Pro Mathematica, Vol. IX, Nos. 17-18, 1995

RIEMANN-HURWITZ PARA CUBRIMIENTOS CICLICOS

Fernando ***Torres***

1. Sea X una curva no singular, irreducible, proyectiva, definida sobre un campo k algebraicamente cerrado de característica p.
Sea $\pi: X \to X/G$ *el cubrimiento cíclico dado por* $G = \langle T \rangle$ *para T un automorfismo de X.*
El objetivo de esta nota es escribir la fórmula de Riemann-Hurwitz para π.
Si p=0, en Farkas-Kra [F-K, pag. 261] está escrito:

$$(1) \qquad 2g - 2 = (ordT)(2\gamma - 2) + \sum_{i=1}^{(ordT-1)} \nu(T^i)$$

donde g es el género de X,
γ *lo es de* $X/\langle G \rangle$, *ordT denota el orden de T y* $\nu(T^i)$ *denota el número de puntos fijos de* T^i.

✏ *Postdoctoral fellow, ICTP, Trieste-Italia.*

Aquí

$$b_\pi := \sum_{i=1}^{(ordT-1)} \nu\,(T^i) \tag{2}$$

indica el número de puntos ramificados de π contados con cierta multiplicidad. Veremos que (1) vale si

p no divide al ord T

y que (2) necesita ser modificada en caso contrario.

2. En general, la fórmula de Riemann-Hurwitz para un cubrimiento de grado n, $\pi : X \to Y$, se escribe

$$2g - 2 = n(2\gamma - 2) + b_\pi,$$

donde g es el género de X, γ lo es de Y, y b_π es el número de ramificación de π. En particular, si $Y = X/G$ donde G es un subgrupo de automorfismos, b_π se calcula usando los grupos de ramificación. Todas las propiedades que usaremos de estos grupos pueden verse en Serre [Se,IV]. Para cada $P \in X$ se define

$$G_0(P) := \{\sigma \in G: \sigma(P) = P\}$$

$$G_i(P) := \{\sigma \in G_0(P) : v_P(\sigma(t) - t) \geq I+1\}, \text{ si } i \geq 1.$$

Aquí v_P es la valorización en P, t un parámetro local en P, i.e., $v_P(t)=1$. Luego tenemos una cadena descendente de subgrupos de G,

$$G_0(P) \supseteq G_1(P) \supseteq G_2(P) \supseteq \ldots$$

Se prueba que existe $s \in \mathbf{N}$ tal que para $i \geq s$, $G_i(P) = \{1\}$ y que para casi todo $P \in X$ (i.e. salvo un número finito) $s=0$, i.e., $G_0(P) = \{1\}$. A continuación se prueba que, poniendo $b_P := \sum_{i=0}^{\infty} (\#G_i(P) - 1)$,

$$b_\pi = \sum_{P \in X} b_P.$$

Observe que $b_P = 0 \Leftrightarrow G_0(P) = \{1\}$. Luego

$$B_\pi = \{P \in X: b_P > 0\} = \{P \in X: \exists\, \sigma \in G \setminus \{1\}: \sigma(P) = P\}.$$

En el caso que $G = \langle T \rangle$, escribiendo $n := \text{ord}T$,

$$B_\pi = \{P \in X : \exists\, 1 \le j < n, \quad T^j(P) = P\}.$$

Particionamos B_π en subconjuntos B_i como sigue

$$B_1 := \{P \in B_\pi : T(P) = P\}$$

$$B_i := \{P \in B_\pi : T^i(P) = P,\ T^j(P) \neq P,\ 0 < j < I\},\ \text{si}\ i \geq 1.$$

Afirmación. $B_i \neq \varnothing \Rightarrow i \mid n$

Prueba. Escriba $n = iq + r$, $0 \le r < n$. Si $P \in B_i$, $P = T^n(P) = T^r(T^{iq}(P)) = P$ y luego $r = 0$. □

