Representaciones de Galois asociadas a curvas elípticas

Miguel Pineda Martín

Representaciones de Galois asociadas a curvas elípticas

Miguel Pineda Martín

Memoria presentada como parte de los requisitos para la obtención del título de Máster Universitario en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Prof. Jose María Tornero Sánchez
Prof. Sara Arias de Reyna Dominguez

Índice general

Abstract / Resumen

Abstract

J.P Serre made, in his article *'Proprietes galoisiénnés des points d'ordre fini des courbes elliptiques'* published in 1972 [9], an study about the image of Galois representations attached to the l-torsion points of elliptic curves without complex multiplication defined over a number field.

The purpose of this project is to develop the tools needed to understand the mentioned article and to present most of the results presented on it. We will pay special attention to the image of representations attached to the l-torsion of an elliptic curves defined over a local field. Lastly, we will present the main theorem of the article and the main ideas of its proof.

Teorema 0.1. *Let E be an elliptic defined over a number field K, without complex multiplication over $\overline{K}$. Then, for almost every prime l, the representation*

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[l]) \simeq \mathrm{GL}_2(\mathbb{F}_l)$$

attached to the l-torsión points is surjective.

Resumen

J.P. Serre realizó, en su artículo *'Proprietes galoisiénnés des points d'ordre fini des courbes elliptiques'* publicado en 1972 [9], un estudio de las imágenes de las representaciones de Galois del grupo los puntos de l-torsión de una curva elíptica sin multiplicación compleja definida sobre un cuerpo de números.

El propósito de este trabajo es desarrollar las herramientas y resultados necesarios para comprender dicho artículo, así como exponer los detalles de muchos de los resultados que se presentan en este. Prestaremos especial atención al estudio de la imagen de las representaciones de Galois asociadas a los puntos de l-torsión de una curva elíptica definida sobre un cuerpo local. Por último, presentaremos el resultado principal del artículo, junto con las ideas principales de la prueba. Dicho resultado es:

Teorema 0.2. *Sea E un curva elíptica definida sobre un cuerpo de números K, sin multiplicación compleja sobre $\overline{K}$. Entonces, para todo l primo, salvo para un número finito, la representación*

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[l]) \simeq \mathrm{GL}_2(\mathbb{F}_l)$$

asociada a los puntos de l-torsión es sobreyectiva.

1 | Preliminares

En este primer capítulo, vamos a estudiar y desarrollar algunas de las herramientas que necesitaremos para probar los resultados principales del trabajo. Concretamente, vamos a hacer un pequeño desarrollo de la teoría de grupos formales y la teoría infinita de Galois. Concluiremos el capítulo con un pequeño estudio de algunos subgrupos de $\mathrm{GL}_2(\mathbb{F}_p)$.

Además durante todo el trabajo, incluido este capítulo, vamos a hacer uso de resultados de teoría de valoraciones. Todos los resultados que necesitaremos están cubiertos en los capítulo II de [6] y están expuestos en el apéndice del trabajo. Además, se asumirán como conocidas las bases de la teoría de cuerpos globales, en concreto el capítulo I de [6] abarca sobradamente los requerimientos para entender el trabajo.

1.1 Teoría infinita de Galois

Todo cuerpo K tiene asociada una extensión de Galois distinguida: su clausura separable $\overline{K}|K$. El grupo de Galois $G := \mathrm{Gal}(\overline{K}|K)$ se denomina el grupo absoluto de Galois de K. Dicha extensión es infinita en general y tiene la ventaja de que contiene a todas las extensiones finitas de Galois de K. Este grupo juega un papel importante en la teoría de Galois. Sin embargo, el teorema de la correspondencia de Galois del caso finito no se generaliza directamente al caso infinito.

Ejemplo 1.1. El grupo absoluto de Galois $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}_p}|\,\mathbb{F}_p)$ de $\mathbb{F}_p$ contiene al automorfismo de Frobenius dado por

$$\forall x \in \overline{\mathbb{F}}_p, \quad \varphi(x) = x^p.$$

El subgrupo $(\varphi) = \{\varphi^n : n \in \mathbb{Z}\}$ tiene el mismo cuerpo fijo que el grupo $G_{\mathbb{F}_p}$ entero. Sin embargo, $(\varphi) \neq G_{\mathbb{F}_p}$. Para comprobar esto, vamos a construir un elemento de $G_{\mathbb{F}_p}$

que no esté en (φ). Elegimos una sucesión $\{a_n\}$ de enteros tales que

$$a_n \equiv a_m \mod m,$$

siempre que $m|n$, pero tal que no exista ningún entero tal que $a \equiv a_n \mod n$ para todo $n \in \mathbb{N}$. Una sucesión de este tipo se puede construir como $a_n = n' x_n$, con $n = n' p^{v_p(n)}$, $n' = 1$ y $1 = n' x_n + p^{v_p(n)} y_n$. Ahora llamamos

$$\psi_n = \phi^{a_n}|_{\mathbb{F}_{p^n}} \in G_{\mathbb{F}_{p^n}}.$$

Si $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, entonces $m|n$. Por tanto, $a_n \equiv a_m \mod m$ de lo que se deduce que:

$$\psi_n|_{\mathbb{F}_{p^m}} = \varphi^{a_n}|_{\mathbb{F}_{p^m}} = \varphi^{a_m}|_{\mathbb{F}_{p^m}} = \psi_m.$$

Notemos que $\varphi|_{\mathbb{F}_{p^m}}$ tiene orden m. Por tanto, los ψ_n definen un automorfismo ψ de $\overline{\mathbb{F}_p} = \cup_{n=1}^{\infty} \mathbb{F}_{p^n}$. Sin embargo, por construcción, ψ no puede pertenecer a (φ), ya que en ese caso $\psi = \varphi^a$ con $a \in \mathbb{Z}$ implicaría que

$$\psi|_{\mathbb{F}_{p^n}} = \varphi^{a_n}|_{\mathbb{F}_{p^n}} = \varphi^a|_{\mathbb{F}_{p^n}}$$

lo cual implicaría a su vez que $a_n \equiv a \mod n$ para todo $n \in \mathbb{N}$, lo cual es una contradicción.

El ejemplo anterior no significa que la correspondencia de Galois no se dé en ningún caso. Sea $\Omega|K$ una extensión algebraica arbitraria, posiblemente infinita. Para tener una correspondencia, primero hay que notar que al grupo de Galois $\mathrm{Gal}(\Omega|K)$ tiene una topología canónica asociada. Esta topología se denomina topología de Krull y se obtiene como sigue. Para cada $\sigma \in G$ consideramos las clases a izquierda

$$\sigma\,\mathrm{Gal}(\Omega|L)$$

como un base de entornos de σ, donde $L|K$ varía en todas las extensiones finitas de Galois de K. Se comprueba fácilmente que esta topología hace de G un grupo topológico.

Proposición 1.1. Para toda extensión de Galois $\Omega|K$ el grupo de Galois $G = \mathrm{Gal}(\Omega|k)$ es compacto y Hausdorff para la topología de Krull.

Demostración. Veamos primero que es Hausdorff. Sean $\sigma, \tau \in G$ distintos, entonces existe una subextensión finita de Galois $L|K$ de $\Omega|K$ tal que $\sigma|_L \neq \tau|_L$. Por tanto,

$\sigma\,\mathrm{Gal}(\Omega|K) \neq \tau\,\mathrm{Gal}(\Omega|K)$, lo cual implica $\sigma\,\mathrm{Gal}(\Omega|K) \cap \tau\,\mathrm{Gal}(\Omega|K) = \emptyset$.
Para probar la compacidad consideramos la aplicación.

$$\begin{aligned} h : G &\longrightarrow \prod_L \mathrm{Gal}(L|K) \\ \sigma &\longmapsto \prod_L \sigma|_L, \end{aligned}$$

donde L recorre todas las subextensiones finitas de Galois $L|K$ de $\Omega|K$, y donde vemos los grupos $\mathrm{Gal}(L|K)$ con la topología discreta. Por el teorema de Tykhonoff el producto es compacto. El homomorfismo h es inyectivo porque $\sigma|_L = \mathrm{Id}_L$ para cada L si, y sólo si, $\sigma = \mathrm{Id}$. Los conjuntos $U = \prod_{L \neq L_0} \mathrm{Gal}(L|K) \times \{\overline{\sigma}\}$ forman una subbase de entornos del espacio $\prod_L \mathrm{Gal}(L|K)$, donde $L_0|K$ varía entre las subextensiones finitas y $\overline{\sigma} \in \mathrm{Gal}(L_0|L)$. Si σ es una preimagen de $\overline{\sigma}$, entonces $h^{-1}(U) = \sigma\,\mathrm{Gal}(\Omega|K)$, por tanto, h es continua. Más aún, se tiene que

$$h(\sigma\,\mathrm{Gal}(\Omega|K) = h(G)) \cap U,$$

de lo que se deduce que h es abierta y, por tanto, homeomorfismo.
De esta manera, para ver que G es compacto nos basta comprobar que $h(G)$ lo es. Para ello, consideramos para cada par de subextensiones $L' \supset L$ finitas de Galois de $\Omega|K$ el conjunto

$$M_{L'|L} = \left\{ \prod_F \sigma_F \in \prod_F \mathrm{Gal}(F|K) \,:\, \sigma_{L'|L} = \sigma_L \right\}.$$

Por definición de G se tiene que:

$$h(G) = \bigcap_{L' \subset L} M_{L'|L}.$$

Por tanto, nos basta probar que los $M_{L'|L}$ son cerrados. Pongamos $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$ y sea S_i el conjunto de las extensiones a L' de σ_i. Entonces,

$$M_{L'|L} = \bigcup_{i=1}^{n} \left(\prod_{F \neq L, L'} \mathrm{Gal}(F|K) \times S_i \times \sigma_i \right)$$

es cerrado, donde $\times$ está denotando al producto directo de grupos.

Con esto, podemos dar el teorema principal de la teoría de Galois para extensiones infinitas.

Teorema 1.1. *Sea $\Omega|K$ una extensión de Galois, entonces la aplicación*

$$L \mapsto \mathrm{Gal}(\Omega|L)$$

es una correspondencia biunívoca entre las subextensiones $L|K$ de $\Omega|K$ y los subgrupos cerrados de $\mathrm{Gal}(\Omega|K)$. Además, los subgrupos abiertos de $\mathrm{Gal}(\Omega|K)$ son exactamente los que corresponden a subextensiones finitas de de $\Omega|K$.

Demostración. Todo subgrupo abierto de $\mathrm{Gal}(\Omega|K)$ también es cerrado, ya que es el complemetario de la unión de sus clases a izquierda, que son abiertas porque $\mathrm{Gal}(\Omega|K)$ es un grupo topológico. Si $L|K$ es una extensión finita $\mathrm{Gal}(\Omega|L)$ es abierto, ya que cada $\sigma \in \mathrm{Gal}(\Omega|L)$ pertenece a un entorno abierto $\sigma\,\mathrm{Gal}(\Omega|N) \subset \mathrm{Gal}(\Omega|L)$, donde $N|K$ es la clausura normal de $L|K$. Si ahora $L|K$ es una subextensión arbitraria, entonces

$$\mathrm{Gal}(\Omega|L) = \bigcap_{i=1} \mathrm{Gal}(\Omega|L_i)$$

donde $L_i|K$ varía entre todas las subextensiones finitas de $L|K$. Como acabamos de ver los subgrupos $\mathrm{Gal}(\Omega|L_i)$ son abiertos y cerrados. En particular, $\mathrm{Gal}(\Omega|L)$ es cerrado.

La aplicación $L \mapsto \mathrm{Gal}(\Omega|L)$ es inyectiva, ya que L es el cuerpo fijo de $\mathrm{Gal}(\Omega|L)$. Sea ahora H un subgrupo cerrado de $\mathrm{Gal}(\Omega|K)$, se tiene que

$$H = \mathrm{Gal}(\Omega|L)$$

con L el cuerpo fijo de H. La inclusión $H \subset \mathrm{Gal}(\Omega|L)$ es trivial. Recíprocamente, sea $\sigma \in \mathrm{Gal}(\Omega|K)$, consideramos el entorno abierto $\sigma\,\mathrm{Gal}(\Omega|L')$ para alguna extensión $L'|K$ finita de Galois. La aplicación $H \longrightarrow \mathrm{Gal}(L'|L)$ dada por la restricción a L' es sobreyectiva, porque su imagen tiene por cuerpo fijo a L, lo cual implica que tiene que ser todo $\mathrm{Gal}(L'|L)$ por el teorema de correspondencia de Galois en el caso finito. De esta manera, podemos elegir $\tau \in H$ tal que $\tau|_{L} = \sigma|_{L}$, i.e. $\tau \in H \cap \sigma\,\mathrm{Gal}(\Omega|L')$. Por tanto, σ está en la clausura de H en $\mathrm{Gal}(\Omega|L)$ que también es cerrado, con lo cual $H = \mathrm{Gal}(\Omega|L)$.

