| \leq C_K\, \mathrm{N}\mathfrak{a},$$

donde $C_K = \big(1 + |\mathrm{N}(\omega_K)| + |\mathrm{Tr}(\omega_K)|\big)$.

Demostración. Sabemos que $\mathcal{O}_K = \mathbb{Z} + \omega_K\mathbb{Z}$ por (1.5). Sea t la parte entera de $(\mathrm{N}\mathfrak{a})^{1/2}$. Luego, entre los $(t+1)^2$ números de la forma $a + b\,\omega_K$ con $0 \leq a, b \leq t$ deben existir dos cuya diferencia esté en $\mathfrak{a}$ pues $\#\mathcal{O}_K/\mathfrak{a} = \mathrm{N}\mathfrak{a} < (t+1)^2$. Llamemos α a tal diferencia que podemos escribir como $\alpha = a + b\,\omega_K$ con $-t \leq a, b \leq t$. Entonces

$$\begin{aligned} |\mathrm{N}(\alpha)| &= |(a + b\omega_K)(a + b\omega'_K)| \\ &= |a^2 + b^2\mathrm{N}(\omega_K) + ab\mathrm{Tr}(\omega_K)| \\ &\leq t^2\,\big(1 + |\mathrm{N}(\omega_K)| + |\mathrm{Tr}(\omega_K)|\big), \end{aligned}$$

por lo que concluimos $|\mathrm{N}(\alpha)| \leq C_K\,\mathrm{N}\mathfrak{a}$. □

Lema 3.4. *En toda clase de ideales existe un representante $\mathfrak{a} \subset \mathcal{O}_K$ tal que $\mathrm{N}\mathfrak{a} \leq C_K$.*

Demostración. Consideremos la clase $[\mathfrak{b}]$ de un ideal fraccionario no nulo $\mathfrak{b}$. Podemos suponer que $\mathfrak{b}^{-1}$ es un ideal entero. Por Lema 3.3 existe $\beta \in \mathfrak{b}^{-1}$ tal que $|\mathrm{N}(\beta)| \leq C_K\,\mathrm{N}\mathfrak{b}^{-1}$. Sea $\mathfrak{a} = \langle\beta\rangle\mathfrak{b}$ en la clase $[\mathfrak{b}]$. Entonces $\mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}^{-1} = \mathrm{N}(\mathfrak{a}\mathfrak{b}^{-1}) = \mathrm{N}\langle\beta\rangle = |\mathrm{N}(\beta)| \leq C_K\mathrm{N}\mathfrak{b}^{-1}$, por lo tanto $\mathrm{N}\mathfrak{a} \leq C_K$. □

Estos tres lemas implican la finitud de h_K (Ejercicio 3).

Teorema 3.5. *El número de clase de K es finito.*

Fijado un cuerpo cuadrático K, el cálculo explícito del número h_K es generalmente complicado. En la actualidad se utilizan métodos computacionales para ello, sin embargo como veremos en la siguiente sección, aún no se entiende completamente su comportamiento.

Calculemos algunos de ellos usando Lema 3.4 y Teorema 2.11. La intención es dar un representante de cada clase de $\mathfrak{I}_K$. Por Lema 3.4 es suficiente buscar dentro de los ideales enteros de norma menor o igual a C_K. Más aún, gracias al teorema de

factorización única de ideales, podemos concentrarnos en los ideales primos. No es difícil chequear que (Ejercicio 4)

$$C_K = \begin{cases} 1+|m| & \text{si } m \equiv 2,3 \pmod 4, \\ \dfrac{2+|1-m|}{4} & \text{si } m \equiv 1 \pmod 4. \end{cases} \tag{3.2}$$

Ejemplo 3.6. Comencemos con el caso $K = \mathbb{Q}[\sqrt{2}]$ en donde $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, $d_K = 8$ y $C_K = 3$. Sea $\mathfrak{p}$ un ideal entero con norma igual a 2 o 3, por lo tanto primo. Esto significa, por (2.4), que $\mathfrak{p}$ divide a $\langle 2\rangle$ o a $\langle 3\rangle$ respectivamente. Tenemos que $\langle 2\rangle = \langle\sqrt{2}\rangle^2$ y $\langle 3\rangle$ es primo pues $\left(\frac{d}{3}\right) = -1$ (ver Teorema 2.11), luego $\mathfrak{p} = \langle\sqrt{2}\rangle$ sólo puede ser igual al ideal principal $\langle 2\rangle$. Concluimos que todo ideal fraccionario es principal, o equivalentemente

$$h_{\mathbb{Q}[\sqrt{2}]} = 1.$$

Ejemplo 3.7. Sea $K = \mathbb{Q}[\sqrt{-1}]$ por lo tanto $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, $d_K = -4$ y $C_K = 2$. En este caso $\langle 2\rangle = \langle 1+\sqrt{-1}\rangle^2$, entonces

$$h_{\mathbb{Q}[\sqrt{-1}]} = 1.$$

Para estos dos ejemplos ya sabíamos que $h_K = 1$ pues en ambos casos $\mathcal{O}_K$ es dominio de factorización única por ser dominio Euclídeo (ver Ejemplo 1.13 y Ejemplo 1.14). Con este mismo método se puede comprobar que $h_K = 1$ para los listados en Ejemplo 1.13 (Ejercicio 5) y en Ejemplo 1.14 (Ejercicio 6), aunque los cálculos necesarios aumentan significativamente a medida que d_K crece.

Ejemplo 3.8. Tomemos $K = \mathbb{Q}[\sqrt{-5}]$, así $\mathcal{O}_K = \mathbb{Z}[-5]$, $d_K = -20$ y $C_K = 6$. Sabemos por Ejemplo 2.9 que no es dominio de ideales principales, y en consecuencia tampoco es dominio de factorización única por Teorema 2.13, entonces $h_K \geq 2$. Tenemos (Ejercicio 7)

$$\begin{array}{rcll} \langle 2\rangle &=& \mathfrak{p}_2^2 & \text{donde} \quad \mathfrak{p}_2 = \langle 2, 1+\sqrt{-5}\rangle, \quad \mathfrak{p}_2 = \mathfrak{p}_2' \\ \langle 3\rangle &=& \mathfrak{p}_3\mathfrak{p}_3' & \text{donde} \quad \mathfrak{p}_3 = \langle 3, 1+\sqrt{-5}\rangle, \quad \mathfrak{p}_3 \neq \mathfrak{p}_3', \\ \langle 5\rangle &=& \mathfrak{p}_5^2 & \text{donde} \quad \mathfrak{p}_5 = \langle\sqrt{-5}\rangle, \quad \mathfrak{p}_5 = \mathfrak{p}_5'. \end{array} \tag{3.3}$$

Luego, todos los ideales enteros de norma menor o igual a 6 son

$$\mathfrak{p}_2, \quad \mathfrak{p}_3, \quad \mathfrak{p}_3', \quad \mathfrak{p}_2^2, \quad \mathfrak{p}_5, \quad \mathfrak{p}_2\mathfrak{p}_3 \quad \text{y} \quad \mathfrak{p}_2\mathfrak{p}_3'.$$

La primera factorización de (3.3) nos dice que $[\langle 1\rangle] = [\langle 2\rangle] = [\mathfrak{p}_2]^2$ por lo tanto $[\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$. Además se tiene que $\mathfrak{p}_2$ no puede ser principal y

$$\begin{aligned} \mathfrak{p}_2\mathfrak{p}_3 &= \langle 6,\, 2(1+\sqrt{-5}),\, 3(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle \\ &= \langle 1+\sqrt{-5}\rangle, \end{aligned}$$

lo que implica

$$\begin{array}{lll} [\mathfrak{p}_2\mathfrak{p}_3] = [\langle 1\rangle], & [\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2], & [\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2], \\ [\mathfrak{p}_2\mathfrak{p}_3'] = [\langle 1\rangle], & [\mathfrak{p}_2^2] = [\langle 1\rangle], & [\mathfrak{p}_5] = [\langle 1\rangle]. \end{array}$$

Esto nos permite concluir

$$\mathfrak{I}_{\mathbb{Q}[\sqrt{-5}]} = \big\{[\langle 1\rangle],\ [\mathfrak{p}_2]\big\} \cong \mathbb{Z}_2 \qquad \text{y} \qquad h_{\mathbb{Q}[\sqrt{-5}]} = 2.$$

Con incluso menos cálculos es posible ver que $h_{\mathbb{Q}[\sqrt{-15}]} = 2$ (Ejercicio 8). Para el resto de los cuerpos con $h_K > 1$ la cantidad de posibilidades aumenta, aunque vale la pena mostrar que $h_{\mathbb{Q}[\sqrt{-23}]} = 3$ (Ejercicio 9).

3.2. Conjeturas de Gauss. El problema de determinar el número h_K se remonta a Gauss en su conocido tratado *Disquisitiones Arithmeticae* sobre formas binarias cuadráticas publicado en 1981. A pesar de que un gran número de prestigiosos matemáticos han trabajado en esta área, existen diversas cuestiones sobre el número h_K que aún no han resueltas. Daremos un breve recorrido sobre algunas ellas para el caso de cuerpos cuadráticos imaginarios. Un excelente resumen histórico hace Dorian Goldfeld [3], quien probó un importante teorema que veremos al fin de estas notas.

El primer avance significativo para entender el número h_K fue debido a Dirichlet en 1839. Este resultado es llamado *Dirichlet class number formula* y se puede escribir como sigue:

$$h_K = \begin{cases} \dfrac{w\sqrt{-d_K}}{2\pi}\, L(1,\chi) & \text{si } d_K < 0, \\ \dfrac{\sqrt{d_K}}{\log(\varepsilon)}\, L(1,\chi) & \text{si } d_K > 0, \end{cases} \tag{3.4}$$

donde d_K es el discriminante de K, w el número de unidades en $\mathcal{O}_K$, ε la unidad fundamental de $\mathcal{O}_K$ y $L(\cdot,\chi)$ la serie L correspondiente al carácter $\chi(n) := \left(\frac{d_K}{n}\right)$, i. e. $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)\, n^{-s}$. Además dio una fórmula finita para el número $L(1,\chi)$, la cual desafortunadamente no es efectiva en la práctica.

Gauss hizo varias conjeturas en su tratado sobre el comportamiento de h_K, tal como

$$\lim_{m\to-\infty} h_{\mathbb{Q}[\sqrt{m}]} = \lim_{d_K\to-\infty} h_K = +\infty,$$

que fue probada por Helbronn en 1934. Además dejó listas de cuerpos cuadráticos imaginarios con números de clase menos a 6, afirmando además que estaban completas. Efectivamente lo estaban. Por ejemplo para $h_K = 1$ son

$$d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

A decir verdad, ésta no es la nómina original de Gauss ya que su trabajo lo realizaba en el contexto de las formas cuadráticas binarias. Recién a mediados de la década del 60', Baker y Stark probaron independientemente que la lista estaba completa para $h_K = 1$, y luego para $h_K = 2$ a principios de los 70'.

La versión moderna de las listas conjeturadas por Gauss es el llamado *Gauss' class number problem* y se puede enunciar de la siguiente manera:

> *Encontrar un algoritmo efectivo para determinar todos los cuerpos cuadráticos imaginarios con número de clase dado.*

En la década del 70', Goldfeld publicó una serie de trabajos relacionando este problema con series L de curvas elípticas sobre $\mathbb{Q}$, y junto con los resultados de Gross y Zagier en esta área en 1985, se obtuvo el siguiente teorema.

Teorema 3.9 (Goldfeld-Gross-Zagier)**.** *Para todo $\varepsilon > 0$ existe una constante $c > 0$ calculable de manera efectiva tal que*

$$h_K > c\ (\log|d_K|)^{1-\varepsilon}$$

para todo cuerpo cuadrático imaginario K.

Este teorema resuelve —salvo una cantidad finita de cálculos— el problema de Gauss sobre el número de clases. De todas maneras, la "cantidad finita" de cálculos necesarios son exageradamente grandes, tanto que sólo se conocía para $h_K \leq 7$ hasta el 2004, año en el que Watkins determinó todos los cuerpos cuadráticos imaginarios con número de

clase menor o igual a 100. Para esto realizó modificaciones en los trabajos de Goldfeld obteniendo una mejor constante c, aunque aún así los cálculos demoraron siete meses dentro de la computadora. Como curiosidad, los cuerpos cuadráticos con número de clase igual a 100 son 1736, y el valor máximo de d_K para éstos es 1856563.

El caso cuadrático real es mucho menos entendido. Finalizamos estas notas con la siguiente conjetura de Gauss aún abierta.

Conjetura 3.10. (Gauss) *Existen infinitos cuerpos cuadráticos reales con número de clase uno.*

3.3. Ejercicios.

1. Sea K un cuerpo cuadrático. Probar que $\mathcal{O}_K$ es un dominio de factorización única si y sólo si $h_K = 1$.
2. Probar Lema 3.2 siguiendo los siguientes pasos.
   - Es suficiente demostrarlo para ideales primos.
   - Si $\mathfrak{p}$ es un ideal primo, entonces $\mathrm{N}\mathfrak{p}$ es p o p^2 para p un primo racional.
   - Concluir la demostración usando Teorema 2.11.
3. Probar Teorema 3.5 como una simple consecuencia de los Lema 3.2, Lema 3.3 y Lema 3.4.
4. Probar (3.2).
5. Probar que $h_K = 1$ para $K = \mathbb{Q}[\sqrt{m}]$ con $m = -2, -3, -7, -11$.
6. Probar que $h_K = 1$ para $K = \mathbb{Q}[\sqrt{m}]$ con $m = 2, 3, 5, 13$.
7. Probar (3.3).
8. Probar que $h_{\mathbb{Q}[\sqrt{-15}]} = 2$.
9. Probar que $h_{\mathbb{Q}[\sqrt{-23}]} = 3$ y dar los representantes de $\mathfrak{I}_{\mathbb{Q}[\sqrt{-23}]}$.

Referencias

[1] S. Alaca, K.S. Williams, *Introductory algebraic number theory*, Cambridge University Press (2004).

[2] K. Conrad, *Factoring in quadratic field*, notas incluidas en su página web.

[3] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bulletin of AMS **13**:1 (1985).

[4] R. Narasimhan, S. Raghavan, S. Rangachari, S. Lal, *Algebraic number theory*, Lecture notes of Tata Institute of Fundamental Research, Bombay (1966).

[5] M.I. Pacharoni, *Aritmética en cuerpos de números*, notas del elENA III, cursos para estudiantes (2006).

FaMAF — CIEM, Universidad Nacional de Córdoba; Medina Allende s/n, Ciudad Universitaria, 5000, Córdoba.

E-mail address: elauret@famaf.unc.edu.ar

Cursos de Nivel Intermedio

ESPECIES COMBINATORIAS

RODRIGO IGLESIAS

RESUMEN. Las funciones y series generatrices son un intrumento clásico para el conteo de estructuras combinatorias de algún tipo (árboles, particiones, grafos, etc.). La teoría de especies combinatorias fue introducida por A. Joyal en 1980 como un método sistemático para definir y analizar estructuras combinatorias y sus series asociadas, dando explicaciones naturales a las manipulaciones algebraicas que se hacen con las funciones generatrices.

Así como la suma y multiplicación en el anillo de caracteres provienen de operaciones en la categoría de las representaciones de un grupo, de manera similar, las operaciones de suma, multiplicación, derivación, composición, etc. entre series formales son manifestaciones de operaciones en una categoría más rica: la de las especies combinatorias.

En el curso vamos a introducir el concepto de especie combinatoria y sus operaciones más básicas, mostrando cómo funcionan en ejemplos importantes como las especies de particiones, permutaciones, árboles y ciclos. Veremos una extensión del concepto de especie, el de las especies ponderadas y sus series, en particular las serie indicatriz de ciclos apuntando a dar esquemáticamente una prueba puramente combinatoria del teorema de enumeración de Polya-Redfield, el cual da un método general para contar las órbitas de una acción del grupo simétrico.

ÍNDICE

Date: 10 de julio de 2012.

Introducción

Supongamos que queremos calcular el número a_n de árboles con raíz con n nodos (etiquetados) así como el número t_n de tipos de isomorfismos de árboles con n nodos (no etiquetados). Para esto es conveniente considerar las funciones generatrices

$$\mathcal{A}(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!}, \qquad\qquad T(x) = \sum_{n\geq 0} t_n x^n$$

puesto que se sabe por los trabajos de Cayley y Pólya entre otros que estas series generatrices satisfacen identidades como

$$\mathcal{A}(x) = xe^{\mathcal{A}(x)}, \qquad\qquad T(x) = x\sum_{n\geq 0} \exp\left(\frac{T(x^n)}{n}\right)$$

De identidades como estas podemos obtener fórmulas de recurrencia para los coeficientes.

De dónde provienen o qué significan estas identidades, o para qué otras estructuras podemos obtener este tipo ecuaciones funcionales o diferenciales, son el tipo de preguntas que queremos responder.

En 1980 A. Joyal introdujo en [4] una teoría que es capaz de dar respuestas satisfactorias a estas preguntas. Las especies combinatorias forman una categoría de objetos con operaciones de suma, multiplicación, composición, derivación, etc., que resultan naturales desde el punto de vista intuitivo o visual y que sin embargo resultan ser los movimientos detrás de escena de varias manipulaciones usuales y menos intuitivas que se hacen con las series generatrices.

Por ejemplo las identidades de arriba son manifestaciones distintas de una única ecuación que indica un isomorfismo entre dos especies:

$$\mathcal{A} = XE(\mathcal{A})$$

Esta ecuación esencialmente dice que especificar un árbol con raíz sobre un conjunto de nodos es equivalente a especificar un nodo y un conjunto de árboles con raíz sobre el resto de los nodos. Una vez planteada la ecuación entre especies, la teoría nos da métodos sistemáticos para deducir ecuaciones entre las diferentes series generatrices.

En estas tres clases el objetivo es introducir las nociones básicas de la teoría de especies combinatorias que nos permitan leer y escribir ecuaciones en esta categoría, apuntando a entender la explicación que ésta da de la teoría enumerativa de Pólya para el cálculo de tipos de estructuras (no etiquetadas) que usualmente son las que presentan mayor dificultad para ser enumeradas.

Para una introducción a las especies combinatorias es muy recomendable el artículo original [4] de A. Joyal así como el muy buen libro [2] de F. Bergeron, G. Labelle y P. Leroux.

1. Especies

Definición 1.1. Una *especie combinatoria* es un functor $M : \mathbb{B} \to \mathbb{E}$ donde $\mathbb{B}$ es el grupoide cuyos objetos son los conjuntos finitos y cuyos morfismos son las biyecciones. $\mathbb{E}$ es la categoría cuyos objetos son los conjuntos finitos y cuyos morfismos son las funciones. Si U es un conjunto finito, $M[U]$ es el conjunto de todas las *estructuras de especie M sobre U*.

En otras palabras, una especie es una regla M que por cada conjunto finito U produce un conjunto finito $M[U]$ –el conjunto de todas las estructuras etiquetadas de especie M–

y por cada biyección $f : U \to V$ –que puede pensarse como una manera de permutar las etiquetas– produce una función $M[f] : M[U] \to M[V]$ de manera que:

i) para todas las biyecciones $f : U \to V$ y $g : V \to W$

$$M[g \circ f] = M[g] \circ M[f]$$

ii) para todos los conjuntos U

$$M[Id_U] = Id_{M[U]}$$

Observar que $M[f]$ es forzosamente una biyección para toda f. Decimos que un elemento s de $M[U]$ es una *M-estructura*, y que U es su *conjunto subyacente*. Dadas M-estructuras $u \in M[U]$ y $v \in M[V]$, una biyección $f : U \to V$ tal que $M[f](u) = v$ es un *isomorfismo* entre u y v, y en tal caso decimos que u y v son M-estructuras isomorfas. El *tipo de isomorfismo* de u es el conjunto de todas las M-estructuras isomorfas a u.

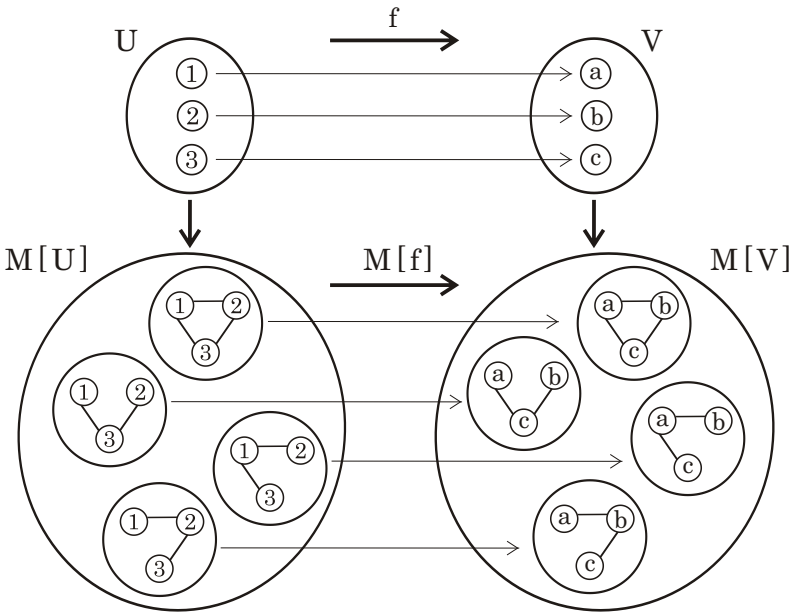


FIGURA 1. El functor M en este caso corresponde a la especie de los grafos conexos. La biyección $M[f]$, llamada *transporte de estructura*, puede verse como un reetiquetamiento de los nodos de los grafos.

1.1. Ejemplos de especies.

Ejemplo 1.2. Una estructura de *esquema simplicial* sobre el conjunto E es una familia $\mathcal{F}$ de subconjuntos no vacíos de E tales que: i) toda parte no vacía de un elemento de $\mathcal{F}$ está también en $\mathcal{F}$ y ii) los singletones $\{x\}$ donde $x \in E$ pertenecen a $\mathcal{F}$. Los elementos de $\mathcal{F}$ son los símplices. La dimensión de un símplice es su cardinal menos uno y la dimensión de un esquema simplicial es el máximo de las dimensiones de los símplices que contiene. La especie de los esquemas simpliciales está dada por el functor Sim que a cada conjunto E le hace corresponder el conjunto $Sim[E]$ de todos los esquemas simpliciales sobre E. Dada una biyección $f : U \to V$ la biyección $Sim[f]$ es la inducida por f.

Las propiedades de las M-estructuras que se preservan por isomorfismos definen subespecies de M. Decimos que N es una *subespecie* de M si para todo E se tiene que $N[E] \subseteq M[E]$ y para cada biyección $f : U \to V$ se cumple $N[f] = M[f]|_{N[U]}$.

Ejemplo 1.3. La especie $\mathcal{G}$ de los *grafos* está definida como la subespecie de Sim tal que $\mathcal{G}[E]$ es el conjunto de todas las estructuras simpliciales de dimensión 1. La especie $\mathcal{G}_c$ denota la subespecie de $\mathcal{G}$ de los *grafos conexos*.

Ejemplo 1.4. La especie de las *forestas* es la subespecie de $\mathcal{G}$ de los grafos sin ciclos. Las forestas conexas forman la especie $\mathfrak{a}$ de los *árboles*. Los árboles con un nodo distinguido del resto forman la especie $\mathcal{A}$ de los *árboles con raíz*, también llamados *arborescencias*. Más precisamente, la especie $\mathcal{A}$ se define por $\mathcal{A}[E] = E \times \mathfrak{a}[E]$ para cada E.

Ejemplo 1.5. Una estructura de *partición* sobre el conjunto E es una familia de subconjuntos no vacíos disjuntos de E cuya unión es E. Denotaremos por Par la especie de las particiones, donde $Par[E]$ es el conjunto de todas las estructuras de partición sobre E.

Ejemplo 1.6. La especie End es la especie de los *endomorfismos*, donde $End[E]$ es el conjunto de todas las funciones de E en E. Si $f : U \to V$ es una biyección y $g \in End[U]$, entonces $End[f](u) = f \circ u \circ f^{-1}$, es decir que el transporte de una estructura de endomorfismo a lo largo de una biyección f está dado por la *conjugación*. Es conveniente a veces visualizar a un endomorfismo de E como un grafo dirigido donde E es el conjunto de nodos y hay una flecha que va de x a y si y sólo si $f(x) = y$. Un *endomorfismo conexo* es un endomorfismo cuyo grafo es conexo. Denotamos por End_c la subespecie de los endomorfimos conexos.

Ejemplo 1.7. La especie $\mathcal{S}$ de las *permutaciones* es la subespecie de End de los endomorfismos biyectivos. La especie $\mathcal{C}$ de los *ciclos* es la subespecie de $\mathcal{S}$ de las permutaciones cuyos grafos son conexos. Convenimos que el conjunto vacío no admite ninguna estructura de ciclo, es decir $\mathcal{C}[\emptyset] = \emptyset$. De esta manera podemos decir que una permutación es un conjunto (posiblemente vacío) de ciclos. En particular $\mathcal{S}[\emptyset] = \{\emptyset\}$ tiene cardinal igual a uno.

Ejemplo 1.8. Denotamos por L la especie de las *listas* u *órdenes lineales*, donde $L[E]$ es el conjunto de todos los órdenes totales sobre E. Un órden lineal puede representarse por un grafo dirigido donde E es el conjunto de nodos y hay una flecha que va de x a y si y sólo si x es el antecesor de y.

Ejemplo 1.9. La especie E es la especie de los *conjuntos*. El conjunto de E-estructuras sobre U tiene un único elemento: $E[U] = \{U\}$. Denotamos por E_+ la especie de los *conjuntos no vacíos*, $E_+[U] = \{U\}$ si U es no vacío y $E_+[U] = \emptyset$ si U es vacío.

Ejemplo 1.10. La especie E_k es la especie de los *k-conjuntos*, es decir, los conjuntos de cardinal k. Está definida por

$$E_k[U] = \begin{cases} \{U\} & \text{si } |U| = k \\ \emptyset & \text{en caso contrario} \end{cases}$$

Es decir que no es posible poner una estructura de k-conjunto a un conjunto que no tenga cardinal k, y si tiene cardinal k entonces posee una única E_k-estructura.

Ejemplo 1.11. La especie X es la especie de los *singletones*. Es la especie E_k en el caso especial $k = 1$:

$$X[U] = \begin{cases} \{U\} & \text{si } |U| = 1 \\ \emptyset & \text{en caso contrario} \end{cases}$$

Ejemplo 1.12. La especie 1 es la especie *conjunto vacío*. Es la especie E_k en el caso especial $k = 0$. Es decir que U tiene una única estructura de conjunto vacío si es vacío, y ninguna estructura de conjunto vacío si no es vacío.

Ejemplo 1.13. La especie 0 es la especie *nula*. No importa cuál sea el conjunto U, éste no tiene 0-estructura alguna, es decir, $0[U] = \emptyset$ para todo U.

1.2. Especies como acciones del grupo S_n. Para cada entero $n \geq 0$ denotamos por $[n]$ el conjunto de los primeros n naturales y por $M[n]$ el conjunto de M-estructuras sobre $[n]$. Cada especie M determina una acción del grupo simétrico S_n de las endofunciones biyectivas de $[n]$ sobre el conjunto $M[n]$. Si $x \in M[n]$ y $\sigma \in S_n$ la acción está dada por

$$\sigma.x = M[\sigma](x)$$

Como M es un functor, se verifica que esta fórmula define un homomorfismo de grupo que va de S_n en $S_{M[n]}$. Es decir que una especie M define una familia de representaciones –una representación para cada n– del grupo simétrico S_n por permutaciones de un conjunto finito. Inversamente, dada una familia de acciones del grupo simétrico, una para cada n, es posible definir sin ambiguedad la especie M correspondiente.

La *órbita* de una M-estructura $x \in M[n]$ es el conjunto de todos los elementos de la forma $M[\sigma]x$ con $\sigma \in S_n$. El *estabilizador* o *grupo de automorfismos* de x es el conjunto de todos los $\sigma \in S_n$ tales que $M[\sigma]x = x$. Cada tipo de estructura de especie M corresponde a una única órbita por la acción de S_n para algún n.

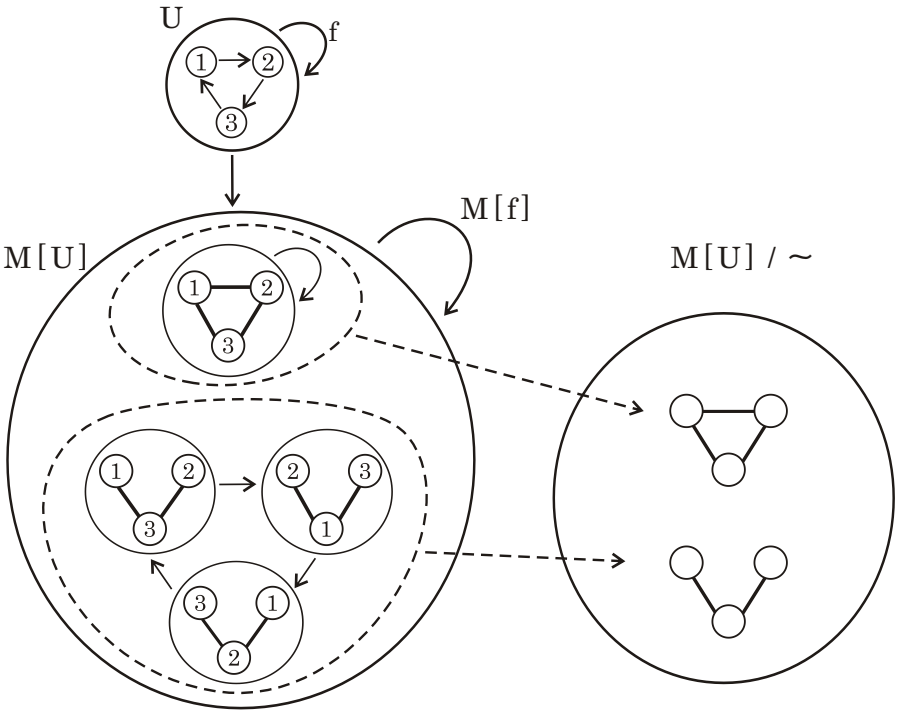


FIGURA 2. Cada permutación de los elementos de U determina una permutación de las estructuras de grafo conexo sobre U. Cada órbita de esta acción de S_3 sobre $M[3]$ corresponde a un tipo de estructura de grafo conexo de 3 vértices.

2. La categoría de las especies

Definición 2.1. Sean M y N dos especies. Un *morfismo* h de M en N es una transformación natural de M en N, considerando que M y N son ambos functores de $\mathbb{B}$ en $\mathbb{E}$.

En otras palabras, un morfismo de especies $h : M \to N$ es una familia de funciones $h_U : M[U] \to N[U]$, una función para cada conjunto finito U, de manera que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M[U] & \xrightarrow{h_U} & N[U] \\ {\scriptstyle M[f]}\downarrow & & \downarrow{\scriptstyle N[f]} \\ M[V] & \xrightarrow{h_V} & N[V] \end{array}$$

Podemos interpretar al morfismo h como una construcción que a partir de una M-estructura produce una N-estructura de manera que da lo mismo reetiquetar antes de la construcción que después.

Si para cada U el morfismo h_U es inversible, es decir, si h_U es una función biyectiva, decimos que h es un *isomorfismo de especies*. Si $f : M \to N$ es un isomorfismo, se dice que M y N son especies *isomorfas o combinatorialmente equivalentes* y si bien la notación $M \simeq N$ es usual, por regla se escribe $M = N$ sobreentendiendo que M y N no son necesariamente iguales sino sólo isomorfas.

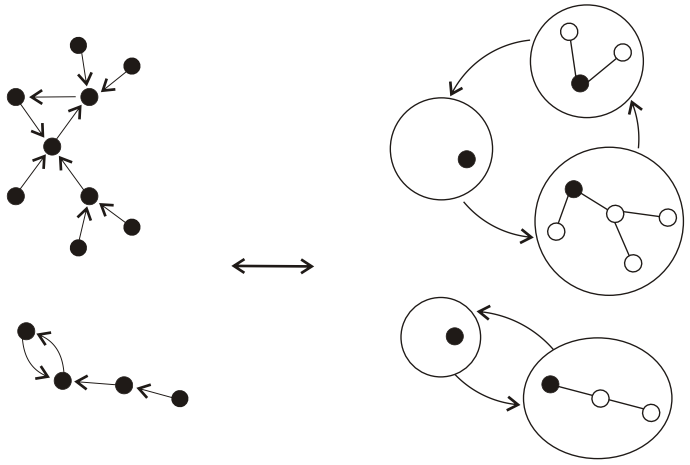
Ejemplo 2.2. Sea $h : \mathcal{G} \to Par$ el morfismo que para cada estructura de grafo $g \in \mathcal{G}[U]$ sobre un conjunto de nodos U, construye la partición $h_U(g) \in Par[U]$ del conjunto U determinada por las componentes conexas del grafo g.

Ejemplo 2.3. Sea Inv la especie de las involuciones, esto es, $Inv[U]$ es el conjunto de todos los endomorfismos f de U tales $f^2 = Id$. Sea $\mathcal{G}_2$ la especie de los grafos (no dirigidos) cuyas componentes conexas son de tamaño ≤ 2. Si f es una involución en $Inv[U]$ definimos $h_U(f)$ como el grafo con nodos en U tal que $u, v \in U$ están conectados si y sólo si $f(u) = v$. Se verifica que h define un isomorfismo entre Inv y $\mathcal{G}_2$.

Ejemplo 2.4. Sea $\mathcal{S}(\mathcal{A})$ la especie de las *permutaciones de árboles con raíz*. Una estructura de especie $\mathcal{S}(\mathcal{A})$ sobre un conjunto U se contruye de la siguiente manera. Primero se elige una partición π de U. Luego sobre cada parte π_i se elige una estructura de árbol a_i con raíz r_i, y sobre el conjunto de miembros de la partición se elige una permutación σ. Vamos a definir un isomorfismo $h : \mathcal{S}(\mathcal{A}) \to End$. Dada una $\mathcal{S}(\mathcal{A})$-estructura p sobre U, definimos un endomorfismo $h_U(p) : U \to U$ como sigue. Sea $u \in U$, y sea π_i el miembro de la partición que contiene a u y a_i es árbol sobre el miembro π_i. Si u no es la raíz r_i entonces $h_U(p)(u)$ se define como el vecino de u en a_i más cercano a la raíz de r_i. Si $u = r_i$ entonces $h_U(p)(u) = r_{\sigma(i)}$. La construcción h determina un isomorfismo entre End y $\mathcal{S}(\mathcal{A})$. La figura 3 ilustra este isomorfismo.

3. Series asociadas a una especie

3.1. Serie generatriz y serie de tipos. Son problemas fundamentales de la combinatoria enumerativa calcular los cardinales de $M[n]$ y de $M[n]/\sim$ para alguna especie dada. Vamos a definir ahora algunos invariantes de las especies cuyo cálculo involucra resolver estos problemas. Por invariante nos referimos a cualquier objeto que se asocie a cada especie de manera que especies isomorfas reciban el mismo objeto.



Endomorfismos $\simeq$ Permutaciones de árboles con raíz

FIGURA 3. Isomorfimo entre la especie *End* de los endomorfismos de un conjunto y la especie $\mathcal{S}(\mathcal{A})$ de las permutaciones de árboles con raíz

Definición 3.1. Sea M una especie, sea $M[n]$ el conjunto de M-estructuras sobre el conjunto $[n] = \{1, ..., n\}$ y $|M[n]|$ su cardinal. La *serie generatriz de* M o *serie exponencial de* M es la serie formal $M(x)$ definida por

$$M(x) = \sum_{n \geq 0} |M[n]| \frac{x^n}{n!}$$

Si h es un isomorfismo entre las especie M y N, tenemos biyecciones $h_{[n]}$ entre $M[n]$ y $N[n]$ para cada n, por lo tanto $M(x) = N(x)$, lo que muestra que la serie generatriz es un invariante. Más aún, para cada n la biyección $h_{[n]}$ es un isomorfismo entre la acción de S_n sobre $M[n]$ y la acción de S_n sobre $N[n]$. Por lo tanto la cantidad de órbitas en ambas acciones es idéntica, es decir, $|M[n]/\sim| = |N[n]/\sim|$ para todo n. Esto indica que la siguiente serie también es un invariante.

Definición 3.2. Sea M una especie y sea $M[n]/\sim$ el conjunto de los tipos de M-estructuras sobre $\{1, ..., n\}$. La *serie de tipos de estructuras* de M es la serie formal $\widetilde{M}(x)$ definida por

$$\widetilde{M}(x) = \sum_{n \geq 0} |M[n]/\sim| \, x^n$$

La serie de tipos de M-estructuras puede describirse como la serie generatriz de la siguiente especie $\widetilde{M}$ asociada a M.

Definición 3.3. Sea M una especie. Una $\widetilde{M}$-estructura sobre un conjunto U es un par (s, m) donde m es una M-estructura sobre U y s es un automorfismo de m, es decir que s es una estructura de permutación sobre U tal que $M[s](m) = m$.

Proposición 3.4. *La serie generatriz de la especie* $\widetilde{M}$ *es igual a la serie de tipos de estructuras de la especie* M*.*

Prueba: El grupo S_n actúa en $M[n]$ por la acción $s.m = M[s](m)$. Para cada $m \in M[n]$ definimos $Aut(m)$ como el conjunto de los s tales que $s.m = m$ y definimos

$Orb(m)$ como el conjunto de todos los $t \in M[n]/\sim$ es una órbita de la acción denotamos por $|t|$ la cantidad de elementos en la órbita t. Entonces

$$\left|\widetilde{M}[n]\right| = \sum_{(s,m),s.m=m} 1 = \sum_{m\in M[n]} |Aut(m)| = \sum_{m\in M[n]} \frac{n!}{|Orb(m)|}$$
$$= n! \sum_{t\in M[n]/\sim} \sum_{m\in t} \frac{1}{|Orb(m)|} = n! \sum_{t\in M[n]/\sim} \sum_{m\in t} \frac{1}{|t|}$$
$$= n! \sum_{t\in M[n]/\sim} 1 = n!\,|M[n]/\sim|$$

□

Ejemplo 3.5. Sea E la especie de los conjuntos. Entonces $E[n]$ consiste en una única estructura para cada n, de manera que $|E[n]| = |E[n]/\sim| = 1$. Luego

$$E(x) = \sum_{n\geq 0} \frac{x^n}{n!} = e^x \qquad \widetilde{E}(x) = \sum_{n\geq 0} x^n = \frac{1}{1-x}$$

Asimismo

$$E_k(x) = \frac{x^k}{k!} \qquad \widetilde{E}_k(x) = x^k$$

y

$$E_+(x) = e^x - 1 \qquad \widetilde{E}_+(x) = \frac{x}{1-x}$$

En particular las series generatrices de la especie singleton X, de la especie 1 del conjunto vacío y de la especie nula 0 son

$$X(x) = x \qquad 1(x) = 1 \qquad 0(x) = 0$$

Ejemplo 3.6. Consideremos la especie $\mathcal{S}$ de las permutaciones. Como $|\mathcal{S}[n]| = n!$ tenemos que la serie generatriz es

$$\mathcal{S}(x) = \sum_{n\geq 0} x^n = \frac{1}{1-x}$$

La órbita o tipo de una permutación σ está caracterizada por su descomposición en ciclos. Si σ_i es la cantidad de ciclos de tamaño i, el tipo de σ está dado por la secuencia $\sigma_1\sigma_2...\sigma_n$, donde $\sigma_1 + 2\sigma_2 + 3\sigma_3... + n\sigma_n = n$. Tales secuencias están en biyección con los diagramas de Ferrer de n puntos, o con el conjunto de particiones del número n. Una partición del número n es una forma de escribir a n como suma de números naturales, sin importar el orden de los sumandos. Por lo tanto $|\mathcal{S}[n]/\sim| = p(n)$, donde $p(n)$ es la cantidad de particiones de n. La serie generatriz de los números $p(n)$ es bien conocida, ver por ejemplo [3], de la cual obtenemos

$$\widetilde{\mathcal{S}}(x) = \sum_{n\geq 0} p(n)\ x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)...}$$

Ejemplo 3.7. Consideremos la especie L de las listas. Sobre $[n]$ podemos formar $n!$ listas diferentes, es decir que $|L[n]| = n!$. Además podemos obtener cualquier lista reetiquetando los elementos de cualquier otra, es decir que $L[n]$ consiste en una única órbita. Entonces

$$L(x) = \frac{1}{1-x} \qquad \widetilde{L}(x) = \frac{1}{1-x}$$

Observemos que $\mathcal{S}$ y L tienen la misma serie generatriz. Sin embargo $\mathcal{S}$ y L no son isomorfas como especies ya que sus series de tipos son distintas. Esto prueba que la serie generatriz no es un invariante completo de las especies. Por otro lado, vemos que E y L tienen la misma serie de tipos de estructuras. Sin embargo sus series generatrices son distintas, lo que muestra que no son isomorfas. Por lo tanto la serie de tipos de estructura tampoco es un invariante completo.

4. Operaciones con especies

4.1. Suma y producto. La *suma* o *unión disjunta* $U+V$ de dos conjuntos U y V se define como

$$U+V=(U\times\{1\})\ \cup(V\ \times\{2\}).$$

Si $f:U\to U'$ y $g:V\to V'$ son dos funciones, la función $f+g:U+V\to U'+V'$ se define por

$$(f+g)(u,1)=f(u)\qquad (f+g)(v,2)=g(v).$$

Si bien $U+V$ no es igual a $V+U$, hay un isomorfismo entre ambos conjuntos. Asimismo $U+(V+W)\simeq(U+V)+W$.

Definición 4.1. La *suma* de dos especies M y N es la especie $M+N$ definida por

$$(M+N)[U]=M[U]+N[U]\qquad (M+N)[f]=M[f]+N[f]$$

donde $f:U\to V$ es una biyección entre conjuntos finitos.

Intuitivamente, poner una estructura de especie $M+N$ sobre un conjunto U es elegir entre poner sobre U una M-estructura o una N-estructura.

Observar que $|(M+N)[n]|=|M[n]|+|N[n]|$ para todo n. El conjunto de órbitas en $(M+N)[U]$ es la unión disjunta del conjunto de las órbitas en $M[U]$ con el conjunto de las órbitas en $N[U]$. Por lo tanto

Proposición 4.2. *La series asociadas a la suma $M+N$ son*

$$(M+N)(x)=M(x)+N(x)\qquad \widetilde{(M+N)}(x)=\widetilde{M}(x)+\widetilde{N}(x)$$

Definición 4.3. La especie *producto* MN se define por

$$(MN)[U]=\sum_{U_1+U_2=U}M[U_1]\times N[U_2]\qquad (MN)[f]=\sum_{U_1+U_2=U}M[f|_{U_1}]\times N[f|_{U_2}]$$

Esto significa que poner sobre U una estructura de especie MN consiste en elegir un subconjunto U_1, poner sobre U_1 una M-estructura y poner sobre su complemento U_2 una N-estructura. Se puede probar que:

Proposición 4.4. *Cualesquiera sean las especies M, N y H, tenemos los siguientes isomorfismos de especies:*

i) $(MN)H=M(NH)$
ii) $MN=NM$
iii) $H(M+N)=HM+HN$

Si $M_1,M_2,...,M_n$ son especies, poner sobre U una estructura de la especie producto $M_1M_2...M_n$ consiste en particionar U en n subconjuntos U_i (posiblemente algunos vacíos) y poner sobre U_i una estructura de especie M_i. En particular, si M es una especie, poner sobre U una estructura de especie M^n consiste en elegir para cada $i=1,...,n$ un subconjunto U_i de manera que los U_i son disjuntos y cubren a U, y luego poner sobre cada U_i una M-estructura. Remarquemos que en una M^n-estructura las partes U_i tienen un orden.

