Soluciones algebraicas de ecuaciones diferenciales (o la cuarta sucesión de Sloane)

Teresa Crespo

jueves 2 de febrero de 2006
Seminari de Teoria de Nombres (UB-UAB-UPC)
Facultat de Nàutica

Consideramos el siguiente problema:

"Dada una ecuación diferencial lineal con coeficientes en $\mathbb{C}(z)$, ¿cómo reconocer si todas sus soluciones son funciones algebraicas sobre $\mathbb{C}(z)$?"

Esta cuestión fué planteada por Fuchs y Schwarz y retomada por Klein en su libro del icosaedro [K1]. En su artículo sobre las ecuaciones hipergeométricas de Gauss [S], Schwarz da una respuesta completa a esta pregunta para este tipo de ecuaciones diferenciales.

1. Función hipergeométrica de Gauss

Para $a, b, c \in \mathbb{R}$, $c \notin \mathbb{Z}_{\leq 0}$, se define la *función hipergeométrica de Gauss* por

$$F(a,b,c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n \tag{1}$$

donde el símbolo de Pochhammer $(x)_n$ se define por

$(x)_0 = 1$

$(x)_n = x(x+1)\dots(x+n-1)$.

El radio de convergencia de (1) es 1 salvo si a o b son enteros no positivos y en este caso tenemos un polinomio. En particular

$$P_n(z) = \frac{1}{n!}\frac{d^n}{dz^n}(1-z^2)^n = 2^n F(-n, n+1, 1; \frac{1+z}{2})$$

son los polinomios de Legendre;

$$T_n(z) = (-1)^n F(-n, n, \frac{1}{2}; \frac{1+z}{2})$$

es el polinomio de Chebyshev definido por $T_n(\cos z) = \cos(nz)$.

La función hipergeométrica de Gauss (1) admite prolongación analítica mediante su representación por la integral de Euler

$$F(a,b,c;z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tz)^{-a}\, dt.$$

Las funciones hipergeométricas aparecen también en la determinación de los periodos de la red del plano complejo asociada a una curva elíptica. Concretamente

$$\omega_1(\lambda) = \int_{-\infty}^{0} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = i\pi F(\frac{1}{2}, \frac{1}{2}, 1; 1-\lambda),$$
$$\omega_2(\lambda) = \int_{1}^{\infty} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = \pi F(\frac{1}{2}, \frac{1}{2}, 1; \lambda),$$

son los periodos de la curva elíptica $y^2 = x(x-1)(x-\lambda)$, con λ número complejo cumpliendo $|\lambda| < 1, |\lambda - 1| < 1$ (ver [H]).

Puede comprobarse fácilmente que la función hipergeométrica de Gauss $F(a, b, c; z)$ es solución de la ecuación diferencial

$$Y'' + \frac{(a+b+1)z - c}{z(z-1)} Y' + \frac{ab}{z(z-1)} Y = 0 \tag{2}$$

Vemos ahora algunas cuestiones de ecuaciones diferenciales lineales definidas sobre el cuerpo $\mathbb{C}(z)$.

2. Ecuaciones diferenciales fuchsianas

2.1 Singularidades regulares

Para una ecuación diferencial

$$Y^{(n)} + a_1(z)\, Y^{(n-1)} + \cdots + a_{n-1}(z)\, Y' + a_n(z)\, Y = 0 \tag{3}$$

con $a_i(z) \in \mathbb{C}(z)$, un punto P de $\mathbb{P}^1(\mathbb{C})$ se llama regular si las funciones a_i no tienen polo en P. Si $P \in \mathbb{C}$ (resp. $P = \infty$) es punto singular, consideramos el límite $\lim_{z \to P} (z-P)^i a_i(z)$ (resp. $\lim_{z\to\infty} z^i a_i(z)$). Si este límite existe y es finito para $i = 1, \dots, n$, el punto P es *singularidad regular*.

La ecuación (3) se llama *Fuchsiana* si todos los puntos de $\mathbb{P}^1(\mathbb{C})$ son regulares o singularidades regulares.

Suponemos ahora que 0 es un punto singular regular de la ecuación (3). Escribimos la ecuación en términos del operador diferencial $D = z\dfrac{d}{dz}$. A partir de la igualdad de operadores $\dfrac{d^r}{dz^r} \cdot z = r\dfrac{d^{r-1}}{dz^{r-1}} + z\dfrac{d^r}{dz^r}$, para $r \geq 1$, puede probarse por recurrencia

$$z^r \frac{d^r}{dz^r} = D(D-1)\cdots(D-r+1). \tag{4}$$

Multiplicando (3) por z^n i usando (4), la ecuación queda en la forma

$$F(D, z)(Y) := D^n Y + b_1(z) D^{n-1} Y + \cdots + b_{n-1} DY + b_n(z) Y = 0. \tag{5}$$

La condición de singularidad regular implica que las funciones $b_i(z)$ son holomorfas en el entorno de $z = 0$.

2.2 Soluciones formales en series de potencias

Teorema 1 (de Cauchy). *Supongamos que* 0 *es un punto regular de (3), entonces existen* n *series de Taylor en* z, $f_1, \ldots, f_n$ *, soluciones de (3), linealmente independientes sobre* $\mathbb{C}$*, con radio de convergencia positivo. Además, toda serie de Taylor solución de (3) es combinación lineal de* $f_1, \ldots, f_n$ *con coeficientes en* $\mathbb{C}$.

Prueba. Buscamos una solución en serie de potencias $y = \sum_{k\geq 0} c_k z^k$. Multiplicando (3) por z^n i usando (4), obtenemos

$$D(D-1)\cdots(D-n+1)\,Y + \sum_{i=1}^{n} z^i a_i(z) D(D-1)\cdots(D-(n-i)+1)\,Y = 0.$$

Escribimos $z^i a_i(z) = \sum_{j=i}^{\infty} a_{ij} z^j$ y, para cada $j \geq 1$, ponemos $P_j(X) = \sum_{i=1}^{j} a_{ij} X(X-1)\cdots(X-(n-i)+1)$. Sustituyendo y en la ecuación, obtenemos la relación de recurrencia

$$k(k-1)\cdots(k-n+1)c_k + \sum_{j=1}^{k} P_j(k) c_{k-j} = 0.$$

Como $P_j(k-j) = 0$, para $1 \leq j \leq k < n$, la recurrencia es trivial para $k \leq n-1$. Por tanto podemos fijar $c_0, \cdots, c_{n-1}$ arbitrariamente y los coeficientes c_k con $k \geq n$ quedan fijados por la relación de recurrencia. Obtenemos pues n soluciones linealmente independientes de (3) que son base del espacio vectorial de soluciones.