Por último, si H es un subgrupo abierto ya hemos visto que también es cerrado y, por tanto, de la forma $\mathrm{Gal}(\Omega|L)$. Pero $\mathrm{Gal}(\Omega|K)$ es la unión disjunta de los σH con $\sigma \in \mathrm{Gal}(\Omega|K)$. Ahora bien, como $\mathrm{Gal}(\Omega|K)$ es compacto, bastan una cantidad finita para cubrir el grupo. Luego H tiene índice finito, lo cual implica que la extensión $L|K$ es de grado finito. ∎

Observación 1.1. Sea $\Omega|K$ una extensión de Galois y sea $\Omega|L$ una subextensión de Galois. En este caso, $\mathrm{Gal}(\Omega|L) \lhd \mathrm{Gal}(\Omega|K)$. En efecto, la aplicación

$$\begin{aligned} \theta : \mathrm{Gal}(\Omega|K) &\longrightarrow \mathrm{Gal}(L|K) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

está bien definida por ser L una extensión normal y su núcleo es el subgrupo cerrado $\mathrm{Gal}(\Omega|L)$. Además, como $\Omega|L$ es una extensión separable, el morfismo anterior es sobreyectivo. Por tanto,

$$\frac{\mathrm{Gal}(\Omega|K)}{\mathrm{Gal}(\Omega|L)} \cong \mathrm{Gal}(L|K).$$

De la observación y el teorema anteriores se deduce que tenemos una base de entornos del elemento neutro formada por subgrupos normales. Esto lleva a dar la abstracción teórica de esta propiedad usando solo teoría de grupos.

Definición 1.1. *Un grupo profinito es un grupo topológico G que es Hausdorff, compacto y admite una base de entornos de $1 \in G$ formada por subgrupos normales.*

No es difícil probar que todos los grupos profinitos se pueden construir a través de sus subgrupos normales mediante el límite inverso.

Proposición 1.2. Si G es un grupo profinito y N varía entre todos sus subgrupos normales abiertos, entonces se tiene el siguiente isomorfismo y homeomorfismo:

$$G \cong \varprojlim_N G/N$$

Recíprocamente, si $\{G_i, g_{ij}\}$ es un sistema proyectivo de de grupos finitos, entonces

$$G = \varprojlim_i G_i$$

es un grupo profinito.

Demostración. Las definiciones de límite inverso y sistema proyectivo se pueden encontrar en ([6] IV.2) y la prueba en ([6] IV.2.8)

En particular, el resultado anterior implica que podemos ver los grupos de Galois como

$$\mathrm{Gal}(\Omega|K) = \varprojlim_L \mathrm{Gal}(L|K)$$

con $L|K$ subextensiones finitas de Galois de $\Omega|K$.

1.2 Propiedades de los grupos asociados a los grupos formales

Como se verá más adelante, a cada curva elíptica podemos asociar lo que se conoce como grupo formal. En esta sección vamos a desarrollar las propiedades generales de los grupos formales que necesitaremos en este trabajo. En el capítulo siguiente integraremos esta teoría con la de las curvas elípticas. Comenzamos definiendo grupo formal conmutativo.

Definición 1.2. *Un grupo formal conmutativo $F(X,Y)$ es una serie de potencias sobre un anillo R (conmutativo y con elemento unidad) en dos variables X, Y verificando las siguientes propiedades:*

a) $F(0,X) = X = F(X,0)$.
b) $F(F(X,Y),Z) = F(X,F(Y,Z))$.
c) $F(X,Y) = F(Y,X)$.

Observación 1.2. Se comprueba fácilmente usando las condiciones anteriores que:

$$F(X,Y) = X + Y + \sum_{i\geq 1, j\geq 1} c_{ij} X^i Y^j, \quad c_{ij} \in R.$$

Observación 1.3. Sean $G, H \in R[\![X,Y]\!]$, la primera propiedad de la definición nos da la siguiente equivalencia:

$$G = H \iff F(G,0) = F(H,0) \iff F(0,G) = F(0,H).$$

Esto es el equivalente a la propiedad cancelativa de grupos.

Vamos a probar ahora la existencia de elemento inverso, para ello llamaremos I al ideal generado por X e Y en $R[\![X,Y]\!]$.

Proposición 1.3. Sea $F \in R[\![X,Y]\!]$ un grupo formal. Existe un único $i(X) \in R[\![X,Y]\!]$ tal que $F(X, i(X)) = 0$.

Demostración. Como hemos dicho antes F es de la siguiente forma:

$$F(X,Y) = X + Y + \sum_{i\geq 1, j\geq 1} c_{ij} X^i Y^j,$$

para unos ciertos $c_{ij} \in R$. Vamos a construir el inverso iterativamente. En primer lugar, ponemos $g_1 = -T$. Así,

$$F(T, g_1) = T - T + \sum_{i\geq 1, j\geq 1} c_{i,j} T^i (-T)^j = \sum_{i\geq 1, j\geq 1} c_{i,j} T^i (-T)^j \in I^2.$$

Ponemos ahora $g_2 = T + b_2T^2$ con b_2 a elegir. Evaluando de nuevo,

$$F(T, g_2) = b_2T^2 + \sum_{i\geq 1, j\geq 1} c_{i,j}T^i(-T + b_2T^2)^j.$$

Si elegimos ahora $b_2 = c_1$, los términos de grado 2 se anulan y $F(T, g_2) \in I^3$. Podemos continuar de esta forma y construir una sucesión $\{g_i\}$ tal que $F(T, g_i) \in I^{i+1}$. La sucesión construida es una sucesión de Cauchy en el anillo de las series formales $R[\![T]\!]$ y su límite es la inversa $i(T)$ que buscábamos. Por construcción verifica que $F(T, i(T)) = 0$. Además también cumple $F(i(T), T) = 0$, por la conmutatividad.

La unicidad del inverso se demuestra igual que en teoría de grupos. Sea $j(T)$ una serie de potencias tal que $F(T, j(T)) = 0$. Entonces,

$$\begin{aligned} i(T) &= F(0, i(T)) = F(F(i(T), T), i(T)) = F(i(T), F(T, i(T))) \\ &= F(i(T), 0) = F(i(T), 0) = F(i(T), F(T, j(T))) \\ &= F(F(i(T), T), j(T)) = F(0, j(T)) = j(T). \end{aligned}$$

Seguimos ahora con la definición de homomorfismo de grupos formales.

Definición 1.3. *Sean $F, G \in R[\![X, Y]\!]$ dos grupos formales. Un homomorfismo $f : F \longrightarrow G$ es una serie de potencias $f \in R[\![T]\!]$ tal que*

$$f(F(X, Y)) = G(f(X), f(Y))$$

Observación 1.4. Si $f : F \longrightarrow G$ es un homomorfismo de grupos formales, entonces $f(0) = 0$. En efecto,

$$\begin{aligned} 0 &= G(f(0), i(f(0))) = G(G(f(0), f(0)), i(f(0))) \\ &= G(f(0), G(f(0), i(f(0)))) = G(f(0), 0) = f(0) \end{aligned}$$

Sea F un grupo formal. Podemos definir una familia de endomorfismos de F, $\{[n]T\}$ por inducción de la siguiente manera,

a) $[0](T) := 0$.
b) $[n + 1](T) := F([n](T), T)$.

También podemos definir $[m](T)$ cuando m es un entero negativo. En efecto, ya tenemos definido $[0](T)$, y se define inductivamente como

$$[m](T) = F\left([m+1](T), i(T)\right).$$

Lema 1.1. Sea $a \in R^*$ y sea $f(T) \in R[\![T]\!]$ una serie de potencias de la forma

$$f(T) = aT + \text{términos de orden superior.}$$

Entonces, existe una única serie de potencias $g(T) \in R[\![T]\!]$ tal que

$$f(g(T)) = T.$$

Además, dicha serie también satisface que $g(f(T))$.

Demostración. Basta que construyamos una sucesión de polinomios $g_n(T) \in R(T)$ tal que

$$f(g_n(T)) \equiv T \mod T^{n+1} \quad \text{y} \quad g_{n+1}(T) \equiv g_n(T) \mod T^{n+1},$$

ya que en ese caso el límite de la sucesión existe en $R[\![T]\!]$ y claramente cumple $f(g(T)) = T$. Para construir la sucesión, ponemos $a_1 = a^{-1}T$ y supongamos que hemos construido $g_{n-1}(T)$ con las propiedades anteriores. Ponemos

$$g_n(T) = g_{n-1}(T) + \lambda T^n.$$

Buscamos un λ adecuado. Usando la hipótesis de inducción tenemos que

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}(T)) + a\lambda T^n \qquad \mod T^{n+1} \\ &\equiv T + bT^n + a\lambda T^n \qquad \mod T^{n+1}, \end{aligned}$$

para algún $b \in R$. Basta tomar $\lambda = -a^{-1}b$.

Siguiendo el mismo procedimiento tenemos que existe $h(T)$ tal que $g(h(T)) = T$. Tenemos, por tanto, que:

$$g(f(T)) = g(f(g(h(T)))) = g(f \circ g(h(T))) = g(h(T)) = T.$$

Pasamos a probar la unicidad, supongamos que existe $G(T) \in R[\![T]\!]$ tal que $f(G(T)) = T$. Se tiene que:

$$g(T) = g(f(G(T))) = (g \circ f)(G(T)) = G(T).$$

Por tanto, hemos probado la unicidad de g. ∎

Proposición 1.4. Sea F un grupo formal sobre un anillo R y sea $m \in \mathbb{Z}$. Se tienen:

a) $[m](T) = mT +$ términos de orden superior.
b) Si $m \in R^*$, entonces $[m] : F \longrightarrow F$ es un isomorfismo.

Demostración. La primera afirmación es trivial y la segunda se deduce del lema anterior.

1.2.1 El diferencial invariante de un grupo formal

Sea, de nuevo, F un grupo formal sobre un anillo R arbitrario. En este contexto, llamaremos forma diferencial formal a expresiones de la forma $P(T)dT$ con $P(T) \in R[\![T]\!]$.

Definición 1.4. *Un diferencial invariante sobre F/R es una forma diferencial*

$$\omega(T) = P(T)dT \in R[\![T]\!]dT$$

tal que

$$\omega \circ F(T,S) = \omega(T).$$

Esto último significa que

$$P(F(T,S))F_X(T,S) = P(T),$$

donde F_X denota la derivada formal con respecto a la primera variable. Por último, diremos que dicho diferencial está normalizado si $P(0) = 1$.

Proposición 1.5. Sea F/R un grupo formal. Existe un único diferencial invariante normalizado para dicho grupo formal. Además viene dado por la siguiente fórmula:

$$\omega = F_X(0,T)^{-1}dT.$$

Además, todo diferencial invariante sobre F/R es de la forma $a\omega$ para algún $a \in R$.

Demostración. Supongamos que $P(T)dT$ es un diferencial invariante sobre F/R, este debe cumplir

$$P(F(T,S))F_X(T,S) = P(T).$$

Si ponemos $T = 0$, como $F(0,S) = S$ obtenemos lo siguiente:

$$P(S)F_X(0,S) = P(0).$$

Como $F_X(0,S) = 1 + \cdots$, la ecuación nos dice que $P(S)$ está completamente determinado por el valor $P(0)$. Además, esto implica que todo diferencial invariante es de la forma $a\omega$ con $a \in R$ y

$$\omega = F_X(0,T)^{-1}dT.$$

Como el diferencial ω está normalizado solo queda ver que ω así definido es, en efecto, invariante. Es decir, vamos a probar que

$$F_X(0,F(T,S))^{-1}F_X(T,S) = F_X(0,T)^{-1}.$$

Para probar esto, vamos a derivar con respecto a U la igualdad que nos da la propiedad asociativa

$$F(U,F(T,S)) = F(F(U,T),S).$$

De esta manera, obtenemos

$$F_X(U,F(T,S)) = F_X(F(U,T),S)F_X(U,T).$$

Basta poner ahora $U = 0$.

Corolario 1.1. Sean F/R y G/R dos grupos formales con diferenciales invariantes ω_F y ω_G respectivamente. Sea $f : F \longrightarrow G$ un homomorfismo. Entonces,

$$\omega_G \circ f = f'(0)\omega_F.$$

Donde f' denota la derivada formal de la serie formal f.

Demostración. Comenzamos haciendo el siguiente cálculo,

$$(\omega_G \circ f)(F(T,S)) = \omega_G(G(f(T),f(S))) = \omega_G(f(T)) = (\omega_G \circ f)(T),$$

donde la última igualdad se deduce de la invariancia de ω_G. Por tanto, $\omega_G \circ f$ es un diferencial invariante para F. Esto implica que es de la forma $a\omega_F$. Basta hacer ahora comprobar en la igualdad que $f'(0) = a$.

Corolario 1.2. Sea F/R un grupo formal y sea $p \in \mathbb{Z}$ un primo. Existen series de potencias $f(T), g(T) \in R[\![T]\!]$ tales que $f(0) = g(0) = 0$ y tales que:

$$[p](T) = pf(T) + g(T^p).$$

Demostración. Sea $\omega(T)$ el diferencial invariante normalizado de F. Como $[p]'(0) = p$, el corolario anterior nos dice que

$$p\omega(T) = (\omega \circ [p])(T) = (1 + \cdots)[p]'(T)dT.$$

La última igualdad se deduce de la regla de la cadena y de que ω está normalizada. La serie $(1 + \cdots)$ es invertible en $R[\![T]\!]$, de lo que se sigue que

$$[p]'(T) \in pR[\![T]\!].$$

Por tanto, cada término aT^n en la serie $[p](T)$ cumple que $a \in pR$ o que $p|n$.