Proposición 4.5. *La serie generatriz del producto MN es*

$$(MN)(x) = M(x)N(x)$$

Prueba: El cardinal del conjunto de MN-estructuras sobre n es

$$|(MN)[n]| = \sum_{U_1+U_2=U} |M[U_1]|\,|N[U_2]| = \sum_{k=0}^{n} \binom{n}{k} |M[k]|\,|N[n-k]|$$

$$= n! \sum_{k=0}^{n} \frac{|M[k]|}{k!}\,\frac{|N[n-k]|}{(n-k)!}$$

Entonces

$$(MN)(x) = \sum_{n\geq 0} \frac{|(MN)[n]|}{n!}\,x^n = \sum_{n\geq 0}\sum_{k=0}^{n} \frac{|M[k]|}{k!}\,x^k\,\frac{|N[n-k]|}{(n-k)!}\,x^{n-k} = M(x)\;N(x)$$

□

Ejemplo 4.6. Sea $\mathcal{D}$ la especie de las permutaciones que no tienen puntos fijos, es decir, $\mathcal{D}[U]$ es el conjunto de las biyecciones $\sigma : U \to U$ tales que $\sigma(u) \neq u$ para todo $u \in U$. Se puede ver que la especie $\mathcal{S}$ de todas las permutaciones es isomorfa al producto de la especie E de los conjuntos por la especie $\mathcal{D}$, es decir, $\mathcal{S} = E\mathcal{D}$. Entonces $\mathcal{S}(x) = E(x)\mathcal{D}(x)$, lo que permite deducir una forma cerrada de la serie generatriz de $\mathcal{D}$:

$$\mathcal{D}(x) = \frac{e^{-x}}{1-x} = \left(1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + ...\right)\left(1 + x^2 + x^3 + x^4 + ...\right)$$

$$= \sum_{n\geq 0}\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) x^n$$

Esto muestra que $\mathcal{D}[n] = n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right)$, de donde vemos que cuando $n \to \infty$ la probabilidad de que una permutación tomada al azar no tenga un punto fijo tiende a $1/e$.

También se puede verificar que la serie de tipos de estructura se comporta bien con respecto a la suma y multiplicación de especies.

Proposición 4.7. *Si M y N son especies entonces*

$$(\widetilde{M+N})(x) = \widetilde{M}(x) + \widetilde{N}(x), \qquad (\widetilde{MN})(x) = \widetilde{M}(x)\widetilde{N}(x).$$

4.2. Composición de especies. Sea N una especie tal que $N[0] = \emptyset$. Dotar a un conjunto finito U de una N^n-estructura consiste en particionar a U en una familia ordenada de exactamente n subconjuntos no vacíos $U_1, U_2, ..., U_n$ y elegir sobre cada U_i una N-estructura. Podemos pensar que cada parte U_i está rotulada con un número del 1 al n. El grupo S_n actúa sobre estas estructuras intercambiando estos rótulos. Una estructura de especie N^n/S_n corresponde a una órbita de esta acción, es decir, consiste en particionar U en n partes no vacías sin rotular y colocar sobre cada parte una N-estructura. Se puede ver que la serie generatriz de N^n/S_n es

$$(N^n/S_n)(x) = \frac{N(x)^n}{n!}$$

Sea M una especie cualquiera. La especie *composición* $M(N)$ se define como sigue. Especificar una $M(N)$-estructura sobre un conjunto U consiste en especificar

i) una partición π del conjunto U, con miembros $U_1, U_2, ...$

ii) una M-estructura sobre el conjunto $\pi = \{U_1, U_2, ...\}$ de los miembros de esa partición

iii) una N-estructura sobre cada conjunto U_i

Proposición 4.8. *La serie generatriz de la composición de dos especies satisface*

$$M(N)(x) = M(N(x))$$

Prueba: Sea M_n la especie que asigna una M-estructura cuando el conjunto subyacente tiene cardinal n, y no asigna estructura en caso contrario. Similarmente, sea $M_n(N)$ la subespecie de $M(N)$ donde la partición del conjunto tiene exactamente n miembros. Entonces

$$M = \sum_{n\geq 0} M_n \qquad\qquad M(N) = \sum_{n\geq 0} M_n(N)$$

De la definición de $M(N)$ podemos ver que $M_n(N) = M_n \times (N^n/S_n)$. En particular

$$M_n(N)(x) = |M[n]|\,(N^n/S_n)(x) = |M[n]|\,\frac{N(x)^n}{n!}$$

Luego

$$M(N)(x) = \sum_{n\geq 0} |M[n]|\,\frac{N(x)^n}{n!} = M(N(x))$$

□

Ejemplo 4.9. La especie $\mathcal{S}(\mathcal{A})$ de las permutaciones de árboles con raíz está ilustrada en la parte derecha de la Figura 3. Efectivamente, es una composición de la especie $\mathcal{S}$ de las permutaciones con la especie $\mathcal{A}$ de los árboles con raíz. El conjunto U es particionado en miembros, sobre cada miembro vemos una estructura de árbol con raíz y vemos una estructura exterior de permutación sobre el conjunto de los miembros.

Ejemplo 4.10. Una estructura de partición sobre un conjunto U consiste en especificar una partición de U en miembros U_i, sobre cada U_i colocar una estructura de conjunto no vacío, y sobre el conjunto de los miembros colocar una estructura de conjunto. Dicho brevemente, una partición es un conjunto de conjuntos no vacíos. Entonces $Par = E(E_+)$. De este isomorfismo de especies se deduce que

$$Par(x) = e^{e^x - 1}$$

En forma similar podemos calcular la serie generatriz de las particiones en k partes. Esta especie se puede expresar como $E_k(E_+)$. Por lo tanto su serie generatriz es

$$E_k(E_+)(x) = \frac{(e^x - 1)^k}{k!}$$

Ejemplo 4.11. Colocar una estructura de permutación sobre un conjunto U consiste en especificar una partición de U en miembros U_i, sobre cada U_i colocar una estructura de ciclo, y sobre el conjunto de los miembros colocar una estructura de conjunto. Es decir, una permutación es un conjunto de ciclos (que por definición son de longitud no nula). Entonces $\mathcal{S} = E(\mathcal{C})$. La serie generatriz de la especie de las permutaciones con exactamente k ciclos es

$$E_k(\mathcal{C})(x) = \frac{1}{k!}\log^k\left(\frac{1}{1-x}\right)$$

5. Especies ponderadas

La serie generatriz de una especie M da una medida de la especie M en el sentido que es una recopilación de los cardinales $|M[n]|$, los cuales son una medida natural de los tamaños de los conjuntos $M[n]$ de M-estructuras sobre $\{1, ..., n\}$. El cardinal de un conjunto finito es, en particular, una función μ que a cada conjunto finito A le asigna un elemento de un semianillo $\mathbb{S}$ –el de los números naturales– que satisface:

i) $\mu(A + B) = \mu(A) + \mu(B)$,

ii) $\mu(A \times B) = \mu(A)\mu(B)$.

Permitiendo que el semianillo $\mathbb{S}$ sea arbitrario podemos obtener medidas más refinadas de los conjuntos de estructuras. Por ejemplo, en lugar de medir el conjunto de los grafos de n nodos por su cardinal, podemos asociarle el polinomio $g_{n0}+g_{n1}x+g_{n2}x^2+...$ donde g_{nk} es la cantidad de estructuras de grafo con k puentes sobre un conjunto de n nodos. A continuación veremos una manera de construir tales medidas considerando la categoría de los conjuntos ponderados.

5.1. Categoría de los conjuntos ponderados. Sea $\mathbb{M}$ un monoide donde cada elemento tiene un número finito de factorizaciones. Un *conjunto ponderado* es un par (A, ω) donde A es un conjunto y ω es una función $\omega : A \to \mathbb{M}$. En tal caso decimos que ω es una $\mathbb{M}$-ponderación y que $\omega(a)$ es el peso de a.

Un *morfismo* entre conjuntos ponderados (A, ω) y (B, ν) es una función $f : A \to B$ que preserva los pesos, es decir, tal que $\nu \circ f = \omega$.

La *suma* $(A, \omega)+(B, \nu)$ de conjuntos ponderados es el par $(A+B, \omega+\nu)$ donde $A+B$ es la union disjunta de A y B y la ponderación $\omega+\nu$ está definida por $(\omega+\nu)(x) = \omega(x)$ si $x \in A$ y $(\omega + \nu)(x) = \nu(x)$ si $x \in B$.

El *producto* $(A, \omega) \times (B, \nu)$ de conjuntos ponderados es el par $(A \times B, \omega \times \nu)$ donde $A \times B$ es el producto cartesiano y $\omega \times \nu$ está definida por $(\omega \times \nu)(a, b) = \omega(a)\nu(b)$.

El anillo de *series formales* $\mathbb{Z}[\mathbb{M}]$ es el anillo de las combinaciones lineales formales de elementos de $\mathbb{M}$. Un elemento f de $\mathbb{Z}[\mathbb{M}]$ es de la forma

$$f = \sum_{x \in \mathbb{M}} f(x)x$$

donde $f(x)$ es un número entero y es nulo excepto para un conjunto finito de elementos de $\mathbb{M}$. La suma y el producto en $\mathbb{Z}[\mathbb{M}]$ están dados por

$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = \sum_{uv=x} f(u)g(v)$$

Un conjunto $\mathbb{M}$-ponderado es *sumable* si $\omega^{-1}(m)$ es un conjunto finito para todo peso $m \in \mathbb{M}$.

Sea $\mathbb{E}_{\mathbb{M}}$ la categoría cuyos objetos son los conjuntos $\mathbb{M}$-ponderados sumables y cuyos morfismos son las funciones que preservan las ponderaciones.

Sea $(A, \omega) \in \mathbb{E}_{\mathbb{M}}$. La *cardinalidad* (o *peso total*) de A es la serie formal en $\mathbb{Z}[\mathbb{M}]$ definida por

$$|A|_\omega = \sum_{a \in A} \omega(a)$$

Proposición 5.1. *Si* $A, B \in \mathbb{E}_{\mathbb{M}}$ *entonces*

$$|A + B|_{\omega+\nu} = |A|_\omega + |B|_\nu$$
$$|A \times B|_{\omega\times\nu} = |A|_\omega |B|_\nu$$

5.2. Especies ponderadas y sus series asociadas. Una *especie ponderada* es un functor $M_\omega : \mathbb{B} \to \mathbb{E}_{\mathbb{M}}$. Es decir que M_ω es una regla que

i) para cada conjunto finito U produce un conjunto $\mathbb{M}$-ponderado sumable $M[U] = (M[U], \omega_U)$

ii) para cada biyección $f : U \to V$ produce una función $M[f] : M_\omega[U] \to M[V]$ que preserva los pesos de manera que

a) para todas las biyecciones $f : U \to V$ y $g : V \to W$

$$M[g \circ f] = M[g] \circ M[f]$$

b) para todos los conjuntos U

$$M[Id_U] = Id_{M[U]}$$

La función $M[f]$ se llama el *tranporte de estructura a lo largo de* f. Se deduce de la definición que $M[f]$ es una biyección que preserva los pesos y por lo tanto

$$|M[U]|_{\omega_U} = |M[V]|_{\omega_V}$$

El cardinal $|M[U]|_{\omega_U}$ lo vamos a notar más simplemente por $|M[U]|_\omega$ y una especie ponderada M la vamos notar por M_ω donde ω hace referencia a la familia de ponderaciones ω_U.

La *serie generatriz* de una especie ponderada M se define como

$$M_\omega(x) = \sum_{n \geq 0} |M[n]|_\omega \ \frac{x^n}{n!}$$

Si u y v son estructuras en $M[U]$ y $M[V]$ respectivamente tales que $M[f](u) = v$, decimos que u y v son isomorfas. Observar que en tal caso $\omega_U(u) = \omega_V(v)$, por lo tanto el peso de las estructuras es constante a lo largo de cada clase de isomorfismo. Esto permite definir sin ambiguedad el *peso* $\omega(t)$ *de un tipo de estructura* t como el peso $\omega(a)$ de cualquier estructura a que represente a la clase t. De esta manera, la ponderación de $M[U]$ induce una ponderación del conjunto $M[U]/\sim$ de los tipos de estructuras y la cardinalidad de $M[U]/\sim$ queda definida como

$$|M[U]/\sim|_\omega = \sum_{t \in M[U]/\sim} \omega(t)$$

La *serie generatriz de tipos* de la especie ponderada M se define como

$$\widetilde{M_\omega}(x) = \sum_{n \geq 0} |M[n]/\sim|_\omega \ x^n$$

Ejemplo 5.2. Sea $\mathcal{S}$ la especie de las permutaciones. Sea $\sigma \in \mathcal{S}[n]$ una estructura de permutación sobre el conjunto $[n] = \{1, ..., n\}$ y sea σ_i la cantidad de ciclos de tamaño i en su descomposición en ciclos. Para cada biyección $f : [n] \to [n]$ tenemos una biyección $\mathcal{S}[f] : \mathcal{S}[n] \to \mathcal{S}[n]$ dada por el functor $\mathcal{S}$. Es decir que $\mathcal{S}$ determina una acción del grupo de permutaciones sobre el conjunto de las estructuras de permutación dada por $\mathcal{S}[f](\sigma) = f\sigma f^{-1}$. Es útil interpretar esta acción representando a σ por su grafo asociado y a f como un reetiquetamiento de los vértices del grafo. La descomposición en componentes conexas corresponde a la descomposición de σ en ciclos. La órbita de la permutación σ abarca a todas las permutaciones con la misma descomposición. Luego podemos identificar al *tipo de la permutacíón* σ con la secuencia $\sigma_1, \sigma_2, ...$ El peso de σ

se define como $\omega(\sigma) = s_1^{\sigma_1} s_2^{\sigma_2} s_3^{\sigma_3} ... s_n^{\sigma_n}$. La cardinalidad de $\mathcal{S}[n]$ es

$$|\mathcal{S}[n]|_\omega = \sum_{\sigma \in \mathcal{S}[n]} s_1^{\sigma_1} s_2^{\sigma_2} ... s_n^{\sigma_n} = \sum_{r_1+2r_2+...+nr_n=n} p(r_1, ..., r_n)\ s_1^{r_1} s_2^{r_2} ... s_n^{r_n}$$

donde $p(r_1, ..., r_n)$ es la cantidad de permutaciones sobre $[n]$ con peso $s_1^{r_1} s_2^{r_2} ... s_n^{r_n}$. Observemos que $p(r_1, ..., r_n)$ es el cardinal de la órbita de una permutación de tipo $r_1, r_2, ...$ Entonces para calcularlo es suficiente calcular el estabilizador de una permutación tal. Si interpretamos a σ como un grafo etiquetado, debemos contar cuántos reetiquetamientos preservan la estructura de grafo etiquetado.

Una forma de reetiquetar preservando al grafo es que cada etiqueta se mantenga en su componente conexa , produciendo en cada componente un corrimiento cíclico. En una componente de i elementos tenemos i tales corrimientos. Por lo tanto hay $1^{r_1} 2^{r_2} 3^{r_3} ...$ formas diferentes de reetiquetar de esta manera.

Por otro lado, podemos intercambiar en bloque las etiquetas entre componentes de igual tamaño, preservando un orden prefijado en cada componente cíclica. Hay $r_1! r_2! r_3! ...$ intercambios de este tipo. Estos movimientos de las etiquetas conmutan con los del tipo anterior.

Puede verse que cualquier reetiquetamiento que preserve la estructura de grafo de σ se obtiene de forma única como composición de un movimiento del primer tipo compuesto con uno del segundo tipo. Por lo tanto el estabilizador de σ tiene cardinal $1^{r_1} r_1! 2^{r_2} r_2! 3^{r_3} r_3! ...$ y por lo tanto

$$p(r_1, ..., r_n) = \frac{n!}{1^{r_1} r_1! 2^{r_2} r_2! 3^{r_3} r_3! ...}$$

De aquí obtenemos que la serie generatriz de la especie de las *permutaciones ponderadas* es

$$\begin{aligned}
\mathcal{S}_\omega(x) &= \sum_{n \geq 0} \sum_{r_1+2r_2+3r_3+...+nr_n=n} \frac{n!\ s_1^{r_1} s_2^{r_2} ... s_n^{r_n}}{1^{r_1} r_1! 2^{r_2} r_2! 3^{r_3} r_3! ... n^{r_n} r_n!}\ \frac{x^n}{n!} \\
&= \sum_{r_1, r_2, ... \in \mathbb{Z}_{\geq 0}} \frac{1}{r_1!} \left(\frac{x\ s_1}{1}\right)^{r_1} \frac{1}{r_2!} \left(\frac{x\ s_2}{2}\right)^{r_2} \frac{1}{r_3!} \left(\frac{x\ s_3}{3}\right)^{r_3} ... \\
&= \prod_{k=1}^{\infty} \left(\sum_{r=0}^{\infty} \frac{1}{r!} \left(\frac{x\ s_k}{k}\right)^r \right) = \exp\left(x\ \left(\frac{s_1}{1} + \frac{s_2}{2} + \frac{s_3}{3} + ...\right)\right)
\end{aligned}$$

Ejemplo 5.3. Consideremos la especie Par de las particiones. Si $\pi \in Par[n]$ es una partición del conjunto $[n]$ y π_i es el número de partes de tamaño i en π, se define el peso $\omega(\pi)$ como el monomio $s_1^{\pi_1} s_2^{\pi_2} ... s_n^{\pi_n}$.

Al igual que en el caso de la especie de permutaciones, cada tipo de partición está caracterizado por su peso. Es decir que las órbitas de la acción del grupo simétrico sobre el conjunto $Par[n]$ son distinguidas por el peso ω.

La cardinalidad de $Par[n]$ es

$$|Par[n]|_\omega = \sum_{\pi \in Par[n]} s_1^{\pi_1} s_2^{\pi_2} ... s_n^{\pi_n} = \sum_{r_1+2r_2+...+nr_n=n} q(r_1, ..., r_n)\ s_1^{r_1} s_2^{r_2} ... s_n^{r_n}$$

donde $q(r_1, ..., r_n)$ es la cantidad de particiones sobre $[n]$ con peso $s_1^{r_1} s_2^{r_2} ... s_n^{r_n}$. El cálculo de $q(r_1, ..., r_n)$ es muy similar al caso de la especie de permutaciones en el ejemplo anterior. Es suficiente calcular el subgrupo estabilizador de una partición de tipo $r_1, r_2, ..., r_n$.

Por un lado tenemos los reetiquetamientos que mantienen cada etiqueta dentro de la misma parte donde habita. Hay $(1!)^{r_1}(2!)^{r_2}(3!)^{r_3}...(n!)^{r_n}$ de estos movimientos de etiquetas. Por otro lado están los movimientos que intercambian las etiquetas en bloque entre partes de igual tamaño manteniendo un orden prefijado en cada parte. Hay $r_1!r_2!...r_n!$ de estos reetiquetamientos, los cuales conmutan con los anteriores. Luego

$$q(r_1,...,r_n) = \frac{n!}{r_1!(1!)^{r_1}\ r_2!(2!)^{r_2}...r_n!(n!)^{r_n}}$$

Obtenemos así la función generatriz

$$\mathrm{Par}_\omega(x) = \sum_{n\geq 0} \sum_{r_1+2r_2+...+nr_n=n} \frac{n!\ s_1^{r_1}s_2^{r_2}...s_n^{r_n}}{(1!)^{r_1}r_1!(2!)^{r_2}r_2!(3!)^{r_3}r_3!...(n!)^{r_n}r_n!}\ \frac{x^n}{n!}$$

$$= \exp\left(x\ \left(\frac{s_1}{1!}+\frac{s_2}{2!}+\frac{s_3}{3!}+...\right)\right)$$

Observar que sustituyendo x por 1 y s_i por z^i se obtiene $e^{(e^z-1)}$, la función generatriz ordinaria de la especie de particiones.

Las operaciones de suma y producto de especies ponderadas se definen imitando la definición de suma y producto de especies ordinarias reemplazando la suma y producto cartesiano de conjuntos por sus versiones ponderadas. En forma análoga se verifica que las series generatrices y las series de tipos de especies ponderadas se comportan bien con respecto a estas operaciones.

Proposición 5.4. *Si M_ω y N_μ son especies ponderadas entonces*

$$(M_\omega + N_\mu)(x) = M_\omega(x) + N_\mu(x), \qquad (M_\omega N_\mu)(x) = M_\omega(x)N_\mu(x).$$

$$(\widetilde{M_\omega + N_\mu})(x) = \widetilde{M_\omega}(x) + \widetilde{N_\mu}(x), \qquad (\widetilde{M_\omega N_\mu})(x) = \widetilde{M_\omega}(x)\widetilde{N_\mu}(x).$$

5.3. Serie indicatriz de ciclos. Dada una especie (ordinaria) M, observamos que la especie $\widetilde{M}$ –cuyas estructuras son los pares (m,σ) donde σ es un automorfismo de la M-estructura m– tiene una ponderación natural. El peso de un elemento (m,σ) es $s_1^{\sigma_1}s_2^{\sigma_2}...$ donde σ_i es la cantidad de ciclos de longitud i en σ. Denotamos a esta especie ponderada por $\widehat{M}$. La serie generatriz de $\widehat{M}$ como especie ponderada se puede escribir como

$$\widehat{M}(x) = \sum_{n\geq 0} \frac{x^n}{n!}\left(\sum_{\sigma\in S_n} |M[\sigma]|\ \ s_1^{\sigma_1}s_2^{\sigma_2}s_3^{\sigma_3}...\right)$$

donde $M[\sigma]$ es el conjunto de M-estructuras sobre $[n]$ que son fijadas por la permutación σ de $[n]$. La *serie indicatriz de ciclos de M* (o simplemente serie de ciclos) es la serie formal en las variables $s_1, s_2, ...$ definida por

$$Z_M(s_1,s_2,s_3,...) = \widehat{M}(1).$$

Ejemplo 5.5. Sea M la especie E de los conjuntos. En este caso $\widehat{M}$ coincide con la especie ponderada de las permutaciones $\mathcal{S}_\omega$. De acuerdo al cálculo que ya efectuamos de la serie $\mathcal{S}_\omega(x)$ obtenemos que la serie de ciclos de E está dada por

$$Z_E(s_1,s_2,...) = \exp\ \left(\frac{s_1}{1}+\frac{s_2}{2}+\frac{s_3}{3}+...\right)$$

De las propiedades de las series ponderadas vemos que

$$Z_{M+N} = Z_M + Z_N, \qquad Z_{MN} = Z_M Z_N.$$

Veamos que la serie de ciclos es un refinamiento de la serie generatriz y de la serie de tipos a la vez.

Observar que el cardinal del conjunto $M[\sigma]$ sólo depende del tipo $n_1, n_2...$ de la permutación σ. Entonces podemos escribir $M[\sigma] = M[n_1, n_2, ...]$.

Proposición 5.6. *La serie de ciclos de M se puede escribir como*

$$Z_M(s_1, s_2, ...) = \sum_{n_1+2n_2+3n_3+...<\infty} |M[n_1 n_2...]| \, \frac{s_1^{n_1} s_2^{n_2} s_3^{n_3}...}{1^{n_1} n_1!\ 2^{n_2} n_2!\ 3^{n_3} n_3!...}$$

Prueba: La identidad se consigue agrupando los términos de acuerdo al tipo de cada permutación σ en la suma original y recordando que $1^{n_1} n_1!\ 2^{n_2} n_2!\ 3^{n_3} n_3!...$ es el cardinal del subgrupo estabilizador de una permutación de tipo $n_1, n_2, ...$ cuando el grupo S_n actúa por conjugación sobre el conjunto de las permutaciones. □

Corolario 5.7. *La serie generatriz de M se obtiene como*

$$Z_M(x, 0, 0, ...) = M(x)$$

Sea $M/\sim$ el conjunto de tipos de M-estructuras, esto es, un elemento t de $M/\sim$ es una órbita en $M[n]$ por la acción de S_n para algún n. Si G es un subgrupo de S_n entonces el *índice de ciclos* de G se define como

$$Z(G) = \frac{1}{|G|} \sum_{\sigma \in G} s_1^{\sigma_1} s_2^{\sigma_2} s_3^{\sigma_3}...$$

Dado $x \in t$, con $t \in M/\sim$, si G_x es el subgrupo estabilizador de x observamos que $Z(G_x)$ sólo depende de t, por lo tanto denotamos por $Z(G_t)$ y por $|G_t|$ al índice de ciclos y al cardinal de G_x respectivamente. La cantidad de elementos en la órbita t la denotamos por $|t|$.

Proposición 5.8. *La serie de ciclos de M se puede escribir como*

$$Z_M(s_1, s_2, ...) = \sum_{t \in M/\sim} Z(G_t)$$

Prueba:

$$Z_M = \sum_{n\geq 0} \frac{1}{n!} \sum_{(x,\sigma)\in \widetilde{M}[n]} s_1^{\sigma_1} s_2^{\sigma_2}... = \sum_{n\geq 0} \frac{1}{n!} \sum_{x\in M[n]} \sum_{\sigma \in G_x} s_1^{\sigma_1} s_2^{\sigma_2}...$$

$$= \sum_{n\geq 0} \sum_{t\in M[n]/\sim} \frac{1}{n!} \sum_{x\in t} \sum_{\sigma\in G_x} s_1^{\sigma_1} s_2^{\sigma_2}... = \sum_{n\geq 0} \sum_{t\in M[n]/\sim} \frac{|t|}{n!} \sum_{\sigma\in G_t} s_1^{\sigma_1} s_2^{\sigma_2}...$$

$$= \sum_{n\geq 0} \sum_{t\in M[n]/\sim} \frac{1}{|G_t|} \sum_{\sigma\in G_t} s_1^{\sigma_1} s_2^{\sigma_2}... = \sum_{t\in M/\sim} Z(G_t)$$

□

Corolario 5.9. *La serie de tipos de estructura de M se obtiene como*

$$Z_M(x, x^2, x^3, ...) = \widetilde{M}(x)$$

Prueba: El cálculo anterior muestra que

$$Z_M(x,x^2,x^3,...) = \sum_{n\geq 0}\sum_{t\in M[n]/\sim}\frac{1}{|G_t|}\sum_{\sigma\in G_t}x^{\sigma_1+2\sigma_2+3\sigma_3+...}$$

$$= \sum_{n\geq 0}\sum_{t\in M[n]/\sim}\frac{1}{|G_t|}\sum_{\sigma\in G_t}x^n = \sum_{n\geq 0}\sum_{t\in M[n]/\sim}x^n = \widetilde{M}(x)$$

□

6. Teorema de Redfield-Pólya

Un problema fundamental en combinatoria es contar el número de órbitas cuando un grupo actúa sobre un conjunto finito. Una especie M brinda una familia de acciones –una para cada n– del grupo S_n sobre el conjunto de M-estructuras $M[n]$. Entonces el problema de contar las órbitas de estas acciones es equivalente al de calcular la serie de tipos $\widetilde{M}(x)$.

Como vimos, la serie de tipos se comporta bien con respecto a las operaciones de suma y multiplicación de especies. Sin embargo, no puede decirse lo mismo respecto de la operación de composición. En efecto, la identidad $\widetilde{M(N)}(x) = \widetilde{M}(\widetilde{N}(x))$ es falsa. Por ejemplo, si $\mathcal{S}$, E y $\mathcal{C}$ son las especies de las permutaciones, los conjuntos y los ciclos respectivamente, tenemos el isomorfismo de especies $\mathcal{S} = E(\mathcal{C})$. En efecto, una permutación es un conjunto de ciclos. Sin embargo sus series de tipos son

$$\widetilde{\mathcal{S}}(x) = \prod_{n\geq 0}\frac{1}{1-x^n} \qquad \widetilde{\mathcal{C}}(x) = \frac{x}{1-x} \qquad \widetilde{E}(x) = \frac{1}{1-x}$$

Dado que la composición es una operación fundamental en la construcción de especies interesantes, es importante disponer de un método para calcular la serie de tipos de estructura de una composición. La clave está en interpretar a la serie de tipos como $Z_M(x,x^2,x^3,...)$ puesto que la serie de ciclos satisface la siguiente ley de sustitución.

Proposición 6.1. *Sean M y N especies, tal que $N[\emptyset] = \emptyset$. Entonces*

$$Z_{M(N)}(s_1,s_2,s_3,...) = Z_M(Z_N(s_1,s_2,s_3,...), Z_N(s_2,s_4,s_6,...), Z_N(s_3,s_6,s_9,...),...)$$

Nos referiremos a esta identidad como el *teorema de enumeración de Pólya* o teorema de Redfield-Pólya. En esta sección damos una guía para probar esta identidad de series formales basándonos en la prueba y la teoría formulada por Joyal en [4].

Como consecuencia inmediata de esta fórmula obtenemos

Corolario 6.2. *La serie de tipos de estructura de la composición de especies está dada por*

$$\widetilde{M(N)}(x) = Z_M(\widetilde{N}(x), \widetilde{N}(x^2), \widetilde{N}(x^3),...)$$

Ejemplo 6.3. De la expresión que obtuvimos para la serie de ciclos de la especie de los conjuntos obtenemos que

$$\widetilde{E(N)}(x) = \exp\left(\frac{N(x)}{1} + \frac{N(x^2)}{2} + \frac{N(x^3)}{3} + ...\right)$$

Para probar la proposición 6.1 debemos calcular la serie generatriz de la especie ponderada $\widehat{M(N)}$. Es decir que debemos analizar la especie $\widetilde{M(N)}$ con la ponderación determinada por la descomposición en ciclos del automorfismo. Una estructura de especie $\widetilde{M(N)}$ sobre un conjunto U es un par (x,σ) donde x es una $M(N)$-estructura y

σ es una permutación de los elementos de U que fija la estructura x, es decir tal que $M(N)[\sigma]x = x$. En la Figura 4 vemos un ejemplo de una estructura de esta especie y del peso correspondiente.

La $M(N)$-estructura x sobre U es de la forma $x = (m, n_1, n_2, ...)$, es decir consiste en una partición de U, una N-estructura n_i sobre cada miembro U_i de la partición, y una M-estructura m sobre el conjunto de los miembros. Entonces, el automorfismo σ de x induce una permutación $\overline{\sigma}$ entre los miembros de la partición. Observemos que el par $(m, \overline{\sigma})$ es una estructura de especie $\widetilde{M}$ sobre el conjunto de los miembros de la partición de U.

Para entender esta estructura conviene considerar primero el caso en que la permutación inducida $\overline{\sigma}$ consiste en sólo un ciclo. Nos referiremos a tales estructuras como N-coronas. En la Figura 4 podemos observar cómo el automorfismo σ induce la descomposición de una $\widetilde{M(N)}$-estructura como unión disjunta de N-coronas.

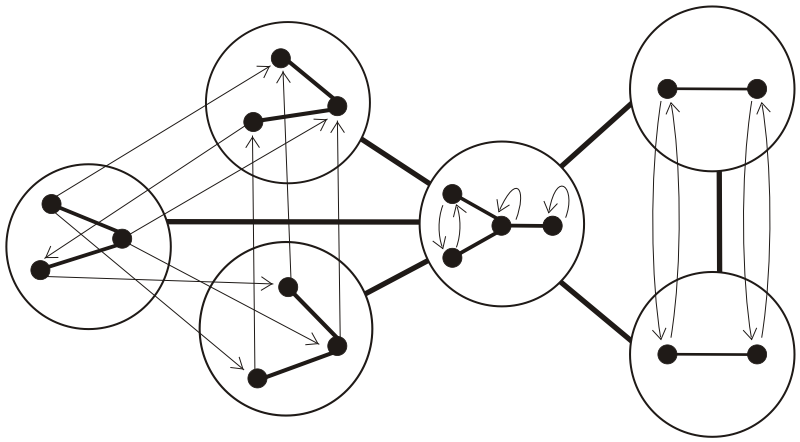


FIGURA 4. Ejemplo de una estructura de una especie de la forma $\widetilde{M(N)}$. En este caso M es la especie de los grafos y N es la especie de los árboles. El automorfismo σ está representado por las flechas delgadas y descompone a la estructura en tres N-coronas. Una corona de longitud 3 que aporta un peso $s_3 s_6$. Otra corona de longitud 1 que aporta un peso $s_1^2 s_2$. Y una última corona de longitud 2 que aporta un peso s_2^2. Por lo tanto el peso total de la estructura es $s_1^2 s_2^3 s_3 s_6$.

6.1. Coronas de N-estructuras. Colocar una estructura de *N-corona de longitud n* sobre conjunto U consiste en particionar al conjunto U en n partes iguales $U_1, U_2, ..., U_n$, colocar una N-estructura sobre cada U_i y especificar biyecciones $\sigma_i : U_i \to U_{i+1}$ (identificando $n+1$ con 1) de manera que realicen isomorfismos de N-estructuras. En otras palabras, una N-corona es un conjunto de N-estructuras junto con un automorfismo que permuta circularmente los miembros de la partición. Denotamos por C_n^N a la especie de las N-coronas de longitud n.

Una estructura de *N-corona marcada* (de longitud n) sobre U consiste en una N-corona de longitud n sobre U junto con un elemento del conjunto $\{U_1, ..., U_n\}$. Denotamos por L_n^N a esta especie. Observar que $\left|L_n^N[U]\right| = n \left|C_n^N[U]\right|$.

Proposición 6.4. *Sea L_n la especie de las listas de longitud n. Entonces tenemos el isomorfismo de especies*

$$L_n^N = \widetilde{N}(L_n)$$

El isomorfismo entre estas especies está sugerido por la Figura 5. La idea es considerar la parte U_i distinguida y componer los isomorfismos saliendo de ella n veces hasta obtener un automorfismo de la U_i distinguida que fija la N-estructura. Toda la información de la L_n^N-estructura queda codificada por este automorfismo junto con las secuencias determinadas por la cadena de composiciones saliendo de cada elemento de U_i.

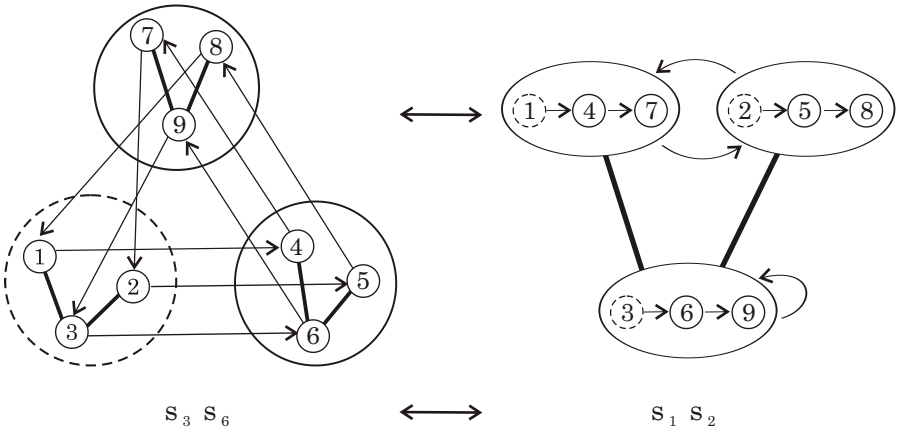


FIGURA 5. Ejemplo del isomorfismo entre la especie de las N-coronas marcadas de longitud n y la especie $\widetilde{N}(L_n)$. En este caso la especie N es la de los árboles y $n = 3$. A la izquierda tenemos una corona de árboles de longitud 3 con uno de los miembros marcados. El automorfismo σ de la corona está compuesto por un 3-ciclo y por un 6-ciclo, por lo tanto el peso de la corona es $s_3 s_6$. A la derecha tenemos el árbol de listas asociado junto con el automorfismo $\overline{\sigma}$ inducido por σ. El peso de $\overline{\sigma}$ se obtiene dividiendo los índices de σ por 3.

El grupo $\mathbb{Z}_n$ actúa naturalmente por automorfismos de la especie L_n^N permutando cíclicamente los U_i. Entonces podemos describir a la especie C_n^N como la especie cociente

$$C_n^N = \widetilde{N}(L_n)/\mathbb{Z}_n \tag{6.1}$$

Cada ciclo c del automorfismo σ de una N-corona de longitud n tiene longitud kn para algún entero k. El correspondiente ciclo $\overline{c}$ del automorfismo inducido $\overline{\sigma}$ tiene longitud k. Teniendo en cuenta este hecho junto con el isomorfismo 6.1 se puede probar la siguiente fórmula para la serie de ciclos de una corona.

Proposición 6.5. *La serie indicatriz de ciclos de la especie de las N-coronas de longitud n está dada por*

$$Z_{C_n^N}(s_1, s_2, s_3, ...) = \frac{1}{n} Z_N(s_n, s_{2n}, s_{3n}, ...)$$

En particular

Corolario 6.6. *La serie generatriz de la especie de las N-coronas de longitud n está dada por*

$$C_n^N(x) = \frac{\widetilde{N}(x^n)}{n}$$

6.2. Conjuntos de k R-estructuras. Sea R una especie tal que $R[0] = \emptyset$. Una $E_k(R)$-estructura sobre U se especifica eligiendo una partición de U en exactamente k miembros y colocando sobre cada miembro una R-estructura. Una manera alternativa de describirla es como la especie cociente $E_k(R) = R^k/S_k$. La serie de ciclos está dada por la siguiente fórmula.

Proposición 6.7. *Sea R una especie tal que $R[0] = \emptyset$. La serie indicatriz de ciclos de la especie de los conjuntos de exactamente k R-estructuras es*

$$Z_{E_k(R)}(s_1, s_2, s_3, ...) = \frac{(Z_R(s_1, s_2, s_3, ...))^k}{k!}$$

Corolario 6.8. *La especie $E_d(C_i^N)$ de los conjuntos de exactamente d N-coronas de longitud i tiene como serie de ciclos a*

$$Z_{E_d(C_i^N)}(s_1, s_2, s_3, ...) = \frac{(Z_N(s_i, s_{2i}, s_{3i}, ...))^d}{i^d d!}$$

Dado un conjunto U podemos especificar una $\widetilde{M(N)}$-estructura sobre U mediante la siguiente serie de pasos.

1. Especificamos una secuencia $d_1, d_2, d_3, ...$ tal que $d_i = 0$ para i mayor que cierto n.
2. Determinamos para cada i un subconjunto U_i de U de manera que los U_i son disjuntos y cubren a U.
3. Elegimos sobre cada U_i una estructura de especie $E_{d_i}(C_i^N)$, es decir, una estructura de conjunto de exactamente d_i N-coronas de longitud i. Cada corona de longitud i tiene i miembros. Sea $\overline{U}$ el conjunto de todos los miembros de coronas y sea $\overline{\sigma}$ la permutación de estos miembros inducida por las coronas.
4. Elegimos sobre el conjunto $\overline{U}$ de los miembros de las coronas una M-estructura que quede fija por la permutación $\overline{\sigma}$. La cantidad de tales M-estructuras sólo depende de la secuencia $d_1, d_2, ...$ y la notamos por $M[d_1, d_2, ...]$

Esta descripción de la especie $\widetilde{M(N)}$ es la guía para establecer el siguiente isomorfismo de especies ponderadas.

Proposición 6.9. *La especie ponderada $\widehat{M(N)}$ se puede expandir como*

$$\widehat{M(N)} = \sum_{d_1, d_2, ...} M[d_1, d_2, ...] \;\; E_{d_1}(C_1^N) \;\; E_{d_2}(C_2^N) \;\; E_{d_3}(C_3^N) \;\; ...$$

Evaluando las series generatrices de ambos miembros obtenemos la siguiente identidad de series formales.

$$Z_{M(N)} = \sum_{d_1, d_2, ...} M[d_1, d_2, ...] \;\; \prod_{i \geq 1} \frac{(Z_N(s_i, s_{2i}, s_{3i}, ...))^{d_i}}{i^{d_i} d_i!}$$

Teniendo en cuenta la expresión para la serie de ciclos obtenida en la Proposición 5.6 el teorema de Redfield-Pólya se obtiene de esta última identidad.

Referencias

[1] J. C. Baez, J. Dolan, *From finite sets to Feynman diagrams*, Mathematics Unlimited - 2001 and Beyond, vol. 1, edited by Björn Engquist and Wilfried Schmid, Springer-Verlag, Berlin, 29-50, (2001).

[2] F. Bergeron, G. Labelle, P. Leroux, *Théorie des espèces et combinatoire des structures arborescentes*, LaCIM, Montréal (1994). English version: *Combinatorial Species and Tree-like Structures*, Cambridge University Press (1998).

[3] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, (1938).

[4] A. Joyal, *Une théorie combinatoire des séries formelles*, Advances in Mathematics **42**, 1-82 (1981).

[5] G. Labelle, P. Leroux (editores), *Combinatiore enumerative*, Lecture Notes in Math. **1234**, 1-82 (1985).

[6] R. P. Stanley, *Enumerative Combinatorics*, Wadsworth Inc., Belmont, (1986).

Av. Alem 1253, Depto. de Matemática, Univ. Nac. del Sur, (8000) Bahía Blanca, Argentina

E-mail address: iglesiasrodrigo@gmail.com

FORMAS DIFERENCIALES EN CURVAS ALGEBRAICAS (UNA INTRODUCCIÓN A LAS CURVAS ALGEBRAICAS)

FEDERICO QUALLBRUNN

RESUMEN. En este curso vamos a tratar de brindar una introducción a la geometría de las curvas algebraicas a partir del estudio de sus formas diferenciales y la relación con integrales abelianas y funciones abelianas.

ÍNDICE

Palabras de advertencia. Las siguiente son las notas de un curso de tres clases de una hora sobre la geometría de curvas algebraicas. El autor NO cree que pueda cubrir el material de estas notas en tres horas. Más bien, las notas servirían de complemento o ampliación al contenido del curso en sí.

Más importante aún, estas páginas no tienen ninguna intención de *explicar* estos temas, como será claro para cualquiera que las hojée. Bajo ningún concepto puede este ser un medio para entender las cosas que acá se cuentan, más bien es un medio para informarse acerca de esta matemática que el autor asegura es muy linda. En todo caso, tal vez el mayor valor que tengan estas notas sea el de dirigir al lector hacia bibliografía más rica e interesante, si eso llegase a suceder me sentiré realizado. Vale

aclarar que mucho del contenido aquí presente está inspirado en las notas del curso del Prof. Cukierman [2].

Como requisitos a este curso conviene tener familiaridad con los elementos básicos de la geometría de variedades tales como atlas, cambios de cartas y coordenadas locales. También ayuda bastante tener algún conocimiento sobre formas diferenciales, más que nada su definición y cómo se comportan bajo cambio de coordenadas.

Introducción

Desde el siglo XVIII los matemáticos estuvieron interesados en estudiar las propiedades de las funciones que son primitivas de funciones racionales o funciones algebraicas. Ejemplos tales como

$$\ln(z) = \int_1^z \frac{ds}{s}, \qquad \arcsin(z) = \int_0^z \frac{ds}{\sqrt{1-s^2}}$$

aparecen típicamente en los primeros cursos de análisis. Fueron originalmente estudiados por sus propiedades analíticas ($\ln(z)$) o por su relación con la geometría clásica ($\arcsin(z)$).
Otras funciones como

$$\phi(z) = \int_0^z \frac{ds}{\sqrt{1-s^4}}, \qquad \psi(z) = \int_0^z \frac{ds}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

son menos conocidas (no tienen nombre propio, por lo menos no en análisis 1), pero aparecen frecuentemente como soluciones a problemas de mecánica o problemas de rectificación de curvas (cálculos de longitud de arco).

Las propiedades del logarítmo y la exponencial bien pueden deducirse, como lo hacen en [1], de la clásica fórmula:

$$\ln(a) + \ln(b) = \ln(ab).$$

Asimismo también hay fórmulas similares para las funciones trigonométricas inversas, aunque son menos lindas:

$$\arcsin(a) + \arcsin(b) = \arcsin(a\sqrt{1-b^2} + b\sqrt{1-a^2}).$$

Esta fórmula, que puede deducirse de la fórmula de la suma del seno o bien derivando respecto de a de los dos lados, también puede usarse para deducir las propiedades de las funciones trigonométricas.