Falta ver que cualquier solución en serie de potencias tiene radio de convergencia positivo. Para ello, elegimos $C > 1$ tal que $|P_j(k)| < C^j k^{n-1}$ para todo par j, k, $|c_j| < C^{2j+1}$ para $j = 0, \cdots n-1$ y $(k(k-1)\cdots(k-n+1))^{-1} < C/k^n$ para todo $k \geq n$. Probamos por inducción sobre k que $|c_k| < C^{2k+1}$. Para $k < n$, se cumple por la elección de C. De la relación de recurrencia, obtenemos la desigualdad

$$|c_k| \leq \frac{C}{k^n} \sum_{j=1}^{k} C^j k^{n-1} |c_{k-j}|.$$

Usando la hipótesis de inducción,

$$|c_k| \leq \frac{C}{k^n} k^{n-1} \sum_{j=1}^{k} C^j \cdot C^{2(k-j)+1} < C^{2k+1}.$$

Por tanto, los coeficientes c_k están acotados exponencialmente y la serie de potencias tiene radio de convergencia positivo. $\square$

2.3 Soluciones formales en puntos singulares regulares

Suponemos ahora que 0 es un punto singular regular de la ecuación (3). Buscamos soluciones de la forma

$$y = z^\rho \sum_{k \geq 0} c_k z^k. \tag{6}$$

Desarrollamos los coeficientes de (5) en serie de Taylor, $b_i(z) = \sum_{j=0}^{\infty} b_{ij} z^j$ y ponemos

$$\begin{cases} F_0(D) &= D^n + b_{10} D^{n-1} + b_{20} D^{n-2} + \cdots + b_{n0} \\ F_j(D) &= b_{1j} D^{n-1} + b_{2j} D^{n-2} + \cdots + b_{nj} \quad \text{para} \quad j > 0. \end{cases}$$

La ecuación se escribe entonces

$$F(D,z)(Y) = \sum_{j=0}^{\infty} z^j F_j(D)(Y) = 0$$

y sustituyendo y, obtenemos

$$\begin{aligned} F(D,z)(y) &= \textstyle\sum_{i=0}^{\infty} \sum_{j=0}^{\infty} z^j F_j(D)(c_i z^{\rho+i}) \\ &= \textstyle\sum_{i=0}^{\infty} \sum_{j=0}^{\infty} z^{\rho+i+j} F_j(\rho+i) c_i \\ &= \textstyle\sum_{k=0}^{\infty} z^{\rho+k} \left[\sum_{i=0}^{k} F_{k-i}(\rho+i) c_i \right] = 0. \end{aligned}$$

Esta expresión se anula idénticamente si los coeficientes c_i cumplen las relaciones

$$\sum_{i=0}^{k} F_{k-i}(\rho+i) c_i = 0 \quad (k \geq 0). \tag{7}$$

En particular, para obtener $c_0 \neq 0$, ρ debe ser raíz de la ecuación polinomial

$$F_0(X) = X^n + b_{10} X^{n-1} + \cdots + b_{n0} = X^n + b_1(0) X^{n-1} + \cdots + b_n(0) = 0.$$

Esta ecuación se llama *ecuación indicial*, sus raíces se llaman *exponentes locales* en el punto singular $z = 0$.

A partir de (4), se obtiene que la ecuación indicial en un punto $P \in \mathbb{C}$, regular o singularidad regular, en términos de los coeficientes de (3) es

$$
\begin{aligned}
&X(X-1)\cdots(X-n+1)\\
&\quad+\textstyle\sum_{k=1}^{n} lim_{z\to P}(z-P)^k a_k(z)X\cdots(X-n+k+1)\\
&\qquad\qquad\qquad\qquad\qquad\qquad+lim_{z\to P}(z-P)^n a_n(z)=0.
\end{aligned}
$$

Si ∞ es punto regular o singularidad regular, la ecuación indicial en ∞ es

$$
\begin{aligned}
&X(X+1)\cdots(X+n-1)\\
&\quad+\textstyle\sum_{k=1}^{n}(-1)^k lim_{z\to\infty} z^k a_k(z)X\cdots(X+n-k-1)\\
&\qquad\qquad\qquad\qquad\qquad\qquad+(-1)^n lim_{z\to\infty} z^n a_n(z)=0.
\end{aligned}
$$

Los exponentes locales satisfacen la

Relación de Fuchs. *Si $\rho_1(P),\rho_2(P),\cdots,\rho_n(P)$ son los exponentes locales en un punto $P\in\mathbb{P}^1$, se cumple*

$$\sum_{P\in\mathbb{P}^1}(\rho_1(P)+\rho_2(P)+\cdots+\rho_n(P)-\binom{n}{2})=-2\binom{n}{2}.$$

Teniendo en cuenta que en un punto regular, los exponentes locales son $0,1,\cdots,n-1$, tenemos que la suma es de hecho finita.

Ahora, si dos soluciones independientes corresponden al mismo exponente ρ, restándolas obtenemos otra solución correspondiente a otro exponente mayor ρ' que también debe cumplir la ecuación indicial. Por tanto, cada exponente local da lugar a lo sumo a una solución en serie de potencias de la forma (6) .

Si $F_0(\rho)=0$, $F_0(\rho+k)\neq 0$ para todo entero positivo k, podemos elegir $c_0\neq 0$ y cada uno de los coeficientes c_k siguientes queda unívocamente determinado por las relaciones (7). Pero, si ρ y $\rho+k$ son ambos exponentes locales, con k entero positivo, la relación $\sum_{i=0}^{k}F_{k-i}(\rho+i)c_i=0$ puede ser incompatible.