Asi

$$B_\pi = \bigcup_{i \mid n} B_i$$

y además es claro que la unión es disjunta. Además si $P \in B_i$, la fibra $\pi^{-1}(\pi(P))$ es

$$\{P, \ldots, T^{i-1}(P)\}$$

y luego si $\#\pi(B_i) = x_i$, entonces

$$\# B_i = i\, x_i\ .$$

La extensión $X \to X/G$ es Galosiana, en el sentido que $d_P = d_{P'}$ si $\pi(P) = \pi(P')$. Luego

$$b_\pi = \sum_{i \mid N} \sum_{P \in B_i} d_P = \sum_{i \mid N} \sum_{\pi(P) \in \pi(B_i)} i d_P\ .$$

Afirmación. $\pi(P) \in \pi(B_i) \Rightarrow G_o(P) = \langle T^i \rangle$.

Prueba. Por definición $T^i \in G_o(P)$. Sea $T^h \in G_o(P)$. Sea $h = iq + r$, $0 \le i < r$. Entonces $P = T^h(P) = T^r(T^i(P))^q$ implica $T^r(P) = P$ y luego $r = 0$ □

Escribamos

$$d_P = (\#G_o(P) - 1) + \Lambda(P)$$

con

$$\Lambda(P) = \sum_{j=1}^{\infty} (\#G_j(P) - 1).$$

Entonces $$d_P = \frac{n-i}{i} + \Lambda(P) \qquad \text{y}$$

(3) $$b_\pi = \sum_{i|n} (n-i)x_i + \sum_{i|n} \sum_{\pi(P)\leq\pi(B_i)} i\,\Lambda(P)$$

3. Puntos fijos. Sea $G = \langle T \rangle$, ord $G = n$.

Afirmación. $(a,n) = d \Rightarrow Fix(T^a) = Fix(T^d)$.

Prueba. Como $a = dj \Rightarrow (T^d(P) = P \Rightarrow T^a(P) = P)$.

Como $d = au + nv \Rightarrow (T^a(P) = P \Rightarrow T^d(P) = P)$. □

Definamos $I_d := \{a \leq n\text{-}1: (a,n) = d\}$. Entonces $\#I_d = \varphi(\frac{n}{d})$ donde φ es la función de Euler y

$$\{1,\ldots,n\text{-}1\} = \bigcup_{d|n} I_d .$$

Luego

$$\sum_{i=1}^{n-1} \nu(T^i) = \sum_{d|n} \sum_{i\in I_d} \nu(T^i) = \sum_{d|n} \varphi(\frac{n}{d}) \nu(T^d).$$

Ahora estableceremos la relación entre $Fix(T^d)$ y los B^i de la § 2.

Afirmación.

$$Fix(T^d) = \bigcup_{i|d} B_i .$$

Prueba. Si $P\in B_i \Rightarrow P\in Fix(T^d)$ para $i|d$. Sea $P\in Fix(T^d)$. Si $T(P) = P$ entonces $P\in B_1$. Suponga $T(P) \neq P$ y sea i tal que $T^j(P) \neq P$ para $1 \leq j < i$, más, $T^i(P) = P$. Si $d = iq+r$ entonces $T^r(P) = P$ implica $r = 0$, y así $P\in B_i$ para $i|d$. □

Luego

$$\sum_{i=1}^{n-1} \nu\,(T^i) = \sum_{d|n} \varphi\,(\frac{n}{d}) \sum_{i|d} i\,x_i$$

$$= \sum_{i|n} \sum_{\substack{d \equiv 0 \bmod i \\ d|n}} \varphi\,(\frac{n}{d})\, i\,x_i$$

y usando $\sum_{q|n/i} \varphi\,(q) = \frac{n}{i} - 1$ obtenemos

$$\sum_{i=1}^{n-1} \nu\,(T^i) = \sum_{i|n} (n-1)\,x_i\,.$$

En conclusion, el término b_π en (3) es:

$$b_\pi = \sum_{i=1}^{n-1} \nu\,(T^i) + \sum_{i|n} \sum_{\pi(P) \in \pi(B_i)} i\,\Lambda(P)\,. \tag{4}$$

4. *p* no divide al *n* := ord *T*.