Estudiando problemas de elasticidad, Bernoulli mostró que sería útil conocer propiedades de la función $\phi(z) = \int_0^z \frac{ds}{\sqrt{1-s^4}}$. Para esta función Fagnano encontró en 1718 la fórmula

$$2\phi(a) = \phi(\frac{2a\sqrt{1-a^4}}{1+a^4}),$$

y en 1756 Euler descubrió que valía la fórmula más general:

$$\phi(a) + \phi(b) = \phi(\frac{a\sqrt{1-b^4} + b\sqrt{1-a^4}}{1+a^2b^2}).$$

El problema de Euler. Estos descubrimientos llevaron a Euler a formular el problema de estudiar las funciones que admiten fórmula de la suma, más en concreto:
Sea φ una función algebraica, es decir, una función implícitamente definida por una ecuación del tipo

$$f(x, \varphi(x)) = \varphi^n + f_1(x)\varphi^{n-1} + \cdots + f_{n-1}(x)\varphi + f_0(x) = 0$$

donde los $f_i(x)$ son polinomios en x.
Sea también una función racional de dos variables $R(x, y) \in \mathbb{C}(x, y)$.
A partir de estos datos consideramos la función

$$\xi(z) = \int_{z_0}^{z} R(s, \varphi(s))ds.$$

Pregunta 0.1 (Euler)**.** ¿Se puede encontrar siempre una función algebraica $g(a, b)$ en a y b tal que valga

$$\xi(a) + \xi(b) = \xi(g(a, b))?$$

¿Para qué tipo de funciones $\xi(z)$ existe una fórmula así?

Después que Euler formuló esta pregunta Lagrange encontró una fórmula de este tipo para la función $\psi(z)$ de más arriba. Entre 1824 y 1826 Abel escribió una serie de trabajos en los que muestra que no es siempre posible encontrar una fórmula para la suma como buscaba Euler, pero sí es posible encontrar fórmulas menos fuertes pero más generales.

Teorema 0.1 (N.H.Abel)**.** *Dada la función $\xi(z) = \int_{z_0}^{z} R(s, \varphi(s))ds$ existe un número p, que sólo depende de la ecuación algebraica que verifica φ (o sea sólo depende del polinomio $f(x, y)$) y que tiene la siguiente propiedad:*
Para cualquier $n \in \mathbb{N}$ existen p funciones algebraicas $y_1(x_1, \ldots, x_n), \ldots, y_p(x_1, \ldots, x_n)$ de n variables y una función elemental $v(x_1, \ldots, x_n)$ (composición de funciones algebraicas y logaritmos) tales que

$$\xi(x_1) + \cdots + \xi(x_n) = v + \xi(y_1) + \cdots + \xi(y_p).$$

En pocas palabras el teorema dice que a cualquier suma de n términos la podemos reducir a una suma de p términos más un sumando dado por una función elemental. Las fórmulas de Fagnano, Euler y Lagrange corresponden al caso en que $p = 1$ y la función $v \equiv 0$.

Como todo gran teorema, el de Abel abre más preguntas de las que cierra. ¿Cómo se calcula el número p? ¿Y las funciones y_i? ¿De dónde salió la función v, por qué en las fórmulas de Fagnano y Euler no aparece?

Observación 0.2. El lector avisor se habrá dado cuenta que muchos de los objetos sobre los que estamos hablando hasta acá no están del todo definidos. Por empezar no queda del todo claro cuál es el dominio de las funciones $\xi(z)$. Sabemos, basados en el caso particular de las funciones exponenciales y trigonométricas, que mucho se simplifican los argumentos si consideramos funciones de variable compleja. Por otro lado, al considerar funciones en el plano complejo, hay que especificar las ramas del logaritmo y de las funciones algebraicas que uno esté usando, y así la definición de $\xi(z)$ que se presentó acá resulta ambigua.

Posiblemente estas sutilezas tuvieran sin cuidado a Euler. Posiblemente Abel se haya dado cuenta de que son necesarias ciertas precauciones al usar estas definiciones (después de todo él también fue el primero en estudiar seriamente la cuestión de la

convergencia de series). Fue sin embargo Riemann el que dio a estas cuestiones un marco teórico sólido.

En el siglo XIX Riemann y sus sucesores se dieron cuenta gradualmente que las propiedades de estas funciones y las respuestas a las preguntas antes planteadas están íntimamente relacionadas con la geometría de las curvas algebraicas. Este descubrimiento fue una de las razones que originaron el estudio de las curvas algebraicas y la Geometría Algebraica en general.

Ejercicios.

1. **(Período del péndulo)** Consideremos el problema del péndulo (de masa m sin rozamiento, con una varilla de masa despreciable de longitud $l = 1$) Denotemos $\theta(t)$ es el ángulo con la vertical a tiempo t, y g la gravedad (constante). Sea θ_0 el ángulo inicial del movimiento (es decir $\theta_0 = \theta(0)$ y $\frac{d\theta}{dt}|_{t=0} = 0$). Entonces la energía cinética en tiempo t está dada por

$$K(t) = \frac{1}{2}mv_t^2 = \frac{1}{2}m\left(\frac{d\theta}{dt}(t)\right)^2.$$

   Y la energía potencial por

$$U(t) = mgh_t = mg(1 - \cos(\theta(t)).$$

   Supongamos la hipótesis (de índole físico) que la energía total $K+U$ es constante a lo largo del tiempo.

   a) Deducir que necesariamente se cumple la ecuación diferencial

$$\frac{d\theta}{dt} = \sqrt{2g(\cos(\theta) - \cos\theta_0)}.$$

   b) Analizar la para qué puntos $(t, \theta(t))$ la función $\theta(t)$ es inversible y su inversa es derivable. Denotemos a la inversa $t(\theta)$ (es el tiempo que le lleva al péndulo alcanzar el ángulo θ).

   c) Mostrar que en el intervalo $(0, \theta_0)$ vale la siguiente fórmula para $t(\theta)$:

$$t(\theta) = \frac{1}{\sqrt{2g}}\int_0^\theta \frac{d\upsilon}{\sqrt{\cos(\upsilon) - \cos\theta_0}}.$$

   d) Hacer un cambio de variables para escribir a t como una función de la forma

$$t(z) = \frac{1}{\sqrt{2g}}\int_1^z \frac{ds}{\sqrt{(1-s^2)(s-a)}}.$$

2. Mostrar que, en coordenadas polares, la longitud de arco de la elipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

   está dada en términos de la integral

$$\int_0^1 \frac{1 - k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}},$$

   donde $k = 1 - (\frac{b}{a})^2$.

3. La lemniscata es una curva plana dada por la ecuación

$$(x^2+y^2)^2 = a(x^2-y^2).$$

Dar una expresión para la longitud de arco de la lemniscata en coordenadas polares, como la integral de una función del tipo $\xi(z) = \int_{z_0}^{z} R(s,\varphi(s))ds$.

1. Curvas algebraicas planas

Definición 1.1. Una *curva algebraica plana* C es un subconjunto de $\mathbb{C}^2$ tal que existe algún polinomio de dos variables $f(x,y) \in \mathbb{C}[x,y]$ tal que $C = C(f) := \{(x,y) \in \mathbb{C}^2 | f(x,y) = 0\}$. Si existe un polinomio primo f tal que $C = C(f)$ entonces la curva C se dice *irreducible*.

Afirmación 1.1. *Si C es una curva irreducible entonces existe un polinomio primo f tal que $C = C(f)$, para cualquier otro polinomio primo g tal que $C = C(g)$ existe $\lambda \in \mathbb{C}$ tal que $g = \lambda f$.*

Definición 1.2. Sea $C(f)$ una curva irreducible y f un polinomio primo que la define. Al dominio íntegro $\mathbb{C}[C] := \mathbb{C}[x,y]/(f)$ lo llamamos *anillo de coordenadas* o *anillo de funciones regulares* de la curva y a su cuerpo de fracciones $Frac(\mathbb{C}[C])$ lo llamamos *cuerpo de funciones racionales* de C, también lo denotamos $\mathbb{K}(C)$.

La primera de las ideas que tuvo Riemann para tratar el problema de Euler fue la siguiente: En vez de tratar con "funciones multivaluadas", como por ejemplo

$$\sqrt{(1-x^2)(1-k^2x^2)}$$

hay que considerar la curva asociada a la función, en el caso anterior la curva $y^2 = (1-x^2)(1-k^2x^2)$.

Observación 1.3. Sea $p = (x_0, y_0) \in C$ tal que $\frac{\partial f}{\partial y}|_p \neq 0$. Entonces, por el Teorema de la Función Implícita, existe un abierto $U \subseteq \mathbb{C}$ y una (única) función holomorfa $\varphi : U \to \mathbb{C}$ tal que $g(x_0) = y_0$ y $f(x, \varphi(x)) = 0$ para todo $x \in U$. Es decir que $\varphi(x)$ es una función algebraica de ecuación implícita $f(x,\varphi) = 0$. En ese sentido es que consideramos heurísticamente que la ecuación $f(x,y) = 0$ da lugar a "funciones algebraicas multivaluada". Por ejemplo $f(x,y) = y^2 - x$ da lugar a las diversas determinaciones de la raíz cuadrada.

Hasta Riemann sólo se consideraban las funciones algebraicas definidas en un abierto $U \subseteq \mathbb{C}$ conveniente de manera de poder determinar la función unívocamente. Riemann mostró que la geometría global de la curva $\{f(x,y) = 0\}$ determina el comportamiento de las funciones algebraicas asociadas.

1.1. Curvas racionales y fracciones simples.

Definición 1.4. Una curva algebraica irreducible $C(f)$ (f primo) se dice *racional* si existen funciones racionales $X, Y \in \mathbb{C}(t)$ y $T \in \mathbb{C}(x,y)$ tales que

$$\begin{aligned} f(X,Y) &= 0 \in \mathbb{C}(t), \\ T(X(t),Y(t)) &= t \in \mathbb{C}(t) \quad \text{y} \\ X(T(x,y)) = x, &\quad Y(T(x,y)) = y \quad \text{como elementos del cuerpo } \mathbb{K}(C). \end{aligned}$$

Proposición 1.5. *Sea $f \in \mathbb{C}[x,y]$ primo tal que $C(f)$ es una curva racional. Entonces toda función $\xi(z) = \int_{z_0}^{z} R(s,\varphi(s))ds$ se escribe, en algún entorno simplemente conexo U de z_0 apropiado, como*

$$\xi(z) = S(z,\varphi(z)) + \sum_i b_i \log(T(z,\varphi(z)) - a_i),$$

con $S(x,y), T(x,y) \in \mathbb{C}(x,y)$.

Demostración. Como $C(f)$ es racional existen funciones $X(t)$, $Y(t)$ y $T(x,y)$ con las propiedades de la definición 1.4. Luego en la integral $\int R(s,\varphi(s))ds$ podemos hacer el cambio de variables

$$s = X(t), \quad \varphi(s) = Y(t)$$

de manera que $R(X,Y)\frac{dX}{dt}dt = pdt$, donde $p \in \mathbb{C}(t)$. Ahora a la integral $\int p(t)dt$ podemos aplicarle el método de fracciones simples para encontrarle una primitiva de la forma $r + \sum_i b_i \log(t - a_i)$, con $a_i, b_i \in \mathbb{C}$ y $r \in \mathbb{C}(t)$. Entonces reemplazando $t = T(s,\varphi(s))$ tenemos que la primitiva de $\int R(s,\varphi(s))ds$ es $S(z,\varphi(z)) + \sum_i b_i \log(T(z,\varphi(z)) - a_i)$, donde $S(x,y) = r(T(x,y))$. □

Sabemos ahora que el método de fracciones simples puede extenderse a integrar funciones algebraicas φ tales que cumplan una ecuación $f(x,\varphi(x)) = 0$ con $C(f) \subset \mathbb{C}^2$ una curva racional. Cabe preguntarse cómo reconocer si un polinomio $f \in \mathbb{C}[x,y]$ define una curva racional. No vamos a dar acá un criterio general, sólo mencionamos el siguiente criterio, cuya demostración es caso particular de un procedimiento bastante más general para reconocer curvas racionales.

Proposición 1.6. *Sea $f \in \mathbb{C}[x,y]$ un polinomio primo que sólo contiene monomios de grados r y $r+1$. Entonces la curva $C(f)$ es racional.*

Demostración. Notemos como f_{r+1} y f_r las partes homogéneas de grados $r+1$ y r respectivamente. Reemplazando $y = tx$ en $f(x,y) = 0$ obtenemos $f_r(x,tx) + f_{r+1}(x,tx) = x^r f_r(1,t) + x^{r+1} f_{r+1}(1,t) = 0$, con lo cual obtenemos la parametrización $X = -\frac{f_r(1,t)}{f_{r+1}(1,t)}$, $Y = tX$. □

Ejercicios.

1. *a*) Verificar que una curva $C(f)$ es racional si y sólo si $\mathbb{K}(C(f)) \cong \mathbb{C}(t)$.
   b) Concluir que el teorema de Luroth en teoría de cuerpos implica la siguiente afirmación:
   Sea C una curva algebraica plana. Si existen dos funciones racionales $X(t)$, $Y(t) \in \mathbb{C}(t)$ tales que la aplicación
   $$T : \mathbb{C} \to \mathbb{C}^2$$
   $$t \mapsto (X(t), Y(t))$$
   cumple $Im(T) \subseteq C$, entonces la curva C es racional.
2. Encontrar una primitiva de $1/y(x)$ donde
   $$y(x) = \sqrt[3]{-x^2 + \sqrt{x^4 + 4x^3}} - \sqrt[3]{x^2 + \sqrt{x^4 + 4x^3}}.$$
   (Sugerencia: Observar que $y^3 + axy + bx^2 = 0$ para ciertas $a, b \in \mathbb{C}$.)
3. Probar que toda curva dada por un polinomio f de grado 2 es racional. Concluir que toda función de la forma $\xi(z) = \int_{z_0}^{z} R(s, \sqrt{as^2 + bs + c})ds$ se escribe como suma de funciones algebraicas y logarítmos de funciones algebraicas. (Sugerencia: Usar el mismo cambio de variables que en la demostración de la Proposición 1.6.)

2. Formas diferenciales en curvas regulares.

Para continuar con nuestro estudio de las integrales abelianas vamos a considerar compactificaciones de las curvas afines. Una forma canónica de compactificar una curva plana afín es considerar la proyectivización de la curva.

Sea $f(x,y) = f_0 + \cdots + f_n \in \mathbb{C}[x,y]$ un polinomio de grado n, siendo $f_i(x,y)$ el término homogéneo de grado i de f. Consideremos ahora el polinomio $\overline{f} \in \mathbb{C}[x,y,z]$ definido por $\overline{f}(x,y,z) = \sum_{i=0}^{n} z^{n-i} f_i(x,y)$. Observemos que el polinomio $\overline{f}(x,y,z)$ es *homogéneo* de grado n.

Definición 2.1. La *proyectivización* de la curva $C(f)$ es el subconjunto de $\mathbb{P}^2(\mathbb{C})$ definido como

$$\overline{C(f)} := \{(x:y:z) \in \mathbb{P}^2(\mathbb{C}) \ t.q.: \ \overline{f}(x,y,z) = 0\} \subset \mathbb{P}^2(\mathbb{C}).$$

En general, dado un polinomio homogéneo g cualquiera, decimos que el conjunto

$$C(g) := \{(x:y:z) \in \mathbb{P}^2(\mathbb{C}) \ t.q.: \ g(x,y,z) = 0\} \subset \mathbb{P}^2(\mathbb{C})$$

es una *curva algebraica proyectiva.*

Observación 2.2. En $\mathbb{P}^2$ tenemos el cubrimiento por abiertos afines coordenados. Estos son los abiertos de la forma $U_i := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{C}) \ t.q. : x_i \neq 0\}$. La proyectivización $\overline{C(f)}$ de una curva afín $C(f)$ contiene a la curva afín como un abierto denso. En efecto $C(f) = \overline{C(f)} \cap U_3$.

Por otra parte, siendo cualquier curva proyectiva un cerrado de $\mathbb{P}^2(\mathbb{C})$ (ejercicio: verificar esta afirmación), y siendo que $\mathbb{P}^2(\mathbb{C})$ es una variedad diferencial compacta, tenemos que una curva proyectiva es, como subespacio topológico de $\mathbb{P}^2(\mathbb{C})$ (considerado con la topologia de variedad diferencial), compacto.

Definición 2.3. Una curva algebraica afín $C \subset \mathbb{C}^2$ se dice *regular* si está dada por un polinomio $f \in \mathbb{C}[x,y]$ tal que para todo punto $p \in C$ se tiene $(\frac{\partial f}{\partial x}|_p, \frac{\partial f}{\partial y}|_p) \neq (0,0)$.

Una curva algebraica proyectiva $C \subset \mathbb{P}^2$ se dice *regular* si para todo punto $p \in C$ existe un abierto de la forma $U_i := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 \ t.q. : x_i \neq 0\}$ tal que $C \cap U_i$ es una curva afín regular.

Observación 2.4. Si consideramos el polinomio f como una función holomorfa $f : \mathbb{C}^2 \to \mathbb{C}$ la condición de regularidad nos dice que podemos aplicar el Teorema de la Función Implícita para funciones holomorfas. Supongamos sin pérdida de generalidad que $\frac{\partial f}{\partial x}|_p \neq 0$, tenemos entonces que existe un entorno $U \in \mathbb{C}$ y una función holomorfa $g : U \to \mathbb{C}^2$ tal que $f(g(y), y) = 0, \ \forall y \in U$. En este caso el teorema de las fibras que se ve generalmente en cursos de geometría diferencial tiene una versión holomorfa, que implica que la restricción de la proyección a la curva C, $(x,y) \mapsto y$ es una carta de la única estructura de variedad holomorfa que hace de C una subvariedad holomorfa de $\mathbb{C}^2$ de dimensión 1 (dimensión como variedad compleja). En particular C es una varidead diferencial de dimensión real 2. A una variedad holomorfa de dimensión compleja 1 se la denomina *superficie de Riemann.*

Por lo anterior una curva proyectiva regular tiene también un cubrimiento por abiertos y cartas holomorfas que le dan estructura de subvariedad holomorfa de $\mathbb{P}^2(\mathbb{C})$ de dimensión compleja 1. Más aún, una curva regular es una superficie de Riemann compacta.

2.1. Formas diferenciales en curvas. Ya mencionamos que una forma de tratar con funciones algebraicas era considerar curvas algebraicas en el plano. Así, en vez de tratar con la "función multivaluada" $\sqrt{x}$, simplemente consideramos la restricción de la función $(x, y) \mapsto y$ a la curva $x^2 - y = 0$. Para estudiar integrales de funciones algebraicas vamos a necesitar de otra construcción geométrica, la de forma diferencial. Hablando mal y pronto una forma diferencial sobre una variedad es simplemente algo que tiene sentido integrar. Vamos a tratar de hacer esto más preciso a continuación. Recordamos, sin embargo, que lo recomendable es que el lector ya haya tomado contacto con la noción de formas diferenciables y bajo ningún concepto este apunte es una introducción al tema, para esto recomendamos el libro [6], capítulo 4.

Definición 2.5. Una 1-*forma diferencial holomorfa* en una variedad compleja X es una sección holomorfa del fibrado cotangente $T^*X \to X$. Denotamos al $\mathbb{C}$ espacio vectorial de 1-formas holomorfas $\Omega^1[X]$.

Afirmación 2.1. *Similarmente al caso de formas diferenciales toda* 1*-forma diferencial holomorfa puede escribirse localmente de la forma* $\sum f_i dz_i$ *con* f_i *funciones holomorfas y* z_i *coordenadas locales. En el caso en que la variedad tenga dimensión compleja* 1 *cualquier forma puede escribirse localmente como* $f(z)dz$.

Definición 2.6. Una 1-forma diferencial *meromorfa* en una superficie de Riemann X es una 1-forma ω definida sobre un abierto denso $U \subseteq X$ tal que para todo $p \in X$, existe un entorno de p donde ω puede escribirse como $\omega = f(z)dz$ con f una función *meromorfa*. Observemos que el conjunto de formas meromorfas tiene una estructura de espacio vectorial sobre el cuerpo $K(X)$ de funciones meromorfas. A este espacio lo denotamos $\Omega^1(X)$.

En el caso en que la superficie de Riemann X sea una curva plana tenemos muchas 1-formas sobre X que vienen de restringir 1-formas definidas en el plano $\mathbb{C}^2$ (o $\mathbb{P}^2(\mathbb{C})$) a X. En particular podemos considerar una curva no singular $C(f)$, las 1-formas que se escriben como $g_1(x, y)dx + g_2(x, y)dy$ con $g_i \in \mathbb{C}[x, y]$; y la restricción de estas 1-formas a $C(f)$.

Ejemplo 2.7. Sea $f \in \mathbb{C}[x, y]$ primo y $C = C(f) \subset \mathbb{C}^2$. Supongamos que C es no singular. Considerando que la función f restringida a C es identicamente nula, entonces tenemos que, en C, vale la igualdad $df = 0$, o sea.

$$f_x dx + f_y dy = 0. \tag{2.1}$$

Lema 2.8. *Sea* $f \in \mathbb{C}[x, y]$ *primo de grado* d *y* $X = \overline{C(f)} \subset \mathbb{P}^2(\mathbb{C})$ *la proyectivisación de la curva* $C(f)$. *Supongamos que* X *es no singular. Entonces tenemos bien definida una aplicación lineal*

$$\begin{aligned} \mathbb{C}[x, y]_{\leq d-3} &\longrightarrow \Omega^1[X] \\ h &\longmapsto \omega_h = \frac{h}{\frac{\partial f}{\partial y}} dx, \end{aligned}$$

donde $\mathbb{C}[x, y]_{\leq d-3}$ *denota el espacio vectorial de polinomios de grado menor o igual que* $d - 3$. *Más aún esta aplicación es inyectiva.*

Demostración. Denotemos $f_x = \frac{\partial f}{\partial x}$ y $f_y = \frac{\partial f}{\partial y}$. A priori ω_h es una forma meromorfa sobre la curva afín $C(f)$. Veamos que define una única forma meromorfa en X. Para esto notemos que la curva $C(f)$ vista dentro de $\overline{C(f)} \subset \mathbb{P}^2(\mathbb{C})$ es el conjunto $\{(x : y :$

$1) \in \mathbb{P}^2(\mathbb{C})\ t.q.: \overline{f}(x,y,1) = 0\}$, y que en un punto $(x:y:z) \in \mathbb{P}^2(\mathbb{C})$lo que expresamos en coordenadas afines como ω_g se expresa en coordenadas homogéneas como

$$\omega_h((x:y:z)) = \frac{h(\frac{x}{z}, \frac{y}{z})}{f_y(\frac{x}{z}, \frac{y}{z})} d\left(\frac{x}{z}\right).$$

Luego, si denotamos $\overline{g}(x,y,z)$ el homogeneizado de $g(x,y)$ y $\overline{f_y}(x,y,z)$ el de $f_y(x,y)$, podemos escribir la ecuación de arriba como

$$\omega_h((x:y:z)) = \frac{\overline{h}(x,y,z)}{\overline{f_y}(x,y,z)} \frac{z^{d-1}}{z^e} d\left(\frac{x}{z}\right) = \tag{2.2}$$

$$= \left(\frac{\overline{h}(x,y,z)}{\overline{f_y}(x,y,z)} \frac{z^{d-1}}{z^e}\right) \left(\frac{dx}{z} + \frac{xdz}{z^2}\right), \tag{2.3}$$

donde e es el grado de h. Esta última expresión es la de una forma meromorfa sobre X.

Tenemos entonces una forma meromorfa ω_h sobre X. Vamos a ver que es regular en todo punto. Primero veamos que es regular en el abierto denso $C(f) \subset \overline{C(f)}$.

Tomemos entonces un punto $p \in C(f)$ tal que $f_y(p) = 0$, como X es no singular entonces necesariamente $f_x(p) \neq 0$. Por la identidad del Ejemplo 2.7 llegamos a la conclusión de que vale

$$\omega_h = \frac{h}{f_y} dx = -\frac{h}{f_x} dy.$$

Entonces ω_h es regular en p.

Ahora veamos que ω_h es regular en $\overline{C(f)} \setminus C(f)$. Notemos primero que $\overline{C(f)} \setminus C(f)$ consiste de los (finitos) puntos de la forma $(x:y:0)$ tales que $\overline{f}(x,y,0) = 0$. Usando la expresión (2.3) vemos que, si $e \leq d-3$, entonces ω_h es regular en $(x:y:0) \in \overline{C(f)}$ si y sólo si $\frac{dx}{\overline{f_y}} + \frac{xdz}{\overline{f_y}}$ lo es. Para ver que esta última forma es regular en $X \setminus C(f)$ podemos razonar como en el Ejemplo 2.7 y ver que esto es consecuencia de la regularidad de X. En efecto, escribiendo (2.1) en coordenadas homogéneas tenemos que

$$\overline{f_x}(x,y,z)(dx + \frac{x}{z}dz) = -\overline{f_y}(x,y,z)(dy + \frac{y}{z}dz).$$

Esta fórmula junto a la regularidad de X muestran que ω_h es una forma regular en todo punto.

El hecho de que la aplicación es inyectiva sale fácil del hecho de que la forma ω_h tiene siempre coeficientes no nulos si $h(x,y) \neq 0$. □

El siguiente teorema, que no vamos a demostrar, caracteriza completamente las formas holomorfas en una curva plana no singular.

Teorema 2.9. *Sea X como en el lema anterior. La aplicación*

$$\begin{aligned} \mathbb{C}[x,y]_{\leq d-3} &\longrightarrow \Omega^1[X] \\ g &\longmapsto \omega_h \end{aligned}$$

es un isomorfismo. En particular, si la curva tiene grado d, el $\mathbb{C}$-espacio vectorial de formas diferenciales holomorfas tiene dimensión $(d-1)(d-2)/2$.

Demostración. Ver [7], cap. 7. □

Ejercicios.

1. Dado un polinomio homogéneo $g \in \mathbb{C}[x,y,z]$ y la curva proyectiva plana $X = C(g)$, consideramos el anillo cociente $\mathbb{C}[X] := \mathbb{C}[x,y,z]/(g)$. Lo llamamos *anillo de coordenadas homogéneas* de la curva X.
   a) Mostrar que, al ser g homogéneo, $\mathbb{C}[X]$ tiene una graduación de manera que la proyección $\mathbb{C}[x,y,z] \to \mathbb{C}[X]$ respeta el grado.
   b) Supongamos que $\mathbb{C}[X]$ es un dominio. Consideremos entonces el cuerpo $\mathbb{K}(X) := \{\frac{f}{g} \ t.q. : f,g \in \mathbb{C}[X], \ \deg(f) = \deg(g)\}$ que llamamos *cuerpo de funciones racionales*. Probar que si C es una curva afín tal que $C \subset X$ entonces $\mathbb{K}(C) = \mathbb{K}(X)$.
2. Probar que cualquier curva proyectiva es un cerrado de $\mathbb{P}^2(\mathbb{C})$ (ojo, un polinomio homogéneo de tres variables NO define una función $\mathbb{P}^2 \to \mathbb{C}$).
3. Sea $f(x) \in \mathbb{C}[x]$. Mostrar que si la proyectivización de la curva plana $y^2 - f(x) = 0$ es regular entonces el grado de f es necesariamente menor o igual a 3.
4. *a*) Sea $X = \mathbb{P}^1(\mathbb{C})$ con coordenadas homogéneas $(x : y)$, y sea una 1-forma meromorfa ω que en el abierto $y \neq 0$ se escribe $\omega = f(x)dx$. Entonces necesariamente $f(x)$ es una función racional.
   b) Concluir que $\mathbb{P}^1(\mathbb{C})$ no posee formas holomorfas globales.

3. El teorema de Abel

Recordemos que empezamos estudiando integrales de la forma

$$\xi(z) = \int_{z_0}^{z} R(s, \varphi(s))ds,$$

con $\varphi(s)$ una función satisfaciendo una ecuación polinomial $f(s, \varphi(s)) = 0$. Hasta ahora, para estudiar las funciones $\xi(z)$ del principio, hemos introducido primero curvas algebraicas para pensar a las funciones algebraicas $\varphi(s)$ como funciones sobre una curva algebraica $C(f)$. Luego definimos 1-formas holomorfas y meromorfas en las curvas algebraicas, el propósito de esto es poder pensar en la expresión $\int R(s, \varphi(s))ds$ como la integral de la forma (meromorfa) $\omega = R(x,y)dx$, definida sobre la curva $C(f)$.

Recordemos que, dada una 1-forma diferencial $\eta = f(x)dx$ definida sobre una variedad M, podemos definir la integral de η a lo largo de una curva $[0,1] \xrightarrow{c} M$ como

$$\int_c \eta = \int_0^1 f(c(t))dt,$$

notemos que, si η es una forma holomorfa en una variedad compleja, esta fórmula sigue teniendo perfecto sentido y generaliza la integral curvilínea de funciones complejas. Recordemos que podemos definir una 1-cadena como una combinación entera simbólica de curvas $\sum n_i c_i$ y extender linealmente la definición de integral a cadenas.

Definición 3.1. Sea X una superficie de Riemann y $\eta \in \Omega^1(X)$. El *residuo* de η alrededor de un punto singular p es el número $\operatorname{res}_p(\eta) := \int_c \eta$ donde c es una curva que encierra a p y a ningún otro punto singular de η.

3.1. La aplicación de Abel-Jacobi. Sea X una curva proyectiva regular. Vamos a definir una función cuyo dominio es X, que va a englobar información sobre funciones de la pinta $\xi(z) = \int_{z_0}^{z} R(s, \varphi(s))ds$. Para poder entender esta aplicación es preciso hacer consideraciones sobre la topología y la geometría de X.

El teorema 2.9 afirma que, si X es una curva plana regular, el espacio vectorial $\Omega^1[X]$ de 1-formas holomorfas tiene dimensión finita. De hecho vale una afirmación un poco más general.

Afirmación 3.1. *Sea X una superficie de Riemann compacta. El espacio $\Omega^1[X]$ tiene dimensión finita sobre $\mathbb{C}$. Al número $g = \dim_{\mathbb{C}} \Omega^1[X]$ se le llama el* género *de X.*

Tomemos entonces una base $\omega_1, \ldots, \omega_g$ de $\Omega^1[X]$. Un paso importante en el estudio de las funciones $\xi(z)$ fue considerar simultaneamente las integrales de las formas ω_i. Así uno toma en cuenta la aplicación

$$p \mapsto (\int_{p_0}^{p} \omega_1, \int_{p_0}^{p} \omega_2, \ldots, \int_{p_0}^{p} \omega_g). \tag{3.1}$$

La conveniencia de estudiar tal aplicación estaba explícita en los trabajo de Riemann sobre integrales abelianas y aparentemente en los trabajos originales de Abel sobre el tema también tiene un lugar importante.

La fórmula 3.1, sin embargo, no define ninguna función así como así, por empezar tenemos que darle sentido al dominio y codominio de la aplicación, tarea que en este caso es altamente no trivial.

La fórmula $\int_{p_0}^{p} \omega$ no tiene, a priori, sentido ya que la integral de una 1-forma depende realmente de la curva sobre la cual estamos integrando y no solamente de los puntos inicial y final de la curva. Más precisamente vale la siguiente afirmación:

Afirmación 3.2 (Teorema de Stokes para formas holomorfas)**.** *Sea X una variedad holomorfa, η una p-forma holomorfa y Δ un $p+1$ simplex en X entonces*

$$\int_{\partial\Delta} \eta = \int_{\Delta} d\eta.$$

La forma $d\eta$ se calcula localmente de la misma manera que para formas diferenciales sólo que usando la derivada compleja (y coordenadas complejas).

En particular, como una superficie de Riemann tiene dimensión compleja 1, no hay 2-formas holomorfas no triviales en una superficie de Riemann, por lo que todas las 1-formas holomorfas son cerradas. Esto implica, junto con el teorema de Stokes, que en el caso de superficies de Riemann la integral $\int_c \eta$ de una 1-forma η a lo largo de una curva c sólo depende de la clase de homología de la curva c. En efecto, si c y c' son dos curvas homológicamente equivalentes entonces el ciclo $[c] - [c']$ es el borde de una cadena Δ de dimensión 2 y, usando el teorema de Stokes,

$$\int_c \eta - \int_{c'} \eta = \int_{[c]-[c']} \eta = \int_{\partial\Delta} \eta = \int_{\Delta} d\eta = \int_{\Delta} 0 = 0.$$

Vemos así que es preciso tener en cuenta las clases de homología de 1-cadenas para hablar de la aplicación de Abel-Jacobi, es decir que hay que tener en cuenta al grupo $H_1(X, \mathbb{Z})$. Respecto de este grupo tenemos el siguiente teorema.

Teorema 3.2 (Riemann)**.** *Sea X una superficie de Riemann y sea $g = \dim_{\mathbb{C}} \Omega^1[X]$ el género de X. Entonces $H_1(X, \mathbb{Z}) \cong \mathbb{Z}^{2g}$.*

Demostración. Ver [6] capítulo 1 y referencias ahí dadas. □

Ahora estamos en condiciones de darle sentido a las integrales de la fórmula 3.1. En efecto si tomamos una base $\delta_1, \ldots, \delta_{2g}$ de $H_1(X, \mathbb{Z})$; tenemos que las integrales $\int_{p_0}^{p} \omega$ están definidas a menos de un término de la forma $\sum n_j \int_{\delta_j} \omega$. Más precisamente, si

c y c' son dos curvas (reales) en X que empiezan en p_0 y terminan en p, entonces el 1-ciclo $[c]-[c']$ es homólogo a una combinación entera $\sum n_i\delta_i$ y, por lo tanto, $\int_c \omega - \int_{c'}\omega = \sum n_i \int_{\delta_i}\omega$. Esto hace que considerar las propiedades de la integral $\int_{p_0}^{p}\omega$ se haga muy difícil. Abel se dio cuenta que si se consideran todas las formas holomorfas simultáneamente el panorama sorprendentemente se hace mucho más claro. Vamos a ver por qué.

Sea una base $\omega_1,\dots,\omega_g$ del espacio de 1-formas holomorfas de X, y sea $\delta_1,\dots,\delta_{2g}$ una base de $H_1(X,\mathbb{Z})$. La *matriz de períodos* de X es la matriz de $g\times 2g$

$$\begin{pmatrix} \int_{\delta_1}\omega_1 & \dots & \int_{\delta_{2g}}\omega_1 \\ \vdots & \ddots & \vdots \\ \int_{\delta_1}\omega_g & \dots & \int_{\delta_{2g}}\omega_g \end{pmatrix}.$$

Los $2g$ vectores columna de esta matriz $\Pi_i = (\int_{\delta_i}\omega_1,\dots,\int_{\delta_i}\omega_g)\in\mathbb{C}^g$ se llaman *períodos*. Tenemos que vale lo siguiente

Afirmación 3.3. *Los períodos $\{\Pi_i\}_{1\le i\le 2g}$ forman un conjunto linealmente independiente sobre $\mathbb{R}$. En otras palabras el conjunto*

$$\Lambda := \left\{ \sum_{i=0}^{2g} n_i\Pi_i \ : n_i\in\mathbb{Z} \right\}$$

forma un reticulado *del espacio $\mathbb{C}^g$.*

Notemos que, mientras que la integral $\int_{p_0}^{p}\omega$ está bien definida módulo los $2g$ períodos de ω, que en general forman un conjunto denso en $\mathbb{C}$, el vector

$$\left(\int_{p_0}^{p}\omega_1,\dots,\int_{p_0}^{p}\omega_g\right)$$

está bien definido módulo el reticulado $\Lambda\subset\mathbb{C}$. Luego, eligiendo un punto $p_0\in X$ arbitrario, tenemos que la fórmula

$$p\mapsto\left(\int_{p_0}^{p}\omega_1,\int_{p_0}^{p}\omega_2,\dots,\int_{p_0}^{p}\omega_g\right)$$

define un morfismo de variedades holomorfas.

$$AJ_1 : X\longrightarrow \mathbb{C}^g/\Lambda.$$

Un poco más en general podemos definir, para todo $n\in\mathbb{N}$, morfismos

$$\begin{aligned} AJ_n : X^n &\longrightarrow \mathbb{C}^g/\Lambda. \\ (p_1,\dots,p_n) &\longmapsto \left(\sum_{i=1}^{n}\int_{p_0}^{p_i}\omega_1,\dots,\sum_{i=1}^{n}\int_{p_0}^{p_i}\omega_g\right). \end{aligned}$$

Afirmación 3.4. *Si X es una curva proyectiva y regular la variedad $\mathbb{C}^g/\Lambda$ tiene estructura de variedad algebraica y los morfismos AJ_n son morfismos regulares de variedades algebraicas.*

La(s) demostración(es) de la afirmación de más arriba conforma(n) un hito en la geometría algebraica de segunda mitad del siglo XX. Muchas de las herramientas que conforman la geometría algebraica moderna juegan algún papel en la demostración de la forma más general de este teorema. Sin, embargo, mientras estemos trabajando con curvas proyectivas sobre los números complejos, no vamos a necesitar esta afirmación.

Vamos a usar los morfismos AJ_n para investigar las fórmulas de la suma de las funciones abelianas $\xi(z)$.

3.2. Divisores y equivalencia racional. Si bien no es como fue expresado originalmente, para hablar del teorema de Abel nos conviene usar la noción de divisores en curvas y la de equivalencia racional de divisores.

Definición 3.3. Sea X una curva algebraica. El *grupo de divisores de* X $\mathrm{Div}(X)$ es el grupo abeliano libre generado por los puntos de X. Típicamente notamos los elementos de $\mathrm{Div}(X)$ como $\sum_i n_i[p_i]$, a cada uno de estos elementos lo llamamos un *divisor*. El *grado* de un divisor $\sum_i n_i[p_i]$ es el número $\sum_i n_i \in \mathbb{Z}$. Llamamos *soporte* de D al conjunto de puntos $\{p_i\}$. Al subgrupo de divisores de grado 0 lo denotamos $\mathrm{Div}_0(X)$.

Ejemplo 3.4. Sea X una curva regular proyectiva y $f \in \mathbb{K}(X)$ una función meromorfa. El *divisor de ceros y polos de* f es el divisor $(f) = \sum_{p\in X} \mathrm{ord}_p(f)[p]$. Donde $\mathrm{ord}_p(f)$ es el orden de p como cero o polo de f. Notar que es un divisor bien definido ya que, al ser X proyectiva y regular, es compacta y una función meromorfa sólo puede tener entonces finitos ceros y polos, por lo que la suma es finita. Puede demostrarse que (f) siempre es un divisor de grado 0 (Ver [6] cap. IV.3.18, o [7] cap. 7).

Ejemplo 3.5. Asimismo tenemos, para toda forma meromorfa $\eta \in \Omega^1(X)$ el divisor de ceros y polos de la 1-forma $(\eta) = \sum_{p\in X} \mathrm{ord}_p(\eta)[p]$.

Definición 3.6. Dos divisores D y D' sobre una curva X son *racionalmente equivalentes* (o *linealmente equivalentes*, son sinónimos) si y sólo si existe una función racional f tal que $D - D' = (f)$. Lo denotamos $D \sim_{\mathrm{rat}} D'$.

Observación 3.7. Dos divisores racionalmente equivalentes tienen el mismo grado.

3.3. El teorema de Abel. Como bien señala Kleiman en [4] no existe un único teorema de Abel. Sin, embargo, a partir del libro [8] la siguiente afirmación fue conocida generalmente como EL teorema de Abel:

Teorema 3.8.

$$AJ_n(p_1,\dots,p_n) = AJ_m(q_1,\dots,q_m) \in \mathbb{C}^g/\Lambda \iff \sum_{i=1}^{n}[p_i] - n[p_0] \sim_{\mathrm{rat}} \sum_{i=1}^{m}[q_i] - m[p_0].$$

Sólo vamos a describir la demostración de una de las implicaciones (la que efectivamente es debida a Abel) que es algo menos complicada y basta para dar "fórmulas de la suma" bastante generales.

Demostración. ($\Longrightarrow$) Ver [3] cap. II.2.

($\Longleftarrow$) Definamos una función

$$\mu : \mathrm{Div}_0(X) \to \mathbb{C}^g/\Lambda$$

$$\mu(\sum_i [p_i] - [q_i]) \mapsto \left(\sum_{i=1}^{n} \int_{q_i}^{p_i} \omega_1, \dots, \sum_{i=1}^{n} \int_{q_i}^{p_i} \omega_g \right)$$

(notar que esta función está bien definida, es decir que no depende del agrupamiento de las p_i con las q_i). Ahora, si $D = (f)$, tenemos un morfismo (ejercicio: verificar que la siguiente fórmula define un morfismo de variedades holomorfas)

$$\psi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{C}^g/\Lambda,$$
$$(\lambda_0 : \lambda_1) \mapsto \mu((\lambda_0 \cdot f - \lambda_1)).$$

Si z_i son las coordenadas de $\mathbb{C}^g$, las formas dz_i, con $1 \leq i \leq g$ generan el espacio cotangente $T_p^*(\mathbb{C}^g/\Lambda)$ para todo p. Como $\mathbb{P}^1(\mathbb{C})$ no tiene formas holomorfas globales (ver el ejercicio 4 de la sección anterior) entonces $\psi^*(dz_i) = 0$, luego ψ es constante, por lo tanto $\mu(D) = \psi((0:1)) = \psi((1:0)) = 0$. □

El teorema de Abel nos da un criterio para establecer cuándo tenemos igualdades entre sumas de la forma $\xi(s_1) + \cdots + \xi(s_n) = \xi(s'_1) + \cdots + \xi(s'_m)$ cuando podemos establecer $m = 1$ entonces tenemos una fórmula de la suma como quería Euler. En cualquier caso el teorema nos dice que es clave el estudio de los divisores de grado cero módulo equivalencia racional. De hecho, podemos interpretar parte del teorema de Abel sobre formulas de la suma para funciones abelianas como la siguiente:

Afirmación 3.5. *Sea D un divisor en una curva X (proyectiva, regular) de género g tal que $\deg(D) = 0$. Entonces para todo punto p_0 en un abierto denso U_D de X existen puntos $q_1, \ldots, q_g$ tales que*

$$D \sim_{\text{rat}} \sum_{i=1}^{g} [q_i] - g[p_0].$$

Demostración. Ver [5] cap. II.2 Lemma 5. □

Ejercicios.

1. Dada X curva algebraica proyectiva regular. Tomemos dos bases distintas β y β' de $H_1(X, \mathbb{Z})$, y dos bases distintas Ω y Ω' de $\Omega^1[X]$. Mostrar que los cambios de base entre las matrices de períodos $\Pi_{\beta,\Omega}$ y $\Pi_{\beta',\Omega'}$ definen un isomorfismo de variedades holomorfas entre $\mathbb{C}^g/\Lambda$ y $\mathbb{C}^g/\Lambda'$, donde $\Lambda = \Pi_{\beta,\Omega} \cdot \mathbb{Z}^{2g}$ y $\Lambda' = \Pi_{\beta',\Omega'} \cdot \mathbb{Z}^{2g}$. A esta variedad la llamamos *variedad Jacobiana* de X y la denotamos $\text{Jac}(X)$.
2. **(Descomposición de Hodge en curvas)** Dada una superficie de Riemann compacta sea $\mathcal{A}^i(X)$ el $\mathbb{R}$-espacio vectorial de formas $\mathcal{C}^\infty$ sobre X, considerada como superficie diferencial. Sea δ la diferencial de de Rham usual y

$$0 \to \mathcal{A}^0(X) \xrightarrow{\delta} \mathcal{A}^1(X) \xrightarrow{\delta} \mathcal{A}^2(X) \to 0 \tag{3.2}$$

el complejo de de Rham diferencial, cuya homología es $H^i(X, \mathbb{R})$.

   a) Mostrar que si tomamos $\mathcal{A}^i_{\mathbb{C}}(X) = \mathcal{A}^i(X) \otimes_{\mathbb{R}} \mathbb{C}$ y la sucesión exacta

$$0 \to \mathcal{A}^0_{\mathbb{C}}(X) \xrightarrow{\delta \otimes_{\mathbb{R}} 1} \mathcal{A}^1_{\mathbb{C}}(X) \xrightarrow{\delta \otimes_{\mathbb{R}} 1} \mathcal{A}^2_{\mathbb{C}}(X) \to 0$$

   la cohomología de esta sucesión es $H^i(X, \mathbb{R}) \otimes \mathbb{C} = H^i(X, \mathbb{C})$.

   b) Sea $\mathcal{X}(X)$ el módulo de campos de vectores tangentes (diferenciales) sobre X, observar que $\hom_{\mathbb{C}}(\mathcal{A}^1_{\mathbb{C}}(X), \mathbb{C}) \cong \mathcal{X}(X) \otimes \mathbb{C}$

   c) Sea $U \subseteq X$ un abierto coordenado y $(x, y) : U \to \mathbb{R}^2$ una carta. Probar que $dz := dx + idy$ y $d\overline{z} := dx - idy$ forman una base de $\mathcal{A}^1_{\mathbb{C}}(U)$ como $\mathcal{C}^\infty(U)$-módulo.

   d) En particular si $z : U \to \mathbb{C}$ es una carta holomorfa, tomamos $x = \Re(z)$, $y = \Im(z)$. Ahora formamos dz y $d\overline{z}$ como en el punto anterior. Llamemos $\frac{\partial}{\partial z}$ y $\frac{\partial}{\partial \overline{z}} \in \mathcal{X}(X) \otimes \mathbb{C}$ a la base dual de $\{dz, d\overline{z}\}$. Probar que si $f \in \mathcal{C}^\infty(U) \otimes \mathbb{C}$ es una función diferencial que toma valores en $\mathbb{C}$, la expresión $\frac{\partial f}{\partial \overline{z}} = 0$ tiene sentido y es equivalente a que f cumpla las ecuaciones de Cauchy-Riemann.

   e) Sea $\omega \in \Omega^1[X]$ una 1-forma holomorfa, en particular $\omega \in \mathcal{A}^1_{\mathbb{C}}(X)$. Probar que ω es cerrada (i.e.: $\delta(\omega) = 0$), y que, si es exacta (i.e: si existe f tal que $\delta(f) = \omega$), entonces $\omega = 0$. En particular $\Omega^1[X] \subset H^1(X, \mathbb{C})$.

f) Si $\omega \in \Omega^1[X]$ se expresa localmente como $f(z)dz$ definimos $\overline{\omega}$ localmente como $\overline{f}(z)d\overline{z}$. Mostrar que esto define una forma global $\overline{\omega} \in \mathcal{A}^1_{\mathbb{C}}(X)$. Más aún esta construcción nos da que $\Omega^1[X] \oplus \overline{\Omega^1[X]} \subseteq H^1(X, \mathbb{C})$.