Siempre que no tengamos un sistema completo de soluciones de la forma (6), por tener la ecuación indicial raíces múltiples o raíces que difieren en un entero, esta escasez puede suplirse con soluciones en que aparecen logaritmos.

Distribuimos los exponentes locales en conjuntos, cada uno de ellos formado por exponentes locales que difieren en un entero. Vemos ahora como calcular las soluciones correspondientes a uno de estos conjuntos, formado por h exponentes locales distintos ρ_i con multiplicidades r_i, ordenados con parte real ascendiente. Buscamos soluciones del tipo

$$y=z^\rho\sum_{k\geq 0}u_k z^k. \tag{8}$$

donde los u_k son polinomios en $t:=\log z$ de grado menor que n. Teniendo en cuenta $D(u_i)=\dfrac{du_i}{dt}$, obtenemos

$$\begin{aligned} F(D,z)(y) &= \textstyle\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} z^j F_j(D)(z^{\rho+i}u_i) \\ &= \textstyle\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} z^{\rho+i+j} F_j(D+\rho+i)u_i \\ &= \textstyle\sum_{k=0}^{\infty} z^{\rho+k}\left[\sum_{i=0}^{k} F_{k-i}(D+\rho+i)u_i\right] = 0, \end{aligned}$$

que se anula idénticamente si las u_i cumplen las relaciones

$$\sum_{i=0}^{k} F_{k-i}(D+\rho+i)u_i = 0 \quad (k \geq 0).$$

Esto puede verse como un sistema de ecuaciones diferenciales lineales en la variable $t = \log z$, del cual nos interesa la solución más general en polinomios. La primera ecuación puede escribirse

$$F_0(D+\rho)(u_0) = F_0(\rho)u_0 + \frac{1}{1!}F_0'(\rho)Du_0 + \frac{1}{2!}F_0''(\rho)D^2u_0 + \cdots = 0,$$

y es la ecuación indicial generalizada. Si u_0 es un polinomio en t, no idénticamente 0, esta expresión es un polinomio del mismo grado salvo si $F_0(\rho) = 0$. Para obtener efectivamente una solución, ρ debe pues satisfacer la ecuación indicial. Para $\rho = \rho_1$, tenemos $F_0(D+\rho_1)(u_0) = G_1(D)(D^{r_1}u_0)$ con $G_1(0) \neq 0$, y por tanto, u_0 debe cumplir la ecuación $D^{r_1}u_0 = 0$.

Supongamos hallados los polinomios $u_0, u_1, \cdots, u_{k-1}$. Si $F_0(\rho_1+k) \neq 0$, u_k queda unívocamente determinado como un polinomio cuyo grado no excede el de los anteriores por la fórmula simbólica

$$\begin{aligned} u_k &= -\frac{1}{F_0(D+\rho_1+k)} \textstyle\sum_{i=0}^{k-1} F_{k-i}(D+\rho_1+i)(u_i) \\ &= -(A_0 + A_1D + A_2D^2 + \cdots) \textstyle\sum_{i=0}^{k-1} F_{k-i}(D+\rho_1+i)u_i \\ &= L_k(u_0, u_1, \cdots, u_{k-1}). \end{aligned} \tag{9}$$

Pero si $k = \rho_i - \rho_1$, tenemos $F_0(D+\rho_1+k) = F_0(D+\rho_i) = G_i(D)D^{r_i}$, con $G_i(0) \neq 0$ y por tanto, en vez de (9), tenemos la relación

$$D^{r_i}u_{\rho_i-\rho_1} = L_k(u_0, u_1, \cdots, u_{k-1}), \quad \text{con} \quad k = \rho_i - \rho_1.$$

La estructura de la solución queda completamente determinada por $u_0, \cdots, u_{\rho_h-\rho_1}$ ya que los u_k restantes quedan determinados por una relación del tipo (9). Podemos distinguir los h polinomios críticos $U_i := u_{\rho_i-\rho_1}$ y expresar los restantes explícitamente en la forma

$$u_k = \Lambda_k(U_1, U_2, \cdots, U_h)$$

donde los U_i satisfacen un sistema de ecuaciones de la forma

$$\left\{ \begin{array}{rcl} D^{r_1}U_1 & = & 0 \\ f_{21}(D)U_1 + D^{r_2}U_2 & = & 0 \\ f_{31}(D)U_1 + f_{32}(D)U_2 + D^{r_3}U_3 & = & 0 \\ \cdots & & \end{array} \right. .$$

Obtenemos pues $\sum_{i=1}^{h} r_i$ soluciones linealmente independientes. Puede probarse que tienen radio de convergencia positivo (ver [P]).

Observación. Una ecuación diferencial lineal homogénea que sea ecuación de Fuchs con tres puntos singulares queda determinada por sus puntos singulares y los exponentes locales en cada punto singular.

2.4 Grupo de monodromía

Toda solución analítica de (3) en el entorno de un punto regular puede prolongarse analíticamente a lo largo de todo camino en $\mathbb{C}$ que no pase por ningún punto singular. Sea S el conjunto de singularidades de (3), $z_0 \in \mathbb{P}^1 \setminus S$. Sean $f_1, \ldots, f_n$ soluciones analíticas independientes en el entorno de z_0. Sea $\gamma \in \pi_1(\mathbb{P}^1 \setminus S, z_0)$. Por prolongación analítica a lo largo de γ, obtenemos $\widetilde{f}_1, \ldots, \widetilde{f}_n$ que son de nuevo soluciones de (3). Se tiene por tanto una matriz $M(\gamma) \in \mathrm{GL}(n, \mathbb{C})$ tal que

$$\begin{pmatrix} \widetilde{f}_1 \\ \vdots \\ \widetilde{f}_n \end{pmatrix} = M(\gamma) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}.$$

La aplicación

$$\begin{array}{rccc} \rho : & \pi(\mathbb{P}^1 \setminus S) & \rightarrow & \mathrm{GL}(n, \mathbb{C}) \\ & \gamma & \mapsto & M(\gamma) \end{array}$$

es un morfismo de grupos. Su imagen se llama *grupo de monodromía* de (3). El *grupo de monodromía proyectivo* es el grupo de monodromía módulo escalares, es decir la imagen del grupo de monodromía por el epimorfismo $\mathrm{GL}(n, \mathbb{C}) \twoheadrightarrow \mathrm{PGL}(n, \mathbb{C})$.