1.2.2 Grupos formales en característica p

En este apartado R será un anillo de característica $p > 0$.

Definición 1.5. *Sean F/R y G/R grupos formales y $f : F \longrightarrow G$ un homomorfismo de grupos formales definido sobre R. Llamamos altura de f, y la denotamos* $\mathrm{ht}(f)$ *al mayor entero tal que*

$$f(T) = g\left(T^{p^h}\right),$$

para alguna serie $g(T) \in R[\![T]\!]$ (si $f = 0$, entonces $\mathrm{ht}(f) = \infty$). Se llama altura del grupo formal F a la altura del homomorfismo $[p]$.

Proposición 1.6. Sean F/R y G/R dos grupos formales y sea $f : F \longrightarrow G$ un homomorfismo de grupos formales definido sobre R. Entonces,

a) Si $f'(0) = 0$, entonces $f(T) = f_1(T^p)$ para algún $f_1 \in R[\![T]\!]$.
b) Si ponemos $f(T) = g\left(T^{p^{\mathrm{ht}(f)}}\right)$, entonces $g'(0) \neq 0$.

Demostración. a) Sean ω_F y ω_G los diferenciales invariantes normalizados de F y G respectivamente. Como $f'(0) = 0$, se tiene que

$$0 = f'(0)\omega_F(T) = \omega_G(f(T)) = (1 + \cdots)f'(T)dT.$$

Por tanto, $f'(T) = 0$, luego $f(T) = f_1(T^p)$.

b) Sea $q = p^{ht(F)}$ y $F(X,Y) = \sum a_{ij}X^iY^j$. Llamemos $F^{(q)}(X,Y) = \sum a_{ij}^{(q)}X^iY^j$. Es fácil comprobar, usando que la característica de R es p, que $F^{(q)}$ define otro grupo formal. Vamos a probar que g es un homomorfismo de grupos formales de $F^{(q)}$ a G. Llamando $S^q = X$ y $T^q = Y$, se tiene que:

$$\begin{aligned} g(F^{(q)}(X,Y)) &= g(F(S,T)^q) = f(F(S,T)) = G(f(S), f(T)) \\ &= G(g(S^q), g(T^q)) = G(g(X), g(Y)). \end{aligned}$$

Ahora por reducción al absurdo supongamos que $g'(0) = 0$. Por el apartado anterior,

$$f(T) = g\left(T^{p^{\mathrm{ht}(F)}}\right) = g_1\left(T^{p^{\mathrm{ht}(F)+1}}\right).$$

Esto contradice la maximalidad de $\mathrm{ht}(f)$.

Probamos ahora que la altura tiene un buen comportamiento con la composición.

Proposición 1.7. Sean $F/R, G/R$ y H/R grupos formales. Consideramos una cadena de homomorfismos

$$F \xrightarrow{f} G \xrightarrow{g} H$$

definidos sobre R. Entonces,

$$\mathrm{ht}(g \circ f) = \mathrm{ht}(g) + \mathrm{ht}(f)$$

Demostración. Escribimos

$$f(T) = f_1\left(T^{p^{\mathrm{ht}(f)}}\right) \quad \text{y} \quad g(T) = g_1\left(T^{p^{\mathrm{ht}(g)}}\right).$$

Entonces,

$$(g \circ f)(T) = g_1\left(f_1\left(T^{p^{\mathrm{ht}(f)}}\right)^{p^{\mathrm{ht}(g)}}\right) = g_1\left(\tilde{f}_1\left(T^{p^{\mathrm{ht}(f)+\mathrm{ht}(g)}}\right)\right)$$

donde $\tilde{f}_1$ se obtiene de f_1 elevando cada término a $p^{\mathrm{ht}(g)}$. Por el segundo apartado de la proposición anterior sabemos que los términos lineales de f_1 y g_1 son no nulos, por tanto, lo mismo ocurre con la composición. De esto se deduce la maximalidad de $\mathrm{ht}(f) + \mathrm{ht}(g)$, i.e.

$$\mathrm{ht}(g \circ f) = \mathrm{ht}(g) + \mathrm{ht}(f).$$

1.2.3 Grupos asociados a grupos formales

Sea (K, v) un cuerpo dotado de una valoración con cuerpo residual finito, característica residual p y anillo de valoración $\mathcal{O}$. Sea K_s la clausura separable de K, la valoración v se puede extender de manera única a K_s(ver A.3). Denotamos por v_s a la valoración extendida, por $\mathcal{O}_s$ al anillo de valoración de v_s y por $\mathcal{M}_s$ a su ideal maximal. En esta situación, si $f(T) = \sum_{i\geq 0} a_i T^i \in \mathcal{O}[\![T]\!]$ es una serie formal, denotamos por $\overline{f}(T)$ a la serie obtenida reduciendo los coeficientes de f módulo $\mathcal{M}$.

En este contexto es habitual hablar de la altura de un grupo formal refiriéndonos en realidad a la altura sobre el cuerpo residual.

Definición 1.6. *En las condiciones anteriores, sean F, G dos grupos formales sobre $\mathcal{O}$ y $f : F \longrightarrow G$ un homomorfismo definido sobre $\mathcal{O}$. En esta situación, definimos*

a) La altura de f, denotada $\mathrm{ht}(f)$*, se define como el mayor entero h tal que la reducción de f puede expresarse como*

$$\overline{f}(T) = \overline{g}\left(T^{p^h}\right)$$

para alguna serie formal $\overline{g} \in \mathcal{O}/\mathcal{M}[\![T]\!]$. Si $\overline{f} = 0$, entonces $\mathrm{ht}(f) = \infty$.

b) La altura de F, denotada por $\mathrm{ht}(F)$*, la definimos como la altura de la aplicación $[p] : F \longrightarrow F$.*

Vamos a ver ahora cómo asociar grupos a los grupos formales.

Definición 1.7. *Sea $F(X,Y) \in \mathcal{O}[\![X,Y]\!]$. El grupo asociado a $F(X,Y)$ sobre $\mathcal{O}_s$, que denotaremos $F(\mathcal{M}_s)$, es el conjunto $\mathcal{M}_s$, con las operaciones de grupo:*

a) $x \oplus_F y := F(X,Y)$ para $x, y \in \mathcal{M}_s$.
b) $\ominus_F x := i(x)$ para $x \in \mathcal{M}_s$.

Observación 1.5. Las operaciones anteriores están bien definidas, ya que como los coeficientes de F están en K, la convergencia se da en una extensión finita de K (en $K(x,y)$ para el caso de la suma y en $K(x)$ para el caso del inverso), que es un cuerpo completo.

Proposición 1.8. Sea F/R un grupo formal, se tienen los siguientes:

a) Para cada $n \geq 1$, la aplicación

$$\frac{F(\mathcal{M}^n)}{F(\mathcal{M}^{n+1})} \longrightarrow \frac{\mathcal{M}^n}{\mathcal{M}^{n+1}}$$

inducida por la identidad entre los conjuntos es un isomorfismo de grupos.
b) Todo elemento de orden finito de $F(\mathcal{M})$ tiene orden una potencia de p.

Demostración. a) Basta notar que

$$x \oplus_F y = x + y + \text{términos de orden superior} \equiv x + y \mod \mathcal{M}^{2n}$$

b) Basta ver que no hay ningún elemento de torsión de orden coprimo con p. Por reducción al absurdo supongamos que existen $m \in \mathbb{N}$ y $x \in F(\mathcal{M})$ tales que

$$[m](x) = 0,$$

y $p \nmid m$. Notemos que cuando pasamos al cuerpo residual m no se anula porque no es múltiplo de p. Por tanto, $m \notin \mathcal{M}$, por lo que $m \in R^*$. Se ha visto que si $m \in R^*$, entonces

$$[m] : F(\mathcal{M}) \longrightarrow \mathcal{M}$$

es un isomorfismo de grupos formales. En particular, su kernel es $\{0\}$.

1.3 Subgrupos de $\mathrm{GL}_2(\mathbb{F}_p)$

El resultado principal del trabajo consiste en que ciertas representaciones de dimensión 2 sobre $\mathbb{F}_l$ son sobreyectivas. Por ello, vamos a estudiar en esta sección algunos subgrupos de $\mathrm{GL}_2(\mathbb{F}_l)$ importantes que nos aparecerán más adelante. Además, daremos algunos criterios de sobreyectividad relacionados con estos subgrupos. En lo que sigue, V será un espacio vectorial de dimensión 2 sobre el cuerpo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

1.3.1 Subgrupos de Cartan

Los subgrupos de Cartan pueden definirse en un contexto muy amplio. No obstante, en este trabajo seguiremos la exposición que da Serre en ([9] 2), dando la definición solo para el caso de $\mathrm{GL}_2(\mathbb{F}_p)$.

Dividiremos el estudio de los subgrupos de Cartan en dos casos: los subgrupos de Cartan escindidos y los no escindidos. Sin embargo, antes de dar la definición precisa de dichos subgrupos, vamos a motivar su estudio.

Consideremos el álgebra de endomorfismos de V, que denotaremos $\mathrm{End}(V)$. Dado $s \in \mathrm{End}\, V$, el teorema de Hamilton-Cayley nos dice que s cumple la ecuación:

$$x^2 - \mathrm{tr}(s)x + \det(s) = 0, \tag{1.1}$$

donde estamos identificando $\lambda \in \mathbb{F}_p$ con las matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$. La ecuación anterior también se puede estudiar sobre $\mathbb{F}_p$, en cuyo caso sólo tenemos dos posibilidades:

a) La ecuación (1.1) no tiene raíces en $\mathbb{F}_p$. En ese caso, si consideramos $k = \mathbb{F}_p[\alpha]$ el cuerpo $\mathbb{F}_p$ al que hemos añadido una raíz α del polinomio característico anterior.

Tenemos así una inclusión canónica (como álgebras):

$$\begin{aligned} k &\hookrightarrow \mathrm{End}(V) \\ \alpha &\mapsto s, \end{aligned}$$

definida por el principio de sustitución. De esta manera, k^* es un subgrupo multiplicativo de $\mathrm{End}(V)$. Este tipo de grupos será lo que llamaremos un subgrupo de Cartan escindido.

b) La ecuación (1.1) tiene dos raíces $a, b \in \mathbb{F}_p$. Tenemos entonces que s anula el polinomio $(x-a)(x-b)$. Sin embargo, esto no implica que $s = a$ o $s = b$, ya que $\mathrm{End}(V)$ no es un cuerpo. Esto es lo que va a dar lugar a los subgrupos de Cartan escindidos.

Damos ya las definiciones precisas.

Definición 1.8. *Sea $C \subset \mathrm{GL}(V)$ es un subgrupo de Cartan escindido si existen dos subespacios distintos $D_1, D_2 \subset V$ de dimensión 1, que llamaremos rectas, tales que:*

$$C = \{s \in \mathrm{GL}(V) : sD_1 \subset D_1 \ y \ sD_2 \subset D_2\}.$$

Definición 1.9. *Sea $C \subset \mathrm{GL}(V)$, diremos que C es un subgrupo de Cartan no escindido si existe un cuerpo $k \subset \mathrm{End}(V)$ de cardinal p^2 de manera que $C^* = k$.*

Observación 1.6. Sea C un subgrupo de Cartan escindido, y sean D_1, D_2 las rectas correspondientes. Si tomamos por base un punto de D_1 y otro en D_2, entonces, C puede expresarse como

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

Por tanto, este grupo es un producto de grupos cíclicos y su orden es $(p-1)^2$.

Observación 1.7. Si C es un subgrupo de Cartan no escindido, por definición es el grupo multiplicativo de un cuerpo de p^2 elementos . Por tanto, C es un grupo cíclico de orden $p^2 - 1$.

Definición 1.10. *Diremos que un subgrupo de $C \subset \mathrm{GL}(V)$ es un subgrupo de Cartan si es un subgrupo de Cartan escindido o no escindido.*

Una propiedad de los subgrupos de Cartan que nos será de gran utilidad es que en cierto sentido estos subgrupos constituyen un buen recubrimiento de los subgrupos de $\mathrm{GL}(V)$ de orden p.

Proposición 1.9. Sea $p \neq 2$, y sea $s \in \mathrm{GL}(V)$ un elemento tal que $\mathrm{tr}(s)^2 - 4\det(s) \neq 0$. Entonces, s pertenece a un subgrupo de Cartan y sólo a uno. Este subgrupo es escindido si, y sólo si, $\mathrm{tr}(s)^2 - 4\det(s)$ es un cuadrado en $\mathbb{F}_p$.

Demostración. En primer lugar, supongamos que $\mathrm{tr}(s)^2 - 4\det(s)$ no es un cuadrado en $\mathbb{F}_p$. Entonces, el polinomio $f(x) = x^2 - \mathrm{tr}(s)x + \det(s)$ no tiene raíces en $\mathbb{F}_p$. Consideramos el cuerpo

$$k := \mathbb{F}_p[\alpha] = \frac{\mathbb{F}_p[x]}{(f(x))}.$$

Si consideramos la inclusión $k \subset \mathrm{End}(V)$ que nos da el principio de sustitución identificando α con s, tenemos que $s \in k^*$ y k^* es un subgrupo de Cartan no escindido.