Afirmación:(Teorema de Hodge para curvas)

$$H^1(X, \mathbb{C}) = \Omega^1[X] \oplus \overline{\Omega^1[X]}.$$

3. Usando el teorema de Hodge para curvas probar la Afirmación 3.3.
4. Sea X una curva algebraica proyectiva, f y $g \in \mathbb{K}(X)$ funciones racionales. Demostrar:
   a) $(fg) = (f) + (g)$.
   b) $(\frac{f}{g}) = (f) - (g)$.
   c) $(\frac{1}{f}) = -(f)$.
5. Sean p, $q \in \mathbb{P}^1(\mathbb{C})$, entonces $[p] \sim_{\text{rat}} [q]$.
6. Interpretar la afirm. 3.5 en términos de sumas de funciones abelianas $\sum_i \xi(z_i)$.

4. El teorema de Riemann-Roch

A lo largo de esta sección X siempre va a ser una curva algebraica proyectiva regular e irreducible.

Definición 4.1. Decimos que un divisor $D = \sum_i n_i[p_i] \in \text{Div}(X)$ es *positivo* (lo notamos $D > 0$) si $n_i \in \mathbb{N}$, para todo i. Esto define una relación de orden parcial, decimos que $D > D'$ si y sólo si $D - D' > 0$.

Observación 4.2. Notar que para cualquier par de funciones racionales $f, g \in \mathbb{K}(X)$ vale $\text{ord}_p(f+g) \geq \text{mín}\{\text{ord}_p(f), \text{ord}_p(g)\}$. Luego, si $(f) \geq D$ y $g \geq D$, vale $(f+g) \geq D$.

Definición 4.3. Dado un divisor $D \in \text{Div}(X)$ definimos el espacio $\mathcal{L}(D)$ como el $\mathbb{C}$-espacio vectorial

$$\mathcal{L}(D) := \{f \in \mathbb{K}(X) : (f) + D \geq 0\}.$$

Observación 4.4. Notar que, dado el divisor $D = \sum_i n_i[p_i] - \sum_j m_j[q_j]$, $m_j, n_i \in \mathbb{N}$; el espacio $\mathcal{L}(D)$ no es otra cosa que el espacio de funciones racionales con un cero de orden al menos m_j en cada q_j y un polo de orden a lo sumo n_i en cada punto p_i. En particular $\mathcal{L}(0) = \mathbb{C}$.

Observación 4.5. Si $D \leq D'$ entonces $\mathcal{L}(D) \subseteq \mathcal{L}(D')$.

Lema 4.6. *Sea $D \in \text{Div}(X)$ y $p \in X$. Entonces $\mathcal{L}(D - [p]) = \mathcal{L}(D)$ ó $\mathcal{L}(D - [p])$ es un subespacio de codimensión 1 de $\mathcal{L}(D)$.*

Demostración. Elijamos una coordenada local z alrededor de p. Si $n_p \in \mathbb{Z}$ es el coeficiente que multiplica a $[p]$ en D entonces definimos un funcional $\alpha : \mathcal{L}(D) \to \mathbb{C}$ de la siguiente manera: a f una función racional le asignamos el coeficiente c_{n_p} en su desarrollo en serie de Laurent en coordenada z. Si $\alpha \equiv 0$ entonces $\mathcal{L}(D - [p]) = \mathcal{L}(D)$. Si $\alpha \neq 0$ entonces $\mathcal{L}(D - [p]) = \ker(\alpha)$ es un subespacio de codimensión 1. □

Proposición 4.7. *Sea $D \in \text{Div}(X)$. El espacio $\mathcal{L}(D)$ es de dimensión finita sobre $\mathbb{C}$. De hecho, si escribimos $D = D^+ - D^-$ con D^+ y D^- divisores positivos (mayores que 0) soportados en subconjuntos disjuntos de puntos, tenemos que* $\dim(\mathcal{L}(D)) \leq 1 + \deg(D^+)$.

Demostración. Si $\deg(D^+) = 0$ entonces $D^+ = 0$ por lo que $\dim(\mathcal{L}(D^+)) = 1$. Como $D \leq D^+$ entonces $\mathcal{L}(D) \subseteq \mathcal{L}(D^+)$, en particular $\dim(\mathcal{L}(D)) \leq 1 + \deg(D^+)$.

Ahora procedemos por inducción en el grado de D^+. Supongamos entonces que la proposición es cierta para $\deg(D^+) \leq k-1$. Sea ahora D tal que $\deg(D^+) = k$. Tomemos un punto p del soporte de D^+ y consideremos el divisor $D - [p]$, su parte positiva es $D^+ - [p]$. Por hipótesis inductiva $\dim(\mathcal{L}(D-[p])) \leq 1 + \deg(D^+ - [p])$. Por el lema anterior $\mathcal{L}(D-[p])$ es igual a $\mathcal{L}(D)$ o es un hiperplano en $\mathcal{L}(D)$, lo que prueba la proposición. □

Observación 4.8. Notemos que por la demostración del Lema 4.6 y por la proposición anterior podemos más precisamente decir que, dado D, existen finitos puntos $q_1, \ldots, q_r$ tal que si $p \in X \setminus \{q_1, \ldots, q_r\}$ entonces $\mathcal{L}(D-[p])$ es una hipersuperficie de $\mathcal{L}(D)$. En los otros casos, tenemos $\mathcal{L}(D-[q_i]) = \mathcal{L}(D)$.

Notamos con $\ell(D)$ la dimensión del espacio $\mathcal{L}(D)$.

Definición 4.9. Dado un divisor $D \in \mathrm{Div}(X)$ definimos el espacio $K_X(D)$ como el $\mathbb{C}$-espacio vectorial

$$K_X(D) := \{\eta \in \Omega^1(X) : (\eta) + D \geq 0\}.$$

Similarmente a las demostraciones anteriores se pueden demostrar:

Lema 4.10. *Sea $D \in \mathrm{Div}(X)$ y $p \in X$. Entonces $K_X(D-[p]) = K_X(D)$ ó $K_X(D-[p])$ es un subespacio de codimensión 1 de $K_X(D)$.*

Proposición 4.11. *Sea $D \in \mathrm{Div}(X)$. El espacio $K_X(D)$ es de dimensión finita sobre $\mathbb{C}$.*

Notamos con $\delta(D)$ a la dimensión de $K_X(D)$.

Ahora podemos enunciar el teorema Riemann-Roch, vagamente es un resultado acerca de la relación entre la cantidad de funciones racionales con polos y ceros prescripto y la cantidad de 1-formas con polos y ceros prescriptos. Más precisamente:

Teorema 4.12 (Riemann-Roch)**.** *Sea X una curva regular y proyectiva, de género $g = \dim \Omega^1[X]$. Para todo divisor D sobre X se tiene*

$$\ell(D) - \delta(-D) = \deg(D) - g + 1.$$

Demostración. Ver [7] capitulo 7C. □

Corolario 4.13. *Dados puntos distintos $p_1, \ldots, p_n \in X$ y números complejos $r_1, \ldots, r_n \in \mathbb{C}$ tales que $\sum_i r_i = 0$ existe una $\omega \in \Omega^1(X)$ tal que ω es regular en $X \setminus \{p_1, \ldots, p_n\}$, $\mathrm{ord}_{p_i}(\omega) = -1$ para todo $1 \leq i \leq n$, y $\mathrm{res}_{p_i}(\omega) = r_i$.*

Demostración. Dados puntos distintos $p, q \in X$ existe $\omega \in \Omega^1(X)$ regular en $X \setminus \{p, q\}$ y tal que $\mathrm{res}_p(\omega) = 1$ y $\mathrm{res}_q(\omega) = 0$. Para ver esto, tenemos por Riemann-Roch que $\delta([p]+[q]) = \ell(-[p]-[q]) + 2 + g - 1 = g + 1$ y por el teorema de los residuos toda $\eta \in K_X(p+q)$ cumple $\mathrm{res}_p(\eta) + \mathrm{res}_q(\eta) = 0$. Tomando una $\eta \in K_X(p+q) \setminus \Omega^1[X]$ y tomando $\omega = \eta/\mathrm{res}_p(\eta)$ se tiene lo afirmado.

Ahora elijamos un punto $q \in X \setminus \{p_1, \ldots, p_n\}$ y tomemos ω_i como arriba, regular en $X \setminus \{q, p_i\}$ y tal que $\mathrm{res}_{p_i}(\omega_i) = r_i$ y $\mathrm{res}_q(\omega_i) = -r_i$. Entonces $\omega = \sum_{i=1}^n \omega_i$ responde a la cuestión. □

Definición 4.14. En el espacio $\Omega^1(X)$ definimos tres sub-espacios vectoriales (sobre $\mathbb{C}$):

1. $I = I(X) = \Omega^1[X]$ el conjunto de 1-fromas holomorfas, que también llamamos (siguiendo la terminología clásica) *formas diferenciales de primera especie.*
2. $II = II(X) = \{\omega \in \Omega^1(X) : \mathrm{res}_p(\omega) = 0,\ \forall p \in X\}$ el espacio de *formas diferenciales de segunda especie.*
3. $III = III(X) = \{\omega \in \Omega^1(X) : \mathrm{ord}_p(\omega) \geq -1\ \forall p \in X\}$ el espacio de *formas diferenciales de tercera especie.*

Observación 4.15. Notar que la condición $\omega \in III(X)$ significa que el desarrollo en serie de Laurent de ω alrededor un punto cualquiera es de tipo rdz/z con $r \in \mathbb{C}$.

Proposición 4.16. *Con la notación anterior, tenemos las siguientes relaciones:*

- $II \cap III = I$.
- $df \in II$, *para toda* $f \in \mathbb{K}(X)$.
- $d(\mathbb{K}(X)) \cap I = 0$.
- $d(\mathbb{K}(X)) \cap III = 0$.

Demostración. Ejercicio. □

Proposición 4.17. $\Omega^1(X) = II + III$.

Demostración. Sea $\eta \in \Omega^1(X)$. Como el número de polos de η es finito, por el corolario 4.13, existe $\omega \in III$ tal que $\mathrm{res}_p(\omega) = \mathrm{res}_p(\eta)$ para todo $p \in X$. Entonces $\eta - \omega \in II$ y por lo tanto la descomposición $\eta = (\eta - \omega) + \omega$ satiface lo requerido. □

Esta descomposición nos da una forma de expresar integrales abelianas. En efecto si $\xi(p) = \int_{p_0}^{p} \omega$, con $\omega \in \Omega^1(X)$, podemos escribir a ω como una suma $\omega = df + \omega_2 + \omega_3$ con $\omega_2 \in II$ y $\omega_3 \in III$ (ojo, como II y III no están en suma directa esta escritura no es única). Con lo que, localmente alrededor de p_0, $\xi(p) = f(p) + \xi_2(p) + \log(g(p))$, con f y g algebraicas en X.

Ejercicios

1. Dado el siguiente teorema:

   Teorema 4.18 (Riemann)**.** *Sea X una curva algebraica irreducible proyectiva y regular y $M(X)$ el cuerpo de funciones meromorfas en X, entonces $\mathbb{K}(X) = M(X)$.*

   Mostrar que para todo par de formas η y ω existe $f \in \mathbb{K}(X)$ tal que $\eta = f\omega$.
2. Mostrar que, si $D \sim D'$ entonces $\mathcal{L}(D) \cong \mathcal{L}(D')$.
3. Probar que existe un divisor K tal que $K_X(D) \cong \mathcal{L}(K - D)$ para todo $D \in \mathrm{Div}(X)$.
4. Probar que si $\omega \in III$ entonces $\omega = rdg/g$ con $g \in \mathbb{K}(X)$, $r \in \mathbb{C}$.

5. Lo que quedó en el tintero

5.1. Curvas singulares. Dijimos al principio que la teoría de formas diferenciales en curvas surgió a partir del estudio de funciones abelianas como por ejemplo

$$\phi(z) = \int_0^z \frac{ds}{\sqrt{1 - s^4}}.$$

Esta función sería, en todo caso, la integral de una forma diferencial sobre la curva proyectiva $C(f)$ con $f = z^2y^2 - x^4$. Sin embargo $C(f)$ es una curva singular. La teoría para curvas singulares se apoya fuertemente en su contraparte para curvas no singulares, para cada curva X tenemos una curva no singular $\hat{X}$ (no necesariamente plana) y un

morfismo $\hat{X} \to X$ que llamamos *resolución de singularidades* de X. Todos los teoremas mencionados aquí se generalizan a curvas singulares y la principal herramienta para generalizarlos es estudiar la resolución de singularidades de X.

5.2. La formulación algebraica. Todos los resultados vistos aquí tienen formulaciones algebraicas que son suceptibles de ser traducidos a curvas definidas sobre cuerpos que no son necesariamente $\mathbb{C}$. Se empieza por notar que el anillo de coordenadas de una curva afín regular es un ejemplo de *dominio de Dedekind* y se desarrolla una teoría análoga con *diferenciales de Kähler* en lugar de diferenciales holomorfas. La versión puramente algebraica del teorema de Abel, sin embargo, es un poco más larga de explicar que la que vimos acá, ya que no hace uso ni de integrales de 1-formas, ni de cocientes por reticulados como $\mathbb{C}^g/\Lambda$.

5.3. Teoría de Hodge en curvas. Muchas de las generalizaciones de los resultados vistos acá para varidades algebraicas de dimensión mayor pasan por la *descomposición de Hodge* de los grupos $H^i(X, \mathbb{C})$. Si bien la teoría de Hodge en general puede ser un tema arduo, el caso particular de curvas requiere menos herramientas y es un buen ejemplo para empezar a entender la teoría más general de la topología de las variedades algebraicas.

Referencias

[1] T. Apostol, *Calculus*, Wiley **Vol.1** (1967).
[2] F. Cukierman, *Notas sobre Integrales Abelianas*, Sociedad Matemática Peruana (2008).
[3] P. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Wiley Classics Library Edition (1994).
[4] S. Kleiman *The Picard scheme*, ICTP Lecture notes.
[5] S. Lang *Abelian Varieties*, Interscience tracts in pure and applied mathematics **Vol. 7** (1958).
[6] R. Miranda, *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Mathematics **Vol. 5** (1995).
[7] D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, Grundlehren der mathematischen Wissenschaften **Vol. 221** (1995).
[8] H. Weyl, *Die Idee der Riemannsche Fläche*, Mathematische Vorlesungen an der Universität Göttingen **Vol. 5** (1923).

Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, Departamento de matemática. Ciudad Universitaria, Pabellón 1, Ciudad Autónoma de Buenos Aires.

E-mail address: fquallb@dm.ub.ar

Cursos de Nivel Avanzado

INTRODUCCIÓN A LA TEORÍA DE ELIMINACIÓN

NICOLÁS BOTBOL

RESUMEN. El objeto de estudio de estas notas es la teoría de eliminación, y en particular, nos concentraremos en estudiar resultantes. Cuando hablamos de resultantes, precisamente nos referimos a resultantes homogéneas en el espacio proyectivo, que llamaremos, resultante de Macaulay. Esta resultante surge como una generalización de la resultante de Sylvester para dos polinomios univariados.

Dado un conjunto de n polinomios homogéneos $f_1, \dots, f_n$ en n variables con coeficientes en un anillo A, introduciremos la noción de ideal eliminante, $\mathfrak{A}$ de A, que resultará bajo ciertas condiciones un ideal principal, y cuyo generador llamaremos Resultante homogénea de $f_1, \dots, f_n$. Veremos que el conjunto de ceros de $\mathfrak{A}$ en $\mathrm{Spec}(A)$ parametriza los coeficientes para los cuales los polinomios $f_1, \dots, f_n$ tienen un cero común.

Veremos además que esta resultante puede ser calculada como el determinate de un complejo de A-módulos y que además coincide con la parte en codimensión 1 de un ideal de menores maximales de una cierta matriz M, que se lo conoce como ideal inicial de Fitting de M.

ÍNDICE

2010 *Mathematics Subject Classification.* 13P15, 13P20, 13D02, 13D45, 14Q10.

Partially supported by UBACYT 20020100100242, CONICET PIP 112-200801-00483, and ANPCyT PICT 2008-0902.

Introducción

El objeto de estudio de estas notas es la teoría de eliminación, y en particular, nos concentraremos en estudiar resultantes. Cuando hablamos de resultantes, precisamente nos referimos a resultantes homogéneas en el espacio proyectivo, que llamaremos, resultante de Macaulay. Esta resultante surge como una generalización de la resultante de Sylvester para dos polinomios univariados, que repasaremos en la Sección 1.

El contexto será el siguiente: A un anillo conmutativo con unidad que se supondrá casi siempre íntegro y noetheriano, $R = A[X_1, \dots, X_n]$ el anillo de polinomios con coeficientes en A con la graduación habitual, donde $\deg(X_i) = 1$ y $\deg(a) = 0$ para todo $a \in A$ y R_+ su ideal irrelevante de elementos de grado positivo. Sea $f_1, \dots, f_n$ una sucesión regular de n polinomios homogéneos, con $\deg(f_i) = d_i > 0$, e $I = (f_1, \dots, f_n)$.

El anillo cociente $B = R/I$ es un anillo graduado, con la graduación heredada de R. El ideal homogéneo 0 de B, tiene una descomposición $0 = \mathfrak{p} \cap \mathfrak{q}$, donde $\mathfrak{q}$ es la componente R_+-primaria o componente irrelevante y $\mathfrak{p} = H^0_{R_+}(B)$ es un ideal homogéneo que se define pasando al cociente por I al ideal $\mathrm{TF}_{R_+}(I)$ de *formas de inercia* de I en R.

Escribamos $\overline{B} := B/H^0_{R_+}(B)$. Naturalmente, los subesquemas cerrados de $\mathrm{Proj}(R)$ definidos por $\mathrm{Proj}(B)$ y $\mathrm{Proj}(\overline{B})$ coinciden. Además, llamando B_ν y $\overline{B}_\nu$ a las partes homogéneas de grado ν, se tiene que $B_\nu = \overline{B}_\nu$ si ν es suficientemente grande. Precisamente, para que B_ν y $\overline{B}_\nu$ coincidan, basta encontrar un valor ν_0 tal que $H^0_{R_+}(B)_\nu = 0$ si $\nu \geq \nu_0 := \sum_i (d_i - 1) + 1$, que llamaremos índice de saturación de I (el estudio del valor ν_0 está contenido en la última parte del Apéndice B, dedicado a la regularidad de Castelnuovo-Mumford).

Como R es un anillo graduado sobre A, $\mathrm{Proj}(R)$ es un esquema proyectivo sobre $\mathrm{Spec}(A)$, y también lo es $\mathrm{Proj}(B) = \mathrm{Proj}(\overline{B})$. Llamando π a la proyección $\pi : \mathrm{Proj}(R) \to \mathrm{Spec}(A)$, así como a la proyección inducida $\pi : \mathrm{Proj}(B) \to \mathrm{Spec}(A)$, obtenemos que la imagen de $\mathrm{Proj}(B)$ por π está dada por el *ideal eliminante* $H^0_{R_+}(B) \cap A = H^0_{R_+}(B)_0$, que denotaremos por $\mathfrak{A}$. Esto será estudiado en detalle en la Sección 2, donde además probaremos el Teorema Principal de Eliminación, Teorema 2.7, que establece la relación entre el ideal de coeficientes $\mathfrak{A}$ y la existencia de ceros comunes de I para esos coeficientes.

Mejor que el ideal de eliminación $\mathfrak{A}$, es el ideal de Fitting $\mathfrak{F} := \mathrm{Fitt}_0(B_\nu)$ con $\nu \geq \nu_0$ (típicamente $\nu = \nu_0$), ya que no sólo es principal en codimensión 1, con el mismo conjunto de ceros que $\mathfrak{A}$, sino que además verifica propiedades funtoriales muy convenientes, como ser estable por cambios de base. Además, su parte de codimensión 1 y puede ser calculado mediante un producto alternado de determinantes.

Como lo señaló Jouanolou, Hurwitz demostró en 1913 (ver [Hur13]) que, en el caso de polinomios homogéneos genéricos $f_1, \ldots, f_r$ -y este será nuestro contexto- el complejo Koszul es acíclico en grados positivos si el número de polinomios r es menor o igual al número de variables n, ya que forman una sucesión regular. Desde alrededor de 1930 se sabe que las resultantes homogéneas se pueden calcular como el invariante de McRae de este complejo, y a esto es a lo que nos referíamos al decir que la parte de codimensión 1 de $\mathfrak{F} := \mathrm{Fitt}_0(B_\nu)$ con $\nu \geq \nu_0$ puede ser calculado mediante un producto alternado de determinantes, que vienen de los diferenciales de este complejo de Koszul graduado, en grado ν con $\nu \geq \nu_0$.

En la Sección 3 recordaremos la definición de este complejo, y desarrollaremos las herramientas necesarias para nuestras aplicaciones. En la Sección 4 veremos, en el Teorema 4.1 que el ideal $\mathfrak{A}$ es primo y principal y que por lo tanto define una subvariedad de $\mathrm{Spec}(A)$ de codimensión 1. Luego, probaremos que $\mathfrak{A} = \mathrm{ann}_A(B_\nu)$ si $\nu \geq \nu_0$, es decir, que es un A-módulo de torsión. Al final de esa sección, mostraremos que (con hipótesis) todo A-módulo M de torsión define un divisor $\mathrm{div}(M)$, y que dada una resolución libre de M, este divisor puede ser calculado mediante un producto alternado de determinantes. Como mencionamos, esta resolución será el complejo de Koszul de $f_1, \ldots, f_r$ en grado $\nu \geq \nu_0$. En la Sección 5 definiremos y estudiaremos los ideales de Fitting mencionados, así como el invariante de MacRae, lo que completará el estudio de la resultante de Macaulay.

Es importante entender la diferencia que estamos marcando entre los ideales $\mathfrak{A}$ y $\mathfrak{F}$: Mientras que el primero es principal e irreducible y describe la *imagen cerrada de* $\pi : \mathrm{Proj}(B) \to \mathrm{Spec}(A)$, el segundo no lo será y describe la *imagen de Fitting de* π, pero el divisor asociado a $\mathfrak{F}$ coincide con $\mathfrak{A}$ lo cual dice que la parte en codimensión 1 de $V(\mathfrak{F})$ coincide con $V(\mathfrak{A})$, y en particular como conjuntos también coinciden.

Como ya se dijo, a lo largo de estas notas, estudiaremos la relación y propidades de estos dos ideales, ya que, como mencionamos, el primero es más intuitivo geométricamente, pero el segundo presenta mejores propiedades algebraicas. Un estudio más detallado sobre imágenes cerradas e imágenes de Fitting se puede encontrar en [EH00, Cap. V].

Notación. En estas notas, los anillos serán todos conmutativos y con unidad, éstas son hipótesis habituales en el área, aunque parte de la teoría pueda desarrollarse sin ellas.

Cuando llamemos A a un anillo, en general estaremos pensando en que A es el anillo de coeficientes universales $\mathbb{Z}[\{U_{i,\alpha}\}]$ o un anillo de coeficientes arbitrario, pero esto es simplemente una intuición que debería ayudar al lector a entender la geometría de fondo. En general A no será provisto de una graduación, y por lo tanto el esquema que le asociaremos será $\mathrm{Spec}(A)$. Cuando querramos indicar que A es un cuerpo, comúnmente escribiremos k en lugar de A.

El anillo R, por lo general será un anillo de polinomios en n variables X_i, con coeficientes en A o en k. Nos interesará dotar a R de la graduación habitual, donde $\deg(X_i) = 1$ y $\deg(a) = 0$ para todo $a \in A$. Esta graduación nos permitirá definir en R el ideal maximar irrelevante de elementos de grado positivos $R_+ := (X_1, \ldots, X_n)$ y geométricamnte le asociamos a R el esquema proyectivo $\mathrm{Proj}(R)$ que se escribe $\mathbb{P}^{n-1}_A$ o $\mathbb{P}^{n-1}_k$ según corresponda.

Notaremos con $f_1, \ldots, f_r$ al conjunto de R polinomios homogéneos, en n variables X_i, con coeficientes en A, es decir, elementos homogéneos de R. Típicamente f_i tendrá

grado d_i, es decir, $f_i \in R_{d_i}$. Estudiaremos principalmente el caso en que $r = n$, y que forman una sucesión regular en R. Esto dice que el cociente $B := R/I$ es una intersección completa.

Frecuentemente escribiremos,

$$f_i = \sum_{|\alpha|=d_i} u_{\alpha,i} X^\alpha$$

con $u_{\alpha,i} \in A$, $\alpha = (\alpha_0, \dots, \alpha_n)$, $|\alpha| = \alpha_0 + \cdots + \alpha_n$, $X^\alpha = X_0^{\alpha_0} \cdots X_n^{\alpha_n}$ y $f_{\alpha,i} \in A$ para todo α y todo i. También nos permitiremos reemplzar las $u_{\alpha,i}$ por $U_{\alpha,i}$, cuando querramos indicar que son variables. Es decir, la diferencia radica en que en el primer caso tenderíamos a creer que están especializadas y que A es un anillo de coeficientes cualquiera, mientras que en el segundo no lo están y $A = \mathbb{Z}[\{U_{i,\alpha}\}]$ es el anillo de coeficintes universales.

En cualquier caso, escribamos $I := (f_1, \dots, f_r) \subset R_+$, ideal homogéneo de R, y $B := R/I$. Como I es homogéneo, B es un R-módulo graduado, con la graduación heredada de R. Escribiremos $\mathrm{Proj}(B)$ para denotar el subesquema de $\mathrm{Proj}(R)$ definido por I, que comúnmente se escribe $V(I)$.

Más en general, dado un ideal J de un anillo S, escribiremos $V(J)$ par denotar $\mathrm{Spec}(S/J)$. También, si S fuera un anillo graduado estándar y J homogéneo, $V(J)$ podrá denotar $\mathrm{Proj}(S/J)$. Esta notación es habitual y hace referencia a la intuición de pensar $V(J)$ como una subvariedad del espacio afín o proyectivo asociado al anillo de polinomios S definida por "los ceros" de f, donde f recorre todos los elementos de J.

1. Resultante univariada

En esta primera parte, estudiaremos la resultante de dos polinomios univariados y de dos polinomios homogéneos en dos variables. Esta teoría clásica que data del siglo XIX nos permitirá comprender con facilidad el contexto geométrico y algebraico de la teoría de eliminación general, así como de remarcar el caracter universal de la resultante.

1.1. Definición. Sea A un anillo conmutativo con unidad. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Escribamos

$$f_1(X) = \sum_{i=0}^{d_1} a_i X^i, \text{ y } f_2(X) = \sum_{i=0}^{d_2} b_i X^i. \tag{1.1}$$

A estos dos polinomios les asociamos la matriz Sylvester definida como sigue.

Definición 1.1. Sean A un anillo conmutativo con unidad, $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$, como en (1.1). La matriz

$$\mathrm{Syl}(f_1, f_2) = \begin{pmatrix} a_{d_1} & 0 & \cdots & 0 & b_{d_2} & 0 & \cdots & 0 \\ a_{d_1-1} & a_{d_1} & & \vdots & \vdots & b_{d_2} & & \vdots \\ \vdots & a_{d_1-1} & \ddots & 0 & b_0 & \vdots & \ddots & \\ a_0 & \vdots & & a_{d_1} & 0 & b_0 & & 0 \\ 0 & a_0 & & a_{d_1-1} & \vdots & 0 & \ddots & b_{d_2} \\ \vdots & & \ddots & \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

de $(d_1 + d_2) \times (d_1 + d_2)$ con coeficientes en A, se llama *matriz de Sylvester* de f_1, f_2.

Definición 1.2. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Definimos la *Resultante de Sylvester* de f_1, f_2, como

$$\mathrm{Res}_X(f_1, f_2) = \det(\mathrm{Syl}(f_1, f_2))$$

1.2. Propiedades elementales. Los polinomios f_1, f_2 definen un morfismo de A-módulos

$$\begin{array}{ccc} A[X]_{<d_2} \oplus A[X]_{<d_1} & \xrightarrow{\partial} & A[X]_{<d_1+d_2} \\ (h_1, h_2) & \mapsto & h_1 f_1 + h_2 f_2 \end{array} \tag{1.2}$$

En estos términos, la Proposición 1.3 dice que $\mathrm{Res}_X(f_1, f_2) \in \mathrm{im}(\partial)$. Además, es fácil ver que la matriz de ∂ en bases canónicas coincide con la matriz $\mathrm{Syl}(f_1, f_2)$ (ver ejercicio 2).

Proposición 1.3. *Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Entonces, existen dos polinomios h_1, h_2 tales que $\deg(h_i) < d_i$, $i = 1, 2$ y $\mathrm{Res}_X(f_1, f_2) = f_1 h_1 + f_2 h_2 \in A[X]$.*

Demostración. Es inmediato verificar que se tiene la siguiente igualdad de vectores

$$(X^{d_1+d_2-1}, X^{d_1+d_2-1}, \ldots, X, 1)\,\mathrm{Syl}(f_1, f_2) = (X^{d_2} f_1, \ldots, X f_1, f_1, X^{d_1} f_2, \ldots, X f_2, f_2)$$

Desarrollando la regla de Cramer se tiene que

$$\mathrm{Res}_X(f_1, f_2) \cdot 1 = \det M,$$

donde M es la matriz que se obtiene a partir de $\mathrm{Syl}(f_1, f_2)$ reemplazando la última fila por el vector $(X^{d_2} f_1, \ldots, X f_1, f_1, X^{d_1} f_2, \ldots, X f_2, f_2)$.

Calculando $\det(M)$ por la última fila, se tiene lo buscado. □

Para polinomios sobre un anillo íntegro, se tiene el sigueinte resultado, que es una de las motivaciones principales para el estudio de las resultantes.

Proposición 1.4. *Sea A un anillo íntegro con cuerpo de fracciones K. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$ y sea ∂ un morfismo de A-módulos como en (1.2). Entonces son equivalentes*

1. *∂ es inyectivo,*
2. *$\mathrm{Res}_X(f_1, f_2) \neq 0$,*
3. *f_1 y f_2 son coprimos en $K[X]$.*

Demostración. La equivalencia entre los puntos 1. y 2. se desprende del Ejercicio 3. Para ver que 1. y 3. son equivalentes, supongamos primero que f_1 y f_2 son coprimos en $K[X]$, y que existen polinomios h_1 y h_2 tales que $\deg(h_i) < d_i$, $i = 1, 2$, y $\partial(h_1, h_2) = 0$. Esto último dice que $h_1 f_1 = -h_2 f_2$, y entonces, $f_1 | h_2$ y $f_2 | h_1$, de lo cual se deduce, observando los grados, que $h_1 = h_2 = 0$. Si f_1 y f_2 no son coprimos en $K[X]$, entonces existe un polinomio h de grado positivo tal que $f_i = h g_i$, con $\deg(g_i) < \deg(f_i) = d_i$, $i = 1, 2$. Sea $d \in A$ el producto de los denominadores de g_1 y g_2. La no-inyectividad de ∂ se defuce del hecho que $0 = d(f_2 f_1 - f_1 f_2) = h(g_2 f_1 - g_1 f_2)$, es decir de que $0 \neq (g_2, -g_1) \in \ker(\partial)$. □

Como consecuencia de esto se tiene que $\mathrm{Res}_X(f_1, f_2) \neq 0$ si y solo si f_1 y f_2 tienen una raíz común en una extensión algebraica de K (ver Ejercicios 4 y 5).

Si introducimos una nueva variable Y para homogeneizar a los polinomios f_1, f_2, podemos definir la resultante homogénea de dos polinomios homogéneos bivaluados de la siguiente forma:

Definición 1.5. Sean $f_1, f_2 \in A[X,Y]$ dos polinomios homogeéneos de grado $d_1, d_2 > 0$. Definimos

$$\mathrm{Res}_{X,Y}(f_1(X,Y), f_2(X,Y)) := \mathrm{Res}_X(f_1(X,1), f_2(X,1)).$$

1.3. La universalidad de la resultante. Una de las propiedades más importantes de la resultante, es su carácter universal. Para ello, escribamos

$$f_1(X) = \sum_{i=0}^{d_1} a_i X^i, \text{ y } f_2(X) = \sum_{i=0}^{d_2} b_i X^i, \tag{1.3}$$

y sea $A = \mathbb{Z}[a_0, \dots, a_{d_1}, b_0, \dots, b_{d_2}]$ el anillo de polinomios en $d_1 + d_2 + 2$ variables, llamado *anillo de coeficientes universales* de f_1, f_2. Sea k un anillo conmutativo con unidad, y $\epsilon : A \to k$ un morfismo de anillos que se extiende a $\epsilon : A[X] \to k[X]$ poniendo $\epsilon(X) = X$.

Considere el siguiente diagrama:

$$\begin{array}{ccc} A[X] \times A[X] & \xrightarrow{\mathrm{Res}_X} & A \\ \downarrow{\scriptstyle \epsilon\times\epsilon} & & \downarrow{\scriptstyle \epsilon} \\ k[X] \times k[X] & \xrightarrow{\mathrm{Res}_X} & k \end{array} \tag{1.4}$$

La universalidad de la resultante se traduce a decir que el diagrama (1.4) conmuta, es decir que, dados dos polinomios $f_1, f_2 \in A[X]$ como en (1.3)

$$\mathrm{Res}_X(\epsilon(f_1), \epsilon(f_2)) = \epsilon\,\mathrm{Res}_X(f_1, f_2) \in k.$$

Esta propiedad de la resultante es una de las propiedades principales que desearemos conservar al extender la teoría al contexto multivaluado.

La intuición detrás de esta propiedad esencial es que una especialización de coeficientes corresponde a un morfismo de evaluación $\epsilon : A \to k$. Por ejemplo, si $\mathfrak{p}$ es un primo de A, podemos considerar el morfismo $\epsilon_{\mathfrak{p}}$ que resulta de la composición $A \to A_{\mathfrak{p}} \to \kappa(\mathfrak{p}) := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, donde el primero es el morfismo inyectivo de localización en $\mathfrak{p}$ y el segundo es pasar al cociente por el único ideal maximal de $A_{\mathfrak{p}}$. El morfismo $\epsilon_{\mathfrak{p}}$ corresponde a "una evalución". Esto es claro si $\mathfrak{p} = \mathfrak{m}$ es maximal, ya que en ese caso $\kappa(\mathfrak{m}) := A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} = A/\mathfrak{m}$. Interpretamos geométricamente al morfismo $\epsilon_{\mathfrak{p}}$ como la inclusión del punto $\mathrm{Spec}(\kappa(\mathfrak{p}))$ en $\mathrm{Spec}(A)$.

Gracias a esta universalidad, podremos concentrarnos en estudiar las propiedades de la resultante sobre el anillo de coeficientes universales $\mathbb{Z}[\{U_{i,\alpha}\}]$, y luego deducir propiedades en otros contextos mediante un cambio de base (o aplicando un morfismo de evaluación ϵ).

Ejercicios.

1. Sean $f_1, f_2 \in A[X]$ dos polinomios de grado $d_1, d_2 > 0$. Entonces $\mathrm{Res}_X(f_1, f_2) = (-1)^{d_1 d_2}\,\mathrm{Res}_X(f_2, f_1)$.
2. Probar que la matriz de ∂ definida en (1.2) en bases canónicas coincide con la matriz $\mathrm{Syl}(f_1, f_2)$ y deducir que $\mathrm{Res}_X(f_1, f_2) \in \mathrm{im}(\partial)$. Comparar con la Proposición 1.3.
3. Sea $\partial : A^n \to A^n$ un morfismo de A-módulos. Sea M la matriz de ∂ en dos bases cualesquiera de A^n. Entonces ∂ es inyectivo sii $\det(M) \neq 0$.
4. Sea A un anillo íntegro con cuerpo de fracciones K y sean $f_1, f_2 \in A[X]$. Entonces $\mathrm{Res}_X(f_1, f_2) \neq 0$ si y solo si f_1 y f_2 tienen una raíz común en una extensión algebraica de k.

5. Sea k un cuerpo y $f_1, f_2 \in k[X]$. Entonces, $\dim_k \ker \mathrm{Syl}(f_1, f_2) = \deg(\gcd(f_1, f_2))$

2. Teoría de Eliminación

En esta sección demostraremos el Teorema Principal de la Teoría de eliminación. Éste puede formularse en un lenguaje geométrico, como haremos en la primera parte, y en uno más algebraico como haremos más adelante. En la Sección 4 relacionaremos estos resultados con lo que llamaremos la resultante homogénea o resultante de Macaulay.

Sea A un anillo (conmutativo con unidad). Consideremos el anillo de polinomios $R := A[X_1, \ldots, X_n]$, con la $\mathbb{Z}$-graduación dada por $\deg(X_i) = 1$ para todo i y $\deg(a) = 0$ para todo $a \in A$, y escribamos $R_+ := (X_1, \ldots, X_n)$ el ideal irrelevante de R.

Sean $f_1, \ldots, f_r$ elementos homogéneos de R, con $\deg(f_i) = d_i$ para todo i. Concretamente, cada f_i se escribe de la forma

$$f_i = \sum_{|\alpha|=d_i} u_{\alpha,i} X^\alpha$$

con $u_{\alpha,i} \in A$, $\alpha = (\alpha_0, \ldots, \alpha_n)$, $|\alpha| = \alpha_0 + \cdots + \alpha_n$, $X^\alpha = X_0^{\alpha_0} \cdots X_n^{\alpha_n}$ y $f_{\alpha,i} \in A$ para todo α y todo i.

Escribamos $I := (f_1, \ldots, f_r) \subset R_+$, ideal de R, y $B := R/I$. Como I es homogéneo, B es un R-módulo graduado, con la graduación heredada de R.

Antes de continuar, permitámosnos observar algunas propiedades del anillo cociente B que serán de utilidad.

Observación 2.1. Sea $B := R/I$ el anillo graduado, con $B_d = R_d/(I \cap R_d)$. Se tiene que

1. Como $I \cap A = 0$, entonces $B_0 = A$.
2. B está generado como anillo por A y B_1.
3. Para todo entero no-negativo d, B_d es un A-módulo finitamente generado.

Trabajaremos, frecuentemente en el contexto universal, es decir, supondremos que los coeficientes $u_{\alpha,i}$ son variables, que notaremos $U_{\alpha,i}$, y el anillo A será el anillo, $A := \mathbb{Z}[U_{\alpha,i} : i = 1, \ldots, r, |\alpha| = d_i]$, de *coeficientes universales* de los polinomios f_i.

2.1. El Teorema Principal de Eliminación geométricamente. Obsérvese que los elementos f_i son polinomios en las variables X_j, con coeficientes en A, con los cual A puede ser pensado como el anillo de coeficientes que parametriza al sistema $\{f_1 = \cdots = f_n = 0\}$, del cual queremos eliminar las variables X_j's.

Desde un punto de vista geométrico, siendo B un anillo graduado con coeficientes en A, se tiene que:

$$\mathrm{Proj}(B) \hookrightarrow \mathrm{Proj}(R) := \mathbb{P}_A^{n-1} = \mathbb{P}_{\mathbb{Z}}^{n-1} \times \mathrm{Spec}(A).$$

Esta inclusión de esquemas está inducida por el morfismo suryectivo de anillos $R \to B$ que consiste en pasar al cociente por I.

Asociado al espacio $\mathbb{P}_A^{n-1}$ hay una proyección natural $\pi : \mathbb{P}_A^{n-1} \to \mathrm{Spec}(A)$. La restricción de π a $\mathrm{Proj}(B)$, $\pi : \mathrm{Proj}(B) \to \mathrm{Spec}(A)$ define un subesquema (cerrado) de $\mathrm{Spec}(A)$, $Z := \pi(\mathrm{Proj}(B))$. El ideal de definición de Z en $\mathrm{Spec}(A)$, que notaremos $\mathfrak{A}$,

está dado por el núcleo del morfismo natural de anillos asociado a la proyección π, es decir:

$$\begin{aligned}\mathfrak{A} &:= \ker(A \to \Gamma(\mathrm{Proj}(B), \mathcal{O}_{\mathrm{Proj}(B)})) = \ker(A \to \prod_i B_{(X_i)}) \\ &= (I :_R (R_+)^\infty) \cap A = H^0_{R_+}(B)_0.\end{aligned}$$

La primera igualdad se deduce de que cada sección $s \in \Gamma(\mathrm{Proj}(B), \mathcal{O}_{\mathrm{Proj}(B)})$ está unívocamente determinada por sus restricciones a cada abierto afin $D^+(X_i) = \mathrm{Spec}(B_{(X_i)})$. La segunda y tercera igualdad es simplemente observar que

$$H^0_{R_+}(B) := \bigcup_{\ell \geq 1} (0 :_B (R_+)^\ell) = \ker(B \to \prod_i B_{(X_i)})$$

y que A se incluye en B en grado cero, es decir, que

$$\ker(A \to \prod_i B_{(X_i)}) = \ker(B \to \prod_i B_{(X_i)}) \cap A = H^0_{R_+}(B)_0.$$

A partir del razonamiento anterior concluimos que el proceso de eliminación consiste en calcular $H^0_{R_+}(B)_0$. Es interesante notar que $H^0_{R_+}(B) = (I :_R (R_+)^\ell)/I = I^{\mathrm{sat}}/I$, donde I^{sat} es la saturación de I respecto del ideal irrelevante R_+. El lector más familiarizado con la teoría de esquemas, podrá observar que los anillos B y $B/H^0_{R_+}(B)$ definen el mismo subesquema proyectivo de $\mathbb{P}^{n-1}_A$.

Definición 2.2. Definimos el *ideal eliminante de I* como

$$\mathfrak{A} := H^0_{R_+}(B)_0 = (I :_A (R_+)^\infty).$$

Si A es el anillo de polinomios $k[U_1, \ldots, U_m]$, $\mathrm{Spec}(A) = \mathbb{A}^m_k$ el espacio afín de dimesnión m sobre k. Sea $\mathbb{P}^{n-1}_k$ el espacio proyectivo de dimensión n sobre k. El espacio producto $\mathbb{P}^{n-1}_k \times \mathbb{A}^m_k$, viene provisto de sus dos proyecciones naturales, y nos centraremos en estudiar la proyección respecto de la segunda coordenada, que llamaremos π, definida como $\pi(x, y) = y \in \mathbb{A}^m_k$. Sea

$$W := \{(x, y) \in \mathbb{P}^{n-1}_k \times \mathbb{A}^m_k : f_i(x, y) = 0,\ \forall i\}$$

un subconjunto de $\mathbb{P}^{n-1}_k \times \mathbb{A}^m_k$.