Aquí vamos a ver que (4) $\Rightarrow$ (2), i.e., $\Lambda(P) = 0$, o equivalentemente, $G_1(P)=\{1\}$. Los $G_i(P)$ son normales en $G_o(P)$. En particular $G_{i+1}(P)$ es normal en $G_i\,(P)$ y podemos analizar los cocientes $G_i\,/\,G_{i+1}$. (De ahora en adelante prescindiremos del "(P)"). Para esto, se usan los subgrupos del grupo de elementos invertibles del anillo local $\mathcal{O}$ en P. Si $\mathcal{M}$ es el ideal maximal de $\mathcal{O}$, $\mathcal{U} := \mathcal{O} \setminus \mathcal{M}$ es el grupo en cuestión. Se define $\mathcal{U}^{(o)} := \mathcal{U}$, $\mathcal{U}^{(i)} := 1+m^i$, $i \geq 1$ y se prueba que $\mathcal{U}^{(0)} / \mathcal{U}^{(1)} \simeq k^*$ (grupo multiplicativo de k) y para $i \geq 1$, $\mathcal{U}^{(i)} / \mathcal{U}^{(i+1)}$ isomorfo a $(k,+)$.

A continuación, se prueba que G_i / G_{i+1} es isomorfo a un subgrupo de $\mathcal{U}^{(i)} / \mathcal{U}^{(i+1)}$. Así,

(4.1) G_o/G_1 es cíclico cuyo orden es coprimo con p. Esto sigue del hecho que $G_o/G_1 \hookrightarrow k^*$ y siendo G_o/G_1 finito, este deberá ser cíclico. Lo del orden sigue por propiedades de raíces de la unidad (ver e.g. Lang [L, pág. 276]).

(4.2) Si p=0, entonces $G_1 = \{1\}$ y G_o es cíclico.

Para $i \geq 1$, $G_i / G_{i+1} \subset \mathcal{U}^{(i)} / \mathcal{U}^{(i+1)} = (k,+)$. Como este último no tiene subgrupos finitos cíclicos (p=0) entonces G_i / G_{i+1} . Como G_i={1} para i grande, sigue el resultado. Una prueba analítica de que G_o es cíclico puede verse en [F-K, III 7.7].

(4.3) Si p>0, entonces para $i \geq 1$, G_i / G_{i+1} son abelianos y producto directo de grupos cíclicos de orden p. G_1 es un p-grupo, i.e., su orden es potencia de p.

Esto sigue del hecho de que subgrupos finitos de $(k,+)$ son $\mathbf{F}_P$-espacios vectoriales. Siendo el orden de G_1 el producto de los órdenes de los G_i / G_{i+1} entonces G_1 es p-grupo.

Afirmación. p no divide al n = ord $G \Rightarrow G_1 = \{1\}$.

Si $p = 0$ sigue de 4.2. Sea $p > 0$. Tenemos

$$\text{ord } G_1 \mid \text{ord } G_o \mid \text{ord } G.$$

Si $G_1 \supsetneq \{1\}$, por 4.3 p|ord G_1 una contradicción. □

5. p no divide al n:= ord T.

Escribiendo $n = p^x q$ con $p \nmid q$, este caso se reduce a analizar $n = p^x$. Por (4.1) se sigue que $G_o = G_1$. Esto ya aumenta el sumando en (4). Defina e por

$$\# G_o = \# G_1 = p^e.$$

En la secuencia

$$G_o = G_1 \supseteq G_2 \supseteq \ldots$$

estamos interesados en los números i con

$$G_i \supsetneq G_{i+1}.$$

Sean $i_1 < i_2 < \ldots < i_\gamma$ tal que

$$G_o = G_1 = \ldots = G_{i_1} \supsetneq G_{i_1+1} = \ldots = G_{i_2} \supseteq \ldots \supsetneq G_{i_{r-1}+1} = \ldots = G_{i_r} \supsetneq G_{i_r+1} = \{1\}.$$

Suponga $G_o = G_1 = < S >$, ord(S) = p^e. Será suficiente analizar a que G_i pertenecen las potencias $S, S^P, S^{P^2}, \ldots, S^{P^{e-1}}$. Para simplificar los cálculos estableceremos las siguientes observaciones:

5.1 Sea $\sigma \in G_o$. Entonces $\sigma \in G_i \Leftrightarrow \sigma(t)/t \equiv 1 \mod m^i$.

($\Rightarrow$)$\sigma \in G_i \Rightarrow V_P(\sigma(t)-t) \geq i+1$. Esto significa que $\sigma(t)-t = ut^j$ con $u \in \mathcal{U}$, $j \geq i+1$.