Para la ecuación diferencial (3), una extensión de Picard-Vessiot es un cuerpo diferencial K con cuerpo de constantes $\mathbb{C}$, generado diferenciablemente sobre $\mathbb{C}(z)$ por un sistema fundamental de soluciones de (3). El grupo de Galois diferencial de (3) es el grupo $\mathbf{G}$ de automorfismos diferenciales de K sobre $\mathbb{C}(z)$. El grupo $\mathbf{G}$ es un grupo algebraico, subgrupo del grupo lineal $\mathrm{GL}(n, \mathbb{C})$. Para una ecuación diferencial fuchsiana, el grupo de Galois diferencial $\mathbf{G}$ es la clausura de Zariski del grupo de monodromía. Por tanto, el tener un sistema fundamental de soluciones contenido en una extensión algebraica de $\mathbb{C}(z)$ equivale a la finitud del grupo de monodromía. Teniendo en cuenta que el subcuerpo de K generado diferenciablemente sobre $\mathbb{C}(z)$ por el determinante wronskiano de un sistema fundamental de soluciones es el cuerpo fijo por el subgrupo del grupo de Galois diferencial $\mathbf{G}$ formado por las matrices del grupo especial lineal $\mathrm{SL}(n, \mathbb{C})$, se tiene que el grupo de monodromía es finito si y sólo si lo es el grupo de monodromía proyectivo y el wronskiano es algebraico sobre $\mathbb{C}(z)$.

2.5 La ecuación hipergeométrica

La ecuación hipergeométrica (2) tiene tres puntos singulares $0, 1, \infty$ que son singularidades regulares. Escribimos los exponentes locales en el esquema de Riemann:

$$\begin{array}{ccc} 0 & 1 & \infty \\ \hline 0 & 0 & a \\ 1-c & c-a-b & b \end{array} \tag{10}$$

Sea P un punto regular de (2). Con origen en P, trazamos tres bucles en el plano complejo g_0, g_1, g_∞, alrededor de $0, 1, \infty$, respectivamente, con $g_0 g_1 g_\infty = 1$. Las correspondientes matrices de monodromía M_0, M_1, M_∞ cumplen $M_0 M_1 M_\infty = 1$ y M_0, M_∞ generan el grupo de monodromía.

A partir de los valores de los exponentes locales dados en el esquema de Riemann (10), tenemos que los valores propios de M_0 son $1, e^{2\pi i(1-c)}$, los de M_1, $1, e^{2\pi i(c-a-b)}$ y los de M_∞, $e^{2\pi i a}, e^{2\pi i b}$.

Observación: Toda ecuación fuchsiana de orden 2 con tres puntos singulares puede transformarse en una ecuación hipergeométrica mediante

-una transformación de Möbius $S(z) = \dfrac{az+b}{cz+d}, ad - bc \neq 0$ que envíe los puntos singulares a $0, 1, \infty$. Obtenemos entonces una ecuación con esquema de Riemann de la forma

$$\begin{array}{ccc} 0 & 1 & \infty \\ \hline \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \end{array}$$

donde $\alpha + \beta + \gamma + \alpha' + \beta' + \gamma' = 1$ por la relación de Fuchs.

-multiplicación de las soluciones por $z^{-\alpha}(1-z)^{-\beta}$. El esquema de Riemann obtenido corresponde a una ecuación hipergeométrica con parámetros adecuados.

3. Soluciones algebraicas

Sean f, g dos soluciones independientes de la ecuación hipergeométrica en un entorno de z_0. El cociente $D(z) = f/g$ considerado como aplicación de $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ en $\mathbb{P}^1$ se llama aplicación de Schwarz y tenemos

Teorema 2 (de Schwarz). *Sea $\lambda = |1-c|, \mu = |c-a-b|, \nu = |a-b|$ y supongamos $0 \leq \lambda, \mu, \nu < 1$. Entonces $D(z)$ aplica $\mathbb{H} \cup \mathbb{R}$ biyectivamente en un triángulo curvilíneo de vértices $D(0), D(1), D(\infty)$ con ángulos $\lambda\pi, \mu\pi, \nu\pi$.*

El grupo de monodromía proyectivo describe el comportamiento del cociente f/g de las dos soluciones de la base cuando éstas se prolongan a lo largo de un camino de $\pi(\mathbb{P}^1 \setminus S)$. Se obtiene en la forma siguiente. Sea W el grupo generado por las reflexiones respecto de una arista del triángulo curvilíneo. El grupo de monodromía proyectivo es el subgrupo de W formado por los elementos que son producto de un número par de reflexiones. A partir de las triangulaciones de la esfera, se obtienen todos los posibles valores λ, μ, ν que corresponden a ecuaciones con todas las soluciones algebraicas. Estos valores, junto con los correspondientes grupos de monodromía proyectivos, son los que aparecen en la llamada *Lista de Schwarz* [S]. Posteriormente, haciendo cociente por la relación de equivalencia proyectiva, Klein [K2] obtiene la llamada *Lista básica de Schwarz*. Decimos que dos operadores diferenciales L y L' son *proyectivamente equivalentes* si, en cualquier punto de $\mathbb{P}^1$, todo cociente de dos soluciones independientes de L es tambien cociente de soluciones independientes de L'. Reproducimos a continuación la lista básica de Schwarz.

(λ, μ, ν)	$=$	$(1, 1/n, 1/n)$	da grupo	cíclico	de orden	n
	$=$	$(1/2, 1/2, 1/n)$	da grupo	diedro	de orden	2n
	$=$	$(1/2, 1/3, 1/3)$	da grupo	tetraédrico	de orden	12
	$=$	$(1/2, 1/3, 1/4)$	da grupo	octaédrico	de orden	24
	$=$	$(1/2, 1/3, 1/5)$	da grupo	icosaédrico	de orden	60

En general, las ecuaciones diferenciales de orden 2 con grupo de monodromía proyectivo finito quedan caracterizadas por el siguiente teorema de Klein. Notemos que toda ecuación diferencial lineal de orden 2 es proyectivamente equivalente a una en *forma normalizada*: $Y'' + a_2(z)Y = 0$.