Supongamos ahora que $\mathrm{tr}(s)^2 - 4\det(s)$ es un cuadrado en $\mathbb{F}_p$. En este caso, $f(x)$ tiene dos raíces en $\mathbb{F}_p$. Esto implica que s tiene dos autovalores distintos, ya que $f(x)$ es polinomio característico de s y $\mathrm{tr}(s)^2 - 4\det(s) \neq 0$. Esto implica que existen $v, w \in V$ dos vectores linealmente independientes tales que $s(v) = av$ y $s(w) = bw$. En particular, s pertenece al subgrupo de Cartan escindido determinado por las rectas $\langle v \rangle$ y $\langle w \rangle$.
Solo queda ahora probar que s no puede estar en dos subgrupos de Cartan distintos. Por reducción al absurdo supongamos que $s \in C_1 \cap C_2$ con $C_1, C_2 \subset \mathrm{GL}(V)$ subgrupos de Cartan distintos. Sin pérdida de generalidad, podemos restringirnos a estudiar los siguientes tres casos:

a) C_1 **es escindido y** C_2 **es no escindido.** Como $s \in C_1$, los autovalores de s están en $\mathbb{F}_p$ y, como $\mathrm{tr}(s)^2 - 4\det(s) \neq 0$, dichos autovalores son distintos. En particular, s no es una homotecia. Ahora bien, todo elemento de C_2 que no sea una homotecia genera C_2, visto como extensión de cuerpos de $\mathbb{F}_p$. Sin embargo, esto implica que s no puede cumplir ninguna ecuación de segundo grado con soluciones en $\mathbb{F}_p$, lo cual es una contradicción.
b) C_1 **y** C_2 **son escindidos.** En este caso, s tiene que dejar fijas al menos a tres rectas vectoriales distintas, lo cual implica que es una homotecia. Sin embargo, no puede ser una homotecia porque $\mathrm{tr}(s)^2 - 4\det(s) \neq 0$ implica que los autovalores de s son distintos.
c) C_1 **y** C_2 **son no escindidos.** De nuevo, todo elemento que no sea una homotecia en un subgrupo de Cartan no escindido determina el grupo entero porque genera la extensión. Por tanto, C_1 y C_2 no pueden ser distintos, lo cual es una contradicción.

Estudiemos ahora qué sucede en el caso en que $\mathrm{tr}(s)^2 - 4\det(s) = 0$. En este caso, la ecuación

$$x^2 - \mathrm{tr}(s)x + \det(s) = 0$$

tiene una raíz doble $a \in \mathbb{F}_p$. De esta manera, a es un autovalor de s. Hay dos posibilidades: o bien s es una homotecia, o bien, s tiene como matriz:

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

con $b \neq 0$, respecto a una base adecuada. En este caso, el orden de s es $p(p-1)$. Por tanto, uniendo esto al estudio anterior tenemos el siguiente resultado:

Proposición 1.10. Se dan los siguientes puntos:

a) Sea $s \in \mathrm{End}(V)$, entonces $\mathrm{tr}(s)^2 - 4\det(s) \neq 0$ si, y sólo si, $(o(s), p) = 1$.
b) La unión de todos los subgrupos de Cartan es el conjunto de elementos de $\mathrm{GL}(V)$ de orden coprimo con p y la intersección de todos los subgrupos de Cartan es el subgrupo de las homotecias.

Hacemos ahora una pausa para definir algunos conceptos más que vamos a necesitar.

Definición 1.11. *Sea C un subgrupo de Cartan escindido, determinado por las rectas D_1 y D_2. Diremos que el subgrupo de C que deja fijos los elementos de una de las dos rectas es un semi-subgrupo de Cartan escindido.*

Observación 1.8. Escogiendo una base conveniente, un semi-subgrupo de Cartan se escribe como $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$

En el estudio que haremos en capítulos posteriores tendremos que considerar el normalizador de un subgrupo de Cartan. Comenzamos dando la definición.

Definición 1.12. *Sea G un grupo y $S \subset G$ un subconjunto. Se define el normalizador de S en G como*

$$N_S := \{g \in G : gSg^{-1} = S\}$$

Observación 1.9. Siguiendo la notación de la definición anterior, si S es un subgrupo el normalizador N_S también es un subgrupo. De hecho, es el mayor subgrupo que contiene a S como subgrupo normal.

La propiedad más importante del normalizador de un subgrupo de Cartan es la siguiente:

Proposición 1.11. Sea C un subgrupo de Cartan, y sea N su normalizador en $\mathrm{GL}(V)$. Entonces, el índice $(N : C) = 2$.

Demostración. Comenzamos dando la prueba para el caso en que C sea un subgrupo de Cartan escindido. Llamemos $D_1 = \langle v_1 \rangle$ y $D_2 = \langle v_2 \rangle$ a las rectas que caracterizan a C. Sea $s \in N$, por definición existen $x, x' \in C$ tales que:

$$sx = x's.$$

Llamemos λ_i, λ_i' a los autovalores asociados a D_i de x y x' respectivamente. De esta manera, se tiene que:

$$\begin{aligned} \lambda_1 s(v_1) &= s(x(v_1)) = x'(s(v_1)), \\ \lambda_2 s(v_2) &= s(x(v_2)) = x'(s(v_2)). \end{aligned}$$

Por tanto, $s(v_1)$ y $s(v_2)$ son autovectores distintos de x'. Esto implica que, o bien $s(v_i) \in D_i$ con $i \in \{1, 2\}$, o bien $s(v_1) \in D_2$ y $s(v_2) \in D_2$. En el primer caso, $s \in C$ y en el segundo $s \in N \setminus C$. En este último caso, es fácil comprobar usando la caracterización anterior que los elementos de $N \setminus C$ están en la misma clase de N/C. Por tanto, $(N : C) = 2$.

Pasamos ahora al caso en que $C = \langle g \rangle$ es un subgrupo de Cartan no escindido. Este caso es similar al anterior desde cierto punto de vista. Para entender esto, vamos a hacer algunas observaciones. Podemos ver el grupo C como un subgrupo de $\mathrm{GL}_2(\mathbb{F}_{p^2})$. De esta manera, mediante la identificación de $\mathbb{F}_{p^2}^*$ con C y aplicando el teorema de Hamilton-Cayley el polinomio característico de g tiene dos raíces distintas sobre $\mathbb{F}_{p^2}$. Por tanto, existen L_1 y L_2 rectas vectoriales sobre $\mathbb{F}_{p^2}$ que se quedan fijas mediante g. Más aún, como los elementos de C son potencias de g, todos los elementos de C dejan fijas dichas rectas. De esta manera, podemos ver C como los elementos de $\mathrm{GL}_2(\mathbb{F}_{p^2})$ tales que dejan fijas a las rectas L_1 y L_2.

Por otro lado, dado $s \in N_C$ consideremos el automorfismo de cuerpos

$$\begin{aligned} \varphi_s : k &\longrightarrow k \\ x &\longmapsto sxs^{-1}, \end{aligned}$$

donde $k = C \cup \{0\}$. En particular, $\varphi_s \in \mathrm{Gal}(k/\mathbb{F}_p) = \{\mathrm{Id}, \phi\}$ para cada $s \in N_C$, con ϕ el automorfismo de Frobenius, i.e. para cada $x \in k$, $\phi(x) = x^p$. Estamos ahora en

condiciones de realizar un estudio similar al que hicimos en el caso en que C era no escindido.

Sea $s \in N_C$ y sean $x, x' \in C$ tales que:

$$sx = x's.$$

Como expusimos antes, podemos ver la ecuación anterior en $\mathrm{GL}_2(\mathbb{F}_{p^2})$. Si ponemos $L_1 = \langle v_1 \rangle$ y $L_2 = \langle v_2 \rangle$, llamemos $\lambda_i, \lambda_i' \in \mathbb{F}_{p^2}$ a los autovalores asociados a la recta L_i de x y x' respectivamente. Tenemos así que:

$$\begin{aligned} s(\lambda_1 x(v_1)) &= s(x(v_1)) = x'(s(v_1)) \\ s(\lambda_2 x(v_2)) &= s(x(v_2)) = x'(s(v_2)) \end{aligned}$$

Ahora dividimos en dos casos gracias al estudio de las aplicaciones φ_s. El primero de ellos en el que:

$$\begin{aligned} \lambda_1 s(x(v_1)) &= s(x(v_1)) = x'(s(v_1)), \\ \lambda_2 s(x(v_2)) &= s(x(v_2)) = x'(s(v_2)). \end{aligned}$$

y el segundo es en el que:

$$\begin{aligned} \lambda_1^p s(x(v_1)) &= s(x(v_1)) = x'(s(v_1)), \\ \lambda_2^p s(x(v_2)) &= s(x(v_2)) = x'(s(v_2)). \end{aligned}$$

De nuevo, $s(v_i)$ es un autovector de x'. Uno de los casos anteriores corresponde al caso en que s deja fijas las rectas L_1 y L_2, en cuyo caso $s \in C$, y el otro corresponde al caso en que las intercambia. De nuevo, ambos casos se dan, en el primero $s \in C$ y en el segundo caso todos los elementos de $N \setminus C$ están en la misma clase de N/C. Por tanto $(N : C) = 2$.

Observación 1.10. Habida cuenta de la prueba de la proposición anterior, si C es un subgrupo de Cartan los elementos de $N_C \setminus C$ pueden caracterizarse del modo siguiente:

a) Si C es un subgrupo de Cartan escindido determinado por las rectas D_1 y D_2, entonces los elementos de $N_C \setminus C$ son los elementos $s \in \mathrm{GL}(V)$ tales que $s(D_1) = D_2$ y $s(D_2) = D_1$. Eligiendo adecuadamente una base, estos elementos se pueden escribir como $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$.

b) Si C es un subgrupo de Cartan no escindido y $k = \mathbb{F}_p(\sqrt{a})$ el cuerpo correspondiente. Entonces, los elementos de $N_C \setminus C$ son los elementos $s \in \mathrm{GL}(V)$ tales que, para todo $x \in k$, $v \in V$ verifican:

$$s(bv) = b^p s(v).$$

Eligiendo una base conveniente se pueden expresar de la forma $\begin{pmatrix} c & d \\ -ad & -c \end{pmatrix}$.

Observación 1.11. Sea C un subgrupo de Cartan y N su normalizador. Llamamos C_1, N_1 la imagen de C y N por la proyección $\mathrm{GL}_2(\mathbb{F}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$ respectivamente. Entonces, usando las descripciones anteriores de los elementos de C y N, se comprueba que N_1 es un grupo diedral, i.e. está generado por unos elementos $x \in C_1$, $\sigma \in N_1 \setminus C_1$ tales que $\sigma x \sigma = x^{-1}$, $\sigma^2 = 1$ y x genera C_1.

Otra propiedad de los normalizadores de los subgrupos de Cartan que nos será muy útil es que esencialmente solo pueden contener un subgrupo de Cartan.

Proposición 1.12. Sea C un subgrupo de Cartan de $\mathrm{GL}(V)$ y N su normalizador.

a) Si $C' \subset N$ es un subgrupo de Cartan no escindido y $p \geq 3$, entonces $C = C'$
b) Si $C' \subset N$ es un subgrupo de Cartan escindido (resp. un semi-subgrupo de Cartan escindido) y $p \geq 5$, entonces $C = C'$ (resp. $C' \subset C$).

Demostración. Consideramos la aplicación natural

$$\mathrm{GL}(V) \longrightarrow \mathrm{PGL}(V) := \mathrm{GL}(V)/\mathbb{F}_p^*$$

Llamaremos C_1, N_1 y C_1' a las imágenes por esta aplicación de C, N y C' respectivamente. Es fácil comprobar que la imagen de un subgrupo de Cartan escindido por esta aplicación es un grupo cíclico de orden $p-1$ y la imagen de un subgrupo de Cartan no escindido es un grupo cíclico de orden $p+1$. En las hipótesis de esta proposición, C_1' es un grupo cíclico de orden mayor que 2. Sea s un generador de C_1', como los elementos de $N_1 \setminus C_1$ son de orden 2 (esto se comprueba usando las expresiones matriciales de la observación anterior), $s \in C_1$. Ahora bien, dos subgrupos de Cartan distintos tienen intersección trivial, por lo que $C_1 = C_1'$, lo cual implica que $C = C'$.

El caso de un semi-subgrupo de Cartan es análogo al caso escindido. ∎

1.3.2 Subgrupos de Borel

Junto con los subgrupos de Cartan, el siguiente tipo de subgrupos serán los que nos aparecerán en nuestro estudio posterior.

Definición 1.13. *Diremos que un subgrupo $B \subset \mathrm{GL}(V)$ es un subgrupo de Borel si existe una recta vectorial D de V tal que:*

$$B = \{s \in \mathrm{GL}(V) : sD \subset D\}.$$

Es fácil comprobar que si B es un subgrupo de Borel, se puede elegir una base de manera que las matrices de B sean las matrices de la forma:

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

En particular, el orden de un subgrupo de Borel es $p(p-1)^2$.