Luego es claro que $\sigma(t)/t \equiv 1 \bmod m^i$.

($\Leftarrow$)De $\sigma(t)-t \in m^{i+1}$ obtenemos $V_P(\sigma(t)-t) \geq i+1$ □

5.2 Sea $\sigma \in G_o \setminus \{1\}$. Consideremos

$$i_\sigma := \min\{i \geq 0: \sigma \notin G_i\}.$$

Afirmamos que

$$i_\sigma = V_P(\sigma(t)-t).$$

Para ver esto, observe que por definición de los G_i tenemos

$$\sigma \in G_{V_P(\sigma(t)-t)-1} \setminus G_{V_P(\sigma(t)-t)}$$

lo que implica la igualdad arriba. □

Sea μ el entero dado por

$$V_P(S(t)-t) = \mu+1.$$

Esto significa que $S(t)-t = a\,t^{\mu+1}$, $a \in \mathcal{U}$. Queremos computar $V_P(S^P(t)-t)$.

5.3 Afirmación: Si $1 \leq i < p$ entonces $S^i \in G_\mu \setminus G_{\mu+1}$.

Vemos que $s(t) = t+tA$, $A \in m^u \setminus m^{u+1}$. Aplicamos S y luego

$$S^2(t) = t+tA+t(1+A)S(A),$$

y luego módulo m^{u+1}

$$S^2(t) \equiv t+tA+tS(A).$$

Inductivamente llegamos a la conclusión que

$$S^i(t) \equiv t+tA+\ldots+ tS^{i-1}(A) \bmod m^{u+1}.$$

Es claro que $S^i(t)/t \equiv 1 \bmod m^u$ y luego $S^i \in G_u$. Ahora probaremos que $S^i(t)/t \equiv 1 \bmod m^{u+1}$. Si lo anterior no ocurre entonces

$$(*) \qquad A+\ldots+S^{i-1}(A) \equiv 0 \bmod m^{u+1}.$$

Si $A = at^u$ con $a \in U$ entonces $S(A) = S(a)\,(S(t))^n = S(a)t^u\,(1+A)^n$, y luego $S(A) \equiv S(a)t^u \bmod m^{n+1}$ y así inductivamente vemos que (*) implica

$$(*_1) \qquad a + S(a) +\ldots+ S^{i-1}(a) = 0;$$

aplicamos S y obtenemos

$$a = S^{i}(a).$$

Ahora $(i,p^e) = 1$ (i es $< p$), luego

$$1 = ij + hp^e$$

para ciertos $j,h \in \mathbb{Z}$. Consecuentemente

$$S^1 = S^{ij} \circ S^{hp^e}$$

y sigue que $S(a) = a$. De la ecuación $(*_1)$ entonces tenemos

$$i\,a = 0$$

que contradice el hecho de que la característica es p.□

5.4 Afirmación: $S^{P} \in G_{u+1}$.

Los cálculos anteriores son válidos para el exponente p. Considerando $\mathcal{O}_P/_{n}^{u+1} \subset\!\!\rightarrow \mathcal{O}_P/_{n} = k$ (aquí entra k algebraicamente cerrado) se ve que $(*_1)$ es del tipo $p\tilde{a}$ y luego cero. Consecuentemente

$$S^{P}(t)/_{t} \equiv 1 \mod m^{u+1} \qquad \square$$

Lo anterior muestra que G_u / G_{u+1} tiene orden p.