Teorema 3 (de Klein). *Sea $L(Y) = 0$ una ecuación diferencial lineal de orden 2 en forma normalizada, con grupo de monodromía proyectivo G finito. Entonces existe una única ecuación hipergeométrica $H(Y) = 0$, con grupo de monodromía proyectivo G y una función racional $f : \mathbb{P}^1 \to \mathbb{P}^1$ tal que para todo cociente $\tau(z)$ de soluciones independientes de $H(Y) = 0$, $\tau(f(z))$ es cociente de soluciones independientes de $L(Y) = 0$. Además, la función f es única módulo transformaciones de Möbius que dejen H invariante y permuten sus puntos singulares.*

En el caso de la *ecuación de Lamé*, con parámetros $n \in \mathbb{Q}, g_2, g_3, B \in \mathbb{C}$:

$$Y'' + \frac{P'(z)}{2P(z)} Y' - \frac{n(n+1)z + B}{P(z)} Y = 0$$

donde $P(z) := 4z^3 - g_2 z - g_3$ tiene tres ceros z_1, z_2, z_3 distintos, Beukers-van der Waall [B-W] y Liţcanu [L1], completando trabajos de Baldassarri y Chiarelotto, determinan en qué casos todas las soluciones son algebraicas. En este caso, el esquema de Riemann es

z_1	z_2	z_3	∞
0	0	0	$-n/2$
$1/2$	$1/2$	$1/2$	$(n+1)/2$

Teniendo en cuenta que el determinante wronskiano W de una base del espacio de soluciones de una ecuación diferencial lineal (3) cumple $W' = -a_1 W$, obtenemos que para la ecuación de Lamé, el wronskiano siempre es una función algebraica. Beukers y van der Waall usan que el grupo de monodromía de la ecuación de Lamé es un grupo de reflexiones formado por matrices con determinante ± 1. Liţcanu usa el hecho que, para $n \notin \mathbb{Z} + \frac{1}{2}$ la función racional f en el teorema de Klein tiene a lo sumo tres puntos de ramificación y es por tanto una función de Belyi. Su método se basa en el estudio del "dessin d'enfant" asociado por la correspondencia de Grothendieck a esta función de Belyi. Las cuestiones básicas de "dessins d'enfants" pueden verse en [C-X]. Se tiene

Teorema 4.

1. *Si $n \in \mathbb{Z} + \frac{1}{2}$, la ecuación de Lamé tiene soluciones algebraicas si y sólo si su grupo de monodromía proyectivo es el grupo de Klein. (Brioschi, Halphen)*
2. *No hay ecuación de Lamé con grupo de monodromía proyectivo cíclico.*
3. *No hay ecuación de Lamé con grupo de monodromía proyectivo tetraédrico.*
4. *Si el grupo de monodromía proyectivo de la ecuación de Lamé es octaédrico, entonces $n \in \mathbb{Z} + \{\pm\frac{1}{4}, \pm\frac{1}{6}\}$.*
5. *Si el grupo de monodromía proyectivo de la ecuación de Lamé es icosaédrico, entonces $n \in \mathbb{Z} + \{\pm\frac{1}{6}, \pm\frac{1}{10}, \pm\frac{3}{10}\}$.*
6. *Si el grupo de monodromía proyectivo de la ecuación de Lamé es diedro, entonces $n \in \mathbb{Z}$. Si $n \in \mathbb{Z}$ y el grupo de monodromía proyectivo es finito, entonces es diedro de orden al menos 6.*

En sentido contrario a los enunciados del teorema anterior, se tienen los resultados siguientes, obtenidos mediante "dessins d'enfants".
-Dados $n \in \mathbb{Z}$, $N \in \mathbb{N}$, Liţcanu (para $n = 1$) y Dahmen (para n general) obtienen una fórmula explícita para el número de ecuaciones de Lamé, módulo equivalencia proyectiva, con parámetro n y grupo de monodromía proyectivo el grupo diedro de orden $2N$ (cf. [L2], [D]).
-Para cada n en $\mathbb{Z} + \{\pm\frac{1}{4}, \pm\frac{1}{6}\}$ (resp. $\mathbb{Z} + \{\pm\frac{1}{6}, \pm\frac{1}{10}, \pm\frac{3}{10}\}$), Nakanishi construye una ecuación de Lamé con parámetro n y monodromía proyectiva octaédrica (resp. icosaédrica) (cf. [N]).

En el caso de las ecuaciones de orden 2 con 4 puntos singulares, la ecuación ya no queda determinada por los puntos singulares y los exponentes locales, es decir por datos locales, como en el caso de tres puntos singulares. En el caso de cuatro puntos, hay un parámetro (B en el caso Lamé) no determinado por datos locales. Éste se llama *parámetro accesorio* de la ecuación. Se sabe poco de cómo depende el grupo de monodromía del parámetro accesorio. En el caso de la ecuación de Lamé, pueden encontrarse condiciones sobre B para que el grupo de monodromía sea un determinado grupo finito (fijando n en el conjunto adecuado) a partir de productos simétricos de la ecuación y representaciones del grupo.

Beukers-Heckmann [B-H] determinan el grupo de monodromía para la función hipergeométrica generalizada y en particular cuando ésta es algebraica sobre $\mathbb{C}(z)$. La función hipergeométrica generalizada se define por

$$ {}_nF_{n-1}(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_{n-1}|z) = \sum_{k=0}^{\infty} \frac{(\alpha_1)_k \ldots (\alpha_n)_k}{(\beta_1)_k \ldots (\beta_{n-1})_k k!} z^k. $$

Es solución de una ecuación diferencial lineal de orden n con singularidades regulares en $0, 1, \infty$.