1.3.3 Criterios de sobreyectividad

Para terminar esta sección vamos a dar algunos resultados que nos garanticen la sobreyectividad de homomorfismos de grupos que vayan a $\mathrm{GL}(V)$.

Proposición 1.13. Sea G un subgrupo de $\mathrm{GL}(V)$ de orden divisible por p. Entonces, se da una de las siguientes posibilidades:

a) G contiene a $\mathrm{SL}(V)$.
b) G está contenido en algún subgrupo de Borel de $\mathrm{GL}(V)$.

Demostración. Sea $x \in \mathrm{GL}(V)$ de orden p. Dicho elementose puede representar eligiendo adecuadamente una base por la matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. En efecto, eligiendo el primer punto de la base adecuadamente x se puede representar por una matriz de la forma $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. Ahora bien, como x es de orden p, la matriz es necesariamente de la forma $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Eligiendo ahora adecuadamente el segundo punto de la base tenemos que x está representado por $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Gracias a esta representación tenemos que x deja fija a una única recta vectorial de V que llamaremos D_x. Dividimos la prueba en dos casos:

a) **Para cada elemento $x \in G$ de orden p, la recta D_x es la misma**. Llamaremos D a dicha recta. El orden de $\mathrm{GL}(V)$ es $p(p+1)(p-1)^2$. Por tanto, los p-grupos de Sylow de G son de orden p. Por los teoremas de Sylow, todos los elementos de orden p de G son conjugados. Esto implica que si $x \in G$ es un elemento de orden p, entonces

$$\forall \sigma \in G, (\sigma^{-1} x \sigma)(D) = D,$$

por hipótesis. Esto implica que:

$$\forall \sigma \in G, x(\sigma(D)) = \sigma(D).$$

Como la única recta que deja fija x es D, tenemos que $\sigma(D) = D$ para cada $\sigma \in G$. Luego G está contenido en el subgrupo de Borel determinado por D.

b) **Hay, al menos, dos rectas distintas**. En ese caso si tomamos a dos de los generadores de dichas rectas como base, tenemos que el grupo G contiene a los elementos del subgrupo

$$\left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \right\rangle.$$

Basta ahora comprobar que

$$\left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \right\rangle = \mathrm{SL}_2(\mathbb{F}_p).$$

Para probar el último resultado de este capítulo necesitamos los siguientes lemas que daremos sin demostración, pues su prueba, aunque no es difícil, requiere un desarrollo demasiado extenso y que no aporta a los propósitos del trabajo:

Lema 1.2. Sea k un cuerpo y sea $H \leq \mathrm{PGL}_2(k)$ un subgrupo finito de orden coprimo con $\mathrm{char}(k)$. Supongamos además que H no es cíclico ni diedral . Entonces, H es isomorfo a uno de los grupos $\mathbb{A}_4, \mathbb{S}_4$ o $\mathbb{A}_5$

Demostración. [9] Prop. 16

Lema 1.3. Sean C un subgrupo de Cartan y $X \in C$ una matriz no escalar, i.e. no es una homotecia. Si $A \in \mathrm{GL}_2(\mathbb{F}_l)$ es una matriz tal que $AXA^{-1} \in C$, entonces A pertence al normalizador de C.

Demostración. Distinguimos dos casos: Supongamos primero que C es un grupo de Cartan escindido. Eligiendo una base adecuada, podemos escribir C como el grupo:

$$C = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x \neq 0, y \neq 0 \right\}.$$

Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_l)$ y $X = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in C$ no escalar, i.e. $x \neq y$. Se tiene que:

$$AXA^{-1} = \frac{1}{ad-bc} \begin{pmatrix} adx - bcy & ab(-x+y) \\ cd(x-y) & -bcx + ady \end{pmatrix} \in C \iff ab(y-x) = cd(x-y) = 0.$$

Como $x \neq y$, se tiene que $ab = cd = 0$. Se comprueba fácilmente que estas condiciones implican que A pertenece al normalizador de C.

Supongamos ahora que C es un subgrupo de Cartan escindido. Sea ε el entero más pequeño que genera $\mathbb{F}_l$. Eligiendo una base adecuada de C, tenemos que C es de la forma:

$$C = \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} : (x, y) \neq (0, 0) \right\}.$$

Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_l)$ y $X = \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix}$ una matriz no escalar, i.e. $y \neq 0$. Se tiene que la matriz

$$AXA^{-1} = \frac{1}{ad-bc} \begin{pmatrix} -acy\varepsilon - bcx + adx + bdy & a^2y\varepsilon - b^2y \\ -c^2y\varepsilon + d^2y & acy\varepsilon - bcx + adx - bdy \end{pmatrix}$$

pertence a C si, y sólo si,

$$\begin{cases} \dfrac{-acy\varepsilon - bcx + adx + bdy}{-bc + ad} = \dfrac{acy\varepsilon - bcx + adx - bdy}{-bc + ad}, \\ \dfrac{a^2y\varepsilon - b^2y}{-bc + ad} = \dfrac{\varepsilon(-c2y\varepsilon + d2y)}{-bc + ad} \end{cases}$$

y ambas cantidades son no nulas. Teniendo en cuenta que $ad - bc \neq 0 \neq y$, podemos simplificar el sistema anterior, de manera que $AXA^{-1} \in C$ si, y sólo si,

$$\begin{cases} ac\varepsilon = bd, \\ c^2\varepsilon^2 + (a^2 - d^2)\varepsilon - b^2 = 0 \end{cases}$$

e $y(-ac+bd)\varepsilon - x(bc-ad) \neq 0$ o $d^2 \neq -c^2\varepsilon$. En primer lugar, notemos que la segunda ecuación siempre se da porque ε no es un cuadrado. Distinguimos ahora dos casos:

a) **Caso en que** $b = 0$. En este caso, $ac\varepsilon = 0$, $\varepsilon \neq 0$ y como A es invertible $a \neq 0$. Por tanto, $c = 0$. De la segunda ecuación se deduce que $a^2 - b^2 =$, con lo cual $a = \pm b$. De esta manera, la matriz A es de la forma:

$$\begin{pmatrix} a & 0 \\ 0 & \pm a \end{pmatrix}$$

y se comprueba fácilmente que A está en el normalizador del subgrupo de Cartan.

b) **Caso en que** $b \neq 0$. En este caso, podemos despejar $d = ac\varepsilon/b$ y sustituyendo se obtiene:

$$c^2\varepsilon^2 + (a^2 - (ac\varepsilon/d)^2)\varepsilon - b^2 = 0.$$

Esta ecuación se puede factorizar como:

$$(a^2\varepsilon - b^2)(b^2 - c^2\varepsilon^2) = 0.$$

El primer término no puede ser 0 porque ε no es un cuadrado. Por tanto, $b = \pm c\varepsilon$ y $d = \pm e$. En este caso, un simple cálculo permite probar que $AXA^{-1} \in C$.

Proposición 1.14. Sea G un subgrupo de $\mathrm{GL}(V)$ distinto del total. Entonces,

a) Si G contiene a un subgrupo de Cartan no escindido, entonces o bien G está contenido en un subgrupo de Borel, o bien G está contenido en el normalizador de un subgrupo de Cartan.
b) Si G contiene a un semi-subgrupo de Cartan escindido y $p \neq 5$, entonces o bien G está contenido en un subgrupo de Borel, o bien G está contenido en el normalizador de un subgrupo de Cartan.

Demostración. Dividimos la prueba en dos casos:

1. p **divide a** $|G|$. En este caso, la proposición anterior nos dice que G está contenido en un subgrupo de Borel o G contiene a $\mathrm{SL}_2(V)$. En este segundo caso, tanto si G contiene a un subgrupo de Cartan no escindido como si contiene a un semi-subgrupo de Cartan escindido, se comprueba fácilmente que la aplicación $\det : G \longrightarrow \mathbb{F}_p^*$ es sobreyectiva. Ahora bien, como $\mathrm{SL}(V) \subset G$, esto implica que $G = \mathrm{GL}(V)$, lo cual es una contradicción.

2. **El orden de G es coprimo con p.** Aplicando ahora el lema anterior para el cuerpo $\mathbb{F}_p$ y llamando H a la imagen de G en $\mathrm{PGL}(V)$, obtenemos la posibilidades siguientes:

   i) H es cíclico y está contenido en la imagen de algún subgrupo de Cartan, por la proposición 2. Por tanto, G está contenido en algún subgrupo de Cartan.

   ii) H es diedral, i.e. contiene un subgrupo normal cíclico C' no trivial de índice 2. En este caso, G está contenido en el normalizador de un subgrupo de Cartan. Para probar esto, nos basta probarlo para $\pi^{-1}(H)$, con $\pi : \mathrm{GL}(V) \longrightarrow \mathrm{PGL}(V)$ la proyección natural. Como π es homomorfismo de grupos, $\pi^{-1}(C') \lhd \pi^{-1}(H)$. Es fácil comprobar que como $(p, |G|) = 1$, el grupo $\pi^{-1}(C')$ es cíclico de orden coprimo con p y, por la proposición 2, está contenido en algún subgrupo de Cartan C. Por tanto, como $\pi^{-1}(C')$ es un subgrupo normal de $\pi^{-1}(H)$, entonces $\pi^{-1}(H)$ está contenido en el normalizador N de C. En efecto, consideremos $A \in G$ y $\pi(A) \in \pi(G) = H$. Por tanto, para toda matriz $X \in \mathrm{GL}_2(\mathbb{F}_l)$ tal que $\pi(X) \in C'$,

   $$\pi(AXA^{-1}) = \pi(A)\pi(X)\pi(A^{-1}) \in C',$$

   ya que $C' \lhd H$. Luego $AXA^{-1} \in \pi(C') \subset C$. En particular, podemos escoger un elemento $X_1 \in C'$, distinto de la identidad, y un elemento $X \in \pi^{-1}(C')$ tal que $\pi(X) = X_1$. Además, X no es una matriz escalar porque su imagen no es la identidad. Basta ahora aplicar el lema 1.3.

   iii) H es isomorfo a $\mathbb{A}_4, \mathbb{S}_4$ o $\mathbb{A}_5$. Esto no puede darse si $p = 2, 3$. Estamos suponiendo que $p \neq 5$ y la imagen de C es un grupo cíclico de orden $p \pm 1 \geq 6$ y los grupos $\mathbb{A}_4, \mathbb{S}_4, \mathbb{A}_5$ no contienen elementos de orden superior a 5. Por tanto, este caso no puede darse.

2 | Curvas elípticas

Durante todo este capítulo K será un cuerpo perfecto, i.e. toda extensión algebraica de K es separable, y $\overline{K}$ denotará su clausura algebraica. Trabajaremos siempre sobre el plano proyectivo $\mathbb{P}^2(K)$ sobre el cuerpo K. Por simplicidad en la notación escribiremos $\mathbb{P}^2$ cuando estemos trabajando sobre $\overline{K}$. Daremos por conocidas las nociones de variedad algebraica (proyectiva e irreducible), curva, morfismo entre variedades algebraicas, aplicaciones racionales y cuerpo de funciones racionales asociadas a una variedad (todo esto se puede encontrar en los capítulos I y II de [10]). Ocasionalmente necesitaremos usar algunos resultados de geometría algebraica, cuando esto suceda los enunciaremos brevemente, junto con una referencia de su prueba.

2.1 Teoría General

El objeto sobre el que basaremos nuestro estudio serán las curvas elípticas.

Definición 2.1. *Una curva elíptica es un par $(E, \mathcal{O})$, donde E es una curva algebraica no singular de género 1 sobre $\overline{K}$ y $\mathcal{O}$ es un punto de dicha curva. Generalmente, denotaremos por E a la curva elíptica omitiendo $\mathcal{O}$. Diremos que la curva elíptica E está definida sobre K, lo cual será denotado por E/K, si lo está como curva algebraica y el punto $\mathcal{O}$ tiene coordenadas en K.*

Sea una curva elíptica E/K. Haciendo uso del teorema de Riemann-Roch se puede probar que E es isomorfa (sobre K) a una curva de $\mathbb{P}^2$ dada por una ecuación de la forma:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

con $a_1, \ldots, a_6 \in K$ y siendo $\mathcal{O}$ el punto del infinito de la curva $[0 : 1 : 0]$. A las curvas de este tipo se les dice que están en forma de Weierstrass. Gracias a esto, para

estudiar las curvas elípticas nos basta estudiar las curvas no singulares de este tipo, a pesar de que una misma curva puede tener varios modelos de este tipo.

Si la característica del cuerpo es distinta de 2, se puede simplificar la ecuación, mediante el cambio de variables

$$y \mapsto \frac{1}{2}(y - a_1x - a_3),$$

obteniendo así una curva en forma:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

donde

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Los nombres asignados a estas cantidades no son arbitrarios y los reservaremos durante todo el trabajo para dichas cantidades. Además, definimos también las siguientes cantidades

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3, \\ j &= c_4^3/\Delta. \end{aligned}$$

Estas cantidades tienen cada una un significado en términos de propiedades de la curva. Más adelante, vamos a mostrar algunos de ellos, para un estudio más detallado ver ([10] III.1).