Lo anteriormente dicho demuestra el siguiente resultado:

Corolario 2.3. *Con la notación precedente, se tiene que*

$$\pi(W) = V(\mathfrak{A}).$$

En la subsección siguiente daremos una herramienta necesaria para calcular un (el) generador del ideal eliminante $\mathfrak{A}$.

2.2. Sobre la R_+-torsión de B. Pasaremos ahora a dar una interpretación del ideal $\mathfrak{A}$ en término de anuladores.

Lema 2.4. *Se tiene la siguiente igualdad de ideales de A*

$$\mathfrak{A} := H^0_{R_+}(B)_0 = \bigcup_{\ell \geq 1} \mathrm{ann}_A(B_\ell).$$

Demostración. Para cada par $(\nu, \ell) \in \mathbb{Z}^2_{\geq 0}$, definimos el morfismo A-lineal

$$\Theta_{\nu,\ell} : B_\nu \to \mathrm{Hom}_A(B_\ell, B_{\nu+\ell})$$

definido por $\Theta_{\nu,\ell}(b) = (c \mapsto c \cdot b)$, con $b \in B_\nu$, $c \in B_\ell$ y $c \cdot b \in B_{\nu+\ell}$.

Como $H^0_{R_+}(B) := \bigcup_{\ell \geq 1}(0 :_B (R_+)^\ell)$, se tiene que para cada $\nu \geq 1$,

$$H^0_{R_+}(B)_\nu = \bigcup_{\ell \geq 1} \ker(\Theta_{\nu,\ell}). \tag{2.1}$$

Como $I \subset R_+$, entonces $A \cap I = 0$ y por lo tanto $B_0 = A$, con lo cual

$$\mathrm{ann}_A(B_\ell) = \ker(\Theta_{0,\ell}) \text{ para todo } \ell \geq 0. \tag{2.2}$$

A partir de (2.1) y (2.2) se tiene que $H^0_{R_+}(B)_0 = \bigcup_{\ell \geq 1} \mathrm{ann}_A(B_\ell)$. □

Obsérvese que como B está generado en grado 1 como se mencionó en la Observación 2.1, el morfismo de multiplicación $B_1 \otimes B_\ell \to B_{\ell+1} : c_1 \otimes c_\ell \mapsto c_1 c_\ell$ es suryectivo, y todo elemento $c \in B_{\ell+1}$ puede ser descompuesto como $c = \sum_i c_1^i \otimes c_\ell^i$. Con la notación del Lema 2.4 , dado $b \in \ker(\Theta_{\nu,\ell})$ se tiene que $bc = b(\sum_i c_1^i \otimes c_\ell^i) = \sum_i c_1^i \otimes bc_\ell^i = 0$ en $B_{\nu+\ell+1}$ y por lo tanto, se tiene para cada $(\nu, \ell) \in \mathbb{Z}^2_{\geq 0}$ la inclusión

$$\ker(\Theta_{\nu,\ell}) \subset \ker(\Theta_{\nu,\ell+1}).$$

Esto dice que $\mathrm{ann}_A(B_\ell) \subset \mathrm{ann}_A(B_{\ell+1})$ para todo $\ell \geq 0$, y por lo tanto $H^0_{R_+}(B)_0$ puede ser calculado mediante el colímite filtrante $\varinjlim_\ell \mathrm{ann}_A(B_\ell)$.

Una pregunta que surge en este punto es ¿Existe un valor de ℓ a partir del cual esta cadena ascendiente de anuladores se estaciona? ¿Cuál?

El siguiente resultado responde la primera pregunta, el Lema B.4 responde a la segunda cuando I está generado por una sucesión regular.

Lema 2.5. *Sea $\nu_0 \geq 0$ un entero tal que $H^0_{R_+}(B)_{\nu_0} = 0$. Entonces, para todo entero $\ell \geq 0$ se tiene que*

$$\mathrm{ann}_A(B_{\nu_0}) = \mathrm{ann}_A(B_{\nu_0+\ell}).$$

Demostración. A partir de (2.1), con la notación del Lema 2.4 y la hipótesis sobre ν_0, se tiene que

$$0 = H^0_{R_+}(B)_{\nu_0} = \bigcup_{\ell \geq 1} \ker(\Theta_{\nu_0,\ell}),$$

de lo se obtiene que $\ker(\Theta_{\nu_0,\ell}) = 0$ para todo $\ell \geq 1$. Repitiendo los argumentos anteriores, se tiene que si $a \in \mathrm{ann}_A(B_{\nu_0+\ell})$ entonces $aB_{\nu_0} \subset \ker(\Theta_{\nu_0,\ell}) = 0$ para todo $\ell \geq 0$. Luego $aB_{\nu_0} = 0$ y se concluye que $a \in \mathrm{ann}_A(B_{\nu_0})$. □

Obsérvese que un tal entero $\nu_0 \geq 0$ tal que $H^0_{R_+}(B)$ siempre existe ya que $H^0_{R_+}(B)$ es un R-módulo de torsión (ver Ejercicio 2) y será estudiado en el Lema B.4 cuando I está generado por una sucesión regular.

El lema anterior prueba que una vez alcanzado un entero ν_0 para el cual $H^0_{R_+}(B)_{\nu_0} = 0$, entonces el ideal eliminante $\mathfrak{A}$ puede ser calculado como $\mathrm{ann}_A(B_{\nu_0})$, y lo resumimos en el siguiente corolario. Un tal entero ν_0 se llama *índice de saturación de I*, ya que $I^{\mathrm{sat}}_{\nu_0} = I_{\nu_0}$.

Corolario 2.6. *Sea $\nu_0 \geq 0$ un entero tal que $I^{\mathrm{sat}}_{\nu_0} = I_{\nu_0}$. Entonces,*

$$\mathfrak{A} = \mathrm{ann}_A(B_{\nu_0}).$$

2.3. El Teorema Principal de eliminación. Recordemos que el Lema 2.4 nos permitía escribir al ideal eliminante $\mathfrak{A}$ en término de anuladores, de la siguiente forma

$$\mathfrak{A} := H^0_{R_+}(B)_0 = \bigcup_{\ell \geq 1} \operatorname{ann}_A(B_\ell).$$

Es fácil ver que el ideal $\mathfrak{A}$ también puede ser escrito como sigue

$$\mathfrak{A} = \{f \in A : fX_i^\ell \in I, \text{ para todo } i \text{ y algún } \ell \geq 1\}. \tag{2.3}$$

El siguiente resultado es conocido como Teorema Principal de Eliminación y constituye el resultado principal de esta sección.

Teorema 2.7 (de Eliminación)**.** *Sea A un anillo conmutativo, $R := A[X_1, \ldots, X_n]$, $I \subset R_+$ un ideal homogéneo de R, $\mathfrak{A}$ su ideal eliminante, k un cuerpo y $\rho : A \to k$ un morfismo de anillos. Entonces $\rho(\mathfrak{A}) = 0$ sii existe un cero no-trivial de I en $\overline{k}$.*

Para demostrar el teorema anterior, haremos uso del siguiente lema:

Lema 2.8. *Sea A un anillo conmutativo, M un A-módulo de tipo finito, k un cuerpo y $\rho : A \to k$ un morfismo de anillos. Entonces, $M \otimes_A k \neq 0$ sii $\rho(\operatorname{ann}_A(M)) = 0$.*

Demostración. Si existe un elemento $a \in \operatorname{ann}_A(M)$ tal que $\rho(a) \in \rho(\operatorname{ann}_A(M))$ es no nulo en k, entonces $\rho(a)$ anula $M \otimes_A k$ ya que a anula a M. Como $M \otimes_A k$ es un k-espacio vectorial, entonces no tiene torsión, entonces debería ser $M \otimes_A k = 0$.

Veamos que si $M \otimes_A k \neq 0$ entonces $\rho(\operatorname{ann}_A(M)) = 0$. Para ello, supongamos que $M \otimes_A k \neq 0$. Como M es de tipo finito, existe una sucesión exacta de la forma

$$0 \longrightarrow K \xrightarrow{\iota} A^p \xrightarrow{\pi} M \longrightarrow 0.$$

Tensorizando por k se obtiene la sucesión exacta

$$K \otimes_A k \xrightarrow{\iota \otimes id_k} k^p \longrightarrow M \otimes_A k \longrightarrow 0.$$

El hecho de que $M \otimes_A k \neq 0$ dice que $\iota \otimes id_k : K \otimes_A k \to k^p$ es suryectiva. Luego, existen elementos $a_1, \ldots, a_p \in K$ tales que la familia $\{\iota(a_1) \otimes_a k, \ldots, \iota(a_p) \otimes_a k\}$ es una base de k^p. Sea $[a] = [a_1 | \cdots | a_p] \in \operatorname{Mat}_{p,p}(A)$ la matriz de multiplicación por $a_1, \ldots, a_p$ en base canónica. La observación anterior nos dice que $\rho([a])$ es una matriz inversible, y que por lo tanto $\det(\rho([a])) \neq 0$, y como ρ es morfismo, $\det([a]) \neq 0$. El Ejercicio 3 dice que $\det([a])A^p \subset K$ y por lo tanto, $0 \neq \det([a]) \in \operatorname{ann}_A(M)$, lo cual prueba que $\operatorname{ann}_A(M) \neq 0$. □

Estamos ahora en condiciones de demostrar el Teorema 2.7.

Demostración del Teorema 2.7. Supongamos que existe $0 \neq \zeta \in \overline{k}^n$, que es un cero común de I, es decir, $\rho(f)(\zeta) = 0$ en $k \subset \overline{k}$ para todo $f \in I$. Sea $f \in \mathfrak{A}$, como vimos en (2.3) se tiene que $fX_i^\ell \in I$, para todo i y algún $\ell \geq 1$. En particular, se tiene que

$$\rho(fX_i^\ell)(\zeta) = (\rho(f)X_i^\ell)(\zeta) = \rho(f)\zeta_i^\ell = 0.$$

Como $\zeta \neq 0$, existe un i tal que $\zeta_i \neq 0$, de lo cual se deduce que $\rho(f) = 0$. Esto prueba que $\rho(\mathfrak{A}) = 0$.

Supongamos ahora que $\rho(\mathfrak{A}) = 0$, y consideremos $B = R/I$. Recordemos que (por la Observación 2.1) B es graduado con B_d finitamente generado como A-módulo para cada d y B como anillo está generado por A y B_1. Además, se tiene que la multiplicación

$$B_1 \otimes_A B_d \to B_{d+1} : b \otimes b' \mapsto bb'$$

es suryectiva. El Lema 2.4 dice que $\mathfrak{A} = \bigcup_{\ell\geq 1} \operatorname{ann}_A(B_\ell)$, y entonces para $d \geq 1$, $\operatorname{ann}_A(B_d) = 0$, y por lo tanto $\rho(\operatorname{ann}_A(B_d)) = 0$. Aplicando el Lema 2.8 con $M = \operatorname{ann}_A(B_d)$ se tiene que $B_d \otimes_A k \neq 0$.

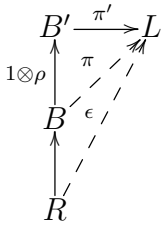
Tensorizando B con k sobre A se tiene $B' := B \otimes_A k$, que es graduado y que verifica que $B'_0 = k$ y que B'_d es un k espacio vectorial no nulo de dimensión finita. Además B'_1 está generado por $\{x_1, \ldots, x_n\}$, siendo x_i la clase de X_i en B', y el morfismo de multiplicación $B'_1 \otimes_A B'_d \to B'_{d+1} : b \otimes b' \mapsto bb'$ es suryectivo. De esta forma, si existiera un entero ℓ tal que $x_i^\ell = 0$ en B' para todo i, se tendría que $B'_d = 0$ para todo $d \geq n(\ell - 1) + 1$, lo que contradiría la no nulidad de B'_d.

Esto dice que existe un elemento $\zeta \in B'_1$ tal que $0 \neq \zeta^d \in B'_d$ para todo $d \geq 1$.

Supongamos que $1 - \zeta \in B'$ fuera inversible, es decir, que existe $\sigma \in B'$ tal que $(1 - \zeta)\sigma = 1$ y $\sigma = \sum_{i=0}^m \sigma_i$, con $\sigma_i \in B'_i$. Desarrollando se tiene que $\sigma_0 + \sum_{i=1}^m (\sigma_i - \zeta\sigma_{i-1}) - \zeta\sigma_m$, lo cual prueba que $\sigma_0 = 1$, $\sigma_i = \zeta\sigma_{i-1}$ es decir que $\sigma_i = \zeta^i$ para $i = 1, \ldots m - 1$, y que $\zeta^{m+1} = 0$, lo cual es absurdo. Esto prueba que $1 - \zeta \in B'$ no es inversible en B'.

Como $1 - \zeta \in B'$ no es inversible en B', existe un ideal maximal $\mathfrak{m}$ que lo contiene. Sea $L = B'/\mathfrak{m}$ el cuerpo cociente y $\pi' : B' \to L$ la proyección natural. Claramente $(\zeta) = 1$, y la restricción de π' a $B'_0 = k$ da un morfismo natural $\iota : k \hookrightarrow L \subset \overline{k}$.

El diagrama conmutativo



muestra que el morfismo π' se levanta a un mofismo π, que a su vez se levanta a un morfismo ϵ. El morfismo $\epsilon : R \to L \subset \overline{k}$ satisface que $\epsilon(X_i) = \pi'(x_i)$. Definiendo $\zeta_i := \epsilon(X_i) \in L$, se tiene que $(\zeta_1, \ldots, \zeta_n) \in \overline{k}^n$, y que $f(\zeta_1, \ldots, \zeta_n) = 0$ para todo $f \in I$. □

Ejercicios.

1. Sea R un anillo conmutativo, sea I un ideal de R y M un R-módulo. Entonces $(0 :_M I^\ell) = \operatorname{Hom}_R(R/I^\ell, M)$.
2. Sea R un anillo graduado y M un R-módulo de R_+-torsión. Entonces, existe un entero ν_0 tal que $H^0_{R_+}(M)_\nu = 0$ para todo $\nu \geq \nu_0$.
3. En el contexto de la demostración del Lema 2.8, pruebe que $\det([a])A^p \subset K$.

3. El complejo de Koszul

El complejo de Koszul fue primeramente introducido por Jean-Louis Koszul para definir una teoría de cohomología para álgebras de Lie, y resultó ser una construcción homológica muy valiosa para el álgebra conmutativa.

En esta sección, supondremos que R es un anillo conmutativo, con unidad (y no necesariamente noetheriano ni local por ahora). Sea M un R-módulo.

Si y es un elemento de R, entonces el endomorfismo de R-módulos, multiplicar por y (que se denotará con y), nos da un complejo: $\mathbf{K}_\bullet(y) : 0 \to R \xrightarrow{y} R \to 0$, que resulta ser el complejo de Koszul asociado a y.

Este caso simple ilustra dos propiedades importantes del complejo de Koszul. Si se indexa con la posición cero a la copia de R que está a la derecha y con uno a la que está a la izquierda, se puede observar que la homología en lugar cero es la imagen homomórfica de R módulo los múltiplos de y. Mientras que la homología en primer lugar representa el anulador del elemento y. Es decir: $H_1(\mathbf{K}_\bullet(y)) = \operatorname{ann}(\{y\})$ y $H_0(\mathbf{K}_\bullet(y)) = R/R(y)$.

Supóngase ahora que se tienen dos elementos x, y en R, considérese la sucesión (ordenada) x, y, que se puede pensar como un vector en R^2. Se construye el complejo de Koszul, $\mathbf{K}_\bullet(x, y)$, asociado a la sucesión x, y, de la siguiente forma:

$$\mathbf{K}_\bullet(x,y): \quad 0 \to R \xrightarrow{\partial_1} R^2 \xrightarrow{\partial_0} R \to 0.$$

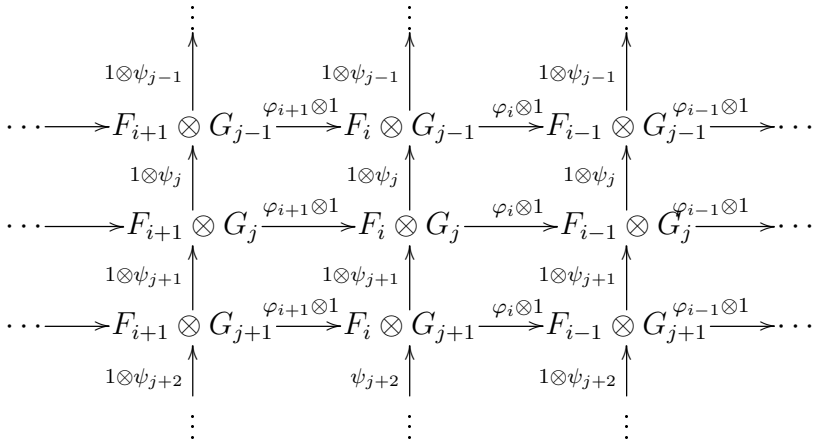
Donde los morfismos ∂_0 y ∂_1 son tales que ∂_0 es la matriz vertical $(x, y)^t$ y ∂_1 es la matriz horizontal $(-y, x)$. La condición $(x, y)^t \cdot (-y, x) = 0$ dice que $\mathbf{K}_\bullet(x, y)$ resulta ser un complejo.

Más generalmente, dados elementos $x_1, \ldots, x_n$ del anillo R, se construye el complejo de Koszul asociado a la sucesión (importa el orden) $x_1, \ldots, x_n$, denotado por $\mathbf{K}_\bullet(x_1, \ldots, x_n)$, como el producto tensorial en la categoría de R-complejos de los complejos $\mathbf{K}_\bullet(x_i)$, para cada i. Asumiremos ahora que los productos tensoriales, y las construcciones de álgebras simétricas y exteriores son como R-módulos.

Recordemos que el producto tensorial de complejos se define de la siguiente forma: Dados $\mathbf{F}_\bullet$ y $\mathbf{G}_\bullet$ dos complejos de cadenas de R-módulos, acotados inferiormente.

$$\mathbf{F}_\bullet: \quad \cdots \to F_i \xrightarrow{\varphi_i} F_{i-1} \xrightarrow{\varphi_{i-1}} \cdots, \text{ y } \mathbf{G}_\bullet: \quad \cdots \to G_i \xrightarrow{\psi_i} G_{i-1} \xrightarrow{\psi_{i-1}} \cdots.$$

Se tiene el siguiente diagrama asociado al producto tensorial:



El complejo total asociado a este complejo doble se lo llama complejo producto tensorial de $\mathbf{F}_\bullet$ y $\mathbf{G}_\bullet$ y se lo escribe $\mathbf{F}_\bullet \otimes_R \mathbf{G}_\bullet$: $\cdots \xrightarrow{\phi_{k+2}} D_{k+1} \xrightarrow{\phi_{k+1}} D_k \xrightarrow{\phi_k} D_{k-1} \xrightarrow{\phi_{k-1}} \cdots$, donde $D_k = \bigoplus_{i+j=k} F_i \otimes G_j$, y los morfismos ϕ_k están definidos de la siguiente forma:

$\phi_k|_{F_i\otimes G_j} : F_i \otimes G_j \to F_r \otimes G_s$

$\phi_k|_{F_i\otimes G_j} = \varphi_{i-1} \otimes 1$, si $r = i - 1$

$\phi_k|_{F_i\otimes G_j} = (-1)^i 1 \otimes \psi_{j-1}$, si $s = j - 1$

$\phi_k|_{F_i\otimes G_j} = 0$, en caso contrario.

Se verifica fácilmente que con estos morfismos $\mathbf{F}_\bullet \otimes_R \mathbf{G}_\bullet$ es un complejo de cadenas, que es el producto tensorial de $\mathbf{F}_\bullet$ con $\mathbf{G}_\bullet$ en la categoría de complejos.

Como se comentó antes se puede obtener el complejo de Koszul asociado a una sucesión arbitraria (finita), $x_1, \ldots, x_n$, de elementos del anillo R, $\mathbf{K}_\bullet(x_1, \ldots, x_n)$, mediante

la tensorización de los complejos $\mathbf{K}_\bullet(x_i)$, es decir

$$\mathbf{K}_\bullet(x_1,\ldots,x_n) = \bigotimes_{1\leq i\leq n} \mathbf{K}_\bullet(x_i).$$

De esto se deduce que como el producto tensorial de complejos es conmutativo (salvo isomorfismos), entonces el complejo de Koszul asociado a una sucesión, resulta invariante (salvo isomorfismos) por reordenamientos en la sucesión. Es decir, dado σ un elemento del grupo de automorfismos G_n, se tiene que

$$\mathbf{K}_\bullet(x_1,\ldots,x_n) = \bigotimes_{1\leq i\leq n} \mathbf{K}_\bullet(x_i) \simeq \bigotimes_{1\leq i\leq n} \mathbf{K}_\bullet(x_{\sigma(i)}) = \mathbf{K}_\bullet(x_{\sigma(1)},\ldots,x_{\sigma(n)}).$$

Esta construcción puede automatizarse usando el álgebra exterior (cf. [Eis95]).

Recordemos (sin demostración), algunos de los resultados más importantes para nuestras aplicaciones que involucran al complejo de Koszul. Las demostraciones de estos resultados se pueden consultar en [Eis95].

Primero veamos que si bien el complejo no determina si una dada sucesión es regular o no, determina algo aun más importante: dada una sucesión $x_1,\ldots,x_n$, éste permite determinar la longitud de una sucesión regular maximal en el ideal $I=(x_1,\ldots,x_n)$.

Teorema 3.1. *Sea N un módulo finitamente generado sobre un anillo R. Supóngase que $H_j(\mathbf{K}_\bullet(x_1,\ldots,x_n)\otimes N)=0$ para $j>n-r$, y que $H_{n-r}(\mathbf{K}_\bullet(x_1,\ldots,x_n)\otimes N)\neq 0$, entonces toda N-sucesión maximal en $I=(x_1,\ldots,x_n)\subseteq R$ tiene longitud r.*

Se notará también por $\mathbf{K}_\bullet(x_1,\ldots,x_n;N)$ al complejo $\mathbf{K}_\bullet(x_1,\ldots,x_n)\otimes N$. (Se suele notar $\mathbf{K}^R_\bullet(x_1,\ldots,x_n;N)$, cuando no se sobrentiende que el anillo de base es R).

En particular se tiene el siguiente resultado:

Corolario 3.2. *: Si $x_1,\ldots,x_n$ es una N-sucesión en I, que genera I. Entonces el complejo de Koszul $\mathbf{K}_\bullet(x_1,\ldots,x_n;N)$ resulta acíclico, es decir, es una resolución libre del módulo $R/I\otimes N$.*

Como es sabido, todo módulo libre es proyectivo, entonces el complejo $\mathbf{K}_\bullet(\mathbf{X};N)$ resulta una resolución proyectiva del módulo $R/I\otimes_R N$. De esto último, tomando homología, se obtienen los funtores derivados del funtor $\_\otimes_R N$, con lo cual, resulta que $H_i(\mathbf{K}_\bullet(\mathbf{X};N))=\mathrm{Tor}^R_i(R/I,N)$.

Además, resulta que esta es la resolución más corta posible del módulo. Como la longitud del complejo es finita, entonces también se tiene que sólo finitas homologías pueden ser no nulas, esto nos permite asociarle al módulo $R/I\otimes_R N$ un valor entero no negativo que se denomina *profundidad* del módulo.

3.1. El complejo de Koszul graduado. Lamentablemente la recíproca del corolario anterior es falsa en el caso general, aunque resulta cierta si el anillo de base es local o graduado. Éste último es el contexto general de estas notas, ya que en nuestras aplicaciones R es un anillo de polinomios sobre un anillo conmutativo A.

Teorema 3.3. *Sea N un módulo finitamente generado sobre un anillo local (o graduado) R con ideal maximal (o maximal homogéneo) $\mathfrak{m}$. Sea $x_1,\ldots,x_n$ una sucesión en $\mathfrak{m}$. Supóngase que para algún i se tiene que $H_i(N\otimes\mathbf{K}_\bullet(x_1,\ldots,x_n))=0$, entonces se tiene que $H_j(N\otimes\mathbf{K}_\bullet(x_1,\ldots,x_n))=0$ para todo $j\geq i$.*

En particular si $H_1(N\otimes\mathbf{K}_\bullet(x_1,\ldots,x_n))=0$, entonces $x_1,\ldots,x_n$ forma una sucesión N-regular en $\mathfrak{m}$.

Esto permite dar para el caso local una versión más fuerte del corolario anterior

Corolario 3.4. *Dado un anillo local (o graduado) R con ideal maximal (o maximal homogéneo) $\mathfrak{m}$, y N un R-módulo finitamente generado . Sea $I = (x_1, \dots, x_n)$ un ideal propio de R, que contiene una sucesión N-regular de longitud n. Entonces $x_1, \dots, x_n$ es una sucesión N-regular.*

De aquí se deduce un resultado de importante valor geométrico, ya que éste expresa la naturaleza geométrica del concepto de profundidad anteriormente mencionado.

Corolario 3.5. *Dado un anillo R y N un R-módulo finitamente generado, se tiene que si $x_1, \dots, x_r$ es una sucesión N-regular, entonces $x_1^m, \dots, x_r^m$ también lo es, para todo natural m.*

Nos concentraremos ahora en estudiar al complejo de Koszul en el contexto específico de nuestras aplicaciones. Para ello, sea R un anillo graduado, $R = \oplus_{i\geq 0} R_i$, M un R-módulo graduado, e $I = (x_1, \dots, x_n)$ un ideal homogéneo de R, donde $\deg(x_i) = d_i$ para todo i. Entonces el complejos de Koszul $\mathbf{K}_\bullet(x_1, \dots, x_n; M)$ hereda la graduación de R y se escribe

$$\mathbf{K}_\bullet(x_1, \dots, x_n; M): \quad \cdots \to \bigoplus_{1\leq i<j\leq r} M(-d_i - d_j) \to \bigoplus_{1\leq i\leq r} M(-d_i) \to M \to M/I \to 0,$$

donde $M(-d)_e = M_{e-d}$, y las flechas son morfismos de módulos graduados, de grado cero.

Sea r, n y $d_1, \dots, d_r$ enteros positivos, y sean $f_1, \dots, f_r$ polinomios homegéneous de grado $d_1, \dots, d_r$ en las variables $\mathbf{X} := X_1, \dots, X_n$ definidos como

$$f_i(\mathbf{X}) = \sum_{|\alpha|=d_i} U_{i,\alpha}\mathbf{X}^\alpha,$$

para todo $i = 1, \dots, r$, donde $\alpha \in \mathbb{N}^n$.

Sea $A := \mathbb{Z}[U_{i,\alpha} : |\alpha| = d_i,\ i = 1, \dots, r]$ y escribamos $R = A[\mathbf{X}]$.

Lema 3.6. *Si $r \leq n$ entonces $f_1, \dots, f_r$ es una sucesión regular en R.*

Demostración. Para cada $i = 1, \dots, r$ sea $\epsilon_i := U_{i,(0,\dots,0,d_i,0,\dots,0)}$ el coeficiente correspondiente a $X_i^{d_i}$ del polinomio f_i.

Obsérvese que todos los coeficientes $U_{i,\alpha}$ restantes forman una sucesión regular en R. Además, el cociente de R por estos $U_{i,\alpha}$ es isomorfo a $\mathbb{Z}[\epsilon_1, \dots, \epsilon_r][\mathbf{X}]$ y $f_i = \epsilon_i X_i^{d_i}$ en el cociente.

Es fácil ver que en $\mathbb{Z}[\epsilon_1, \dots, \epsilon_r][\mathbf{X}]$ los polinomios $X_1 - \epsilon_1, \dots, X_r - \epsilon_r$ también forman una sucesión regular, que el anillo cociente queda isomorfo a $\mathbb{Z}[\mathbf{X}]$, y que $f_i = X_i^{d_i+1}$ en el cociente.

Finalmente, sabemos que $X_1^{d_1+1}, \dots, X_r^{d_r+1}$ es una sucesión regular en $\mathbb{Z}[\mathbf{X}]$ independientemente del orden. □

Se tiene entonces como corolario el siguiente resultado

Corolario 3.7. *Sea $I = (f_1, \dots, f_n)$, entonces el complejo de Koszul*

$$\mathbf{K}_\bullet(f_1, \dots, f_n; R): \quad \cdots \to \bigoplus_{1\leq i<j\leq r} R(-d_i - d_j) \to \bigoplus_{1\leq i\leq r} R(-d_i) \to R \to 0,$$

es una resolución libre graduada y finita de R/I.

Ejercicios.

1. Sea (R, R_+) un anillo local (o graduado) $x_1, \ldots, x_n \in R_+$. Entonces $x_1, \ldots, x_n$ es una sucesión regular en R sii para todo $i = 0, \ldots, n-1$, x_{i+1} no está en ningún primo asociado de $(x_1, \ldots, x_{i-1})$.
2. Si los elementos $x_1, \ldots, x_n \in R$ forman una sucesión regular en R, entonces $x_1^{\ell_1}, \ldots, x_n^{\ell_n}$ también.
3. Si un ideal I de un anillo conmutativo Noetheriano puede ser generado por una suceción regular, entonces puede ser generado por un conjunto de elementos que son una sucesión regular en cualquier orden.
4. Sea $\phi : R \to S$ un morfismo de anillos, sean $r_1, \ldots, r_n \in S$ y $s_i := \phi(r_i) \in R$. Si $r_1, \ldots, r_n$ forman una sucesión regular en R, entonces para todo R-módulo M, $H_i(\mathbf{K}_\bullet(r_1, \ldots, r_n) \otimes_R M) = \operatorname{Tor}_i^S(S/(s_1, \ldots, s_n r), M)$.
5. Sea $\mathbf{K}_\bullet(\mathbf{X})$ el complejo de Koszul asociado a la sucesión $\mathbf{X}$, y supongamos que x_j es una unidad de A. Entonces el complejo $\mathbf{K}_\bullet(\mathbf{X})$ resulta acíclico.

4. Resultante

En esta sección definiremos y estudiaremos el objeto principal de estas notas, que es la resultante homogénea, o resultante de Macaulay.

4.1. Resultante de Macaulay. Sea r, n y $d_1, \ldots, d_r$ enteros positivos, y sean $f_1, \ldots, f_r$ polinomios homegéneous de grado $d_1, \ldots, d_r$ en las variables $\mathbf{X} := X_1, \ldots, X_n$ definidos como

$$f_i(\mathbf{X}) = \sum_{|\alpha|=d_i} U_{i,\alpha} \mathbf{X}^\alpha,$$

para todo $i = 1, \ldots, r$, donde $\alpha \in \mathbb{N}^n$.

Sea $A := \mathbb{Z}[U_{i,\alpha} : |\alpha| = d_i,\ i = 1, \ldots, r]$ y escribamos $R = A[\mathbf{X}]$.

Teorema 4.1. *Si $r = n$ entonces el ideal $\mathfrak{A}$ es un ideal primo y principal de A, generado por un elemento que llamaremos Resultante de $f_1, \ldots, f_n$, que denotaremos* $\operatorname{Res}(f_1, \ldots, f_n)$*, y que verifica que* $\operatorname{Res}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$.

Para demostrar este teorema, vamos a seguir la demostración dada por Jean-Pierre Jouanolou en [Jou91]. Cabe mencionar que el anillo $\mathbb{Z}$ puede ser reemplazado por un anillo conmutativo reducido, con el solo fin de que la resultante no quede definida a menos de constantes.

Para demostrar el Teorema 4.1 anterior, nos apoyaremos en tres lemas. Antes de eso, introducimos la siguiente notación.

Definición 4.2. Dado I un ideal de un anillo graduado R, con ideal irrelevante R_+, se definen las *formas de inercia* de I como

$$\operatorname{TF}_{R_+}(I) := \bigcup_{\ell \geq 0} (I :_R (R_+)^\ell).$$

Esta notación proviene de su nombre *Trägheitsformen*, en alemán, introducidas por Hurwitz en el contexto de la teoría de eliminación.

Lema 4.3. *Para todo entero $j = 1, \dots, n$ se tiene*

$$\mathrm{TF}_{R_+}(I) = \bigcup_{\ell \geq 0} (I :_R X_j^\ell) = \ker(R \to B_{X_j}).$$

Además, $\mathrm{TF}_{R_+}(I)$ *es un ideal primo de* R.

De la segunda parte, intersecando con A, se tiene que $\mathfrak{A}$ es un ideal primo de A.

Demostración. Sea $1 \leq j \leq n$ un entero, y para cada $i = 1, \dots, r$, escribimos U_i para denotar al coeficiente correspondiente al monomio $X_j^{d_i}$ del polinomio f_i. Es decir, si $\beta = d_i \mathbf{e}_j$, siendo $\mathbf{e}_j$ el j-ésimo vector canónico, $U_i = U_{i,\beta}$.

En el anillo $R' := R[X_j^{-1}]$, el polinomio f_i se escribe de la siguiente forma:

$$f_i(\mathbf{X}) = X_j^{d_i}(U_i + \sum_{\alpha \neq \beta} U_{i,\alpha} \mathbf{X}^\alpha X_j^{-d_i}).$$

Sea $A' := \mathbb{Z}[U_{i,\alpha} : i = 1, \dots, r, \alpha \neq \beta]$, con lo cual $A = A'[U_i]$, y escribamos $g_{i,\beta} := \sum_{\alpha \neq \beta} U_{i,\alpha} \mathbf{X}^\alpha X_j^{-d_i}$.

Se obtiene así un isomorfismo de anillos

$$B_{X_j} \xrightarrow{\sim} A'[\mathbf{X}][X_j^{-1}] : U_i \mapsto U_i - f_i / X_j^{d_i} = -g_{i,\beta}.$$

Esto prueba que cualesquiera sean i, j, X_i no es un divisor de cero en B_{X_j}. Entonces la primera parte se desprende de que

$$\ker(R \to B_{X_i}) = \ker(R \to B_{X_i X_j}) = \ker(R \to B_{X_j X_i}) = \ker(R \to B_{X_j})$$

Además, como $\mathbb{Z}$ es íntegro, B_{X_j} también lo es, y por lo tanto, $\mathrm{TF}_{R_+}(I)$ es un ideal primo de R. □

Lema 4.4. *Si* $r < n$ *entonces* $\mathrm{TF}_{R_+}(I) = I$.

Demostración. De la definición de $\mathrm{TF}_{R_+}(I)$ se desprende que $\mathrm{TF}_{R_+}(I) \supset I$. Demostraremos entonces que $\mathrm{TF}_{R_+}(I) \subset I$. Por el Lema 4.3, basta mostrar que si existe un entero ℓ para el cual $X_n^\ell f \in I$ entonces $f \in I$. Si que esto valiera para $\ell = 1$, entonces siendo verdadero para $\ell - 1$ también se tendría para ℓ ya que $X_n^\ell f = X_n(X_n^{\ell-1} f)$. Veamos que vale si $\ell = 1$.

Sea $f \in R$ y escribamos

$$X_n f = \sum_{i=1}^r h_i f_i \in I. \tag{4.1}$$

Se tiene que $\sum_{i=1}^r \overline{h_i f_i} = 0$ en $\overline{R} := R/(X_n)$ y los polinomios f_i son genéricos en las variables $X_1, \dots, X_{n-1}$. Sabemos (por el Lema 3.6) que, como $r \leq n-1$, los polinomios $\overline{f_1}, \dots, \overline{f_r}$ forman una sucesión regular en $\overline{R}$ y entonces el complejo de Koszul $\mathbf{K}_\bullet(\overline{f_1}, \dots, \overline{f_r}; \overline{R})$ es acíclico (ver el Corolario 3.2). Además, la exactitud en la posición 1

$$\cdots \to \bigoplus_{1 \leq i < j \leq r} \overline{R}(-d_i - d_j) \xrightarrow{\partial_1} \bigoplus_{1 \leq i \leq r} \overline{R}(-d_i) \xrightarrow{\partial_1} \overline{R} \to \overline{R}/(\overline{h_1}, \dots, \overline{h_r}) \to 0.$$

del complejo $\mathbf{K}_\bullet(\overline{f_1}, \dots, \overline{f_r}; \overline{R})$ dice que $(\overline{h_1}, \dots, \overline{h_r}) \in \ker(\partial_0)$ si y solo si $(\overline{h_1}, \dots, \overline{h_r}) \in \mathrm{im}(\partial_1)$, es decir, si existen $(\dots, h'_{i,j}, \dots) \in \oplus_{1 \leq i < j \leq n-1} \overline{R}(d_i - d_j)$. Esta última condición es equivalente (Ejercicio 1) a que exista una matriz antisimétrica $H \in \mathrm{Mat}_{r,r}(\overline{R})$ tal que

$$H \cdot (\overline{f_1}, \dots, \overline{f_r})^t = (\overline{h_1}, \dots, \overline{h_r}).$$

Interpretando $\overline{R}$ como $R' := A[X_1, \ldots, X_{n-1}]$, y $H \in \mathrm{Mat}_{r,r}(R')$ definimos $g_i \in R$ de forma tal que

$$H \cdot (f_1, \ldots, f_r)^t = (g_1, \ldots, g_r),$$

donde $\overline{g_i} = \overline{h_i}$ para todo i, es decir que que existe para cada i, existe un polinomio p_i tal que $h_i - g_i = X_n p_i$. Además, como H es antisimétrica, se tiene que $\sum f_i g_i = 0$. Retomando la ecuación (4.1), se tiene

$$X_n f = \sum_{i=1}^{r} (g_i + X_n p_i) f_i = \sum_{i=1}^{r} g_i f_i + X_n \sum_{i=1}^{r} p_i f_i. \tag{4.2}$$

De (4.2) se deduce que $X_n f = X_n \sum_{i=1}^{r} p_i f_i$ en R o equivalentemente (ya que X_n no es divisor de ceros en R) $f = \sum_{i=1}^{r} p_i f_i$, es decir, que $f \in I$. □

Lema 4.5. *Supongamos $r = n$ y sea $f \in \mathrm{TF}_{R_+}(I) \in R$. Entonces $f \in I$ ó f depende de todos los coeficientes $U_{i,\alpha}$ de todos los f_i.*

Demostración. Sea $U = U_{i,\alpha}$ un coeficiente cualquiera, es decir, fijemos algún i y algún α. El coeficiente U corresponde al monomio X^α que aparece en f_i. Supongamos ahora que $f \in \mathrm{TF}_{R_+}(I)$ no depende U, y veamos que $f \in I$.

Escribamos $g_i := f_i - UX^\alpha$ y consideremos el morfismo de álgebras $\phi : R_{X_1 \cdots X_n} \to R_{X_1 \cdots X_n}$ definido como $U \mapsto -g_i/X^\alpha$, $U_{j,\beta} \mapsto U_{j,\beta}$ si $(j,\beta) \neq (i,\alpha)$ y $X_j \mapsto X_j$ para todo j. Obsérvese que $\phi(f_i) = 0$ para todo i, y que como f y f_j no dependen de U si $j \neq i$, entonces $\phi(X_n^\ell f) = X_n^\ell f$ para todo ℓ y $\phi(f_j) = f_j$ para todo $j \neq i$.

Como $f \in \mathrm{TF}_{R_+}(I)$, se tiene que $X_n^\ell f = \sum_i h_i f_i \in I$ para algún $\ell \in \mathbb{N}$. Aplicando ϕ a la identidad anterior, usando que $\phi(f_i) = 0$, $\phi(f_j) = f_j$ si $j \neq i$, y escribiendo $h_i' := \phi(h_i)$ se tiene que

$$\phi(X_n^\ell f) = \sum_{j \neq i} h_j' f_j \in R_{X_1 \cdots X_n}.$$

Multiplicando por una potencia conveniente X^β de las X_i's se obtiene la siguiente igualdad en R

$$X^\beta \phi(X_n^\ell f) = X^\beta X_n^\ell f = \sum_{j \neq i} h_j'' f_j \in R.$$

Esto último dice que si escribimos $I' := (f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$ el ideal generado por $n-1$ polinomios, entonces $f \in \mathrm{TF}_{R_+}(I')$. El Lema 4.4 aplicado con $r = n-1$ nos dice que $\mathrm{TF}_{R_+}(I') = I' \subset I$. □

Vayamos entonces a la demostración del Teorema de eliminación.

Teorema 4.1. *Si $r = n$, entonces el ideal $\mathfrak{A}$ es un ideal primo y principal de A, generado por un elemento que llamaremos Resultante de $f_1, \ldots, f_n$, que denotaremos $\mathrm{Res}(f_1, \ldots, f_n)$, y que verifica que $\mathrm{Res}(X_1^{d_1}, \ldots, X_n^{d_n}) = 1$.*

Demostración. Sea $U = U_{i,\alpha}$ un coeficiente cualquiera, y escribamos $A' := \mathbb{Z}[U_{j,\beta} : (j,\beta) \neq (i,\alpha)]$. Con esta notación, $A = A'[U]$. Como $I \cap A = 0$, el Lema 4.5 dice que todo $0 \neq f \in \mathfrak{A}$ satisface que $\deg_U(f) > 1$. Definamos entonces

$$s := \mín\{\deg_U(f) : 0 \neq f \in \mathfrak{A}\}.$$

Sea $f \in \mathfrak{A}$ que satisface $\deg_U(f) = s$. Como A' es factorial, entonces existe una factorización $f = \prod q_i$ en finitos q_i, con q_i primo en A'.

Como $\mathrm{TF}_{R_+}(I)$ es in ideal primo por el Lema 4.3, entonces $\mathfrak{A} = \mathrm{TF}_{R_+}(I) \cap A$, lo cual implica que existe un i tal que $q_i \subset \mathfrak{A}$. Como $q_i | f$, se tiene que $1 \leq \deg_U(q_i) \leq$

$\deg_U(f) = s$. Como $q_i \in \mathfrak{A}$, por definición de s se tiene que $\deg_U(q_i) = \deg_U(f) = s$. Esto prueba que existe un elemento primo $\mathfrak{r} := q_i \in \mathfrak{A}$.

Veamos ahora que $\mathfrak{A} = \mathfrak{r}A$. En efecto, como A' es íntegro, dado $g \in \mathfrak{A}$, podemos escribir en A, $tg = u\mathfrak{r} + v$, donde $t, u \in A'$ y v verifica que $v = 0$ ó $\deg_U(v) < s$. Como $v = tg - u\mathfrak{r}$, entonces $v \in \mathfrak{A} \subset A$ y $A \cap I = 0$, si $v \neq 0$, entonces por el Lema 4.5 v depende de todos los coeficientes de los f_i, en particular depende de U, pero la elección de s, se tendría que $\deg_U(v) \geq s$, lo cual lleva a una contradicción. Entonces se tiene que $v = 0$ y por lo tanto $tg = u\mathfrak{r}$. Como t no depende de U y R tiene grado positivo en U y es primo, entonces $\mathfrak{r}|g$

Como esto vale para U arbitrario, se tiene que $\mathfrak{r}$ es único a menos de un elemento inversible de A', es decir, de $\mathbb{Z}$. Este elemento es 1 por la normalización elegida en el enunciado. □

4.2. Resultante y divisores. Hemos visto en el Lema 3.6 que si $f_1, \ldots, f_r$ son r polinomios genéricos y $r \leq n$, entonces es una sucesión regular en R. El Corolario 3.7 dice que entonces el complejo de Koszul $\mathbf{K}_\bullet(f_1, \ldots, f_r; R)$ es un complejo de R-módulos acíclico, y en particular, complejo Koszul es acíclico en grados positivos si el número de polinomios r es menor o igual al número de variables n

Veremos ahora cómo $\mathrm{ann}_A(B_\nu)$ puede ser calculado mediante un producto alternado de determinantes, que vienen de los diferenciales de este complejo de Koszul graduado, en grado $\nu \geq \nu_0 := \sum(d_i - 1) + 1$.

En la Sección 4 vimos, en el Teorema 4.1 que el ideal $\mathfrak{A}$ es primo y principal y que por lo tanto define una subvariedad de $\mathrm{Spec}(A)$ de codimensión 1. Luego, probamos entre el Lema 2.4 y el Corolario 2.6 que $\mathfrak{A} = \mathrm{ann}_A(B_\nu)$ si $\nu \geq \nu_0$, es decir, que es un A-módulo de torsión.