4. La sucesión de Sloane A087659

A propósito de funciones hipergeométricas generalizadas, en la Enciclopedia Digital de Sucesiones Enteras de Sloane [Sl], hallamos que

$$ a(n) = {}_3F_2(-n, \frac{n+4}{2}, \frac{n+5}{2}; 3, 2| - 4) $$

es la sucesión de Sloane A087659. Sus primeros valores son

n	a(n)
0	1
1	6
2	57
3	701
4	10147
5	164317
6	2888282
7	54047434
8	1062530119
9	21739192762
10	459685114665
11	9993072855135
12	222421656113435
13	5052215132332492
14	116808526607319823
15	2742986603349411311
16	65306671610636210891

y está probado que es efectivamente una sucesión entera (ver [Sl]). En la página de Sloane, pueden encontrarse otras nueve sucesiones dadas por valores de funciones hipergeométricas generalizadas, aunque no para todas ellas está probado que sean efectivamente sucesiones enteras.

5. Una conjetura de Grothendieck

Consideramos ahora una ecuación diferencial

$$L(Y) = Y^{(n)} + a_1(z)\,Y^{(n-1)} + \cdots + a_{n-1}(z)\,Y' + a_n(z)\,Y = 0,$$

con $a_i \in \mathbb{Q}(z)$. Para casi todo primo p, podemos reducir las funciones racionales $a_i(z)$ módulo p. Las reducciones $a_{i,p}$ están en $\mathbb{F}_p(z)$ y podemos considerar la ecuación diferencial

$$L_p(Y) = Y^{(n)} + a_{1,p}(z)\,Y^{(n-1)} + \cdots + a_{n-1,p}(z)\,Y' + a_{n,p}(z)\,Y = 0.$$

En los años sesenta, A. Grothendieck formuló la conjetura siguiente.

Conjetura de Grothendieck. *Los dos enunciados siguientes son equivalentes.*

1. *La ecuación $L(Y) = 0$ tiene n soluciones, algebraicas sobre $\mathbb{Q}(z)$, linealmente independientes sobre $\overline{\mathbb{Q}}$.*

2. *Para casi todo p, la ecuación $L_p(Y) = 0$ tiene n soluciones en $\mathbb{F}_p(z)$, linealmente independientes sobre $\mathbb{F}_p(z^p)$.*

Prueba de 1 $\Rightarrow$ 2. Sea K una extensión finita de $\mathbb{Q}(z)$ que contiene una base de soluciones $y_1, y_2, \ldots, y_n$ de $L(Y) = 0$. Sea W el wronskiano de $y_1, y_2, \ldots, y_n$. Tenemos $K = \mathbb{Q}(z)[t] = \mathbb{Q}(z)[T]/(F)$, con $F(T) = T^d + b_{d-1}T^{d-1} + \cdots + b_0$ polinomio irreducible de $\mathbb{Q}(z)[T]$ y $t = T \bmod F$. La derivación de $\mathbb{Q}(z)$ se extiende en forma única a K definiendo

$$t' = -\frac{b'_{d-1}T^{d-1} + \cdots + b'_0}{F_T(t)},$$

donde F_T indica derivada de F respecto de T. Invirtiendo F_T módulo F y reduciendo módulo F, obtenemos una expresión de t' como polinomio en t de grado $< d$ con coeficientes en $\mathbb{Q}(z)$. Consideramos ahora primos p tales que

i) $b_{d-1}, \ldots, b_0 \in \mathbb{Z}[z]_p$,

ii) el discriminante de F, respecto de T, es invertible en $\mathbb{Z}[z]_p$,

iii) $y_1, \ldots, y_n \in \mathbb{Z}[z]_p[t]$,

iv) W es un elemento invertible de $\mathbb{Z}[z]_p[t]$.

Estas condiciones excluyen un número finito de primos. Como el discriminante de F es invertible en $\mathbb{Z}[z]_p$, F_T es invertible en $\mathbb{Z}[z]_p[T]$ y por tanto $t' \in \mathbb{Z}[z]_p[t]$, es decir $\mathbb{Z}[z]_p[t]$ es invariante por diferenciación. El ideal (p) es invariante por diferenciación y por tanto $\mathbb{Z}[z]_p[t]/(p)$ es anillo diferenciable, extensión de $\mathbb{F}_p(z)$. Se tiene $\mathbb{Z}[z]_p[t]/(p) = \mathbb{F}_p(z)[T]/(\overline{F})$, para $\overline{F}$ la reducción de F módulo p. Por hipótesis, el discriminante de $\overline{F}$ es invertible y por tanto $\mathbb{Z}[z]_p[t]/(p)$ es un producto $M_1 \times \cdots \times M_s$ de cuerpos M_i, extensiones separables de $\mathbb{F}_p(z)$. Por la unicidad de la extensión de la derivación, cada M_i es subcuerpo diferencial de $\mathbb{Z}[z]_p[t]/(p)$. Sean $\overline{y}_1, \ldots, \overline{y}_n, \overline{W}$ las imágenes de $y_1, \ldots, y_n, W$ en $M = M_1$. Entonces $\overline{W}$ es el wronskiano de $\overline{y}_1, \ldots, \overline{y}_n$ y, renumerando si hace falta los M_i, tenemos que $\overline{y}_1, \ldots, \overline{y}_n$ son linealmente independientes sobre el cuerpo de constantes de M. Usando que M es separable sobre $\mathbb{F}_p(z)$, se puede probar que el cuerpo de constantes de M es M^p y que $1, z, \ldots, z^{p-1}$ es también base de M sobre M^p. Tenemos pues $M = M^p \otimes_{\mathbb{F}_p(z^p)} \mathbb{F}_p(z)$. Por tanto los espacios de soluciones en $\mathbb{F}_p(z)$ y en M de la ecuación diferencial $L_p(Y) = 0$ tienen misma dimensión. En M esta dimensión es n y por tanto también lo es en $\mathbb{F}_p(z)$. $\square$

La conjetura de Grothendieck puede verse como una generalización diferencial de un corolario del teorema de densidad de Chebotarev: Un polinomio con coeficientes en $\mathbb{Q}$ tiene todas sus raíces en $\mathbb{Q}$ si y sólo si las raíces de su reducción módulo p están en $\mathbb{F}_p$ para casi todo p.

En la conjetura de Grothendieck, el enunciado *1.* es equivalente a que el grupo de monodromía de la ecuación sea finito. Puede darse una condición equivalente al enunciado *2.* en términos de p-curvatura. Para definir la p-curvatura es más fácil trabajar con operadores diferenciales en forma matricial.