Más aún, el primer número de ramificación es

$$i_1 = u = V_P(S(t) - t) - 1.$$

Continúa el análisis, considerando $\bar{u}$ ahora como

$$V_P(S^{P}(t) - t) = \bar{u} + 1.$$

Se demuestra que $S^{i} \in G_{\bar{u}} \setminus G_{\bar{u}+1}$ para $p \leq I < p^2$ y que $S^{P^2} \in G_{\bar{u}+1}$. En resumen, se obtienen e números de ramificación evaluando

$$\begin{aligned} i_1 &= V_P(S(t)-t)-1 \\ i_2 &= V_P(S^{P}(t)-t)-1 \\ &\vdots \\ i_e &= V_P\,(S^{P^{e-1}}(t)-t)-1 \end{aligned}$$

Notamos además que

$$G_o = G_{i_1} \underset{+}{\supset} G_{i_2} = G_o^{P} \underset{+}{\supset} G_{i_3} = G_o^{P^2}$$

$$\ldots \underset{+}{\supset} G_{i_2} = G_o^{P^{e-1}} \underset{+}{\supset} G_{i_{e+1}} = \{1\}.$$

En $d(P) = \sum_{i=0}^{\infty} (\#G_i(P) - 1)$ se suma así

$$\sum_{i=0}^{i_1} + \sum_{i=i_1+1}^{i_2} + \ldots + \sum_{i=i_{e-1}+1}^{i_e},$$

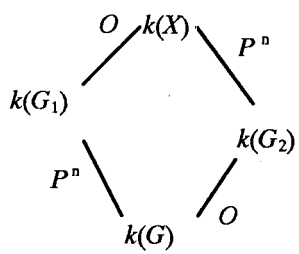
y teniendo presente que $\#G_{i_j} = p^{e-j+1}$, obtenemos

$$(*_3) \quad d(p) = (i_1 + 1)(\#G_o(P) - 1) + \sum_{j=2}^{e} (i_j - i_{j-1})(p^{e-j+1} - 1).$$

Esto ya muestra cómo tiene que ser corregido (2) y la gran diferencia con el caso $p \mid \text{ord}(T)$. Aquí se dice que estamos ante un caso de un recubrimiento con ramificación salvaje ("wild ramification").

5.5 Nota. $\text{ord}(T) = Op^n$, p no divide al $0, 0 > 1$.

Aquí $G \simeq G_1 \times G_2$ donde $\#G_1 = 0$, $\#G_2 = p^n$. Así podemos considerar este caso como una combinación de los anteriores. Sólo diremos cómo se estudia este caso. Denote por $k(H)$ el campo fijo de un grupo. Luego $k(G_1).k(G_2) = k(X)$ y se tiene el diagrama:



Se aplican los casos anteriores a las extensiones $k(X) \mid k(G_1)$ y $k(G_1) \mid k(G)$ y luego se usa que $d_{k(X) \mid k(G)}$ está relacionado con $d_{k(X)|k(G_1)}$ y $d_{k(G_1)|k(G)}$. Aquí entran rudimentos de la teoría de Galois (e.g.[L]) y propiedades del "diferente" ([Se]).

5.6 Observación. Los números de ramificación i_j del caso $n = p^x$ *no* son arbitrarios. Se cumple en general que $i_j \equiv i_h \pmod{p}$ ([Se, pág.70]). En el caso de extensiones abelianas se usa el Teorema de Hasse-Arf para probar que

$$\begin{aligned} i_1 &= i_0 + p\,i_1' \\ i_2 &= i_0 + p\,i_1' + p^2 i_1' \\ &\vdots \end{aligned}$$

donde los $i'_j > 0$ son enteros [loc.cit. pág.76]. También se les relaciona con ciertos enteros que son explicitados usando vectores de Witt para la extensión $k(X) \mid k(G)$ (ver [V-M] y sus referencias).

Referencias

[F-K] *H.M. Farkas, I.Kra:* Riemann Surfaces, 2nd. edition; Springer-Verlag (1992).

[L] *S. Lang:* Algebra, 3th. edition; Addison-Wesley (1993).

[Se] *J.P. Serre:* Local Fields, Springer-Verlag (1979).

[V-M] *R.C. Valentini, M.L. Madan:* Automorphism Group of Algebraic Function Fields, Math. Z. **176,** 39-52 (1981).

feto@ictp.trieste.it

Mathematics Group
ICTP
Trieste - Italy