Mostraremos ahora que todo A-módulo M de torsión con A un dominio noetheriano y factorial, define un divisor $\mathrm{div}(M)$, y que dada una resolución libre de M, este divisor puede ser calculado mediante un producto alternado de determinantes.

En lo que sigue, sólo nos interesará la estructura de A-módulo de los objetos. Es importante que el lector tenga en cuenta que si bien lo que desarrollaremos en esta parte es general para cualquier A-módulo con A un dominio noetheriano y factorial, nuestro es interés está en el caso en que A es el anillo de coeficientes universales de n polinomios genéricos, $M = B_\nu$ con $\nu \geq \nu_0$ y la resolución libre $\mathbf{F}_\bullet$ de M es $\mathbf{K}_\bullet(f_1, \ldots, f_r; R)_\nu$ con $\nu \geq \nu_0$.

Sea A un dominio noetheriano y factorial con cuerpo de fracciones k.

Definición 4.6. Sea A un anillo noetheriano y factorial y sea M un A-módulo de torsión de tipo finito. Denotemos por $\mathrm{div}(M)$ al divisor asociado a M:

$$\mathrm{div}(M) = \sum_{\mathfrak{p} \in \mathrm{ass}_A(M), \mathrm{ht}(\mathfrak{p}) = 1} \ell(M_\mathfrak{p})\mathfrak{p},$$

donde $\mathrm{ass}_A(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \exists m \in M, \mathrm{ann}_A(m) = \mathfrak{p}\}$ es el conjunto de primos asociados a M, $\mathrm{ht}(\mathfrak{p})$ es la altura de $\mathfrak{p}$ y $\ell(M_\mathfrak{p})$ la longitud de $M_\mathfrak{p}$.

Definición 4.7. Si I es un ideal de A, la parte principal de I, que frecuentemente se denota por $[I]$, consiste en el gcd de los generadores de I.

Obsérvese que acá entran la hipótesis de factorialidad requerida sobre A, así como la finita generación de I, que está garantizada por la noetherianidad de A.

Con esta notación, si el ideal I se descompone en factores irreducibles de forma tal que su parte principal es $[I] = \prod_i \mathfrak{p}_i^{\ell_i}$, entonces $\operatorname{div}(A/I) = \sum_i \ell_i \mathfrak{p}_i$.

Teorema 4.8. *A un dominio noetheriano y factorial y $\mathbf{F}_\bullet$ un complejo finito de A-módulos libres finitamente generados. Escribamos*

$$\mathbf{F}_\bullet : 0 \to F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \to 0$$

y supongamos que $F_i = E_{i+1} \oplus E_i$, $E_0 = E_{n+1} = 0$, $\partial_p = \begin{pmatrix} a_p & \phi_p \\ b_p & c_p \end{pmatrix}$, donde $\phi_p : E_p \to E_p$ es un endomorfismo inyectivo. Entonces, $H_i(\mathbf{F}_\bullet)$ es un A-módulo de torsión par todo i, y

$$\sum_i (-1)^i \operatorname{div}(H_i(\mathbf{F}_\bullet)) = \sum_i (-1)^i \operatorname{div}(\det \phi_i).$$

En particular, si $\mathbf{F}_\bullet$ es acíclico, la parte principal de $H_0(\mathbf{F}_\bullet)$, $[H_0(\mathbf{F}_\bullet)]$, está dada por el elemento $\prod_i (\det \phi_i)^{(-1)^{i+1}}$ de A.

Demostración. Sea k el cuerpo de fracciones de A. Debemos probar que $H_i(\mathbf{F}_\bullet)$ es un A-módulo de torsión par todo i, para ello, veamos que $H_i(\mathbf{F}_\bullet) \otimes_A k = 0$. Como A es íntegro, k es la localización en el ideal 0, es playo sobre A, entonces $H_i(\mathbf{F}_\bullet) \otimes_A k = H_i(\mathbf{F}_\bullet \otimes_A k)$.

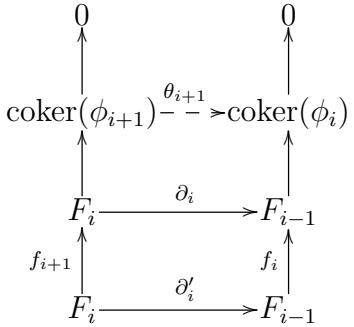
Además, la homología of $F \otimes_A k$ es cero porque $\partial_i \otimes 1$ restringido a $E_i \otimes_A k$ es un automorfismo. Entonces $H_i(F_\bullet)$ es de torsion para todo i.

Sea $\partial'_i = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}$, entonces el complejo $(F_\bullet, \partial'_\bullet)$ tiene homología cero. Definimos la aplicación $fn = id$, $fi = \begin{pmatrix} \phi_{i+1} & 0 \\ c_{i+1} & I \end{pmatrix} : F_i \to F_i$ para todo $i < n$. Como

$$\partial_i \circ f_i = \begin{pmatrix} a_i & \phi_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} \phi_{i+1} & 0 \\ c_{i+1} & I \end{pmatrix} = \begin{pmatrix} 0 & \phi_i \\ 0 & c_i \end{pmatrix} = \begin{pmatrix} \phi_i & 0 \\ c_i & I \end{pmatrix} \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix} = f_{i-1} \circ \partial'_i$$

Esto dice que $\{f_i\}$ definen un morfismo $f_\bullet : (F_\bullet, \partial'_\bullet) \to (F_\bullet, \partial_\bullet)$.

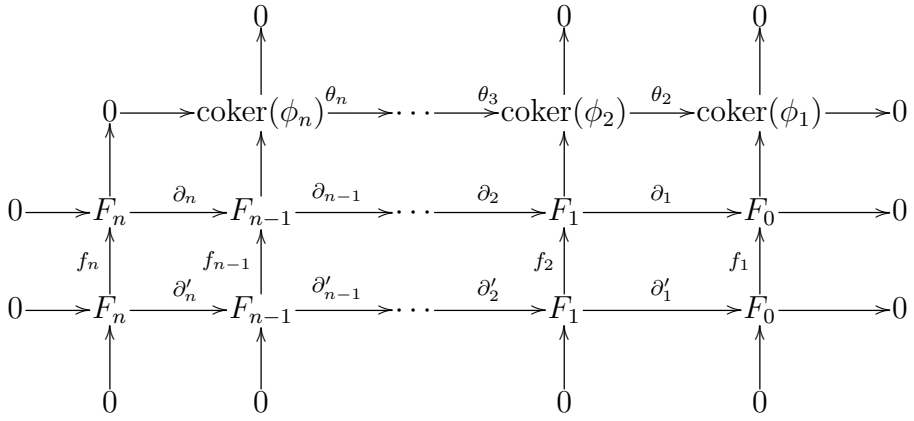
Además, f_i es inyectiva y $\operatorname{coker}(f_i)$ puede ser identificado con $\operatorname{coker}(\phi_{i+1})$. Los morfismos ∂_i y ∂'_i inducen morfismos Θ_{i+1} de acuerdo al siguiente degrama



Esto dice que se tiene una sucesión exacta corta de complejos

$$0 \to (F_\bullet, \partial'_\bullet) \xrightarrow{f_\bullet} (F_\bullet, \partial_\bullet) \to (\operatorname{coker}(\phi_\bullet), \theta_\bullet)[1] \to 0. \tag{4.3}$$

que se escribe en forma de digrama como sigue, donde las columnas son exactas



La sucesión exacta (4.3) da una sucesión exacta larga en homología

$$\cdots \to H_i(F_\bullet, \partial'_\bullet) \to H_i(F_\bullet, \partial_\bullet) \to H_{i+1}(\operatorname{coker}(\phi_\bullet), \theta_\bullet) \to H_{i-1}(F_\bullet, \partial'_\bullet) \to \cdots .$$

Como el complejo $(F_\bullet, \partial'_\bullet)$ es exacto, se tiene que el complejo $(\operatorname{coker}(\phi_\bullet), \theta_\bullet)[1]$ tiene la misma homología que $(F_\bullet, \partial_\bullet)$. Esto es, $H_i(F_\bullet, \partial_\bullet) \cong H_{i+1}(\operatorname{coker}(\phi_\bullet), \theta_\bullet)$, y en particular sus divisores asociados coinciden, de lo cual se deduce que

$$\operatorname{div}(\operatorname{coker}\phi_i) = \operatorname{div}(\operatorname{im}\theta_{i-1}) + \operatorname{div}(\ker\theta_{i-1}) = \operatorname{div}(\operatorname{im}\theta_{i-1}) + \operatorname{div}(\operatorname{im}\theta_i) + \operatorname{div}(H_{i-1}(F_\bullet)).$$

La conclusión sigue del siguiente resultado clásico de Bourbaki [Bou98, Cap. 7, Sec. 4, n. 6, Corolario de la Prop. 13]:

Sea M un A-módulo finitamente generado y ϕ un endomorfismo inyectivo de M. Entonces $\operatorname{div}(\operatorname{coker}\phi) = \operatorname{div}(\det\phi)$. □

Volvamos a nuestro contexto habitual y sea $A = \mathbb{Z}[U_{i,\alpha}]$ es el anillo de coeficientes universales de n polinomios genéricos $f_1, \ldots, f_n$, $M = B_\nu$ con $\nu \geq \nu_0$ y la resolución libre $\mathbf{F}_\bullet$ de M es $\mathbf{K}_\bullet(f_1, \ldots, f_n; R)_\nu$ con $\nu \geq \nu_0$. Se tiene el siguiente resultado.

Corolario 4.9. *El complejo $\mathbf{K}_\bullet(f_1, \ldots, f_n; R)_\nu$ de A-módulos es una resolución de B_ν con diferenciales ∂_i^ν. Además, la parte principal de B_ν, es decir $\operatorname{ann}_A(B_\nu)$, está dada por $\prod_i (\det \partial_i^\nu)^{(-1)^{i+1}}$.*

Esto permite calcular, teniendo una descomposición como la del Teorema 4.8, un (el) generador de $\operatorname{ann}_A(B_\nu)$ como producto alternado de matrices que vienen de los diferenciales ∂_i^ν de $\mathbf{K}_\bullet(f_1, \ldots, f_n; R)_\nu$.

Ejercicios.

1. En el contexto de la demostración del Lema 4.4, $H_1(\mathbf{K}_\bullet(\overline{f_1}, \ldots, \overline{f_r}; \overline{R})) = 0$ es equivalente a que exista una matriz antisimétrica $H \in \operatorname{Mat}_{r,r}(\overline{R})$ tal que

$$H \cdot (\overline{f_1}, \ldots, \overline{f_r})^t = (\overline{h_1}, \ldots, \overline{h_r}).$$

5. Ideales de Fitting

En esta sección desarrollaremos el contenido básico sobre ideales de Fitting, y determinantes de complejos, lo que está estrictamente vinculado con el invariante de McRae, que se define a partir de un A-módulo M, y que bajo buenas condiciones describe la parte de codimensión uno del soporte de M. Quien esté interesado en profundizar las ideas rápidamente expuestas en esta sección, puede consultar el trabajo de McRae [Mac65], que es la fuente original, y el artículo de Northcott [Nor76] en el cuál se trata la existencia y algunas propiedades de este invariante.

Para el cálculo de este invariante, que definiremos a partir de ideales de Fitting, haremos uso de una técnica desarrollada por Cayley conocida como determinante de un complejo. Para esto se puede consultar unas notas de Demazure [Dem84] y un tratamiento más general se puede obtener en el Apéndice del libro [GKZ94].

5.1. Ideales de Fitting. Sea A un anillo conmutativo, F y G dos A-módulos libres, y $\varphi : F \to G$ un morfismo de A-módulos. Consideremos bases para estos módulos, y notemos por $|\varphi|$ a la matriz de φ escrita en estas bases. Definimos $\det_\nu(\varphi)$ como el ideal de A generado por los menores de tamaño $\nu \times \nu$ de $|\varphi|$. Haremos la convención de que la matriz de tamaño nulo tiene determinante 1, con lo cual $\det_\nu(\varphi) = A$ para todo $\nu \leq 0$.

Proposición 5.1. *Sea M un A-módulo finitamente generado, y sean $F \xrightarrow{\varphi} G \to M \to 0$ y $F' \xrightarrow{\varphi'} G' \to M \to 0$ dos presentaciones libres de M. Entonces para todo $\nu \in \mathbb{Z}$ se tiene que*

$$\det{}_{rg(G)-\nu}(\varphi) = \det{}_{rg(G')-\nu}(\varphi').$$

Una demostración de este resultado, como de los siguientes, se puede consultar en [Nor76, Cap. 3.1.]. Podemos ahora dar la definición de los ideales de Fitting:

Definición 5.2. Sea M un A-módulo finitamente generado, y sea $F \xrightarrow{\varphi} G \to M \to 0$ una presentación libre de M, definimos para cada $i \in \mathbb{N}$, el ν-ésimo *invariante de Fitting de M*, como el ideal

$$\mathrm{Fitt}_\nu(M) := \det{}_{rg(G)-\nu}(\varphi).$$

El invariante $\mathrm{Fitt}_0(M)$ suele ser denotado por Fitt y llamado invariante de Fitting inicial de M.

Enunciaremos a continuación algunas propiedades relevantes sobre estos invariantes. Nótese que el item 2, es la mencionada propiedad de cambio de base deseada en nuestra aplicación al cálculo de resultantes.

Proposición 5.3. *Sea M un A-módulo finitamente generado.*

1. *Los invariantes de Fitting de M forman una sucesión creciente:*

$$\mathrm{Fitt}(M) = \mathrm{Fitt}_0(M) \subset \mathrm{Fitt}_1(M) \subset \mathrm{Fitt}_2(M) \subset \cdots .$$

   Más aún, si M puede ser generado por m elementos, entonces $\mathrm{Fitt}_m(M) = A$.
2. *Dado un morfismo $A \to B$ de anillos, se tiene que, para todo $\nu \in \mathbb{N}$*

$$\mathrm{Fitt}_\nu(M \otimes_A B) = \mathrm{Fitt}_\nu(M)B \ .$$

3. *Para todo $\nu \geq 1$ se tiene que* $\mathrm{ann}(M)\,\mathrm{Fitt}_\nu(M) \subset \mathrm{Fitt}_{\nu-1}(M)$. *Más aún, si M puede ser generado por m elementos, entonces*

$$\mathrm{ann}(M)^m \subset \mathrm{Fitt}(M) \subset \mathrm{ann}(M).$$

4. *Si M es un A-módulo que admite una presentación finita (se dice que M es finitamente presentado), entonces cada uno de sus invariantes de Fitting es un ideal finitamente generado de A.*

Enunciaremos a continuación un resultado muy importante conocido como Lema de McCoy, que tampoco demostraremos.

Lema 5.4. *(McCoy) Sea $\varphi : F \to G$ un morfismo entre dos A-módulos libres de rango r_1 y r_2 respectivamente. Entonces φ es inyectiva si y solo si $\operatorname{ann}_A(\det_{r_1}(\varphi)) = 0$. más aún, cuando se está en esta situación se tiene que $r_1 \leq r_2$.*

Utilizaremos este resultado al final de esta sección para obtener una descomposición de un complejo libre, como la deseada en el Teorema 4.8.

5.2. La Característica de Euler. Nuevamente aquí A es un anillo conmutativo, y M es un A-módulo. Antes de poder definir el invariante de McRae de M, que denotaremos por $\mathfrak{S}(M)$, debemos definir algunos conceptos previos que están íntimamente ligados a él.

Definiremos previamente otro invariante, conocido como *Característica de Euler*, que tiene la propiedad de caracterizar a aquellos módulos que tienen anulador trivial.

Lema 5.5. *Sea M un A-módulo, y consideremos dos resoluciones libre finitas $\mathbf{F}_\bullet$ y $\mathbf{F}'_\bullet$ de M, entonces se tiene que $\sum_i (-1)^i r_i = \sum_i (-1)^i r'_i$, donde $r_i = rg(F_i)$ y $r'_i = rg(F'_i)$.*

Ahora podemos definir la Característica de Euler de M como sigue:

Definición 5.6. Sea M un A-módulo que admite una resolución libre finita $\mathbf{F}_\bullet$ por módulos F_i de rango r_i. Definimos la característica de Euler de M como

$$\chi(M) = \sum_{i=0}^{n} (-1)^i r_i.$$

El siguiente teorema, debido a Vasconcelos, caracteriza los módulos cuya característica de Euler es cero, y que serán de interés próximamente.

Lema 5.7. *Sea M un A-módulo que admite una resolución libre finita de longitud finita. Entonces la característica de Eurler de M es un entero no negativo y*

1. *$\chi(M) > 0$ si y solo si $\operatorname{ann}_A(M) = 0$;*
2. *$\chi(M) = 0$ si y solo si $\operatorname{ann}_A(M) \neq 0$, si y solo si $0 :_A \operatorname{ann}_A(M) = 0$.*

Aplicando este resultado en el contexto habitual, donde $M = B_\nu$ para $\nu \geq \nu_0$, deducimos que $\chi(B_\nu) = 0$ ya que $\operatorname{ann}_A(B_\nu) \neq 0$ y está generado por la resultante. La última parte dice que $\operatorname{ann}_A(B_\nu)$ contiene un elemento que no es divisor de cero, que justamente es la resultante mencionada.

5.3. El Invariante de McRae. Estamos ahora en condiciones de definir el invariante de McRae de un A-módulo que admite una resolución libre finita y tal que $\chi(M) = 0$. Nuestra aplicación será como siempre al caso en que A es el anillo de coeficientes universales, y $M = B_\nu$ para $\nu \geq \nu_0$.

De acuerdo con los establecido en el trabajo de Northcott [Nor76], daremos la siguientes definiciones:

Definición 5.8. Si M es un A-módulo que tiene una resolución libre finita de longitud uno de la forma $0 \to F_1 \to F_0 \to M \to 0$ y tal que $\chi(M) = 0$, diremos que M es un *módulo elemental*.

Si M es un A-módulo elemental, entonces el ideal de Fitting inicial $\mathrm{Fitt}(M)$ es principal (además es integro y fraccionario).

Definición 5.9. Notaremos por $\mathfrak{S}(M)$ al ideal de Fitting inicial de estos módulos y lo llamaremos *invariante de McRae* de M. Más en general, si M es un A-módulo. Dada una resolución finita $\mathbf{F}_\bullet$ por módulos elementales F_i, se le asocia un ideal invertible fraccionario

$$\mathfrak{S}(M) = \prod_{i=0}^{n} \mathrm{Fitt}(F_i)^{(-1)^i},$$

que se denomina *invariante de McRae de* M.

Enunciaremos a continuación algunas propiedades importantes del invariante de McRae que están para probar en los ejercicios de esta sección, y cuya demostración se encuentra completa en [Nor76, Cap. 3.6 y 6.2].

Sea M un A-módulo que tiene una resolución finita de módulos elementales. Entonces el ideal $\mathfrak{S}(M)$ de A es un ideal principal generado por un elemento que no es divisor de cero. Además, satisface que $\mathrm{Fitt}(M) \subset \mathfrak{S}(M)$ y es minimal con esta propiedad, es decir, si I es un ideal principal de A que contiene a $\mathrm{Fitt}(M)$, entonces también contiene a $\mathfrak{S}(M)$.

La propiedad anterior implica que si A es un DFU, como lo es el anillo de coeficientes universales, entonces $\mathfrak{S}(M)$ está generado por el gcd de los generadores de $\mathrm{Fitt}(M)$.

Además, hay una serie de equivalencias al hecho de tener una resolución por módulos elementales, que se resumen en el siguiente resultado:

Lema 5.10. *Si M es un A-módulo, entonces las siguientes tres afirmaciones son equivalentes:*

1. *M admite un resolución finita por módulos elementales;*
2. *M admite una resolución libre finita de característica de Euler cero;*
3. *M admite una resolución libre finita y $\mathrm{ann}(M)$ contiene un elemento que no es divisor de cero.*

Esto último nos dice que M admite una resolución libre finita y $\mathrm{ann}(M)$ contiene un elemento que no es divisor de cero, entonces M admite un resolución finita por módulos elementales y por lo tanto podemos definir el invariante de McRae como en la Definición 5.9.

en la próxima parte daremos un método constructivo para calcular el ideal $\mathfrak{S}(M)$.

5.4. Un algoritmo par calcular $\mathfrak{S}(M)$. A partir de ahora supondremos que A es un dominio íntegro, y que M es un A-módulo que admite una resolución finita libre de longitud $n \geq 1$,

$$\mathbf{F}_\bullet : \qquad 0 \to F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \to F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0,$$

tal que $\chi(M) = \sum_i (-1)^i r_i = 0$, donde r_i es el rango del módulo F_i.

Descompongamos ahora los módulos F_i del complejo $\mathbf{F}_\bullet$, empezando desde la izquierda.

Sea $F_n^{(0)} := 0$ y $F_n^{(1)} := F_n$, escribimos entonces $F = F_n^{(0)} \oplus F_n^{(1)}$. Como φ_n es inyectivo, entonces por el Lema de McCoy, 5.4, se tiene que:

1. F_{n-1} se escinde en $F_{n-1}^{(0)} \oplus F_{n-1}^{(1)}$, donde estos dos módulos son libres de rango r_n y $r_{n-1} - r_n$ respectivamente. El morfismo $\varphi_n : F_n \to F_{n-1}$ se puede escribir

matricialmente como $\varphi_n = (c_n \ d_n)$, donde $\det(c_n) \neq 0$. Se reescribe el comienzo de la resolución anterior de la forma

$$\begin{array}{ccccccc} 0 & \longrightarrow & 0 & \longrightarrow & F_{n-1}^{(0)} & \longrightarrow & \cdots \\ & & \oplus & \overset{c_n}{\nearrow} & \oplus & & \\ 0 & \longrightarrow & F_n^{(1)} & \xrightarrow{d_n} & F_{n-1}^{(1)} & \longrightarrow & \cdots \end{array}$$

2. Ahora, como el morfismo c_n es biyectivo sobre el cuerpo de fracciones de A y como $\mathrm{im}(d_n) = \ker(d_{n-1})$, se deduce que F_{n-2} se parte en $F_{n-2}^{(0)} \oplus F_{n-2}^{(1)}$, en dos módulos libres de rango $r_{n-1} - r_n$ y $r_{n-2} - (r_{n-1} - r_n)$ respectivamente. El morfismo $\varphi_{n-1} : F_n \to F_{n-1}$ se escribe matricialmente como

$$\varphi_{n-1} = \begin{pmatrix} a_{n-1} & c_{n-1} \\ b_{n-1} & d_{n-1} \end{pmatrix}$$

, donde $\det(c_{n-1}) \neq 0$. Se reescribe el comienzo de la resolución $\mathbf{F}_\bullet$ como

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & 0 & \xrightarrow{a_{n-1}} & F_{n-2}^{(0)} & \longrightarrow & \cdots \\ & & \oplus & \overset{c_n}{\nearrow} & \oplus & \overset{c_{n-1}\ b_{n-1}}{\nearrow\searrow} & \oplus & & \\ 0 & \longrightarrow & F_n^{(1)} & \xrightarrow{d_n} & F_{n-1}^{(1)} & \xrightarrow{d_{n-1}} & F_{n-2}^{(1)} & \longrightarrow & \cdots \end{array}$$

3. de esta forma se obtiene que para cada $i = 0, \ldots, n$ F_i se escinde como $F_i = F_i^{(0)} \oplus F_i^{(1)}$ con ambos módulos libres de rango $\sum_{j=0}^{n-i-1}(-1)^j r_{i+1+j}$ y $\sum_{j=0}^{n-i}(-1)^j r_{i+j}$ repectivamente, y para $i = 1, \ldots, n$ el morfismo $\varphi_i : F_i^{(0)} \oplus F_i^{(1)} \to F_{i-1}^{(0)} \oplus F_{i-1}^{(1)}$ se escribe matricialmente como

$$\varphi_i = \begin{pmatrix} a_i & c_i \\ b_i & d_i \end{pmatrix},$$

donde el determinante de c_i es no nulo.

4. Finalmente, dado que $\chi(M) = \sum_{j=0}^{n}(-1)^j r_j = 0$, una descomposición de esta forma termina con un morfismo φ_1 que se escribe como $(a_1 \ c_1)^t$, con $\det(c_1) \neq 0$, obteniéndose una resolución libre con morfismos como se ilustra en el diagrama:

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & 0 & \xrightarrow{a_{n-1}} & F_{n-2}^{(0)} & \longrightarrow & \cdots & \cdots & \xrightarrow{a_2} & F_1^{(0)} & \xrightarrow{a_1} & F_0^{(0)} \\ & & \oplus & \overset{c_n}{\nearrow} & \oplus & \overset{c_{n-1}\ b_{n-1}}{\nearrow\searrow} & \oplus & \overset{c_{n-2}}{\nearrow} & & & \overset{c_2}{\nearrow} & \oplus & \overset{c_1\ b_1}{\nearrow\searrow} & \oplus \\ 0 & \longrightarrow & F_n^{(1)} & \xrightarrow{d_n} & F_{n-1}^{(1)} & \xrightarrow{d_{n-1}} & F_{n-2}^{(1)} & \longrightarrow & \cdots & \cdots & \xrightarrow{a_2} & F_1^{(1)} & \xrightarrow{d_1} & F_0^{(1)} \end{array}$$

Obsérvese que se obtiene una familia de matrices cuadradas, que están definidas complementando las filas o columnas de la matriz anteriormente definida, y cuyo determinate es no nulo.

Corolario 5.11. *Con la notación anterior, se tiene*

$$\mathfrak{S}(M) = \det(\mathbf{F}_\bullet)A := \prod_{i=1}^{n} \det(c_i)^{(-1)^{i-1}} A = \frac{\det(c_1)\det(c_3)\ldots}{\det(c_2)\det(c_4)\ldots} A.$$

Vimos que $\mathfrak{S}(M)$ es el menor ideal principal que contiene a $\mathrm{Fitt}(M)$, esto dice que $\mathfrak{S}(M)$ es la parte de codimensión uno de $\mathrm{Fitt}(M)$. A partir de la Proposición 5.3.3., se tiene que los primos asociados de $\mathrm{Fitt}(M)$ son exactamente los mismos que los primos asociados de $\mathrm{ann}_A(M)$. Más precisamente, si A es un DFU, y $P_1, \ldots, P_r$ denotan los factores irreducibles del gcd de un sistema de generadores de $\mathrm{Fitt}(M)$,

entonces $P_1^{\ell_1} \dots P_r^{\ell_r}$ es un generador de $\mathfrak{S}(M)$, donde ℓ_i denota la multiplicidad de $\mathfrak{S}(M)$ en $A/(P_i)$ que también suele escribirse e_i.

Aplicando estos resultados al anillo $A = \mathbb{Z}[U_{i,\alpha}]$ de coeficientes universares, que puede ser reemplazado por otro anillo aplicando la propiedad de cambio de base, tomando $M = B_\nu$ con $\nu \geq \nu_0$, se obtiene que

$$\mathfrak{S}(B_\nu) = \det((\mathbf{K}_\bullet)_\nu)A := \prod_{i=1}^{n} \det(\partial_i^\nu)^{(-1)^{i-1}} A.$$

Además, si $\nu \geq \nu_0$, se tiene que los primos asociados de $\mathrm{Fitt}(B_\nu)$ son exactamente los mismos que los primos asociados de $\mathrm{ann}_A(B_\nu)$, que $\mathrm{ann}_A(B_\nu)$ es principal y primo, y que $\mathfrak{S}(B_\nu)$ es el menor ideal principal que contiene a $\mathrm{Fitt}(B_\nu)$, esto dice que no sólo $\mathfrak{S}(B_\nu)$ es la parte de codimensión uno de $\mathrm{Fitt}(B_\nu)$, sino que $\mathfrak{S}(B_\nu) = \mathrm{ann}_A(B_\nu)$.

Ejercicios.

1. Sea A un anillo conmutativo, y sea M un A-módulo presentado por
$$A^n \xrightarrow{\phi} A^n \to M \to 0,$$
donde $\det(\phi)$ no es divisor de cero en A. Entonces
$$\mathrm{ann}_A(M) = \mathrm{Fitt}_0(M) :_A \mathrm{Fitt}_1(M).$$
2. En el contexto del ejercicio anterior, si M es un A-módulo presentado por
$$A^n \xrightarrow{\phi} A^m \to M \to 0,$$
donde $\det(\phi)$ no es divisor de cero en A, $m > n$, y $\operatorname{depth} \mathrm{ann}_A M = m - n + 1$. Entonces $\mathrm{ann}_A(M) = \mathrm{Fitt}_0(M)$.
3. Sea M un A-módulo que tiene una resolución finita de módulos elementales. Entonces las siguientes afirmaciones son verdaderas:
   a) Supongamos que se tiene dos resoluciones por módulos elementales
   $$0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$
   y
   $$0 \to F'_{n'} \to F'_{n'-1} \to \cdots \to F'_1 \to F'_0 \to M \to 0$$
   del A-módulo M, entonces
   $$\prod_{i=0}^{n} \mathrm{Fitt}(F_i)^{(-1)^i} = \prod_{i=0}^{n'} \mathrm{Fitt}(F'_i)^{(-1)^i}.$$
   b) Si se tiene una sucesión exacta de la forma $0 \to M' \to M \to M'' \to 0$ de A-módulos, donde M' y M'' admiten ambos una resolución finita de módulos elementales, entonces $\mathfrak{S}(M) = \mathfrak{S}(M')\mathfrak{S}(M'')$.
   c) Sea S un conjunto multiplicativamente cerrado de A. Entonces el A_S-módulo M_S tiene una resolución finita de módulos elementales, y además se tiene que $\mathfrak{S}(M)A_S = \mathfrak{S}(M_S)$.
   d) El ideal fraccionario $\mathfrak{S}(M)$ de A, resulta un ideal íntegro de A. Más aún es un ideal principal generado por un elemento que no es divisor de cero, tal que $\mathrm{Fitt}(M) \subset \mathfrak{S}(M)$ y es minimal con esta propiedad, es decir, si I es un ideal principal de A que contiene a $\mathrm{Fitt}(M)$, entonces también contiene a $\mathfrak{S}(M)$.

e) La propiedad (d) implica que cualquier generador de $\mathfrak{S}(M)$ sirve como gcd (máximo común divisor) de cualquier conjunto de generadores de $\mathrm{Fitt}(M)$. En particular, si A es un DFU, $\mathfrak{S}(M)$ está generado por el gcd de los generadores de $\mathrm{Fitt}(M)$.

6. Ejemplos

En esta sección desarrollaremos dos ejemplos de resultantes multihomogéneas, que serán acompañados con el correspondiente códico en Macaulay2 [GS], usando el paquete `EliminationMatrices` desarrollado junto con Laurent Busé y Manuel Dubinsky [BBD12].

Ejemplo 6.1. En este ejemplo veremos un caso muy simple, de dos polinomios homogéneos en dos variables, uno cuadrático y uno lineal. Una aplicación típica de este ejemplo es el caso del cálculo del descriminante de un polinomio f_1.

Sea $A = \mathbb{Q}[a,b,c,d,e]$ y $R = A[x,y]$, $f_1 = ax^2 + bxy + cy^2$ y $f_2 = dx + ey$.

```
i1 : load "EliminationMatrices.m2"

i2 : R=QQ[a,b,c,d,e,x,y];

i3 : f1=a*x^2+b*x*y+c*y^2;

i4 : f2=d*x+e*y;

i5 : vari = {x,y};

i6 : m =matrix {{f1,f2}};

              1       2
o6 : Matrix R  <--- R

i7 : eliminationMatrix(vari,m, Strategy=> Macaulay)

o7 = {2} | a d 0 |
     {2} | b e d |
     {2} | c 0 e |

              3       3
o7 : Matrix R  <--- R

i8 : det(oo)

        2              2
o8 = c*d  - b*d*e + a*e

o8 : R
```

Un ejemplo clásico es calcular la resultante de $f_1 = ax^2 + bxy + cy^2$ y $f_2 = 2ax + by$, que se obtiene substituyendo d por $2a$ y e por b.

```
i9 : substitute(oo,{d=>2*a, e=>b})

          2     2
o9 = - a*b  + 4a c

o9 : R

i10 : factor oo

             2
o10 = (a)(- b  + 4a*c)

o10 : Expression of class Product
```

El hecho de poder evaluar directamente d en $2a$ y e en b es justamente la propiedad de universalidad que tanto hemos remarcado. Eso dice que calcular la resultante conmuta con el morfismo de especialización.

Otra forma de calcular la matriz resultante de Macaulay `Mnu` es como el morfismo

$$M_{\nu_0} := (R(-2) \oplus R(-1) \to R)_{\nu_0}\,.$$

para $\nu_0 = (2-1)+(1-1)+1 = 2$.

```
i11 : K = koszul m

       1      2      1
o11 = R  <-- R  <-- R
      0      1      2

o11 : ChainComplex

i12 : nu = (2-1)+(1-1)+1;

i13 : Mnu = mapsComplex (nu, vari, K)

o13 = {{2} | a d 0 |, 0}
       {2} | b e d |
       {2} | c 0 e |

o13 : List

i14 : de = detComplex (nu, vari, K)

         2              2
o14 = c*d  - b*d*e + a*e

o14 : frac(R)
```

Observar que en el caso en que ν_0 es el índice de saturación, la matriz M_{ν_0} de dos polinomios homogéneos en dos variables, siempre resultará cuadrada. No es así si $\nu > \nu_0$, ni para más polinomios y más variables para ninguún ν. Podemos verificar

este hecho en este ejemplo, así como que el determinante del complejo $\mathbf{K}_\bullet(f_1, f_2; R)_\nu$ no depende de $\nu \geq \nu_0$, y coincide con $cd^2 - bde + ae^2$.

```
i15 : Mnu = mapsComplex (nu+1, vari, K)

o15 = {{3} | a 0 d 0 0 |, {1} | -d |}
       {3} | b a e d 0 |  {1} | -e |
       {3} | c b 0 e d |  {2} | a  |
       {3} | 0 c 0 0 e |  {2} | b  |
                          {2} | c  |

o15 : List
```

Esto dice que el complejo $\mathbf{K}_\bullet(f_1, f_2; R)$ en grado $\nu = 3$ se escribe

$$0 \to R(-3)_\nu \xrightarrow{(-f_2, f_1)} R(-2)_\nu \oplus R(-1)_\nu \xrightarrow{\binom{f_1}{f_2}} R_\nu \to 0,$$

el cual puede escribirse, identificando $R(-3)_\nu$ con A, $R(-2)_\nu \oplus R(-1)_\nu$ con $A^2 \oplus A^3$ y R_ν con A^4

$$0 \to A \xrightarrow{\begin{pmatrix} -d \\ -e \\ a \\ b \\ c \end{pmatrix}} A^2 \oplus A^3 \xrightarrow{\begin{pmatrix} a & 0 & d & 0 & 0 \\ b & a & e & d & 0 \\ c & b & 0 & e & d \\ 0 & c & 0 & 0 & e \end{pmatrix}} A^4 \to 0.$$

```
i16 : de = detComplex (nu+1, vari, K)

         2              2
o16 = c*d  - b*d*e + a*e

o16 : frac(R)
```

Además, el divisor asociado al 0-ésimo ideal de Fitting de M_ν, $\mathrm{Fitt}_0(M_\nu)$, para todo $\nu \geq \nu_0$, no depende de ν. Estudiando la descomposición primaria de $\mathrm{Fitt}_0(M_\nu)$, vemos que la parte principal de $\mathrm{Fitt}_0(M_\nu)$ está dada por el primo $\mathfrak{A} = (cd^2 - bde + ae^2)$.

En este ejemplo, el ideal $\mathrm{Fitt}_0(M_\nu)$ se calcula como el ideal de menores de 4 por 4 (maximales) de la matriz anterior.

```
i17 : minors(4,o15_0)

              2 2                    2         2    2           2       2
o17 = ideal (c d  - b*c*d*e + a*c*e , - b*c*d  + b d*e - a*b*e , a*c*d
      ------------------------------------------------------------------
                   2 2     2         2      3       3      2        2
      - a*b*d*e + a e , c*d e - b*d*e  + a*e , - c*d  + b*d e -a*d*e )

o17 : Ideal of R
```

Su descomposicón primaria se caalcula como sigue

```
i18 : primaryDecomposition oo
```

```
                  2              2                  2   2   2
o18 = {ideal(c*d  - b*d*e + a*e ), ideal (c, a, e , d , b )}

o18 : List
```

De acá leemos que

$$\mathrm{Fitt}_0(M_\nu) = \mathfrak{p} \cap \mathfrak{q},$$

donde $\mathfrak{A} = (cd^2 - bde + ae^2)$ es la parte principal de $\mathrm{Fitt}_0(M_\nu)$, y $\mathfrak{q} = (c, a, e^2, d^2, b^2)$ es la componente soportada sobre el ideal (a, b, c, d, e), es decir, $V(\mathfrak{q})$ es un punto múltiple sobre el origen.

Ejemplo 6.2. En este ejemplo veremos un caso apenas más complicados, de tres polinomios homogéneos en tres variables, uno cuadrático y dos lineal. La elección de los grados está limimitada por el comando `primaryDecomposition`.

Sea $A = \mathbb{Q}[a, b, c, d, e, f, g, h, x, y, z]$ y $R = A[x, y, z]$, $f_1 = ax^2 + bxy + cy^2$ y $f_2 = dx + ey$.

```
i1 : load "eliminationMatrices.m2"

i2 : R=QQ[a,b,c,d,e,f,g,h,x,y,z];

i3 : f1=a*x^2+b*x*y+c*y^2+d*z^2;

i4 : f2=e*x+a*y+f*z;

i5 : f3=g*x+h*y+e*z;

i6 : vari = {x,y,z};

i7 : m =matrix {{f1,f2,f3}};

             1       3
o7 : Matrix R  <--- R
```

Calculamos la matriz resultante de Macaulay `Mnu` como el morfismo

$$M_{\nu_0} := (R(-2) \oplus R(-1) \oplus R(-1) \to R)_{\nu_0}.$$

para $\nu_0 = 2$.

```
i8 : K = koszul m

      1      3      3      1
o8 = R  <-- R  <-- R  <-- R
     0      1      2      3

o8 : ChainComplex

i9 : nu = (2-1)+(1-1)+(1-1)+1

o9 = 2
```

Además, podemos verificar que el determinante del complejo $\mathbf{K}_\bullet(f_1, f_2 f_3; R)_\nu$ no depende de $\nu \geq \nu_0$. Además agregamos el comando `time` para mostrar el poco tiempo de cómputo que estos cálculos insumen, y verificamos que la matriz `Mnu_0` tiene rango máximo.

```
i10 : Mnu = mapsComplex (nu, vari, K)

o10 = {{2} | a e 0 0 g 0 0 |, {1} | -g |, 0}
       {2} | b a e 0 h g 0 |  {1} | -h |
       {2} | 0 f 0 e e 0 g |  {1} | -e |
       {2} | c 0 a 0 0 h 0 |  {1} | e  |
       {2} | 0 0 f a 0 e h |  {1} | a  |
       {2} | d 0 0 f 0 0 e |  {1} | f  |

o10 : List

i11 : rank Mnu_0 == rank target Mnu_0

o11 = true
```

Esto dice que el complejo $\mathbf{K}_\bullet(f_1, f_2; R)$ en grado $\nu = 2$ se escribe

$$0 \to R(-4)_\nu \xrightarrow{\delta_2^\nu} (R(-3) \oplus R(-3) \oplus R(-2))_\nu \xrightarrow{\delta_1^\nu} (R(-2) \oplus R(-1) \oplus R(-1))_\nu \xrightarrow{\delta_0^\nu} R_\nu \to 0,$$

el se escribe, siendo $\nu = 2$, identificando $R(-4)_\nu = R(-3)_\nu = 0$, $R(-2)_\nu \cong A$, $R(-1)_\nu = A^3$ y $R_\nu \cong A^6$, con

$$0 \to 0 \to 0 \oplus 0 \oplus A \xrightarrow{\begin{pmatrix} -g \\ -h \\ -e \\ e \\ a \\ f \end{pmatrix}} A \oplus A^3 \oplus A^3 \xrightarrow{\begin{pmatrix} a & e & 0 & 0 & g & 0 & 0 \\ b & a & e & 0 & h & g & 0 \\ 0 & f & 0 & e & e & 0 & g \\ c & 0 & a & 0 & 0 & h & 0 \\ 0 & 0 & f & a & 0 & e & h \\ d & 0 & 0 & f & 0 & 0 & e \end{pmatrix}} A^6 \to 0.$$

Obsérvese ahora que el cálculo del ideal de Fitting $\mathrm{Fitt}_0(\texttt{Mnu\_0})$ es casi instantáneo:

```
i12 : fitt= time(minors (rank Mnu_0, Mnu_0))
     -- used 0.003 seconds

                3 2         3       4           2        2 2
o12 = ideal (- a e f + a*b*e f - c*e f - a*b*e*f g + 2c*e f g -
      ------------------------------------------------------------
       2     2      3 2     2   2       2 2                      3
      a d*f*g  - c*f g  + 2a e*f h - b*e f h + 2a*d*e*f*g*h + b*f g*h
      ------------------------------------------------------------
           2   2      3 2   4 2    2   3        4    2
      - d*e f*h  - a*f h , a e  - a b*e  + a*c*e  + a b*e*f*g -
      ------------------------------------------------------------
            2       3   2        2 2     3            2
      2a*c*e f*g + a d*g  + a*c*f g  - 2a e*f*h + a*b*e f*h -
      ------------------------------------------------------------
        2               2           2 2    2 2 2     3 3        4
      2a d*e*g*h - a*b*f g*h + a*d*e h  + a f h , - a e  + a*b*e  -
```

```
      ------------------------------------------------------------------
         5        2          3       2     2        2 2     2 2
      c*e  - a*b*e f*g + 2c*e f*g - a d*e*g  - c*e*f g  + 2a e f*h -
      ------------------------------------------------------------------
         3            2           2         3 2        2 2     3 3
      b*e f*h + 2a*d*e g*h + b*e*f g*h - d*e h  - a*e*f h , - a e  +
      ------------------------------------------------------------------
           4      5        2          3       2     2        2 2
      a*b*e  - c*e  - a*b*e f*g + 2c*e f*g - a d*e*g  - c*e*f g  +
      ------------------------------------------------------------------
        2 2         3            2           2         3 2
      2a e f*h - b*e f*h + 2a*d*e g*h + b*e*f g*h - d*e h  -
      ------------------------------------------------------------------
           2 2   3 2         3       4                       2
      a*e*f h , a e h - a*b*e h + c*e h + a*b*e*f*g*h - 2c*e f*g*h +
      ------------------------------------------------------------------
       2   2       2 2      2     2      2   2             2
      a d*g h + c*f g h - 2a e*f*h  + b*e f*h  - 2a*d*e*g*h  -
      ------------------------------------------------------------------
         2   2      2 3      2 3     3 2         3       4
      b*f g*h  + d*e h  + a*f h , - a e g + a*b*e g - c*e g -
      ------------------------------------------------------------------
               2       2   2    2   3      2 3     2
      a*b*e*f*g  + 2c*e f*g  - a d*g  - c*f g  + 2a e*f*g*h -
      ------------------------------------------------------------------
         2                2       2 2       2   2      2   2
      b*e f*g*h + 2a*d*e*g h + b*f g h - d*e g*h  - a*f g*h )

o12 : Ideal of R
```

Su descomposición primaria se calcula así

```
i13 : primaryDecomposition fitt

                3 2        3      4                    2       2   2
o13 = {ideal(a e  - a*b*e  + c*e  + a*b*e*f*g - 2c*e f*g + a d*g  +
      ------------------------------------------------------------------
         2 2     2          2                       2         2 2
      c*f g  - 2a e*f*h + b*e f*h - 2a*d*e*g*h - b*f g*h + d*e h  +
      ------------------------------------------------------------------
         2 2                   3   4 2   6   4       2 2 2    3   2
      a*f h ), ideal(h, g, f, e , a e , a -2a b*e + a b e + 2a c*e )}
```

y se observa que

$$\mathrm{Fitt}_0(M_\nu) = \mathfrak{A} \cap \mathfrak{q},$$

donde $\mathfrak{A} = (a^3e^2 - abe^3 + ce^4 + abefg - 2ce^2fg + a^2dg^2 + cf^2g^2 - 2a^2efh + be^2fh - 2adegh - bf^2gh + de^2h^2 + af^2h^2)$ es la parte principal de $\mathrm{Fitt}_0(M_\nu)$, y $\mathfrak{q} = (h, g, f, e^3, a^4e^2, a^6 - 2a^4be + a^2b^2e^2 + 2a^3ce^2)$ es la componente soportada sobre el ideal (h, g, f, e, a), es decir, $V(\mathfrak{q})$ es un plano múltiple de codimensión 5.