5.1. Sistemas diferenciales y p-curvatura

Recordamos que la ecuación

$$L(Y) = Y^{(n)} + a_1(z)Y^{(n-1)} + \cdots + a_{n-1}(z)Y' + a_n(z)Y = 0,$$

equivale al sistema $Y' = AY$ con matriz $n \times n$

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & \dots & 0 & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & \dots & -a_1 \end{pmatrix}.$$

El paso de sistema matricial a ecuación se hace mediante un vector cíclico del módulo diferencial asociado al sistema . Recordemos que un *módulo diferencial* (o $\mathcal{D}$-módulo) sobre un cuerpo diferencial K con derivación d es un K-espacio vectorial de dimensión finita, que es módulo por la izquierda para el anillo $\mathcal{D} = K[d]$. A un sistema diferencial $Y' = AY$ con $A = (a_{ij})_{1\leq i,j\leq n}$ definido sobre el cuerpo diferencial (K, d), podemos asociarle un módulo diferencial, el K-espacio vectorial $K^n := K \times \cdot^n \cdot \cdot \times K$ con la estructura de $\mathcal{D}$-módulo dada por $de_i = -\sum_j a_{ji}e_j$, para $e_1, \dots, e_n$ base canónica de K^n. Un vector del módulo diferencial K^n tal que él y sus derivados forman base se llama *vector cíclico* (ver [P-S]).

Consideramos un cuerpo K de característica p tal que $[K : K^p] = p$ (donde $K^p := \{x^p | \, x \in K\}$). Entonces $K = K^p(z)$ para algún z y definimos la derivación en K por $z' = 1$. Consideramos el operador diferencial $\partial := \dfrac{d}{dz} - A$, para A matrix $n \times n$ con coeficientes en K. El operador ∂ opera sobre el espacio vectorial K^n y es K^p-lineal. Su potencia p-ésima ∂^p es por tanto también K^p-lineal. Es fácil ver que el operador ∂^p también es K-lineal. En efecto, se tiene la igualdad de operadores $\partial.z = 1 + z.\partial$ y de aquí $\partial^k.z = k\partial^{k-1} + z.\partial^k$, para $k \geq 1$, y por tanto $\partial^p.z = z.\partial^p$. El operador ∂^p se llama la *p-curvatura* de ∂.

Lema 1 (de Cartier). *El operador diferencial $\partial = \dfrac{d}{dz} - A$ con A matriz $n\times$*

n, con coeficientes en K, tiene un espacio de soluciones en K de dimensión n sobre K^p si y sólo si su p-curvatura ∂^p es 0.

Prueba. El operador $\partial : V := K^n \to K$ es K^p-lineal. Supongamos que existen $e_1, \dots, e_n \in V$ en el núcleo de ∂, linealmente independientes sobre K^p. Veamos que también son independientes sobre K. Sea

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = 0,\ \lambda_i \in K. \tag{11}$$

Quitando denominadores, podemos suponer $\lambda_i \in K^p[z]$, ponemos $\lambda_i = b_o^i + b_1^i z + \cdots + b_{p-1}^i z^{p-1}$, con $b_j^i \in K^p$. Tenemos $\partial(bz^a e_i) = baz^{a-1}e_i$ para $b \in K^p$. Por tanto aplicando varias veces ∂ a (11), obtenemos una relación de dependencia sobre K^p. Entonces, ∂^p es cero en la K-base $e_1, \dots, e_n$ de V y por tanto $\partial^p = 0$.

Recíprocamente, si $\partial^p = 0$, la aplicación K^p-lineal ∂ sobre V es nilpotente $\Rightarrow \exists e_1 \neq 0$ en V con $\partial e_1 = 0$. Como Ke_1 es invariante por ∂, ∂ opera sobre $W = V/Ke_1$. Por inducción sobre n, W tiene una base $f_2, \dots, f_n$ sobre K con $\partial f_i = 0$ y cogiendo representantes F_i de los f_i, obtenemos una K-base $e_1, F_2, \dots, F_n$ de V con $\partial F_i \in Ke_1$, $i = 2, \dots, n$. Ponemos $\partial F_i = g_i e_1$, con $g_i \in K$. Ahora tenemos

$$\partial(g_i e_1) = \frac{d}{dz}(g_i e_1) - A g_i e_1 = g_i' e_1 + g_i \partial e_1 = g_i' e_1.$$

Esto vale para todo $g_i \in K$ y obtenemos $\partial^{p-1}(g_i e_1) = g_i^{p-1} e_1$ y por tanto $0 = \partial^p F_i = \partial^{p-1}(g_i e_1) = g_i^{p-1} e_1 \Rightarrow g_i^{p-1} = 0 \Rightarrow g_i = G_i'$, con $G_i \in K$. Sea $e_i = F_i - G_i e_1$, entonces $\partial e_i = \partial F_i - \partial(G_i e_1) = \partial F_i - g_i e_1 = 0 \Rightarrow$ el núcleo de ∂ en V es $K^p e_1 + \cdots + K^p e_n$. $\square$

Se tiene un algoritmo sencillo para calcular la p-curvatura: definimos la sucesión de matrices $A(k)$ por

$$A(1) := A, A(k+1) = \frac{d}{dz}(A(k)) + A.A(k)$$

entonces $A(p)$ módulo p es la matriz de la curvatura.

5.2 Casos probados

B. Dwork (hacia 1970) prueba la conjetura de Grothendieck para ecuaciones hipergeométricas, Beukers-Heckmann para las hipergeométricas generalizadas (1989), Chudnovsky-Chudnovsky en 1985 para la ecuación de Lamé. El trabajo de Honda (1974) publicado póstumamente en 1981 incluye el caso de orden 1. De hecho lo prueba como consecuencia del caso polinomial. Haraoka prueba la conjetura para las ecuaciones de Pochhammer (1994). La ecuación de Pochhammer es una ecuación diferencial de orden

n, generalización de la hipergeométrica de Gauss, en el sentido que sus soluciones tienen una representación integral del tipo de Euler. Es una ecuación libre de parámetros accesorios.