Por último, la curva se puede reducir aún más cuando la característica del cuerpo es distinta de 2 y 3. En dicho caso, el cambio de variables

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

nos da una curva de la forma

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

La cantidad Δ se llama discriminante y nos ayuda a saber si una curva dada en forma de Weierstrass tiene o no puntos singulares.

Definición 2.2. *Sea C una curva en $\mathbb{P}^2$ dada por un polinomio homogéneo $F(X, Y, Z)$. Sea $P \in C$, se dice que el punto P es singular si*

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Se dice que la curva es no singular si todos sus puntos son no singulares.

Proposición 2.1. Una curva dada por una ecuación de Weierstrass es no singular si, y sólo si, $\Delta \neq 0$. En caso de que la curva sea singular, esta sólo tiene un punto singular. La singularidad en ese punto tiene dos tipos posibles:

a) El punto singular es un nodo (las tangentes en el punto son distintas) si, y sólo si, $\Delta = 0$ y $c_4 \neq 0$.
b) El punto singular es una cúspide (las tangentes en el punto son iguales) si, y sólo si, $\Delta = c_4 = 0$.

Demostración. ([10] III.1.4)

2.1.1 Operación de grupo

Sea E/K una curva no singular en forma de Weierstrass,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Denotaremos por $E = E(\overline{K})$ al conjunto de puntos $[x : y : 1] \in \mathbb{P}^2$ que cumple la ecuación, junto con el punto del infinito $\mathcal{O} = [0 : 1 : 0]$. Dados dos puntos de $P, Q \in E(K) := \mathbb{P}^2(K) \cap E$ y una recta L que pase por ellos, se comprueba, usando las fórmulas de Cardano-Vieta, que L corta en un tercer punto a $E(K)$ y en ningún otro, contados con multiplicidad. A este tercer punto lo denotamos $P * Q$.

De esta manera, hemos definido una operación dentro de la curva, pero esta no da estructura de grupo a los puntos de $E(K)$, principalmente por la falta de un elemento neutro. Sin embargo, podemos usar esta operación y el punto $\mathcal{O}$ para dar a $E(K)$ estructura de grupo.

Definición 2.3. *Definimos la "ley de grupo" de una curva elíptica E/K como :*

$$\begin{aligned} \oplus : E(K) \times E(K) &\longrightarrow E(K) \\ (P, Q) &\longmapsto \mathcal{O} * (P * Q). \end{aligned}$$

Proposición 2.2. Sea E/K una curva elíptica, se tienen:

a) $(E(K), \oplus)$ es un grupo abeliano y $\mathcal{O}$ es el elemento neutro de la operación.
b) $(P \oplus Q) \oplus (P * Q) = \mathcal{O}$.
c) La operación

$$\begin{aligned} \oplus : E(K) \times E(K) &\longrightarrow E(K) \\ (P, Q) &\mapsto \mathcal{O} * (P * Q) \end{aligned}$$

es un morfismo entre variedades algebraicas.

Demostración. Las pruebas de a) y b) se pueden encontrar en ([10] III.2.2) y la de c) en ([10] III.3.6)

De esta manera, ya podemos decir que la "ley de grupo de una curva elíptica" es una verdadera ley de grupo. En lo que sigue a la operación de la curva la denotaremos por $+$ en lugar de $\oplus$. De esta manera, denotaremos por $-P$ al opuesto de P por la operación de grupo.

Definición 2.4. *Sean E_1/K y E_2/K dos curvas elípticas y $\phi : E_1(K) \longrightarrow E_2(K)$ un morfismo entre curvas. Diremos que ϕ es una isogenia si $\phi(\mathcal{O}) = \mathcal{O}$.*

Como la ley de grupo de la curva es un morfismo podemos definir la isogenia:

$$\begin{aligned} [n] : E(K) &\longrightarrow E(K) \\ P &\mapsto \underbrace{P + \cdots + P}_{n \text{ veces}} \end{aligned}$$

Observación 2.1. Las operaciones anteriores las hemos definido sobre $E(K)$, en caso de que no especifiquemos el cuerpo y solo escribamos E, nos estaremos refiriendo a $E(\overline{K})$.

Buena parte de este trabajo va a consistir en estudiar la relación que hay entre una curva elíptica definida sobre un cuerpo K junto con su estructura de grupo y el grupo de Galois $\mathrm{Gal}(\overline{K}/K)$. Comenzamos haciendo un primer análisis.

Sea E/K una curva elíptica, dada por una ecuación de Weierstrass:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Para un punto $P = (x_0 : y_0 : 1) \in E$, tenemos la relación

$$y_0^2 + a_1 x_0 y_0 + a_3 y_0 = x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6.$$

Consideramos ahora $\sigma \in \mathrm{Gal}(\overline{K}/K)$ y lo aplicamos a ambos lados de la ecuación. Obtenemos

$$\sigma(y_0)^2 + a_1\sigma(x_0)\sigma(y_0) + a_3\sigma(y_0) = \sigma(x_0)^3 + a_2\sigma(x_0)^2 + a_4\sigma(x_0) + a_6.$$

Por tanto, $P^\sigma := (\sigma(x_0) : \sigma(y_0) : 1) \in E$. Además, $\mathcal{O}^\sigma = \mathcal{O}$. Por tanto, el grupo $\mathrm{Gal}(\overline{K}/K)$ actúa sobre E. Más aún, se tiene el siguiente resultado.

Proposición 2.3. Sea E/K una curva elíptica, se tiene que:

$$\forall \sigma \in \mathrm{Gal}(\overline{K}/K) \quad \forall P, Q \in E \quad (P+Q)^\sigma = P^\sigma + Q^\sigma.$$

Demostración. Si fijamos una ecuación en forma de Weierstass para la curva, la expresión de las coordenadas del punto suma se pueden escribir como funciones racionales en las coordenadas de los sumandos. Esto se debe a que calcular la suma en una curva elíptica consiste en cortar ciertas rectas con una cúbica en $\mathbb{P}^2$. Por tanto, la acción de $\mathrm{Gal}(\overline{K}/K)$ conmuta con la suma. ∎

Estudiar como actúa $\mathrm{Gal}(\overline{K}/K)$ sobre una curva elíptica es un problema demasiado complicado. Para relajar el problema se puede estudiar como actúa $\mathrm{Gal}(\overline{K}/K)$ sobre algún subgrupo. En nuestro caso, vamos a estudiar como actúa el grupo de Galois sobre la torsión de E.

2.2 Torsión y representaciones

En lo que sigue del trabajo haremos la siguiente simplificación en la notación,

$$G_K := \mathrm{Gal}(\overline{K}/K).$$

Además, en caso de que no haya dudas con respecto a qué cuerpo nos estamos refiriendo, el grupo de Galois será denotado simplemente por G. Comenzamos definiendo los distintos grupos de torsión.

Definición 2.5. *Sea E una curva elíptica y $m \in \mathbb{Z}$. Denotamos su grupo de m-torsión por:*

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}.$$

De esta manera, denotamos por

$$E_\infty = \bigcup_{m\in\mathbb{N}} E[m]$$

al grupo de torsión de la curva.

Sea E/K una curva elíptica y sea $P \in E[m]$. Gracias a la proposición 2.3, se tiene lo siguiente

$$[m](P^\sigma) = ([m](P))^\sigma = \mathcal{O}^\sigma = \mathcal{O}.$$

Por tanto, el grupo de Galois actúa sobre cada $E[m]$ y, por tanto, sobre E_∞. Cabe ahora preguntarse qué estructura tiene $E[m]$. La respuesta a esta pregunta es el siguiente teorema que será nuestro punto de partida es el siguiente teorema.

Teorema 2.1. *Sea E una curva elíptica y $m \in \mathbb{Z}$, se tienen:*

a) Si $m \neq 0$ y $\mathrm{char}(\overline{K}) = 0$ o $\mathrm{char}(\overline{K}) = p > 0$ y $p \nmid m$, entonces

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

b) Si $\mathrm{char}(\overline{K}) = p > 0$, entonces se da uno de los siguientes casos:

a) *$E[p^e] = \{\mathcal{O}\}$, para todo $e = 1, 2, 3, \ldots$*
b) *$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$, para todo $e = 1, 2, 3, \ldots$*

Demostración. (Corollary 6.4 [10])

2.2.1 El módulo de Tate

Sea K un cuerpo de característica 0, E/K una curva elíptica y $m \geq 2$. Entonces, por el teorema 2.1 el grupo de puntos de m-torsión es de la forma

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Además, como ya hemos visto, G actúa sobre $E[m]$. De esta manera, para cada m en las condiciones anteriores, obtenemos una representación:

$$\rho_m : G \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Además los grupos $E[m]$ están relacionados mediante el orden que da la divisibilidad, i.e. si $m_1|m_2$ tenemos el morfismo natural

$$E[m_2] \xrightarrow{\left[\frac{m_2}{m_1}\right]} E[m_1].$$

De esta manera, podemos reunir todas las representaciones mediante el límite inverso. Así obtenemos una representación

$$\rho : G \longrightarrow \mathrm{Aut}\left(\varprojlim_m E[m]\right).$$

Además, $\varprojlim E[m] \cong \varprojlim \mathbb{Z}/m\mathbb{Z} \times \varprojlim \mathbb{Z}/m\mathbb{Z} \cong \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$, donde $\widehat{\mathbb{Z}}$ es el anillo de Prüfer, del que es conocido que:

$$\widehat{\mathbb{Z}} \cong \prod_{l \text{ primo}} \mathbb{Z}_l.$$

Por tanto, la representación ρ la podemos ver como

$$\rho : G \longrightarrow \mathrm{Aut}\left(\varprojlim_m E[m]\right) \cong \prod_{l \text{ primo}} \mathrm{GL}_2(\mathbb{Z}_l).$$

Por otro lado, denotamos por E_∞ a la torsión de $E(\overline{K})$, i.e. la unión de todos los E_n. Al igual que antes, el grupo de Galois atúa de manera natural sobre E_∞ y esto nos da una representación

$$\varphi_\infty : G \longrightarrow \mathrm{Aut}(E_\infty)$$

Vamos a ver que estos los morfismos ρ y φ_∞ son esencialmente el mismo. Sea l un primo, denotamos por E_{l^∞} al subgrupo formado por la unión de los puntos de la curva sobre $\overline{K}$ tales que son puntos de l^r-torsión para algún $r \geq 0$. Por definición, tenemos

$$E_\infty = \bigoplus_{l \text{ primo}} E_{l^\infty}, \quad \mathrm{Aut}(E_\infty) = \prod_{l \text{ primo}} \mathrm{Aut}(E_{l^\infty}).$$

Así, podemos componer φ_∞ con las proyecciones correspondientes a cada primo. Por tanto, tenemos representaciones

$$\varphi_{l^\infty} : G \longrightarrow \mathrm{Aut}(E_{l^\infty})$$

Para cada primo l y $r \geq 0$, tenemos la representación

$$\rho_{l^r} : G \longrightarrow \mathrm{Aut}(E[l^r]).$$

Fijado l primo, los grupos $E[l^r]$ y los morfismos

$$E[l^{r+1}] \xrightarrow{[l]} E[l^r]$$

forman un sistema proyectivo.

Definición 2.6. *En las condiciones anteriores, llamamos módulo de Tate al límite inverso*

$$T_l(E) = \varprojlim_n E[l^n].$$

También denotamos por

$$V_l(E) := T_l(E)\left[\frac{1}{l}\right] = T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

En caso de que no haya ambigüedad de a qué curva nos referimos, usaremos la notación V_l y T_l.

Por la propiedad universal del límite inverso para cada primo tenemos una representación

$$\varphi_l : G \longrightarrow \mathrm{Aut}(T_l(E)).$$

Proposición 2.4. Hay un isomorfismo $\mathrm{Aut}(T_l) \longrightarrow \mathrm{Aut}(E_{l^\infty})$.

Demostración. Se tiene que

$$V_l/T_l = T_l[l^{-1}]/T_l = \bigcup_n (l^{-n}T_l)/T_l = \bigcup_n E[l^n] = E_{l^\infty}.$$

Esta observación induce un morfismo

$$\begin{array}{ccc} \mathrm{Aut}(T_l) & \longrightarrow & \mathrm{Aut}(E_{l^\infty}), \\ \phi & \mapsto & \tilde{\phi} \end{array}$$

que viene definido como sigue. Sea $\phi : T_l \longrightarrow T_l$ un automorfismo. Por la descripción anterior de E_{l^∞}, ϕ induce un automorfismo $\tilde{\phi}_n$ de cada $E[l^n] = (l^{-n}T_l)/T_l$ que hace conmutativa el siguiente diagrama,

$$\begin{array}{ccc} E[l^n] & \xrightarrow{\tilde{\phi}_n} & E[l^n] \\ \uparrow & & \uparrow \\ E[l^k] & \xrightarrow{\tilde{\phi}_k} & E[l^k] \end{array}$$

para cualesquiera enteros $n \geq k \geq 0$, donde las flechas verticales son las inclusiones canónicas. De esta manera, si $x \in E_{l^\infty}$ existe $n \geq 0$ tal que $x \in E_{l^n}$.