Obsérvese que, como antes, $\mathfrak{A}$ puede calcularse mediante el determinante del complejo $\mathbf{K}_\bullet(f_1, f_2; R)$ en grado $\nu = 2$, uasando el comando `detComplex (nu, vari, K)`.

Apéndice

El ojectivo de esta sección es complementar el contenido de las notas con dos temas fuertemente vinculados con la teoría de eliminación, y cuyo interés trasciende la aplicación que le daremos.

Estos dos temas con, primero el estudio de los módulos de cohomología local, y luego uno de los invariantes más importantes de un módulo graduado, la regularidad de Castelnuovo-Mumford.

El primero, cohomología local, aparece en nuestras aplicaciones al definir el ideal eliminante, ya que escribimos $\mathfrak{A} = H^0_{R_+}(B)_0$, es decir, como el 0-ésimo módulo de cohomología local de B en grado 0.

El segundo, el estudio de la regularidad de Castelnuovo-Mumford, aparece al querer conocer a partir de qué grado el módulo $H^0_{R_+}(B)_\nu$ se anula. El Lema B.4 da una respuesta a este problema en el caso en que I esté dado por una sucesión regular.

A.1. Cohomología local. La cohomología local fue desarrollada por Alexander Grothendieck en la década de 1960, en parte, para responder a una conjetura de Pierre Samuel acerca de cuándo ciertos tipos de anillos conmutativos son de dominios de factorización única.

La cohomología local se ha convertido en una herramienta indispensable y es objeto de mucha investigación. Mostraremos acá algunas propiedades y aplicaciones de la cohomología local, principalmente orientadas a la teoría de regularidad.

Entre muchos otros atributos, cohomología local permite responder a muchas preguntas aparentemente difícil. Un buen ejemplo de este problema, donde cohomología local ofrece una respuesta parcial, es cuántos generadores tiene un ideal a menos de radical.

A.1.1. Como funtor derivado de $\Gamma_I(-)$. Sea R un anillo noetheriano, $I \subset R$ un ideal y M un R-módulo. Se define

$$\Gamma_I(M) := \{m \in M : \text{ existe } n \in \mathbb{N} \text{ tal que } I^n m = 0\}$$

Observación A.1. Obsérvese que $\mathrm{Hom}_R(R/I, M) = \{m \in M : Im = 0\}$ para todo ideal I de R, se obtiene el isomorfismo natural

$$\Gamma_I(M) \cong \varinjlim \mathrm{Hom}_R(R/I^n, M).$$

Luego, $M \mapsto \Gamma_I(M)$ define un funtor covariante $\Gamma_I(-)$.

Lema A.2. $\Gamma_I(-)$ *es un funtor aditivo exacto a izquierda.*

Demostración. cf. [Hun07, Sec. 2] o [BH93, Prop. 3.5.1] en el caso $I = \mathfrak{m}$. □

Definición A.3. Los funtores de cohomología local $H^i_I(-)$ son los funtores derivados a derecha de $\Gamma_I(-)$. Es decir, si $\mathcal{I}^\bullet$ es una resolución injectiva del R-módulo M, entonces $H^i_I(M) \cong H^i(\Gamma_I(\mathcal{I}^\bullet))$ para todo $i \geq 0$.

Observación A.4. Sea R un anillo noetheriano.

1. Sea M un R-módulo, entonces $H^0_I(M) \cong \Gamma_I(M)$ y $H^i_I(M) = 0$ para todo $i < 0$;
2. si J es un R-módulo injectivo, entonces $H^i_I(J) = 0$ para todo $i > 0$;

3. para todo R-módulo M y todo $i \geq 0$ se tiene
$$H^i_I(M) \cong \lim_{\to} \operatorname{Ext}^i_R(R/I^n, M);$$

Hay una inyección natural
$$\varphi : \operatorname{Ext}^0_R(R/I^n, M) = \hom(R/I^n, M) \to M$$
dada por $\varphi(f) = f(1)$, tal que $\operatorname{im}(\varphi) = \{m \in M : I^n m = 0\} = 0 :_M I^n$.

Aplicando el funtor límte directo $\lim_{\to} \operatorname{Ext}^0_R(R/I^n, M) = \lim_{\to} \hom(R/I^n, M)$ que coincide con la unión $\cup_n m \in M : I^n m = 0$ que a su vez coincide con $\Gamma_I(M)$ por definición.

El funtor $\operatorname{Ext}^i_R(R/I^{\cdot}, -)$ es el i-ésimo derivado del funtor $\hom_R(R/I^n, -)$. Tomando colímites filtrantes, que conmutan con tomar funtores derivados por ser el colímite filtrante un funtor exacto (cf. [Eis95, Prop. A6.4]) se obtiene la equivalencia deseada.

Observación A.5. Sea R un anillo noetheriano.

1. como $H^\bullet_I(-)$ es un δ-funtor, dada una sucesión exacta corta de R-módulos $0 \to M' \to M \to M'' \to 0$, da una sucesión exacta larga de cohomología
$$0 \to \Gamma_I(M') \to \Gamma_I(M) \to \Gamma_I(M'') \to H^1_I(M') \to \cdots$$
2. además, si I y J son ideales de A, como $\{I^n + J^n\}$ es cofinal con $\{(I+J)^n\}$ y $\{I^n \cap J^n\}$ es cofinal con $\{(I \cap J)^n\}$, y $\Gamma_I(\Gamma_J(M)) = \Gamma_J(\Gamma_I(M)) = \Gamma_{I+J}(M)$, de la sucesión exacta corta
$$0 \to R/(I^n \cap J^n) \to R/I^n \oplus R/J^n \to R/(I^n + J^n) \to 0,$$
aplicando $\operatorname{Hom}_R(-, M)$, se tiene la sucesión exacta larga de Mayer-Vietoris
$$0 \to \Gamma_{I+J}(M) \to \Gamma_I(M) \oplus \Gamma_J(M) \to \Gamma_{I\cap J}(M) \to H^1_{I+J}(M) \to \cdots .$$

A.1.2. Como la homología del complejo de Čech. Sea S un anillo noetheriano, $R = S[x_1, \ldots, x_n]$, $\mathfrak{m} := (x_1, \ldots, x_n)$ el único ideal maximal graduado y M un R-módulo. El morfismo de localización en x_i define un complejo
$$\mathcal{C}^\bullet_{\mathfrak{m}}(M) : 0 \to M \to \oplus_i M_{x_i} \to \oplus_{i,j} M_{x_i x_j} \to \cdots$$
Observe que $\ker(M \to \oplus_i M_{x_i}) = \Gamma_{\mathfrak{m}}(M)$. Por lo tanto, $H^0_{\mathfrak{m}}(M) = H^0(\mathcal{C}^\bullet_{\mathfrak{m}})$

Proposición A.6. *Para todo R-módulo M y para todo $i \geq 0$,*
$$H^i_{\mathfrak{m}}(M) = H^i(\mathcal{C}^\bullet_{\mathfrak{m}}).$$

Si R no es noetheriano, el complejo de Čech recién definido no siempre calcula los funtores derivados de $\Gamma_I(-)$ en la categoría de R-módulos. Ni siquiera si I es finitamente generado. Por esta y otras razones, la definición general de cohomología local probablemente debe hacerse en una categoría más amplia (haces sobre $\operatorname{Spec}(R)$, cf. [Har67]).

Ejemplo A.7. Sea p un número primo. Calculamos $H_{\mathfrak{p}}(\mathbb{Z})$, donde $\mathfrak{p}$ es el ideal generado por p. Dado que $\mathbb{Z}$ es un dominio de ideales principales, todos los módulos divisibles son inyectivos, y entonces una resolución inyectiva de $\mathbb{Z}$ está dada por $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

El funtor $\Gamma_{\mathfrak{p}}(-)$ calcula la p^n-torsión para todo n. Aplicando este funtor a la resolución inyectiva, se obtiene que hay un único término que no se anula, que vivie en lugar cohomológico 1, a saber $\Gamma_{\mathfrak{p}}(\mathbb{Q}/\mathbb{Z})$. Por lo tanto todas las cohomologías locales se

anulan, excepto por $H^1_{\mathfrak{p}}(\mathbb{Z})$, que es isomorfa a la p-torsión en $\mathbb{Q}/\mathbb{Z}$. Por la propiedad de factorización única, este módulo puede ser identificado con $\mathbb{Z}[p^{-1}]/\mathbb{Z}$, donde $\mathbb{Z}[p^{-1}]$ es el anillo de los números racionales cuyos denominadores son una potencia de p.

Ejemplo A.8. Un ejemplo muy similar que sea más en la dirección de estas notas es el cálculo de los $H^i_{R_+}(M)$, donde $R = k[X]$, k es un cuerpo, $R_+ = (X)$, y M es un R-módulo finitamente generado.

Por el teorema de estructura para dominio de ideales principales, M es suma directa de módulos cíclicos. Como los funtores de cohomología local conmutan con sumas directas, que basta con calcular la cohomología local de $R/(g)$ para algún $g \in R$.

En primer lugar, calcular la cohomología local de R sobre sí mismo, es decir, cuando $g = 0$. Como en el ejempoplo anterior, como R es un dominio de ideales principales, todo módulos divisible es inyectivo.

La cápsula inyectiva de R es su cuerpo de fracciones $K = k(X)$, y como K/R es divisible, resulta inyectivo.

Así una resolución inyectiva está dada por

$$0 \to R \to K \to K/R \to 0.$$

Ahora aplicamos $\Gamma_{R_+}(-)$ y calculamos la cohomología local como la cohomología del complejo

$$0 \to \Gamma_{R_+}(K) \to \Gamma_{R_+}(K/R) \to 0.$$

Se desprende que $H^j_{R_+}(R) = 0$ para todo $j \neq 1$ y se puede identificar $\Gamma_{R_+}(K/R) \cong H^1_{R_+}(R)$.

Como antes, la propiedad de factorización única muestra que $H_{R_+}(R) \cong R[X^{-1}]/R = k[X, X^{-1}]/k[X]$.

Este módulo tiene una k-base formada por elementos de la forma $\frac{1}{X^n}$, con $n \geq 1$. La multiplicación por X en actúa de forma usual, $X \cdot \frac{1}{X^n} = \frac{1}{X^{n-1}}$ si $n > 1$, y al final, cuando $n = 1$, $X \cdot \frac{1}{X} = 0$.

Para calcular $H^i_{R_+}(R/(g))$ cuando $g \neq 0$, se utiliza la secuencia exacta corta,

$$0 \to R \xrightarrow{\times g} R \to R/(g) \to 0.$$

Esta sucesión exacta corta induce una larga sucesión exacta en cohomología, con las flechas de $H^i_{R_+}(R)$ a $H^i_{R_+}(R)$ dadas por la multiplicación por g. Dado que sólo hay un sólo módulo de cohomología local no nulo de R, se obtiene una sucesión exacta de cuatro términos:

$$0 \to H^0_{R_+}(R/(g)) \to H^1_{R_+}(R) \xrightarrow{\times g} H^1_{R_+}(R) \to H^1_{R_+}(R/(g)) \to 0.$$

Como cada elemento de $H^1_{R_+}(R)$ es anulado por una potencia de R_+, si h es un elemento coprimo con X, entonces h debe actuar como una unidad en $H^1_{R_+}(R)$. Esto último se debe a que existen $a, b \in R$ tales que $ah = 1 - bX$, y $1 - bX$ actúa como una unidad en este módulo. Escribiendo $g = X^n h$ donde $\gcd(h, X) = 1$, se deduce que $H^0_{R_+}(R/(g))$ es el núcleo de la multiplicación por X^n en $H^1_{R_+}(R)$ y $H^1_{R_+}(R/(g))$ es el conúcleo de la multiplicación por X^n. El conjunto de elementos en $H^1_{R_+}(R)$ anulados por X^n es generado por $\frac{1}{X^n}$ y por lo tanto es isomorfo a $R/(X^n)$. Como $H^1_{R_+}(R) = R[X^{-1}]/R$, este módulo es divisible por R, y por lo tanto el conúcleo es 0.

Resumimos los resultados: si $g = 0$, entonces $H^i_{R_+}(R) = 0$ para todo $i \neq 1$, y $H^1_{R_+}(R) \cong R[X^{-1}]/R = \frac{1}{X}k[X^{-1}]$. Si $g \neq 0$, escribimos $g = X^n h$, donde X no divide h, se tiene que $H^i_{R_+}(R/(g)) = 0$ para todo $i \neq 0$ y $H^0_{R_+}(R/(g)) \cong R/(X^n)$.

Como corolario de este ejemplo se desprenden (por inducción) dos resultados: el primero correspondiente al caso $g = 0$

Corolario A.9. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), y sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R. Entonces*

$$H^i_{R_+}(R) = 0 \text{ para todo } i \neq n, \text{ y } H^n_{R_+}(R) \cong \tfrac{1}{X_1 \cdots X_n} A[X_1^{-1}, \ldots, X_n^{-1}].$$

El segundo corolario corresponde al caso $g \neq 0$.

Corolario A.10. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R y $f_1, \ldots, f_n$ n polinomios homogéneos de R, con $\deg(f_i) = d_i$, que forman una sucesión regular en R. Escribamos $B := R/(f_1, \ldots, f_n)$. Entonces*

$$H^i_{R_+}(B) = 0 \text{ para todo } i \neq 0, \text{ y } H^0_{R_+}(B) \cong R/(X_1^{d_1}, \ldots, X_n^{d_n}).$$

A continuación enunciamos una propiedad fundamental de la cohomología local que nos permite cambiar de bases.

Proposición A.11. *Sea R un anillo noetheriano, I un ideal y M un R-módulo. Sea $\phi : R \to R'$ un morfismo de anillos y M' un R'-módulo. Sea I' el ideal $I \cdot R'$ en R'.*

1. *Si ϕ es playa entonces $H^j_I(M) \otimes_R R' \cong H^j_{I'}(M \otimes_R R')$. En particular, la cohomología local conmuta con localización y completación.*
2. *$H^j_I(N) \cong H^j_{I'}(N)$, donde la primera cohomología local es calculada sobre R y la segunda sobre R'.*

Demostración. Elija generadores $x_1, \ldots, x_n$ de I. El primer punto se sigue del hecho que $\mathcal{C}_\bullet(\mathbf{X}; M) \otimes_R R' \cong \mathcal{C}_\bullet(\mathbf{X}; M \otimes_R R')$, y como R' es playo sobre R la cohomología conmuta con $\otimes$.

El segundo punto es consecuencia de los isomorfismos $\mathcal{C}_\bullet(\mathbf{X}; N) \cong \mathcal{C}_\bullet(\mathbf{X}; R) \otimes_R N \cong \mathcal{C}_\bullet(\mathbf{X}; R) \otimes_R R' \otimes_{R'} N \cong \mathcal{C}_\bullet(\phi(\mathbf{X}); R') \otimes_R N \cong \mathcal{C}_\bullet(\phi(\mathbf{X}); N)$. □

Ésto dice que calcular la cohomología local sobre el anillo de base coincide con hacerlo sobre la localización.

B.2. Regularidad de Castelnuovo-Mumford. La regularidad de Castelnuovo-Mumford es un invariante fundamental en álgebra conmutativa y en geometría algebraica. Es una especie de cota universal para invariantes importantes de álgebras graduadas como por ejemplo para el máximo grado de las syzygies de un ideal y para el máximo grado de no-nulidad de los módulos de cohomología local.

Intuitivamente, mide la complejidad de un módulo o de un haz: la regularidad de un módulo aproxima el mayor grado de un generador minimal y la regularidad de un haz estima el menor twist para el cual el haz está generado por sus secciones globales. Este invariante fue usado para medir la complejidad de problemas computacionales en geometría algebraica y en álgebra conmutativa (ver por ejemplo [EG84] o [BM93]).

Se ha intentado encontrar cotas superiores para la regularidad de Castelnuovo-Mumford en termino de invariantes más simples como por ejemplo lo son la dimensión y la multiplicity. De todas formas, la regularidad de Castelnuovo-Mumford no puede ser acotada en término de ninguno de éstos dos, lo cual hace su cálculo aun más interesante y no trivial en muchos casos.

A pesar de que la definición original, dada por Mumford en 1966 en [Mum66] fue enunciada en término de anulación de la cohomología de haces, daremos una definición

puramente algebraica de esta regularidad, en términos de módulos cohomología local, dada originalmente por Ooishi en 1982 [Ooi82]. Cabe mencionar que las dos definiciones puramente algebraicas más populares de regularidad de Castelnuovo-Mumford son, una en término de números de Betti introducida por Eisenbud y Goto en 1984 en [EG84] y la otra usando cohomología local (ver def. en A.3), que es la que adoptaremos.

Hay dos resultados esenciales que motivan definir la regularidad de Castelnuovo-Mumford en términos de cohomología local: el teorema de Grothendieck que establece que $H^i_{\mathfrak{m}}(M) = 0$ para $i > \dim(M)$ y $i < \operatorname{depth}(M)$, así como la no nulidad de estos módulos para $i = \dim(M)$ y $i = \operatorname{depth}(M)$; y el teorema de anulación de Serre que determina la anulación de las piezas graduadas $H^i_{\mathfrak{m}}(M)_\mu$ para todo i, y todo $\mu \gg 0$. La regularidad de Castelnuovo-Mumford es una cota inferior para este grado de anulación.

Si $H^i_{\mathfrak{m}}(M) \neq 0$, se define

$$a_i(M) := \sup\{\mu \mid H^i_{\mathfrak{m}}(M)_\mu \neq 0\}, \tag{B.1}$$

en caso contrario, $a_i(M) := -\infty$. Una notación también frecuente en la literatura es la de "end", en nuestro caso, escribiríamos $a_i(M) := \operatorname{end}(H^i_{\mathfrak{m}}(M))$.

Definición B.1. (Regularidad Castelnuovo-Mumford) Sea M un R-módulo graduado y sea $\ell \in \mathbb{N}_0$. Se define la regularidad de Castelnuovo-Mumford de M a nivel ℓ como

$$\operatorname{reg}^\ell(M) := \sup\{a_i(M) + i : i \geq \ell\}.$$

La regularidad de Castelnuovo-Mumford de M se define como

$$\operatorname{reg}(M) := \operatorname{reg}^0(M).$$

Obsérvese que como $\operatorname{cd}_{\mathfrak{m}}(M) < \infty$, tenemos

$$\operatorname{reg}^\ell(M) \in \mathbb{Z} \cup \{-\infty\}.$$

El máximo sobre los i positivos es también un invariante interesante:

$$\operatorname{greg}(M) := \sup_{i>0}\{a_i(M) + i\} = \operatorname{reg}(M/H^0_{\mathfrak{m}}(M)).$$

Ver Bayer y Mumford [BM93] o [Mum66].

A continuación repasamos algunos hechos simples sobre la regularidad.

Lema B.2. *Sea M un R-módulo graduado finitamente generado $\ell, k \in \mathbb{N}_0$. Luego, se tienen las siguientes afirmaciones:*

1. *Si $k \geq l$ entonces* $\operatorname{reg}^k(M) \leq \operatorname{reg}^\ell(M)$.
2. *Para todo $n \in \mathbb{Z}$ se tiene* $\operatorname{reg}^\ell(M(n)) = \operatorname{reg}^\ell(M) - n$.
3. $\operatorname{reg}(M) = \operatorname{máx}\{\operatorname{end}(\Gamma_{\mathfrak{m}}(M)), \operatorname{reg}^1(M)\}$.
4. $\operatorname{reg}(M/\Gamma_{\mathfrak{m}}(M)) = \operatorname{reg}^1(M/\Gamma_{\mathfrak{m}}(M)) = \operatorname{reg}^1(M) \leq \operatorname{reg}(M)$.
5. *$M = \Gamma_{\mathfrak{m}}(M)$ si y sólo si* $\operatorname{reg}^1(M) = -\infty$.
6. *$M = 0$ si y sólo si* $\operatorname{reg}(M) = -\infty$.

Podemos dar una caracterización alternativas de Regularidad en nivel ℓ, sin necesitar pasar por la definición de los módulos $a_i(M)$:

Para todo $\ell \in \mathbb{N}_0$ y que todo R-módulo graduado finitamente generado tiene:

$$\operatorname{reg}^\ell(M) = \operatorname{ínf}\{r \in \mathbb{Z} : H^i_{\mathfrak{m}}(M)_{r+i-\ell} = 0, \forall i \geq \ell\}. \tag{B.2}$$

A continuación damos dos resultados que son los que motivaron este apéndice sobre regularidad, por su aplicación a estas notas sobre resultantes.

Lema B.3. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), y sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R. Entonces*

$$\operatorname{reg}(R) = 0.$$

Además, $\operatorname{reg}(R) = \operatorname{reg}^\ell(R)$ *para todo* $\ell \leq n$.

Demostración. Por el Corolario A.9 se tiene que $H^i_{R_+}(R) = 0$ para todo $i \neq n$, y $H^n_{R_+}(R) \cong \frac{1}{X_1 \cdots X_n} A[X_1^{-1}, \ldots, X_n^{-1}]$. Aplicando la definición de $a_i(R)$ dada en (B.1)

$$a_n(R) := \sup\{\mu \mid H^n_{\mathfrak{m}}(R)_\mu \neq 0\}, \text{ y } a_i(R) = -\infty \text{ si } i \neq n.$$

Ahora, como $H^n_{\mathfrak{m}}(R)_\mu = \frac{1}{X_1 \cdots X_n} A[X_1^{-1}, \ldots, X_n^{-1}]_\mu$, tenemos $H^n_{\mathfrak{m}}(R)_{-n} \cong \frac{1}{X_1 \cdots X_n} A \neq 0$ y $H^n_{\mathfrak{m}}(R)_\mu = 0$ si $\mu \geq -n+1$. Luego, $a_n(R) = -n$.

Por la Definición B.1 se tiene que $\operatorname{reg}^\ell(R) := \sup\{a_i(R) + i : i \geq \ell\}$, de lo que se deduce que para todo $\ell \leq n$,

$$\operatorname{reg}(R) = \operatorname{reg}^\ell(R) = \operatorname{reg}^n(R) = a_n(R) + n = -n + n = 0. \qquad \square$$

El segundo corolario corresponde al caso $g \neq 0$.

Lema B.4. *Si $R = A[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre un dominio A (esta hipótesis puede ser relajada), sea $R_+ := (X_1, \ldots, X_n)$ el ideal maximal irrelevante de R y $f_1, \ldots, f_n$ n polinomios homogéneos de R, con $\deg(f_i) = d_i$, que forman una sucesión regular en R. Escribamos $B := R/(f_1, \ldots, f_n)$. Entonces*

$$\operatorname{reg}(B) = \sum_i (d_i - 1).$$

Además, $\operatorname{reg}^\ell(R) = -\infty$ *para todo* $\ell \geq 1$.

Demostración. Por el Corolario A.10 se tiene que $H^i_{R_+}(B) = 0$ para todo $i \neq 0$, y $H^0_{R_+}(B) \cong R/(X_1^{d_1}, \ldots, X_n^{d_n})$. Aplicando la definición de $a_i(R)$ dada en (B.1)

$$a_0(R) := \sup\{\mu \mid H^0_{\mathfrak{m}}(R)_\mu \neq 0\}, \text{ y } a_i(R) = -\infty \text{ si } i \neq 0.$$

Sea $\mu_0 := \sum_i (d_i - 1)$. Como $H^0_{R_+}(B) : \mu \cong R/(X_1^{d_1}, \ldots, X_n^{d_n})_\mu$, tenemos que $H^0_{\mathfrak{m}}(B)_{\mu_0}$ es isomorfo al A-módulo $X_1^{d_1-1} \cdots X_n^{d_n-1} A \neq 0$ y $H^0_{\mathfrak{m}}(B)_\mu = 0$ si $\mu \geq \mu_0$. Luego, $a_0(B) = \mu_0$.

Por la Definición B.1 se tiene que $\operatorname{reg}^\ell(B) - \infty$ si $\ell \geq 1$, y que

$$\operatorname{reg}(B) = \operatorname{reg}^0(B) = a_0(B) + 0 = \mu_0. \qquad \square$$

Este resultado demuestra que $H^0_{\mathfrak{m}}(B)_\nu = 0$ si $\nu \geq \nu_0 := \sum_i (d_i - 1) + 1$, y que además, este valor es óptimo.

Ejercicios.

1. Probar que $\Gamma_I(-)$ es un funtor aditivo exacto a izquierda
2. Probar el Corolario A.9.
3. Probar el Corolario A.10.
4. Extender el Corolario A.10 al caso de $r < n$ polinomios homogéneos de $R = A[X_1, \ldots, X_n]$, con $\deg(f_i) = d_i$, que forman una sucesión regular en R.
5. Probar el Lema B.2.

Referencias

[BBD12] Nicolás Botbol, Laurent Busé, and Manuel Dubinsky. Package for elimination theory. *Available on Macaulay2 website*, 2012.

[BH93] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[BM93] Dave Bayer and David Mumford. What can be computed in algebraic geometry? In *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, Sympos. Math., XXXIV, pages 1–48. Cambridge Univ. Press, Cambridge, 1993.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Dem84] Michel Demazure. Une définition constructive du resultant. *Centre de Mathématiques de l'Ecole Polytechnique*, 2(Notes informelles du calcul formel 1984-1994):0–23, May 1984.

[EG84] David Eisenbud and Shiro Goto. Linear free resolutions and minimal multiplicity. *J. Algebra*, 88(1):89–133, 1984.

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes*. Graduate Texts in Mathematics. 197. New York, NY: Springer. x, 294 p., 2000.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[GKZ94] Israel M Gel′fand, Mikhail M Kapranov, and Andrei V Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc, Boston, MA, 1994.

[GS] Daniel R Grayson and Michael E Stillman. Macaulay 2, a software system for research in algebraic geometry. *http://www.math.uiuc.edu/Macaulay2/*.

[Har67] Robin Hartshorne. *Local cohomology*, volume 1961 of *A seminar given by A. Grothendieck, Harvard University, Fall*. Springer-Verlag, Berlin, 1967.

[Hun07] Craig Huneke. Lectures on local cohomology. In *Interactions between homotopy theory and algebra*, volume 436 of *Contemp. Math*, pages 51–99. Amer. Math. Soc, Providence, RI, 2007. Appendix 1 by Amelia Taylor.

[Hur13] Hurwitz. Uber die tragheitsformen eines algebraischen moduls. 3:20, 1913.

[Jou91] Jean-Pierre Jouanolou. Le formalisme du résultant. *Adv. Math*, 90(2):117–263, 1991.

[Mac65] Robert E MacRae. On an application of the Fitting invariants. *J. Algebra*, 2:153–169, 1965.

[Mum66] David Mumford. *Lectures on curves on an algebraic surface*. With a section by G. M. Bergman. Annals of Mathematics Studies, No. 59. Princeton University Press, Princeton, N.J., 1966.

[Nor76] D. G. Northcott. *Finite free resolutions*. Cambridge University Press, Cambridge, 1976. Cambridge Tracts in Mathematics, No. 71.

[Ooi82] Akira Ooishi. Castelnuovo's regularity of graded rings and modules. *Hiroshima Math. J.*, 12:627–644, 1982.

Departamento de Matemática, FCEN, Universidad de Buenos Aires, Argentina
E-mail address: nbotbol@dm.uba.ar

TORRES RECURSIVAS DE CUERPOS DE FUNCIONES SOBRE CUERPOS FINITOS

RICARDO TOLEDANO

RESUMEN. Se estudia el problema de la construcción de torres recursivas de cuerpos de funciones sobre cuerpos finitos con buenas propiedades asintóticas.

ÍNDICE

INTRODUCCIÓN

Un cuerpo de funciones algebraicas F de una variable sobre un cuerpo K es un cuerpo F en el cual existe un elemento x trascendente sobre K tal que la extensión de cuerpos $F/K(x)$ es finita. Una torre de cuerpos de funciones sobre un cuerpo perfecto K es una sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre K que cumple varias condiciones de naturaleza técnica que se detallan en la Sección 1.3. Las torres de cuerpos de funciones han sido estudiadas con bastante profundidad a partir de la década del 80 debido, principalmente, a los trabajos de Goppa [6] y de Tsfasman, Vladut y Zink [12] en los cuales se muestra la utilidad de estas teorías matemáticas en problemas relacionados con la teoría de códigos algebraicos. En este curso veremos ejemplos de construcción de las denominadas torres de cuerpos de funciones sobre cuerpos finitos asintóticamente buenas (ver Secciones 2 y 3). Esta clase de torres es la que tiene importancia en la teoría de códigos pues permitirían la construcción de códigos cuyos parámetros superan ciertas cotas teóricas que, hasta hace un tiempo atrás, se creían que eran muy difíciles de superar. La referencia básica que mencionaremos para ciertos resultados que no demostraremos es el libro de Stichtenoth [11]. También se pueden estudiar varios de los conceptos mencionados en este curso en los libros de Rosen [9] y de Niederreiter y Xing [8] (en particular en el libro de Niederreiter y Xing se estudian también propiedades asintóticas de torres (no recursivas) de cuerpos de funciones con métodos de la teoría de cuerpos de clases). En el capítulo 7 de [11] y en el artículo [4]

de García y Stichtenoth se puede encontrar la mayoría de los resultados básicos de la teoría asintótica de torres recursivas de cuerpos de funciones. Varios resultados de las Secciones 2 y 3 han sido tomados de la tesis doctoral de María Chara (Universidad Nacional del Litoral e IMAL, 2012) a quien agradezco haberme permitido usarlos en estas notas.

1. Definiciones y Resultados Básicos

1.1. Cuerpos de Funciones. Sean $K \subset F$ cuerpos. Decimos que F es un *cuerpo de funciones algebraicas sobre* K si existe un elemento $x \in F$ trascendente sobre K tal que F es una extensión finita de $K(x)$.

El conjunto

$$\tilde{K} := \{z \in F \,:\, z \text{ es algebraico sobre } K\},$$

es un subcuerpo de F que se denomina *cuerpo de constantes de* F *sobre* K. Se tiene que $K \subseteq \tilde{K} \subseteq F$, y se verifica fácilmente que F es un cuerpo de funciones sobre $\tilde{K}$. Decimos que K es *algebraicamente cerrado en* F (o que K *es el cuerpo total de constantes de* F) si $\tilde{K} = K$, es decir, los únicos elementos de F que son algebraicos sobre K son los elementos de K.

Sea F un cuerpo de funciones sobre K. Un *anillo de valuación* de F es un anillo $\mathcal{O} \subseteq F$ que tiene las siguientes propiedades:

I) $K \subsetneq \mathcal{O} \subsetneq F$, y
II) para cualquier $0 \neq z \in F$ se tiene que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Se sabe que $\mathcal{O}$ es un anillo local, es decir, $\mathcal{O}$ tiene un único ideal maximal P (ver [11, Proposición 1.1.5]).

Teorema 1.1. [11, Teorema 1.1.6] *Sea $\mathcal{O}$ un anillo de valuación de un cuerpo de funciones F sobre K y sea P su único ideal maximal. Entonces:*

a) P es un ideal principal.
b) Si $P = t\mathcal{O}$ entonces cualquier $0 \neq z \in F$ tiene una representación única en la forma $z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$.
c) $\mathcal{O}$ es un dominio de ideales principales. Más precisamente, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.

Un *lugar* (o también *primo*) P del cuerpo de funciones F es el ideal maximal de algún anillo de valuaciones $\mathcal{O}$ de F. Cualquier elemento $t \in P$ tal que $P = t\mathcal{O}$ se llama *elemento primo* (o *parámetro local*) para P.

Cada anillo de valuación $\mathcal{O}$ de F determina un único lugar P de F y recíprocamente. Debido a esto, es usual denotar por $\mathcal{O}_P$ al anillo de valuación unívocamente determinado por el lugar P.

El conjunto de lugares de F se denotará por $\mathbb{P}(F)$. Se omite el cuerpo K en esta notación pues para cada lugar P de F se puede probar que $\tilde{K} \subseteq \mathcal{O}_P$.

Un ejemplo básico e importante de cuerpo de funciones es el denominado *cuerpo de funciones racionales* $K(x)$ donde x es un elemento trascendente sobre K. En este caso los anillos de valuaciones están asociados de manera unívoca a los polinomios mónicos irreducibles con coeficientes en K con una excepción: sea $f \in K[x]$ un polinomio mónico e irreducible sobre K. El conjunto

$$\mathcal{O}_f := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0 \text{ y } f \nmid g\},$$

es un anillo de valuación de $K(x)$ y su ideal maximal es

$$P_f := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0,\ f|h \text{ y } f \nmid g\}\,.$$

También el conjunto

$$\mathcal{O}_\infty := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0 \text{ y } deg\, f \leq deg\, g\}\,,$$

es un anillo de valuación de $K(x)$ y su ideal maximal es

$$P_\infty := \{\frac{h(x)}{g(x)} \,:\, h, g \in K[x], g \neq 0 \text{ y } deg\, f < deg\, g\}\,,$$

y se lo denomina *lugar (o lugar o primo) infinito*. Se demuestra en [11, Proposition 1.2.1] que los lugares de $K(x)$ son los arriba mencionados y que

$$deg\, P_f = deg\, f\,,\ deg\, P_\infty = 1 \text{ y } K \text{ es el cuerpo total de constantes de } K(x)\,.$$

Una descripción alternativa de un lugar, que resulta de utilidad en muchos casos, está dada en términos de las denominadas valuaciones discretas de F.

Una *valuación discreta* de F es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:

1) $v(x) = \infty$ si y sólo si $x = 0$.
2) $v(xy) = v(x) + v(y)$ para todo $x, y \in F$.
3) $v(x + y) \geq \text{mín}\{v(x), v(y)\}$ para todo $x, y \in F$.
4) Existe un elemento $z \in F$ con $v(z) = 1$.
5) $v(a) = 0$ para todo $0 \neq a \in K$.

En este contexto el símbolo ∞ representa un elemento que no está en $\mathbb{Z}$ y que satisface las siguientes propiedades: $\infty + \infty = \infty + n = n + \infty = \infty$ y $\infty > m$ para todo $m, n \in \mathbb{Z}$. De las propiedades (2) y (4) se obtiene que $v : F \to \mathbb{Z} \cup \{\infty\}$ es sobreyectiva. La propiedad (3) se llama *Desigualdad Triangular*.

Bajo ciertas condiciones se tiene la igualdad en la Desigualdad Triangular.

Lema 1.2. [11, Lema 1.1.11](Desigualdad Triangular Estricta) *Sea v una valuación discreta de F y sean $x, y \in F$ con $v(x) \neq v(y)$. Entonces*

$$v(x + y) = \text{mín}\{v(x), v(y)\}.$$

Por cada lugar P de F se puede definir una valuación discreta v_P de F de la siguiente manera: sea t un elemento primo para P. Entonces todo $0 \neq z \in F$ tiene una representación única $z = t^n u$ con $u \in \mathcal{O}_P^*$ y $n \in \mathbb{Z}$. Se define

$$v_P(z) := n \quad \text{y} \quad v_P(0) := \infty\,.$$

Teorema 1.3. [11, Teorema 1.1.13] *Sean F un cuerpo de funciones sobre K y P un lugar de F. La función v_P recién definida es una valuación discreta de F. Más aún, tenemos que*

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\},$$

$$\mathcal{O}_P^* = \{z \in F : v_P(z) = 0\},$$

$$P = \{z \in F : v_P(z) > 0\}.$$

En el caso del cuerpo de funciones racionales $K(x)$ las valuaciones discretas están determinadas por los polinomios mónicos e irreducibles con coeficientes en K y por el lugar infinito P_∞ de la siguiente manera (ver [11, Proposition 1.2.1]): si $f \in K[x]$ es mónico e irreducible y $z(x) = h(x)/g(x) \in K(x)$ entonces

$$\nu_{P_f}(z(x)) = n, \text{ si } z(x) = f(x)^n \frac{r(x)}{t(x)},$$

donde $f \nmid r$ y $f \nmid t$. En el caso del lugar infinito P_∞ se tiene que si $z(x) = h(x)/g(x) \in K(x)$ entonces

$$\nu_{P_\infty}(z(x)) = deg\, g - deg\, h\,.$$

Sea P un lugar de F y sea $\mathcal{O}_P$ su anillo de valuaciones. Como P es un ideal maximal, el anillo de clases residuales $\mathcal{O}_P/P$ es un cuerpo que contiene una copia isomorfa de K. Por lo tanto consideraremos que $K \subset \mathcal{O}_P/P$. Para $x \in \mathcal{O}_P$ denotamos por $x(P)$ a la clase de residuos módulo P y para $x \in F \setminus \mathcal{O}_P$ definimos $x(P) = \infty$. Sea $P \in \mathbb{P}(F)$.

a) $F_P := \mathcal{O}_P/P$ es el *cuerpo de clases residuales* de P. La función

$$\begin{array}{ccc} F & \longrightarrow & F_P \cup \{\infty\} \\ x & \longmapsto & x(P) \end{array}$$

se denomina *función de clases residuales*.

b) Definimos el *grado de* P como $deg\, P := [F_P : K]$. Un lugar de grado uno, se dice que es un *lugar racional* de F.

Por ejemplo, los lugares racionales de $K(x)$ están en correspondencia unívoca con los elementos de K y el lugar infinito P_∞. El grado de un lugar es siempre finito, más aún, tenemos el siguiente resultado.

Proposición 1.4. [11, Proposición 1.1.15] *Sean F un cuerpo de funciones sobre K y $P \in \mathbb{P}(F)$. Si $0 \neq x \in P$ entonces*

$$deg\, P \leq [F : K(x)] < \infty.$$

Observación 1.5. Para el caso en que $deg\, P = 1$ tenemos que $F_P = K$, y la función de clases residuales, aplica F en $K \cup \{\infty\}$. En particular, si K es algebraicamente cerrado, todos los lugares son de grado uno, y por lo tanto se puede mirar a cada elemento $z \in F$ como una función

$$\begin{array}{rccc} z: & \mathbb{P}(F) & \longrightarrow & K \cup \{\infty\} \\ & P & \longmapsto & z(P). \end{array}$$

Es por esto que a F se lo denomina cuerpo de funciones. Los elementos de K, interpretados como funciones, son funciones constantes y por esta razón K recibe el nombre de cuerpo de constantes de F.

Sea $z \in F$ y $P \in \mathbb{P}(F)$. Decimos que P es un *cero* de orden m de z si $v_P(z) = m > 0$. Decimos que P es un *polo* de orden m de z si $v_P(z) = m < 0$. Notar que en el caso de $K(x)$ el lugar P_∞ es el polo de x mientras que P_f es el cero (de orden uno) de $f(x)$.

Observación 1.6. [11, Corolario 1.3.4] En un cuerpo de funciones F sobre K todo elemento $0 \neq z \in F$ tiene una cantidad finita de ceros y de polos.

Para evitar complicaciones técnicas y casos patológicos supondremos, de ahora en adelante, que el cuerpo de constantes K es algebraicamente cerrado en F, es decir, $\tilde{K} = K$.

El grupo abeliano libre generado por los lugares de F se denomina *grupo de divisores* de F y lo denotamos por $\mathcal{D}_F$, es decir,

$$\mathcal{D}_F = \left\{ \sum_{P\in\mathbb{P}(F)} n_P P : n_P \in \mathbb{Z} \text{ y casi todo}^1\ n_P = 0 \right\}.$$

Los elementos de $\mathcal{D}_F$ se llaman *divisores* de F. Si $D = \sum_{P\in\mathbb{P}(F)} n_P P \in \mathcal{D}_F$ el *soporte* de D se define como

$$supp\, D := \{P \in \mathbb{P}(F) : n_P \neq 0\}.$$

Un divisor de la forma $D = P$ con $P \in \mathbb{P}(F)$ se dice que es un *divisor primo*. El elemento neutro del grupo de divisores $\mathcal{D}_F$ es el divisor

$$0 := \sum_{P\in\mathbb{P}(F)} r_P P,$$

con $r_P = 0$ para todo $P \in \mathbb{P}(F)$.

Para $Q \in \mathbb{P}(F)$ y $D = \sum n_P P \in \mathcal{D}_F$ definimos $\mathrm{v}_Q(D) := n_Q$, por lo tanto

$$supp\, D = \{P \in \mathbb{P}(F) : \mathrm{v}_P(D) \neq 0\} \quad \text{y} \quad D = \sum_{P\in\mathbb{P}(F)} \mathrm{v}_P(D) P.$$

Definimos un orden parcial en $\mathcal{D}_F$ de la siguiente manera

$$D_1 \leq D_2 \quad \text{si y sólo si} \quad \mathrm{v}_P(D_1) \leq \mathrm{v}_P(D_2) \text{ para todo } P \in \mathbb{P}(F).$$

Si $D_1 \leq D_2$ y $D_1 \neq D_1$ escribiremos que $D_1 < D_2$. Un divisor D se llama *positivo (o efectivo)* si $D \geq 0$.

El *grado* de un divisor D se define como

$$deg\, D := \sum_{P\in\mathbb{P}(F)} \mathrm{v}_P(D) deg\, P.$$

Por la Observación 1.6, sabemos que todo elemento no nulo $z \in F$ tiene una cantidad finita de ceros y polos en $\mathbb{P}(F)$. Por lo tanto la siguiente definición tiene sentido. Sea $0 \neq z \in F$ y denotemos por Z al conjunto de ceros (resp. N al conjunto de polos) de z en $\mathbb{P}(F)$. Entonces definimos

$$(z)_0 := \sum_{P\in Z} v_P(z) P, \qquad \text{el } \textit{divisor de ceros} \text{ del elemento } z,$$

$$(z)_\infty := \sum_{P\in N} (-v_P(z)) P, \qquad \text{el } \textit{divisor de polos} \text{ del elemento } z,$$

$$(z) := (z)_0 - (z)_\infty, \qquad \text{el } \textit{divisor principal} \text{ del elemento } z.$$

Teorema 1.7. [11, Teorema 1.4.11] *Sea $z \in F \setminus K$. Entonces*

$$deg\,(z)_0 = deg\,(z)_\infty = [F : K(z)].$$

En particular, todos los divisores principales tienen grado cero.

A divisor $D \in \mathcal{D}_F$ le corresponde un K-espacio vectorial $\mathcal{L}(D)$ que se denomina *espacio de Riemann-Roch* asociado a D y se define como

$$\mathcal{L}(D) := \{x \in F : v_P(x) \geq -\mathrm{v}_P(D)\} \cup \{0\}.$$

[1] Para todos excepto un número finito.

El espacio de Riemann-Roch, es un espacio vectorial de dimensión finita sobre K, cuya dimensión se denota por $\ell(D)$.

El *género* g de un cuerpo de funciones F sobre K se define como

$$g(F/K) = \text{máx}\{deg\, D - \ell(D) + 1 \,:\, D \in \mathcal{D}_F\}.$$

El género es uno de los invariantes más importantes de un cuerpo de funciones, se puede probar que existe y que es un entero no negativo, (ver [11, Proposición 1.4.14]). Por ejemplo, el género de $K(x)$ es cero para todo elemento x trascendente sobre K. Más aún, un cuerpo de funciones F sobre K es de la forma $K(x)$ si y sólo si F es de género cero y tiene al menos un divisor de grado uno (ver [11, Proposition 1.6.3]).

1.2. Extensiones algebraicas y ramificación. De aquí en adelante supondremos que el cuerpo total de constantes de todo cuerpo de funciones es perfecto. Sean F un cuerpo de funciones sobre K y F' un cuerpo de funciones sobre K' tales que $K \subset K'$ y $F \subset F'$. Supondremos también que que ambas extensiones F'/F y K'/K son algebraicas.

Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$. Decimos que Q *divide* a P o que Q *está arriba* de P si $P \subset Q$. Denotamos esta situación con el símbolo $Q|P$.

Se puede probar (ver [11, Proposición 3.1.4]) que si $Q|P$ entonces existe un único entero $e \geq 1$ tal que $v_Q(x) = e\, v_P(x)$ para todo $x \in F$, y además que $Q \cap F = P$. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$ tales que $Q|P$.

a) El *índice de ramificación* $e(Q|P)$ de Q sobre P se define como el único entero $e(Q|P) := e$ que satisface
$$v_Q(x) = e\, v_P(x).$$
(ver [11, Definición 3.1.5])

b) Decimos que $Q|P$ está *ramificado* si $e(Q|P) > 1$, y que $Q|P$ *no ramifica* si $e(Q|P) = 1$. Decimos que un lugar $P \in \mathbb{P}(F)$ está *ramificado* o *ramifica* en F' si existe $Q \in \mathbb{P}(F')$ tal que $Q|P$ y $e(Q|P) > 1$. En caso contrario decimos que P *no ramifica* en F'.

c) $f(Q|P) := [F'_Q : F_P]$ es el *grado de inercia* (o *grado relativo*) de Q sobre P.

Si F'/F es una extensión algebraica separable y $Q \in \mathbb{P}(F')$ entonces la restricción $Q \cap F$ de Q a F es un lugar de F.

Si F''/F' es otra extensión algebraica separable, y $P \in \mathbb{P}(F)$, $Q \in \mathbb{P}(F')$ y $R \in \mathbb{P}(F'')$ son tales que $R|Q$ y $Q|P$ entonces tenemos que

$$e(R|P) = e(R|Q)e(Q|P) \qquad \text{y} \qquad f(R|P) = f(R|Q)f(Q|P).$$

Teorema 1.8. [11, Teorema 3.1.11](Igualdad Fundamental) *Si F'/F es una extensión finita de cuerpos de funciones y $P \in \mathbb{P}(F)$ entonces*

$$\sum_{\substack{Q \in \mathbb{P}(F') \\ Q|P}} e(Q|P) f(Q|P) = [F' : F].$$

En el caso de que la extensión F'/F sea finita y Galois se tiene que si $Q|P$ y $Q'|P$ entonces $e(Q|P) = e(Q'|P$ y $f(Q|P) = f(Q'|P)$. Por lo tanto si F'/F es una extensión finita y Galois entonces

$$ref = [F' : F]\,,$$

donde r es el número de lugares de F' arriba de P y $e = e(Q|P)$ y $f = f(Q|P)$ para todo $Q \in \mathbb{P}(F')$ arriba de P.

Sea F'/F una extensión finita de cuerpos de funciones de grado n y sea $P \in \mathbb{P}(F)$.

a) Decimos que P se *descompone completamente* en F' si existen exactamente n lugares distintos de F' arriba de P. En este caso se tiene que $e(Q|P) = f(Q|P) = 1$ para todo $Q|P$.
b) Si existe un lugar $Q \in \mathbb{P}(F')$ tal que $e(Q|P) = n$ entonces decimos que el lugar P es *totalmente ramificado* en F'. En este caso se tiene que hay un único lugar de F' arriba de P.
c) Si existe un único lugar $Q \in \mathbb{P}(F')$ arriba de P y $e(Q|P) = 1$ entonces decimos que P es *inerte* en F' y en este caso $f(Q|P) = n$.

En el siguiente resultado se da una condición suficiente para la irreducibilidad de ciertos polinomios con coeficientes en un cuerpo de funciones que, en ciertos casos, es muy útil. Es una versión adaptada a cuerpos de funciones del conocido criterio de irreducibilidad de Eisenstein para polinomios con coeficientes enteros.

Proposición 1.9 (Criterio de Irreducibilidad de Eisenstein)**.** [11, Proposición 3.1.15] *Sea F/K un cuerpo de funciones y consideremos el polinomio*

$$\varphi(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0$$

con coeficientes $a_i \in F$. Supongamos que existe un lugar $P \in \mathbb{P}(F)$ tal que una de las siguientes condiciones vale:

1) $v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ para $i = 1, \ldots, n-1$, y $\operatorname{mcd}(n, v_P(a_0)) = 1$.
2) $v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ para $i = 1, \ldots, n-1$, $\operatorname{mcd}(n, v_P(a_0)) = 1$ y $v_P(a_0) < 0$.

Entonces $\varphi(T)$ es irreducible en $F[T]$. Si $F' = F(y)$ donde y es una raíz de $\varphi(T)$, entonces P tiene una única extensión $P' \in \mathbb{P}(F')$, y tenemos que $e(P'|P) = n$ y $f(P'|P) = 1$, es decir, P es totalmente ramificado en $F(y)/F$.

En muchos casos se construyen extensiones de cuerpos de funciones F adjuntando a F un elemento integral sobre un anillo de valuaciones de ese cuerpo. Como veremos más adelante será importante tener un criterio de integrabilidad utilizando el polinomio mínimo del elemento a adjuntar.

Proposición 1.10. [11, Proposición 3.3.1] *Sea F/K un cuerpo de funciones y sea $F' \supseteq F$ una extensión finita de cuerpos. Sea $R \subset F$ un anillo integralmente cerrado tal que F es el cuerpo cociente de R (se dice también que R es un anillo de holomorfía de F). Para $z \in F'$ denotemos por $\varphi(T) \in F[T]$ a su polinomio mínimo sobre F. Entonces*

$$z \text{ es integral sobre } R \iff \varphi(T) \in R[T].$$

Para determinar el comportamiento de la ramificación de un lugar en extensiones simples en las cuales se conoce el polinomio mínimo del elemento que genera a la extensión, el siguiente teorema, debido originalmente a Kummer, que enunciamos a continuación es de mucha utilidad. Utilizaremos la siguiente notación: dado un lugar P de un cuerpo de funciones F y un polinomio $\psi(T) = \sum c_i T^i \in \mathcal{O}_P[T]$, denotaremos por $\overline{\psi}(T)$ al polinomio

$$\overline{\psi}(T) := \sum c_i(P) T^i \in F_P[T]\,,$$

donde $F_P = \mathcal{O}_{\mathcal{P}}/P$.

Teorema 1.11 (Teorema de Kummer)**.** [11, Teorema 3.3.7] *Sea F/K un cuerpo de funciones. Supongamos que $F' = F(y)$ donde y es un elemento integral sobre $\mathcal{O}_P$, y*

consideremos el polinomio mínimo $\varphi(T) \in \mathcal{O}_P[T]$ *de* y *sobre* F. *Sea*

$$\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i}$$

la descomposición de $\overline{\varphi}(T)$ *en factores irreducibles sobre* F_P *(es decir, los polinomios* $\gamma_1(T), \ldots, \gamma_r(T)$ *son irreducibles, mónicos y distintos dos a dos en* $F_P[T]$ *y* $\epsilon_i \geq 1$*). Consideremos polinomios mónicos* $\varphi_i(T) \in \mathcal{O}_P[T]$ *con*

$$\overline{\varphi}_i(T) = \gamma_i(T) \qquad y \qquad deg\,(\varphi_i(T)) = deg\,(\gamma_i(T)).$$

Entonces para $1 \leq i \leq r$, *existen lugares* $P_i \in \mathbb{P}(F')$ *que satisfacen*

$$P_i|P, \qquad \varphi_i(y) \in P_i \qquad y \qquad f(P_i|P) \geq deg\,(\gamma_i(T)).$$

Más aún $P_i \neq P_j$ *para* $i \neq j$.

Con hipótesis adicionales se pueden obtener los índices de ramificación, grados de inercia y números de lugares arriba de un lugar dado. Supongamos que al menos una de las siguientes hipótesis $(*)$ *o* $(**)$ *vale:*

$$\epsilon_i = 1 \qquad para \qquad i = 1, \ldots, r; \tag{$*$}$$

o

$$\{1, y, \ldots, y^{n-1}\} \quad es\ una\ base\ integral\ para\ P. \tag{$**$}$$

Entonces para $1 \leq i \leq r$ *existe exactamente un lugar* $P_i \in \mathbb{P}(F')$ *tal que* $P_i|P$ *y* $\varphi_i(y) \in P_i$. *Además* $e(P_i|P) = 1$ *y* $f(P_i|P) = deg\,\gamma_i$ *para* $1 \leq i \leq r$. *Por lo tanto* $P_1, \ldots, P_r$ *son los lugares de* $\mathbb{P}(F')$ *que están arriba de* P.

El *divisor diferente* de F'/F es un divisor que se define de la siguiente manera:

$$\mathrm{Diff}(F'/F) := \sum_{P \in \mathbb{P}(F)} \sum_{Q|P} d(Q|P)Q,$$

donde $d(Q|P)$ es un entero no negativo unívocamente definido por P y Q llamado *exponente diferente*, (ver [11, Sección 3.4]). La determinación precisa de este divisor es fundamental para el cálculo del género de extensiones finitas y separables de cuerpos de funciones.

Para poder determinar explícitamente o, al menos, poder encontrar cotas para el divisor diferente, es necesario tener algún control sobre los exponentes diferentes involucrados. El siguiente teorema relaciona el exponente diferente con el índice de ramificación permitiendo en muchos casos obtener aproximaciones y cotas del diferente.

Teorema 1.12 (Teorema del divisor diferente de Dedekind)**.** [11, Teorema 3.5.1] *Siguiendo con la notación anterior tenemos que para todo* $Q|P$

$$d(Q|P) \geq e(Q|P) - 1,$$

y la igualdad vale si y sólo si $e(Q|P)$ *no es divisible por la característica de* $\mathbb{F}_q$.

La denominada *fórmula del género de Hurwitz* establece una importante relación entre los géneros de los cuerpos de funciones que forman una extensión finita y separable.

Teorema 1.13 (Fórmula del género de Hurwitz)**.** [11, Teorema 3.4.13] *Sea* F *un cuerpo de funciones sobre* K *y sea* F'/F *una extensión finita y separable. Denotemos por* K' *al cuerpo de constantes de* F'. *Entonces*

$$2g(F') - 2 = \frac{[F' : F]}{[K' : K]}(2g(F) - 2) + deg\ \mathrm{Diff}(F'/F),$$

donde $\mathrm{Diff}(F'/F)$ *denota al diferente de* F'/F.

Sea F'/F una extensión finita y separable de cuerpos de funciones sobre $\mathbb{F}_q$ y sean Q y P lugares de F' y F respectivamente tales que $Q|P$. Decimos que la extensión $Q|P$ *es moderada* si $char\,(\mathbb{F}_q)$ no divide a $e(Q|P)$; en caso contrario decimos que la extensión $Q|P$ *es no moderada* o *salvaje*. Notar que en el caso moderado, si $e(Q|P) = 1$ entonces la extensión $Q|P$ es moderada. En el caso moderado, si hay ramificación, se dice que la ramificación es moderada. En el caso no moderado hay, necesariamente, ramificación.

Enunciamos ahora un resultado sobre la ramificación en una clase especial de extensiones de cuerpos de funciones llamadas extensiones de Kummer.

Teorema 1.14 (Extensiones de Kummer)**.** [11, Proposición 3.7.3] *Sea F/K un cuerpo de funciones tal que K contiene una raíz n-ésima primitiva de la unidad (con $n > 1$ y* $\mathrm{mcd}(n, char\,(K)) = 1$*). Supongamos que $u \in F$ es un elemento que satisface*

$$u \neq w^d \quad \text{para todo } w \in F \text{ y } d|n,\ d > 1.$$

Sea

$$F' = F(y) \quad \text{con } y^n = u.$$

La extensión F'/F se llama extensión de Kummer de F y se tienen las siguientes propiedades:

1. *El polinomio $\Phi(T) = T^n - u$ es el polinomio mínimo de y sobre F (en particular es irreducible sobre F). La extensión F'/F es una extensión de Galois de grado $[F' : F] = n$; su grupo de Galois es cíclico y los automorfismos de F'/F están dados por $\sigma(y) = \zeta y$ donde $\zeta \in \mathbb{F}_q$ es una n-ésima raíz de la unidad.*
2. *Sea $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$ un lugar arriba de P. Entonces*

$$e(Q|P) = \frac{n}{r_P} \quad y \quad d(Q|P) = \frac{n}{r_P} - 1\,.$$

3. *Si K' denota el cuerpo de constantes de F' entonces*

$$g(F') = 1 + \frac{n}{[K' : K]}\left(g(F) - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}(F)}\left(1 - \frac{r_P}{n}\right) deg\, P\right).$$

Corolario 1.15. *Sea F un cuerpo de funciones y sea $F' = F(y)$ con $y^n = u$ y $u \in F$, donde $n \not\equiv 0 \mod char\,(K)$ y K contiene una n-ésima raíz primitiva de la unidad. Supongamos que existe un lugar $Q \in \mathbb{P}(F)$ tal que* $\mathrm{mcd}(v_Q(u), n) = 1$*. Entonces K es el cuerpo total de constantes del cuerpo F', la extensión F'/F es cíclica de grado n, y*

$$g(F') = 1 + n(g(F) - 1) + \frac{1}{2}\sum_{P \in \mathbb{P}(F)} (n - r_P) deg\, P.$$

1.3. Sucesiones y torres de cuerpos de funciones. La construcción de cuerpos de funciones $F/\mathbb{F}_q$ con abundancia de lugares racionales con respecto al género tiene un papel importante en la teoría algebraica de códigos, (ver [11], [8]). Hay una relación entre $N(F) = N(F/\mathbb{F}_q)$, el número de lugares racionales de F, y $g(F) = g(F/\mathbb{F}_q)$, el género de F, la cual establece que, para q fijo, $N(F)$ no puede ser muy grande con respecto a $g(F)$. Este resultado se conoce como la cota de Hasse-Weil y es uno de los resultados más importantes de la teoría de cuerpos de funciones sobre cuerpos finitos.

Teorema 1.16 (Cota de Hasse-Weil)**.** [11, Teorema 5.2.3] *Sea $F/\mathbb{F}_q$ un cuerpo de funciones. Entonces*

$$|N(F) - (q + 1)| \leq 2g(F)\sqrt{q}.$$

Una mejora de esta cota es debida a Serre (ver [11, Teorema 5.3.1]) y establece que

$$|N(F) - (q+1)| \leq g(F)\lfloor 2\sqrt{q} \rfloor,$$

donde $\lfloor x \rfloor$ denota el piso del número real x, es decir, el mayor entero m tal que $m \leq x$.

Una manera de medir cuán abundante son los cuerpos de funciones $F/\mathbb{F}_q$ con muchos lugares racionales con respecto al género, es mediante la denominada función de Ihara que se define como

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

donde

$$N_q(g) = \text{máx}\{N(F/\mathbb{F}_q) \,:\, g(F/\mathbb{F}_q) = g\}\,.$$

Ihara demuestra en [7] que si q es un cuadrado (es decir, $q = p^{2k}$) entonces $A(q) \geq \sqrt{q} - 1$. Drinfeld y Vladut [2] mostraron que $A(q) \leq \sqrt{q} - 1$ con lo cual $A(p^{2k}) = p^k - 1$. Luego García y Stichtenoth [3] dieron la primera demostración constructiva de que $A(p^{2k}) = p^k - 1$ usando extensiones de Artin-Schreier. Cuando q no es un cuadrado, el valor exacto de $A(q)$ no se conoce. La no trivialidad de $A(q)$ para todo q (es decir que $A(q) \neq 0$) se debe a Serre [10] quien, con métodos de la teoría de cuerpos de clases, demostró que existe una constante $c > 0$ tal que

$$A(q) \geq c \cdot \log q\,,$$

para todo q. Posteriormente Zink [13] mejora esta cota inferior para el caso $q = p^3$ demostrando que

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}\,,$$

y más tarde, Bezerra, Garcia y Stichtenoth [1] generalizaron este mismo resultado para cualquier potencia cúbica, es decir

$$A(q^3) \geq \frac{2(q^2-1)}{q+2}\,,$$

para todo q potencia de un primo. El aspecto distintivo de los trabajos mencionados de Garcia y Stichtenoth está en la obtención de una cota inferior para $A(q)$ mediante la construcción de torres de cuerpos de funciones asintóticamente buenas sobre $\mathbb{F}_q$ (Ver [11] y [4]) definidas recursivamente por una ecuación polinomial en dos variables. Este tipo de construcciones es el de mayor interés en la teoría de códigos y es el principal objeto de estudio de este curso. Comenzamos definiendo el concepto de sucesión admisible.

Una *sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones F_i sobre un cuerpo perfecto K* se dice que es *admisible* si se cumplen las siguientes condiciones:

i) $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$,
ii) la extensión F_{i+1}/F_i es finita y separable para todo $i \geq 0$,
iii) K es el cuerpo total de constantes de cada F_i; es decir, el cuerpo K debe ser algebraicamente cerrado en F_i para cada $i \geq 0$.

Si además se cumple que

iv) $g(F_i) \to \infty$ para $i \to \infty$,

entonces decimos que la sucesión admisible $\mathcal{F}$ es una *torre de cuerpos de funciones sobre K*.

Observación 1.17. La condición IV) se obtiene de las condiciones I), II) y de la siguiente condición que es levemente más débil y es muy útil en la práctica:

iv') existe $i_0 \geq 0$ tal que $g(F_{i_0}) > 1$.

En efecto, por la fórmula del género de Hurwitz, tenemos que

$$g(F_{i+1}) - 1 \geq [F_{i+1} : F_i](g(F_i) - 1) \qquad \forall\, i \geq 0.$$

Como $g(F_{i_0}) > 1$ y $[F_{i+1} : F_i] > 1$, entonces

$$g(F_{i_0}) < g(F_{i_0+1}) < g(F_{i_0+2}) < \cdots,$$

y como el género de un cuerpo de funciones es un número entero, tenemos que $g(F_i) \to \infty$ para $i \to \infty$

Decimos que una sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre K es *recursiva* si existe una sucesión $\{x_i\}_{i=0}^{\infty}$ de elementos trascendentes sobre K y un polinomio en dos variables

$$f(x, y) \in K[x, y]\,,$$

tales que

I) $F_0 = K(x_0)$;
II) $F_{i+1} = F_i(x_{i+1})$ donde x_{i+1} es un cero de $f(x_i, y) \in \mathbb{F}_q[y]$, es decir, $f(x_i, x_{i+1}) = 0$ para $i \geq 0$.

Notar que si el polinomio en una variable $f(x_i, y) \in K[x_i][y]$ es separable entonces la extensión F_{i+1}/F_i es separable.

Asociado a una sucesión recursiva $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones F_i sobre K tenemos el denominado *cuerpo de funciones básico* $K(x, y)$ donde x es trascendente sobre K y $f(x, y) = 0$. Es usual decir que la ecuación $f(x, y) = 0$ *define o genera* a la sucesión $\mathcal{F}$.

En general, trabajaremos con sucesiones recursivas $\mathcal{F}$ sobre $\mathbb{F}_q$ donde $f(x, y)$ es de la forma

$$f(x, y) := a_1(y)b_2(x) - a_2(y)b_1(x),$$

con a_1, a_2, b_1 y b_2 polinomios con coeficientes en $\mathbb{F}_q$ tales que

$$\mathrm{mcd}(a_1, a_2) = \mathrm{mcd}(b_1, b_2) = 1.$$

Notar que de la definición de sucesión recursiva tenemos que cada extensión F_{i+1}/F_i es finita, pues $[F_{i+1} : F_i] \leq deg\,_y(f(x_i, y))$. Además

$$F_i = K(x_0, \ldots, x_i) \qquad \text{para } i \geq 0,$$

y por lo tanto

$$F_0 = K(x_0) \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots.$$

Entonces para probar que una sucesión recursiva $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre K es una torre, basta mostrar que:

I) el polinomio $f(x, y) \in K[x][y]$ es separable, como polinomio en la segunda variable, para cualquier elemento trascendente x sobre K,
II) K es el cuerpo de constantes de todos los F_i,
III) $g(F_{i_0}) > 1$ para algún i_0.

La siguiente proposición (ver [11, Proposición 7.2.15]) da una condición suficiente para que ocurra II).

Proposición 1.18. *Consideremos una sucesión recursiva $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones donde F_0 es un cuerpo de funciones con cuerpo de constantes K y $[F_{i+1} : F_i] < \infty$ para todo $i \geq 0$. Supongamos que para todo $i \geq 0$ existen lugares $P_i \in \mathbb{P}(F_i)$ y $Q_i \in \mathbb{P}(F_{i+1})$ con $Q_i|P_i$ e índice de ramificación $e(Q_i|P_i) > 1$. Entonces $F_i \subsetneq F_{i+1}$.*

Más aún, si suponemos que $e(Q_i|P_i) = [F_{i+1} : F_i]$ *para todo* i*, entonces* K *es el cuerpo de constantes de* F_i *para todo* $i \geq 0$*.*

Si una sucesión recursiva $\mathcal{F}$ es una torre decimos que $\mathcal{F}$ es una *torre recursiva* (de cuerpos de funciones sobre K).

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre K.

a) Decimos que un lugar $P \in \mathbb{P}(F_i)$ se *descompone completamente* en $\mathcal{F}$ si P se descompone completamente en cada extensión F_j/F_i, para $j > i$. El *espacio de descomposición* $Split(\mathcal{F}/F_0)$ de $\mathcal{F}$ sobre F_0 se define como

$$Split(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) \,:\, deg\, P = 1 \text{ y } P \text{ se descompone completamente en } \mathcal{F}\}.$$

b) Decimos que un lugar $P \in \mathbb{P}(F_i)$ *ramifica* en $\mathcal{F}$ si P ramifica en alguna extensión F_i/F_0, para $i > 0$. El *espacio de ramificación* $Ram(\mathcal{F}/F_0)$ de $\mathcal{F}$ sobre F_0 se define como

$$Ram(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) \,:\, P \text{ ramifica en } \mathcal{F}\}.$$

c) Un lugar $P \in \mathbb{P}(F_i)$ está *totalmente ramificado* en $\mathcal{F}$ si P está totalmente ramificado en cada extensión F_j/F_i, para $j > i$. El *espacio de ramificación completa* (o *espacio de ramificación total*) $Cram(\mathcal{F}/F_0)$ de $\mathcal{F}$ sobre F_0 se define como

$$Cram(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : deg\, P = 1 \text{ y } P \text{ es totalmente ramificado en } \mathcal{F}\}.$$

Cuando $K = \mathbb{F}_q$ uno de los problemas principales de esta teoría es la determinación precisa del número $N(F_i)$ de lugares racionales de F_i y del género $g(F_i)$ para cada $i \geq 0$ de una sucesión o torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ dada.

Las siguientes definiciones son relevantes para esta clase de problemas. Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión admisible de cuerpos de funciones sobre $\mathbb{F}_q$. La *tasa de descomposición* $\nu(\mathcal{F}/F_0)$ y el *género* $\gamma(\mathcal{F}/F_0)$ de $\mathcal{F}$ sobre F_0 se definen, respectivamente, como

$$\nu(\mathcal{F}/F_0) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}, \qquad \gamma(\mathcal{F}/\mathbb{F}_0) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}.$$

Si $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$, el *límite* $\lambda(\mathcal{F})$ de $\mathcal{F}$ se define como

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

Se puede probar que la sucesión $\{N(F_i)/[F_i : F_0]\}_{i\geq 0}$ es monótonamente decreciente y que la sucesión $\{(g(F_i) - 1)/[F_i : F_0]\}_{i\geq 0}$ es monótonamente creciente, por lo tanto ambas convergen en $\mathbb{R}_{\geq 0} \cup \{\infty\}$. Luego los límites anteriores existen (en $\mathbb{R} \cup \{\infty\}$) y tenemos que $0 \leq \nu(\mathcal{F}/F_0) < \infty$, $0 < \gamma(\mathcal{F}/F_0) \leq \infty$, y, por la definición de $A(q)$,

$$0 \leq \lambda(\mathcal{F}) \leq A(q), \tag{1.1}$$

para cualquier sucesión admisible $\mathcal{F}$ con $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$, para algún i_0 (ver [11, Capítulo 7]).

Notar que la definición del género de $\mathcal{F}$ tiene sentido incluso en el caso de una sucesión $\mathcal{F}$ de cuerpos de funciones sobre un cuerpo perfecto K.

Una sucesión $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es *asintóticamente buena* si $\nu(\mathcal{F}/F_0) > 0$ y $\gamma(\mathcal{F}/F_0) < \infty$. En caso contrario se dice que $\mathcal{F}$ es *asintóticamente mala*. Por lo tanto, una sucesión admisible $\mathcal{F}$ es asintóticamente mala si $\nu(\mathcal{F}/F_0) = 0$ o si $\gamma(\mathcal{F}/F_0) = \infty$.

Como vimos antes, la condición $g(F_i) \geq 2$ para $i \geq i_0 \geq 0$ implica $g(F_i) \to \infty$ cuando $i \to \infty$. Por lo tanto, cuando hablamos del límite de una sucesión $\lambda(\mathcal{F})$ en realidad estamos hablando del límite de una torre.

Es claro que en el caso de una torre $\mathcal{F}$ tenemos que $\mathcal{F}$ es asintóticamente buena si y sólo si $\lambda(\mathcal{F}) > 0$. Por lo tanto una torre $\mathcal{F}$ es asintóticamente mala si y sólo si $\lambda(\mathcal{F}) = 0$. Si $\lambda(\mathcal{F}) = A(q)$, donde $A(q)$ es la función de Ihara, decimos que $\mathcal{F}$ es *asintóticamente óptima*.

Ejercicios.

1. Demostrar la Proposición 1.18.

2. Construyendo torres de cuerpos de funciones

Como ya dijimos, un problema con importantes consecuencias en la teoría de códigos algebraicos es el cálculo de $A(q)$. De la desigualdad (1.1) vemos que se pueden conseguir cotas inferiores de $A(q)$ calculando, o al menos estimando, el límite $\lambda(\mathcal{F})$ de torres recursivas de cuerpos de funciones sobre $\mathbb{F}_q$. El primer problema a resolver es que la ecuación que define recursivamente a una sucesión sea una torre. Estudiaremos a continuación condiciones suficientes para que una ecuación de la forma $a(y) = b(x)$ defina una torre recursiva de cuerpos de funciones sobre $\mathbb{F}_q$.

Usando propiedades básicas de las valuaciones en un cuerpo de funciones el siguiente lema es inmediato.

Lema 2.1. *Sean F un cuerpo de funciones sobre K, $x \in F$ un elemento trascendente sobre K y $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ un polinomio de grado n. Supongamos además que $i \in \{0, 1, \ldots, n\}$ es el menor índice tal que $a_i \neq 0$. Entonces, si P es un lugar de F, tenemos que*

$$v_P(f(x)) = \begin{cases} v_P(a_i x^i) = i v_P(x) & \text{si } v_P(x) > 0; \\ v_P(a_n x^n) = n v_P(x) & \text{si } v_P(x) < 0. \end{cases}$$

Si $v_P(x) = 0$ entonces $v_P(f(x)) \geq 0$.

Corolario 2.2. *Con las condiciones del lema anterior tenemos que si $v_P(x) \geq 0$ entonces $v_P(f(x)) \geq 0$ y si $v_P(x) < 0$ entonces $v_P(f(x)) < 0$.*

Sea x un elemento trascendente sobre un cuerpo K. Consideremos el cuerpo de funciones racionales $K(x)$ sobre K. Para $\alpha \in K$, denotamos por P_α al único lugar de $K(x)$ asociado al polinomio $x - \alpha$, es decir, P_α es el cero de $x - \alpha$ en $K(x)$. También denotamos por P_∞ al polo de x en $K(x)$.

Teorema 2.3. *Sea K un cuerpo perfecto y sean a, b_1 y b_2 polinomios coprimos dos a dos con coeficientes en K. Supongamos que $deg\,(a) = deg\,(b_1) = m \geq 2$ y que $deg\,(b_2) = m - r$ con $\mathrm{mcd}(m, r) = 1$. Consideremos los siguientes cuerpos de funciones definidos de manera recursiva:*

$$F_0 = K(x_0) \text{ es el cuerpo de funciones racionales sobre } K;$$
$$F_{i+1} = F_i(x_{i+1}) \text{ con } a(x_{i+1}) = b_1(x_i)/b_2(x_i) \text{ para todo } i \geq 0.$$

Entonces $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ es una sucesión recursiva de cuerpos de funciones sobre K. Más aún, se cumple que:

I) *$F_i \subsetneq F_{i+1}$.*

II) *El lugar P_∞, que es el único polo de x_0 en F_0, es totalmente ramificado en la sucesión. En consecuencia, K es el cuerpo total de constantes de F_i para todo $i \geq 0$.*

Si además el polinimo $a(x) - \frac{b_1(x_i)}{b_2(x_i)} \in F_i[x]$ es separable para todo $i \geq 0$, entonces F_{i+1}/F_i es separable para todo $i \geq 0$.

Observación 2.4. Si en el Teorema 2.3 tenemos que $a(T) = T^m$, $deg\,(b_1(T)) = m - r$ y $deg\,(b_2(T)) = m \geq 2$ con $\mathrm{mcd}(m, r) = 1$, entonces se prueba al igual que en el teorema, que el polo de x_i en F_i es totalmente ramificado en F_{i+1} y por lo tanto también se obtiene que K es el cuerpo total de constantes de F_i para todo $i \geq 0$.

Ejercicios.

1. Demostrar el Lema 2.1 y su corolario.
2. Demostrar el Teorema 2.3.

3. Torres de tipo Kummer asintóticamente buenas

En esta sección daremos una demostración de la no trivialidad de la función de Ihara $A(q)$ cuando q es una potencia al menos par de un primo p. Utilizaremos las denominadas torres de tipo Kummer que son sucesiones admisibles y recursivas $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre un cuerpo perfecto K, de característica p, que están definidas por ecuaciones de la forma $y^m = f(x)$ con $\mathrm{mcd}(n, p) = 1$ y para ciertas elecciones adecuadas de $f(x) \in K(x)$.

3.1. Comportamiento asintótico de sucesiones y torres moderadas. Sea F un cuerpo de funciones sobre un cuerpo perfecto K y F' una extensión finita y separable de F. La extensión F'/F se dice que es *moderada* si para todo lugar Q de F' se tiene que el índice de ramificación $e(Q|P)$ es coprimo con la característica de K donde $P = Q \cap F$. En caso contrario se dice que la extensión F'/F es *no moderada* o *salvaje*.

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre un cuerpo perfecto K. Se dice que $\mathcal{F}$ es una sucesión *moderada* si la extensión F_{i+1}/F_i es moderada para todo $i \geq 0$. En caso contrario se dice que $\mathcal{F}$ es una sucesión *no moderada* o *salvaje*.

Uno de los resultados generales más útiles en la teoría de las torres moderadas es el siguiente teorema de Garcia, Stichtenoth and Thomas [5, Theorem 2.1].

Teorema 3.1. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre moderada de cuerpos de funciones sobre $\mathbb{F}_q$. Si*

I) *$\mathcal{F}$ es de ramificación finita, es decir, el conjunto $Ram(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : P$ ramifica en $\mathcal{F}\}$ es finito y*

II) *el conjunto $Split(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : P$ se descompone completamente en $\mathcal{F}\}$ es no vacío,*

entonces $\mathcal{F}$ es asintóticamente buena y además

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_0) - 2 + s}\,,$$

donde $t = |Split(\mathcal{F}/F_0)|$ y $s = \sum_{P \in Ram(\mathcal{F}/F_0)} deg\, P$.

Este resultado nos dice que en el caso de torres moderadas con ramificación finita (es decir, el conjunto de ramificación $Ram(\mathcal{F}/F_0)$ es finito) la existencia de al menos un lugar de F_0 que se descomponga completamente en la torre alcanza para garantizar el buen comportamiento asintótico de la torre. Esto es falso en el caso de torres no moderadas pues se conocen ejemplos de torres $\mathcal{F}$ no moderadas con ramificación finita y género $\gamma(\mathcal{F})$ infinito, con lo cual $\lambda(\mathcal{F}) = 0$ y, por lo tanto, $\mathcal{F}$ es asintóticamente mala. El siguiente lema es un criterio útil para garantizar ramificación finita en una sucesión.

Lema 3.2. *Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión recursiva y admisible de cuerpos de funciones sobre $\mathbb{F}_q$ definido por la ecuación $H(x, y) = 0$ donde $H \in \mathbb{F}_q[x, y]$. Supongamos que existe un conjunto $S_0 \subset \overline{\mathbb{F}}_q$ tal que si $\gamma \in S_0$ y $H(\beta, \gamma) = 0$ entonces $\beta \in S_0$. Sea $\{x_i\}_{i \geq 0}$*

una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ *tal que* $F_0 = \mathbb{F}_q(x_0)$ *y* $F_{i+1} = F_i(x_{i+1})$ *donde* $H(x_i, x_{i+1}) = 0$ *para todo* $i \geq 0$. *Si* Q *es un lugar de* F_i *tal que la clase residual* $x_i(Q) \in S_0$ *entonces* $x_0(Q) \in S_0$.

El lema anterior permite demostrar la siguiente proposición que será de particular utilidad en la construcción de torres asintóticamente buenas de tipo Kummer.

Proposición 3.3. *Sea* $m \geq 2$ *un entero y* q *una potencia de un número primo tal que* $q \equiv 1 \mod m$. *Sea* $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *una sucesión de cuerpos de funciones sobre* $\mathbb{F}_q$ *definida recursivamente por la ecuación*

$$y^m = \frac{b_1(x)}{b_2(x)} \tag{3.1}$$

donde $b_1(T), b_2(T) \in \mathbb{F}_q[T]$ *son polinomios comprimos tales que* $deg\,(b_1(T)) = m$ *y* $deg\,(b_2(T)) = m - r$ *con* $\mathrm{mcd}(m, r) = 1$. *Entonces* $\mathcal{F}$ *es una sucesión admisible y moderada. Supongamos además que existe un conjunto* $S_0 \subset F_q$ *con las siguientes propiedades:*

*(*I*)* $Z_{b_1} \subset S_0$.
*(*II*)* $Z_{b_2} \subset S_0$.
*(*III*)* $Z_{\sigma_\gamma} \subset S_0$, *for all* $\gamma \in S_0$, *donde* $\sigma_\gamma(T) = b_2(T)\gamma^m - b_1(T)$.

Entonces $Ram(\mathcal{F}/F_0)$ *es un conjunto finito. Más precisamente si* $P \in \mathbb{P}(\mathbb{F}_0)$ *es un lugar ramificado en la sucesión* $\mathcal{F}$ *entonces* $P = \mathbb{P}_\infty$ *o* P *es el cero de* $x_0 - \gamma$ *para algún* $\gamma \in S_0$.

Estamos ahora en condiciones de enunciar y demostrar el siguiente resultado que es de importancia para nuestro propósito de hallar una cota inferior no trivial de la función de Ihara en ciertos casos.

Teorema 3.4. *Sea* $m \geq 2$ *un entero y* q *una potencia de un número primo tal que* $q \equiv 1 \mod m$. *Sea* $\beta \in \mathbb{F}_q^*$ *y sea* $h(T) \in \mathbb{F}_q[T]$ *un polinomio separable y de grado* $m - r$ *con* $\mathrm{mcd}(m, r) = 1$ *y* $1 \leq r \leq m - 1$ *tal que* $h(0) = h_0 \neq 0$ *y* $Z_{T^m - (\beta/h_0)} \subset \mathbb{F}_q$. *Supongamos que existe un conjunto* $S_0 \subset \mathbb{F}_q$ *tal que*

*(*I*)* $0 \in S_0$;
*(*II*)* $Z_h \subset S_0$;
*(*III*) para cada* $\gamma \in S_0$ *se tiene que* $Z_{H_\gamma} \subset S_0$ *donde* $H_\gamma(T) = h(T)\gamma^m - \beta T^m$.

Entonces la sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *deinida recursivamente por la ecuación*

$$y^m = \frac{\beta x^m}{h(x)}, \tag{3.2}$$

es una torre de cuerpos de funciones sobre $\mathbb{F}_q$ *tal que*

(a) F_{i+1}/F_i *es una extensión moderada de grado* m *para todo* $i \geq 0$.
(b) Sea $P \in \mathbb{P}(F_0)$ *ramificado en* F_i/F_0 *para algún* $i \geq 1$ *y sea* x_0 *un elemento trascendente sobre* $\mathbb{F}_q$ *tal que* $F_0 = \mathbb{F}_q(x_0)$. *Entonces* P *es el polo* P_∞ *de* x_0 *en* F_0 *o es un cero de* $x_0 - \gamma$ *para algún* $\gamma \in S_0 \setminus \{0\}$.
(c) El cero P_{x_0} *de* x_0 *en* F_0 *se descompone completamente en* F_i/F_0 *para todo* $i \geq 1$.
(d) $\lambda(\mathcal{F}) \geq 2(|S_0| - 2)^{-1}$.

Demostración. La Proposición 3.3 nos dice que $\mathcal{F}$ es admisible y moderada. Sea $\{x_i\}_{i\geq 0}$ una sucesión de elementos trascendentes sobre $\mathbb{F}_q$ tales que $F_0 = \mathbb{F}_q(x_0)$ y $F_{i+1} =$

$F_i(x_{i+1})$ donde

$$x_{i+1}^m = \frac{\beta x_i^m}{h(x_i)} \qquad \forall\, i \geq 0. \tag{3.3}$$

Veremos ahora que el lugar P_{x_0} (el cero de x_0 en F_0) se descompone completamente en F_i/F_0. Sea Q un lugar de F_i que sea un cero de x_0. Luego $Q \cap F_0 = P_{x_0}$ y además, por (3.2), se tiene que Q es un cero de $x_1, x_2, \ldots, x_i$. Notar que P_{x_0} se descompone completamente en F_i/F_0 si y sólo si Q se descompone completamente en F_{i+1}/F_i.

Sea $\tilde{\mathcal{F}} = \{\tilde{F}_i\}_{i=0}^{\infty}$ la sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ en la cual $\tilde{F}_0 = F_0 = \mathbb{F}_q(x_0)$ y $\tilde{F}_i = \tilde{F}_{i-1}(x_i/x_{i-1})$ for all $i \geq 1$. Luego $\tilde{\mathcal{F}}$ está recursivamente definida por la ecuación

$$y^m = \frac{\beta}{h(x)}$$

porque de (3.3) se verifica que

$$\left(\frac{x_{i+1}}{x_i}\right)^m = \frac{\beta}{h(x_i)}, \qquad \forall\, i \geq 0.$$

En realidad se tiene que $\tilde{\mathcal{F}} = \mathcal{F}$ pues $F_{i+1} = \tilde{F}_{i+1}$. Por lo tanto se puede considerar a $\mathcal{F}$ definida por la ecuación

$$y^m = \frac{\beta}{h(x)}.$$

Sea $z = h(x_n)$. Luego $z \in \mathcal{O}_Q^*$ pues $v_Q(z) = v_Q(h(x_n)) = 0$ de modo que $z(Q) \in \mathbb{F}_q^*$. Notar que si $h(T) = h_{m-r}T^{m-r} + \cdots + h_1 T + h_0$ entonces $z(Q) = h_0 \in \mathbb{F}_q^*$.

Reduciendo la ecuación $T^m = \frac{\beta}{h(x_n)}$ módulo Q se obtiene que

$$T^m = \frac{\beta}{z(Q)} = \frac{\beta}{h_0}.$$

Como $\beta/h_0 \neq 0$ y $q \equiv 1 \mod m$ el polinomio $T^m - \beta/h_0 \in \mathbb{F}_q[T]$ es separable. Por hipótesis la ecuación $T^m = \beta/h_0$ tiene m raíces distintas en $\mathbb{F}_q$ y el Teorema de Kummer (Teorema 1.11) dice en este caso que Q se descompone completamente en F_{i+1}/F_i lo cual equivale a que P_{x_0} se descomponga completamente en F_i/F_0. En consecuencia $N(F_i) \geq m^i$ y por lo tanto $g(F_i) \to \infty$ si $i \to \infty$.

Esto demuestra que $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ es una torre de cuerpos de funciones sobre $\mathbb{F}_q$ que satisface (a) y (c) del Teorema 3.4. Notar que también se cumple (b) gracias a la Proposición 3.3. Por lo tanto todo lugar de F_0 ramificado en la torre es P_∞ o el cero de $x_0 - \gamma$ para algún $\gamma \in S_0 \setminus \{0\}$ (recordar que P_{x_0} se descompone completamente).

Finalmente usando el Teorema 3.1 se deduce que

$$\lambda(\mathcal{F}) \geq \frac{2}{|S_0| - 2}\,.$$

□

Estos resultados nos permiten ahora demostrar la no trivialidad de la función de Ihara $A(q)$ para ciertos valores de q:

Teorema 3.5. *Sea $q > 2$ una potencia de un número primo y sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ la sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ definida por la ecuación*

$$y^{q-1} = \frac{x^{q-1}}{x^{q-1} - (x-\alpha)^{q-1}}, \tag{3.4}$$

con $\alpha \in \mathbb{F}_q^*$. Sea $S_0 = \mathbb{F}_q$. Entonces

I) $0 \in S_0$,
II) $Z_f \subset S_0$,
III) *para cada* $\gamma \in S_0$ *se tiene que* $Z_{H_\gamma} \subset S_0$ *donde* $H_\gamma(T) = h(T)\gamma^m - \beta T^m$. *Más precisamente si* $\gamma \in \mathbb{F}_q^*$ *entonces* $\gamma^{q-1} = 1$ *y por lo tanto* $T^{q-1} - f(T) = (T-\alpha)^{q-1}$ *tiene todas su raíces en* $\mathbb{F}_q$.

Por lo tanto

$$\lambda(\mathcal{F}) \geq \frac{2}{q-2}\,,$$

y en consecuencia

$$A(2^n) \geq \frac{2}{2^n-2} \qquad \textit{si } n \geq 2 \quad \textit{y} \quad A(p^{2n}) \geq \frac{2}{p^n-2} \qquad \textit{si } p \textit{ es un primo impar}.$$

Ejercicios.

1. Demostrar el Lema 3.2.
2. Demostrar la Proposición 3.3
3. Demostrar el Teorema 3.5
4. (Problema para una tesis doctoral): Determinar si existen torres recursivas asintóticamente buenas con ramificación infinita.
5. (Problema para otra tesis doctoral): Determinar si existen torres recursivas asintóticamente buenas sobre cuerpos primos (es decir sobre $\mathbb{F}_p$).

Referencias

[1] J. Bezerra, A. Garcia y H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, Journal für die Reine und Angewandte Mathematik, **Vol. 589**, 2005, 159–199.

[2] S. Vlăduţ y V. Drinfel'd, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen., *Vol. 17*, 1983, 68-69.

[3] A. Garcia y H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound*, Inventiones Mathematicae, **Vol. 121**, 1995, 211–222.

[4] A. Garcia y H. Stichtenoth, *Explicit towers of function fields over finite fields*, Topics in geometry, coding theory and cryptography, **Vol. 6**, pp 1-58, Springer, 2007.

[5] A. Garcia, H. Stichtenoth y M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields and their Applications, **Vol. 3**, 1997, 257–274.

[6] V. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl., **Vol. 24**, 1981, 170–172.

[7] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, Journal of the Faculty of Science. University of Tokyo. Section IA. Math. **Vol. 28**, 1981, 721–724.

[8] H. Niederreiter y C. Xing, *Rational points on curves over finite fields: theory and applications*, London Mathematical Society Lecture Note Series, **Vol. 285**, Cambridge University Press, 2001.

[9] M. Rosen, *Number theory in function fields*, GTM **Vol. 210**, Springer, 2002.

[10] J. P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique, **Vol. 296**, 1983, 397–402.

[11] H. Stichtenoth, *Algebraic function fields and codes*, GTM **Vol. 254**, Springer, 2009.

[12] M. Tsfasman, S. Vlăduţ y T. Zink, *Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound*, Mathematische Nachrichten, **Vol. 109**, 1982, 21–28.

[13] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Lecture Notes in Comput. Sci., **Vol. 199**, 503–511, Springer, 1985.

Departamento de Matemática. UNL-FIQ. Santiago del Estero 2928 e IMAL, Güemes 3450. Santa Fe.

E-mail address: ridatole@gmail.com