En 1972, N. Katz prueba la conjetura para conexiones de Gauss-Manin. En [Ka1] propone una reformulación muy general: Si consideramos el grupo de Galois diferencial $\mathbf{G}$ de la ecuación y el de monodromía $\mathbf{M}$, tenemos $\mathbf{M} \subset \mathbf{G} \subset \mathrm{GL}(n, \mathbb{C})$ y $\mathbf{G}$ coincide con la clausura de Zariski $\overline{\mathbf{M}}$ de $\mathbf{M}$ siempre que la ecuación es fuchsiana. Por tanto la finitud del grupo de monodromía equivale a la anulación del álgebra de Lie $\mathcal{G}$ del grupo $\mathbf{G}$. El enunciado de Katz es básicamente que el álgebra de Lie $\mathcal{G}$ de $\mathbf{G}$ sobre $\mathbb{C}(z)$ es la menor subálgebra de Lie algebraica del álgebra de matrices $M(n, \mathbb{C}(z))$ con la propiedad que su reducción módulo p contiene la p-curvatura para casi todo primo p. De hecho en [Ka1] Katz prueba que el enunciado de Grothendieck implica su enunciado, aparentemente más general.

En [Ka2], Katz prueba la conjetura para sistemas rígidos, englobando los casos probados anteriormente. Un sistema rígido queda globalmente determinado por datos locales, es decir por los puntos singulares y los exponentes locales. En 1997, Y. André la prueba más en general para sistemas diferenciales ligados a conexiones de Gauss-Manin sobre grupos de cohomología de de Rham relativa (sistemas diferenciales "que vienen de la geometría") (ver [A]). En particular, el trabajo de André incluye el caso de ecuaciones de orden uno sobre cuerpos de funciones sobre un cuerpo de números, caso del que Chudnovsky-Chudnovsky habían dado una prueba incompleta en 1985.

El primer caso en que la conjetura está totalmente abierta es el de ecuaciones diferenciales lineales sobre $\mathbb{Q}(z)$ de orden 2 con cuatro puntos singulares regulares, exponentes racionales y grupo de Galois $\mathrm{SL}(2, \mathbb{C})$. En este caso habría que probar que el enunciado *2.* de la conjetura no es cierto. La dificultad principal está en que los datos locales no determinan en este caso la ecuación diferencial.

De la misma forma en que una ecuación diferencial lineal con tres puntos singulares regulares se transforma en una ecuación hipergeométrica, toda ecuación diferencial lineal con cuatro puntos singulares regulares puede transformarse en una ecuación de Heun

$$Y'' + \frac{(a+b+1)z^2 - (a+b-d+1+(c+d)a)z + ac}{z(z-1)(z-a)}\, Y' + \frac{ab(z-q)}{z(z-1)(z-a)}\, Y = 0.$$

con puntos singularidades regulares en $0, 1, a, \infty$ (ver [E], [W-W]). El esquema de Riemann es

$$\begin{array}{cccc}
0 & 1 & a & \infty \\
\hline
0 & 0 & 0 & a \\
1-c & 1-d & 1-e & b
\end{array}$$

con $e = a+b+1-c-d$. La constante q es el llamado *parámetro accesorio*, cuya presencia se debe al hecho mencionado anteriormente que una ecuación fuchsiana de segundo order con cuatro (o más) puntos singulares no queda determinada por los puntos singulares y los exponentes locales.

Bibliografía.

[A] Y. André, Sur la conjecture des p-courbures de Grothendieck-Katz et un problème de Dwork, Geometric aspects of Dwork theory. Vol. I, 55–112, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

[B-H] F. Beukers, G. Heckmann, Monodromy for the hypergeometric function ${}_nF_{n-1}$, Invent. Math. 95 (1989), 325–354.

[B-W] F. Beukers, A. van der Waall, Lamé equations with algebraic solutions, J. Differential Equations 197 (2004), 1–25.

[C-X] T. Crespo, X. Xarles, Dibuixos d'infants, Notes del Seminari de Teoria de Nombres, UB-UAB-UPC, n. 12, Barcelona 2005, ISBN. 84-934244-0-4.

[D] S. Dahmen, Counting Integral Lamé Equations by Means of Dessins d'Enfants, Trans. Amer. Math. Soc., aparecerá.

[E] A. Erdélyi et alt., Higher transcendental functions, vol. III, McGraw-Hill, New York, 1955.

[F] L. Fuchs, Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten, J. reine angew. Math. 66 (1866), 121-160.

[H] D. Husemöller, Elliptic Curves, Springer 1987.

[K1] F. Klein, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade, Birkhäuser, 1993.
Versión inglesa: Lectures on the icosahedron and the solution of equations of the fifth degree, Dover, 2003.

[K2] F. Klein, Ueber lineare differentialgleichungen, Math. Ann. 12 (1878), 167-179.

[Ka1] N. Katz, A conjecture in the arithmetic theory of differential equations, Bull. Soc. Math. France 110 (1982), 203-239; corrección: Bull. Soc. Math. France 110 (1982), 347-348.

[Ka2] N. Katz, Rigid local systems, Annals of Math. Studies 139, Princeton University Press, 1996.

[L1] R. Liţcanu, Lamé operators with finite monodromy—a combinatorial approach, J. Differential Equations, 207 (2004), 93–116.

[L2] R. Liţcanu, Counting Lamé differential operators, Rend. Sem. Mat. Univ. Padova 107 (2002), 191–208.

[N] K. Nakanishi, Lamé operators with projective octahedral and icosahedral monodromies, Rend. Sem. Mat. Univ. Padova 115 (2005), 109–129.
[P] E.G.C. Poole, Introduction to the theory of linear differential equations, Oxford : The Clarendon Press, 1936.
[P-S] M. van der Put, M.F. Singer, Galois theory of linear differential equations, Springer-Verlag, 2003.
[S] H.A. Schwarz, Ueber diejenigen Fälle, in welchen die Gaussische Hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt, J. reine angew. Math. 75 (1873), 292-335.
[Sl] N.J.A. Sloane, The on-line encyclopedia of integer sequences, http://www.research.att.com/∼njas/sequences/
[W-W] E.T. Whittaker, G.N. Watson, A course of modern analysis, Cambridge University Press, 1940.