Definimos $\tilde{\phi}(x) := \tilde{\phi}_n(x)$. Gracias al diagrama anterior esta definición no depende del

n elegido. Veamos que el morfismo así definido es sobreyectivo. Sean $\psi \in \mathrm{Aut}(E_{l^\infty})$ y $k \geq 0$ un entero. Mediante la restricción podemos obtener unos morfismos:

$$\psi_k : E[l^k] \longrightarrow E[l^k].$$

Estos morfismos cumplen el siguiente diagrama conmutativo:

$$\begin{array}{ccc} E[l^n] & \xrightarrow{\psi_n} & E[l^n] \\ {\scriptstyle [l^{n-k}]}\downarrow & & \downarrow{\scriptstyle [l^{n-k}]} \\ E[l^k] & \xrightarrow{\psi_k} & E[l^k] \end{array}$$

para $n \geq k$, ya que los morfismos $[r]$ vienen definidos por aplicar la suma de manera iterada y ψ es morfismo de grupos. De hecho, como ψ es automorfismo, cada ψ_k también lo es. Usando ahora la propiedad universal del límite inverso obtenemos un automorfismo $\phi : T_l \longrightarrow T_l$ tal que $\tilde{\phi} = \psi$. Además, por la unicidad del limite inverso también se tiene la inyectividad.

Habida cuenta de la proposición anterior podemos identificar φ_l con φ_{l^∞} y podemos reducir el estudio de cómo actúa el grupo de Galois sobre cada subgrupo de torsión de la curva a estudiar cómo es dicha acción sobre cada $E[l^k]$, para cada $k \in \mathbb{N}$, y sobre el módulo de Tate T_l, para cada primo l.

2.2.2 El pairing de Weil

Terminamos esta sección presentando una herramienta que necesitaremos más adelante. Sea $m \geq 2$ un entero, que supondremos coprimo con p en el caso en que $\mathrm{char}(K) = p > 0$. Sabemos que

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Así, $E[m]$ es un $\mathbb{Z}/m\mathbb{Z}$-módulo libre de rango 2. De esta manera, podemos definir una aplicación multilineal alternada no degenerada sobre $E[m]$ fijando una base $\{T_1, T_2\}$ y poniendo,

$$\det : E[m] \times E[m] \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad \det(aT_1 + bT_2, cT_1 + dT_1) = ad - bc.$$

Sin embargo, definir esta aplicación de esta manera tiene dos problemas. En primer lugar el valor del determinante depende de la base elegida. Esto no es demasiado grave

ya que cambiar de base es simplemente multiplicar por un elemento de $(\mathbb{Z}/m\mathbb{Z})^*$. Sin embargo el otro problema es más serio, el determinante no es Galois invariante, i.e. si $P, Q \in E[m]$ y $\sigma \in G$ entonces $\det(P^\sigma, Q^\sigma)$ y $\det(P, Q)^\sigma$ no son iguales en general.

Ambos problemas se pueden solventar simultáneamente, modificando la aplicación para que tome valores en las raíces m-ésimas de la unidad. Para ello, haremos uso del siguiente lema.

Lema 2.1. Un divisor $\sum n_i(P_i)$ es el divisor asociado a alguna función si, y solo si, se cumplen las siguientes condiciones:

a) $\sum_i n_i = 0$.
b) $\sum_i [n_i]P_i = \mathcal{O}$.

Demostración. ([10] III.3.5). ∎

Sea $T \in E[m]$, sabemos que existe $f \in \overline{K}(E)$ tal que

$$\operatorname{div}(f) = m(T) - m(\mathcal{O})$$

Elegimos ahora $T' \in E$ tal que $[m]T' = T$. De la misma manera, usando el lema, existe $g \in \overline{K}(E)$ tal que

$$[m]^*(P) - [m]^*(Q) = \sum_{R \in E[m]} ((T' + R) - (R)),$$

donde $[m]^*$ denota el morfismo inducido por $[m]$ en los divisores. Es fácil comprobar ahora que las funciones $f \circ [m]$ y g^m tienen los mismos divisores. Por tanto, multiplicando por una constante apropiada en $\overline{K}^*$, podemos suponer que

$$f \circ [m] = g^m.$$

Si ahora elegimos otro punto de m-torsión $S \in E[m]$, que puede ser igual a T, tenemos que

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Por tanto, como función de X $g(X + S)/g(X)$ solo puede tomar una cantidad finita de valores, las raíces m-ésimas de la unidad. En particular, el morfismo

$$E \longrightarrow \mathbb{P}^1, \quad X \mapsto g(X + S)/g(X)$$

no es sobreyectivo, por lo que es constante. Esto nos permite definir un pairing

$$e_m : E[m] \times E[m] \longrightarrow \mu_m,$$

poniendo

$$e_m(S,T) = \frac{g(X+S)}{g(X)},$$

con $X \in E$ cualquier punto tal que $g(X+S)$ y $g(X)$ estén bien definidos (no sean cero). Notemos que la función g depende del punto T. Se comprueba que aunque g está definida salvo multiplicación por una constante de $\overline{K}^*$, el cociente $g(X+S)/g(X)$ no depende de la constante elegida ni del punto X. De aquí en adelante, llamaremos a esta aplicación el e_m-pairing de Weil

Proposición 2.5. En las condiciones del inicio de la sección el e_m-pairing de Weil tiene las siguientes propiedades:

a) Es bilineal:

$$\begin{aligned} e_m(S_1+S_2,T) &= e_m(S_1,T)e_m(S_2,T), \\ e_m(S,T_1+T_2) &= e_m(S,T_1)e_m(S,T_2). \end{aligned}$$

b) Es alternada:

$$e_m(T,T) = 1.$$

En particular, $e_m(S,T) = e_m(T,S)^{-1}$.

c) Es no degenerada, i.e. si $e_m(S,T) = 1$ para todo $S \in E[m]$, entonces $T = \mathcal{O}$.

d) Es compatible con la acción de Galois:

$$\forall \sigma \in G, \quad e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma).$$

e) Se da la siguiente relación de compatibilidad con la operación de la curva:

$$\forall S \in E[mm'], \forall T \in E[m], \quad e_{mm'}(S,T) = e_m([m']S,T).$$

Demostración. ([10] II.8.1)

2.3 El grupo formal de una curva elíptica

En esta sección vamos a ver como se puede asociar a cada curva elíptica una ley de grupo formal y qué relación guarda dicha ley con la estructura de grupo de la curva. Para ello usaremos los resultados sobre grupos formales que ya vimos en el capítulo anterior.

2.3.1 Desarrollo alrededor de $\mathcal{O}$

Sea E/K una curva elíptica. En este apartado vamos a estudiar cómo se comporta nuestra curva y la operación en un entorno de $\mathcal{O}$. Para ello, hacemos el siguiente cambio de variables (transformación birracional afín):

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}.$$

Con estas coordenadas el punto $\mathcal{O}$ es ahora el $(0,0)$. Además la función $z(x,y) - x/y$ tiene un cero de orden 1 en $\mathcal{O}$, esto es, en el anillo local $K[E]_{\mathcal{O}}$ la función z es un parámetro de uniformización. De esta manera, la ecuación de Weierstrass ahora se convierte en

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3 =: f(z,w).$$

Gracias a esta ecuación podemos sustituir la expresión de w en ella misma de manera iterada. Una primera iteración nos lleva a:

$$\begin{aligned} w = z^3 &+ a_1 z^4 + (a_1^2 + a_2) z^5 + (a_1^3 + 2a_1 a_2 + a_3) z^6 \\ &+ (a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4) z^7 + \cdots \end{aligned}$$

Si seguimos iterando vamos obteniendo una expresión de la forma $w = z^3(1 + A_1 z + A_2 z^2 + \cdots)$, donde los $A_n \in \mathbb{Z}[a_1, \ldots, a_6]$. Por supuesto, hay que comprobar que $w(z)$ tiene sentido en $\mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$ y que se tiene la igualdad

$$w(z) = f(z, w(z))$$

en el mismo anillo de series formales. Una descripción más precisa del procedimiento anterior sería la siguiente. Consideramos la sucesión de polinomios definida por inducción como sigue:

$$\begin{cases} f_1(z,w) &= f(z,w) \\ f_n(z,w) &= f_{n-1}(z, f(z,w)). \end{cases}$$

Queremos definir

$$w(z) := \lim_n f_n(z,0).$$

Vamos a ver que este límite tiene sentido en $\mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$.

Proposición 2.6. Se tienen:

a) El límite $\lim_n f_n(z,0)$ existe, i.e. es un elemento de $\mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$.

b) La serie formal $w(z)$ es la única serie de potencias de $\mathbb{Z}[a_1, \dots, a_6][\![z]\!]$ que cumple que:
$$w(z) = 0 \quad \text{y} \quad w(z) = f(z, w(z)).$$

c) Si el anillo de polinomios $\mathbb{Z}[a_1, \dots, a_6]$ lo convertimos en un anillo graduado poniendo los pesos $\text{wt}(a_i) = i$, cada coeficiente de A_n de la serie de potencias $w(z)$ es un polinomio homogéneo de peso n.

Para probar esto necesitamos una versión del lema de Hensel (en el apéndice hemos dado una versión más general, ver A.2), que enunciamos a continuación.

Teorema 2.2 (Lema de Hensel). *Sea R un anillo de valoración discreta completo e $I = (\pi)$ su ideal primo. Sea $F(w) \in R[w]$ un polinomio. Supongamos que existen $n \in \mathbb{N}$ y $a \in R$ tales que*
$$F(a) \in I^n \quad y \quad F'(a) \in R^*.$$
Entonces, para cada $\alpha \in R^*$ tal que $F'(a) \equiv \alpha \mod I$, la sucesión
$$w_0 = a, \quad w_{m+1} = w_m - \frac{F(w_m)}{\alpha}$$
converge a un $b \in R$ tal que $F(b) = 0$ y
$$b \equiv a \mod I^n.$$
Si además R es un dominio de integridad, dicho b está determinado de manera única.

Demostración (del Lema de Hensel). Sea α tal que $F'(a) \equiv \alpha \mod I$. En particular,
$$\alpha \in F'(\alpha) + I \subset R^* + I = R^*(1 + I) = R^*,$$
donde la última igualdad se da porque $1 + I = R^*$ (si $1 + u\pi = u'\pi^n$, entonces $1 \in I$ y esto es una contradicción). Por tanto, α es una unidad. Por simplicidad con la notación, vamos a hacer la prueba con
$$w_0 = 0, \quad F(0) \in I^n, \quad F'(0) \equiv 1 \mod I, \quad w_{m+1} = w_m - F(w_m).$$
En caso de que esto no sea así basta hacer el cambio $F(w) \mapsto F(w + a)/\alpha$. Como $w_0 = 0$ y $F(0) \in I^n$,
$$\forall m \geq 0, \quad w_m \in I^n \Rightarrow w_m - F(w_m) \in I^n.$$
Por tanto,
$$\forall m \geq 0, \quad w_m \in I^n.$$

Probamos ahora por inducción que

$$\forall m \geq 0, \quad w_m \equiv w_{m+1} \mod I^{m+n}.$$

Para $m = 0$, ya lo hemos visto. Supongamos ahora que el resultado es cierto para todos los enteros estrictamente menores que m. Es fácil comprobar la factorización siguiente:

$$F(X) - F(Y) = (X - Y)\left(F'(0) + XG(X,Y) + YH(X,Y)\right),$$

donde $H, G \in R[X,Y]$. Entonces,

$$\begin{aligned} w_{m+1} - w_m &= w_m - F(w_m) - w_{m-1} + F(w_{m-1}) \\ &= w_m - w_{m-1} + F(w_{m-1}) - F(w_m) \\ &= (w_m - w_{m-1})(1 - F'(0) - w_m G(w_m, w_{m-1}) \\ &\quad -w_{m-1}H(w_m, w_{m-1})) \in I^{n+m}. \end{aligned}$$

La última línea se tiene porque por hipótesis de inducción $w_m - w_{m-1} \in I^{n+m-1}$, por la hipótesis de que $F'(0) \equiv 1 \mod I$ y por la hipótesis de que $w_m, w_{m-1} \in I^n$. Con esto hemos probado que la sucesión $\{w_m\}$ es de Cauchy, pues hemos visto que:

$$w_{m+1} - w_m \in I^{n+m}.$$

Por la completitud de R, existe $b \in R$ tal que $b = \lim w_m$. Además, como todos los $w_m \in I^n$, $b \in I^n$. Si tomamos límite ahora en la definición por recurrencia de los w_m, obtenemos

$$b = b - F(b).$$

Por tanto, $F(b) = 0$.

Por último, vamos a probar la unicidad. Supongamos que existe $c \in I^n$ tal que $F(c) = 0$. Entonces,

$$0 = F(b) - F(c) = (b - c)(F'(0) + bG(b,c) + cH(b,c)).$$

Si $b \neq c$, entonces

$$F'(0) + bG(b,c) + cH(b,c) = 0.$$

Ahora bien, esto implica que $F'(0) \in I$, lo que contradice que $F'(0) \equiv 1 \mod I$. ∎

Demostración (de la proposición 2.6). Los apartados 1. y 2. se deducen directamente del lema de Hensel poniendo $R = \mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$, $I = (z)$, $F(w) = f(z,w) - w$,

$a = 0$ y $\alpha = -1$.

Veamos el tercer apartado, asignando los pesos $\mathrm{wt}(z) = -1$ y $\mathrm{wt}(w) = -3$, $f(z, w)$ es un polinomio homogéneo de peso -3 del anillo graduado $\mathbb{Z}[a_1, \dots, a_6, z, w]$ y es fácil ver que los f_m cumplen la misma propiedad. En particular,

$$f_m(z, 0) = z^3(1 + B_1 z + B_2 z^2 + \cdots + B_N z^N)$$

es homogéneo de peso -3. Por tanto, $\mathrm{wt}(B_n) = n$ y, tomando límite los A_n tienen la misma propiedad.

De esta manera, hemos desarrollado en serie de potencias las funciones coordenadas. Recuperando las coordenadas x, y obtenemos el siguiente desarrollo en serie de Laurent,

$$\begin{aligned} x(z) &= \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \cdots \\ y(z) &= -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z + \cdots \end{aligned}$$

Notemos que los coeficientes de la inversa de una serie formal se pueden calcular. De la misma manera, podemos invertir $2y(z) + a_1 x(z) + a_3$ admitiendo una cantidad finita de términos $1/z^n$. Por tanto, podemos desarrollar el diferencial invariante como

$$\begin{aligned} \omega(z) &= \frac{dx(z)}{2y(z) + a_1 x(z) + a_3} \\ &= (1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + 2a_3) z^3 \\ &\quad + (a_1^4 + 3a_1^2 a_2 + 6a_1 a_3 + a_2^2 + 2a_4) z^4 + \cdots) dz \end{aligned}$$

Con todo esto, las series $(x(z), y(z))$ son una solución formal a la ecuación de Weiestrass:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Sería interesante poder generar puntos de E evaluando en z. Sin embargo, no hay una manera natural de asociar elementos de K a cada z. Sin embargo, si suponemos que K es un cuerpo local completo, con R su anillo de valoración, $\mathcal{M}$ su ideal maximal y suponemos además que $a_1, \dots, a_6 \in R$, las series $x(z)$ e $y(z)$ convergen para todo $z \in \mathcal{M}$ y, por tanto, $(x(z), y(z)) \in E(K)$. Esto nos da una aplicación

$$\begin{aligned} \mathcal{M} &\to E(K), \\ z &\mapsto (x(z), y(z)). \end{aligned}$$

Dicha aplicación es inyectiva porque $-x(z)/y(z) = z$ nos da la inversa. Esta aplicación será clave cuando estudiemos las curvas elípticas sobre cuerpos locales.

Volvamos por ahora a seguir trabajando de manera formal, vamos a ver como se comporta la suma de las curvas elípticas en términos de las series formales. Sean z_1 y z_2 variables independientes para las series formales, llamemos $w_1 = w(z_1)$ y $w_2 = w(z_2)$. Si llamamos

$$(z_3, w_3) = (z_1, w_1) + (z_2, w_2),$$

donde la suma es la suma de las curvas elípticas en el plano (z, w), vamos a escribir z_3 como una serie formal en z_1y z_2. Es un ejercicio de cómputo comprobar que $z_3(z_1, z_2) =: F(z_1, z_2)$ es un grupo formal (ver 1.2), los detalles acerca de esto se pueden encontrar en ([10] IV.1).

Terminamos la sección con un resultado que nos relaciona la altura de los morfismos entre los grupos formales de curvas elípticas con los morfismos entre dichas curvas. Para dar dicho resultado, tenemos que desarrollar algunos conceptos de geometría algebraica antes.

Notación 2.1. Sean V_1/K y V_2/K dos variedades proyectivas algebraicas sobre K y $\phi : V_1 \longrightarrow V_2$ un morfismo entre dichas curvas definido sobre K. Este morfismo induce una inyección en los cuerpos de funciones:

$$\begin{aligned} \phi^* : K(V_2) &\hookrightarrow K(V_1) \\ f &\longrightarrow f \circ \phi \end{aligned}$$

Aunque no es trivial en el caso de que las variedades anteriores sean curvas, la extensión de cuerpos que induce el morfismo ϕ siempre es una extensión finita, lo cual motiva la siguiente definición.

Definición 2.7. *Sea $\phi : C_1 \longrightarrow C_2$ un morfismo de curvas. Definimos el grado de ϕ como:*

$$\deg \phi = [K(C_1) : K(C_2)]$$

De la misma manera, se define el grado de inseparabilidad de ϕ, $\deg_i \phi$ *(resp. el grado de separabilidad,* $\deg_s \phi$*) como el de la extensión asociada a ϕ.*

Teorema 2.3. *Sean K un cuerpo de característica positiva, E_1/K y E_2/K curvas elípticas y $\phi : E_1 \longrightarrow E_2$ una isogenia no nula definida sobre K. Esta induce un homomorfismo de grupos formales $f : \hat{E}_1 \longrightarrow \hat{E}_2$. Entonces,*

$$\deg_i(\phi) = \mathrm{ht}(f)$$

Demostración. Consideramos $\phi : E_1/K \longrightarrow E_2/K$ una isogenia.

Si ϕ es el p^r-ésimo morfismo de Frobenius, i.e. el morfismo $\phi : E_1 \longrightarrow E_1^{(q)}$ dado por:

$$[x : y : z] \mapsto [x^q : y^q : z^q],$$

donde $q = p^r$ y $E_1^{(q)}$ es la curva dada por la misma ecuación que C pero con sus coeficientes elevados a q. Este morfismo es puramente inseparable, i.e. su extensión asociada es puramente inseparable. Por tanto, $\deg \phi = \deg_i \phi = p^r$ y $f(T) = T^{p^r}$. Por tanto, $\mathrm{ht}(\phi) = p^r$.

Si ϕ es un morfismo separable, denotemos por ω al diferencial invariante de E_2 y $\omega(T)$ el diferencial invariante del grupo formal $\hat{E}_2$. Como ϕ es separable, $\phi^*\omega \neq 0$([10] II.4.2). Por tanto,

$$(\omega \circ f)(T) = f'(0)\omega(T) \neq 0.$$

De lo que se sigue que $f'(0) \neq 0$, y, por tanto, $\mathrm{ht}(f) = 0$.

Por otro lado, toda isogenia se puede escribir como composición de un morfismo de Frobenius y un morfismo separable ([10] II.2.12). Así que, habida cuenta de la proposición 1.7 y los dos casos anteriores, hemos probado el resultado. ∎

Corolario 2.1. Sea E/K una curva elíptica definida sobre un cuerpo de característica positiva. Entonces, el grupo formal asociado a la curva tiene altura 1 o 2.

Demostración. La prueba de esto consiste en recordar que la aplicación $\phi = [p]$ tiene grado p^2. ∎

2.4 Curvas elípticas sobre cuerpos locales

En el capítulo anterior hemos desarrollado la teoría de grupos formales y en la sección anterior hemos visto como obtener una ley de grupo formal asociada a las curvas elípticas. También hemos sacado algunas consecuencias geométricas gracias a ese desarrollo. Se ha visto que se le puede sacar mucho partido a las leyes de grupos formales cuando sabemos que las series de potencias convergen. El sitio más propicio para explotar este punto parecen ser los cuerpos locales completos. Esto es lo que motiva este capítulo.

Presentamos la notación que vamos a seguir durante el capítulo. Sea K un cuerpo

local completo con respecto a una valoración v. Denotaremos por R a su anillo de valoración, por $\mathcal{M}$ su ideal de valoración, por π un parámetro de uniformización de R y por $k = R/\mathcal{M}$ el cuerpo residual.

2.4.1 Ecuación mínima de Weierstrass

Sea E/K una curva elíptica y sea

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

una ecuación de Weierstrass para E. Las transformaciones $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ mantienen la forma de la ecuación y cambian los coeficientes $a_i \mapsto u^i a_i$. Si elegimos u como una potencia suficientemente grande de π, podemos hacer que los coeficientes estén en R. En ese caso, se cumple $v(\Delta) \geq 0$.

Definición 2.8. *Sea E/K una curva elíptica, una forma de Weierstrass asociada a dicha curva con $a_i \in R$ se dice mínima si de entre la formas que cumplen que sus coeficientes están en R, $v(\Delta)$ alcanza el mínimo.*

Proposición 2.7. Se tienen las siguientes propiedades asociadas a las formas mínimas de Weierstrass.

a) Toda curva elíptica E/K tiene una ecuación mínima de Weierstrass asociada.
b) Una ecuación mínima de Weierstrass es única salvo un cambio de coordenadas de la forma:
$$x = u_2x' + r, \quad y = u_3y' + u_2sx' + t.$$
con $u \in R^*$ y $r, s, t \in R$.
c) El diferencial invariante
$$\omega = \frac{dx}{2y + a_1x + a_3}$$
asociado a una forma de Weierstrass mínima es única salvo multiplicación por una unidad, i.e. un elemento de R^*.

Demostración. La prueba de esto es bastante fácil conociendo cómo cambian los coeficientes mediante los cambios que preservan las formas de Weierstrass, una referencia es ([10] VII.1).

2.4.2 Reducción modulo π

Dentro del cuerpo K tenemos la aplicación natural siguiente que se suele llamar *reducción*,

$$\begin{array}{ccc} R & \longrightarrow & R/\pi R = k \\ t & \mapsto & \tilde{t} \end{array}$$

Queremos tener una aplicación de este tipo sobre las curvas. Sea E/K una curva elíptica. Si elegimos una ecuación mínima de Weierstrass para esa curva, podemos aplicar la reducción en los coeficientes para obtener una nueva curva (posiblemente no singular) de la forma,

$$\tilde{E} : y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6.$$

A la curva $\tilde{E}/k$ la llamaremos reducción módulo π de E. De la misma manera si $P = [x_0, \dots, x_n] \in \mathbb{P}^n$ podemos encontrar un representante para este punto tales que $x_0, \dots, x_n \in R$ y, al menos, alguna de las coordenadas esté en R^*. Así, podemos definir una aplicación de reducción

$$\mathbb{P}^n(K) \longrightarrow \mathbb{P}^n(k)$$

que viene dada por,

$$[x_0, \dots, x_n] \mapsto [\tilde{x}_0, \dots, \tilde{x}_n]$$

De esta manera, podemos mandar un punto $P \in E(K)$ a un punto $\tilde{P} \in \tilde{E}(k)$. Denotaremos por $\tilde{E}_{ns}(k)$ al conjunto de puntos de $\tilde{E}(k)$ que son no singulares. Se puede comprobar mediante cálculos elementales que este conjunto tiene estructura de grupo ([10] III.2.5).

Definición 2.9. *Definimos los siguientes subconjuntos*

$$\begin{array}{rcl} E_0(K) & := & \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}, \\ E_1(K) & := & \{P \in E(K) : \tilde{P} = \tilde{O}\}. \end{array}$$

El siguiente paso es probar que estos subconjuntos son grupos y ver qué relación tienen con el grupo $\tilde{E}_{ns}(k)$. La siguiente proposición nos da mucha información a este respecto.

Proposición 2.8. Existe una sucesión exacta de grupos abelianos

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0,$$

donde la aplicación de la derecha es la reducción módulo π.

Demostración. Comenzamos probando que la reducción es sobreyectiva. En primer lugar, sea

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

una ecuación mínima de Weierstrass para E. Denotamos por $\tilde{f}(x,y)$ al polinomio reducido. Sea $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in \tilde{E}_{ns}(k)$ un punto. Como es no singular, se tiene que o bien

$$\frac{\partial \tilde{f}}{\partial x}(\tilde{\alpha}, \tilde{\beta}) = 0, \qquad \text{o bien,} \quad \frac{\partial \tilde{f}}{\partial y}(\tilde{\alpha}, \tilde{\beta}) = 0.$$

Sin pérdida de generalidad suponemos que estamos en el segundo caso. Elegimos $x_0 \in R$ tal que $\tilde{x}_0 = \tilde{\alpha}$ y buscamos una solución de la ecuación

$$f(x_0, y) = 0.$$

Si reducimos módulo π esa ecuación, $\tilde{\beta}$ es una raíz que es simple por la condición de ser no singular. Ahora bien, por el lema de Hensel (ver A.2) podemos levantar a un $\tilde{y_0} = \tilde{\beta}$ que cumpla la ecuación. De esta manera, la aplicación es sobreyectiva. Lo siguiente que vamos a hacer es probar que $E_0(K)$ es subgrupo de $E(K)$ y la aplicación de reducción es un homomorfismo de grupos $E_0(K) \longrightarrow \tilde{E}_{ns}(k)$. Notemos que si probamos esto la exactitud de la sucesión es trivial.

Las operaciones de grupo de $E(K)$ y $\tilde{E}_{ns}(k)$ vienen dadas por la intersección de la curva con rectas de $\mathbb{P}^2$. Sea L/K una recta de $\mathbb{P}^2$, siempre podemos encontrar una ecuación de la forma

$$Ax + By + Cz = 0$$

con $A, B, C \in R$ y, al menos, alguno de los coeficientes en R^*. De esta manera, la recta reducida viene dada por la ecuación

$$\tilde{L} : \tilde{A}x + \tilde{B}y + \tilde{C}z = 0.$$

Sean $P_1, P_2 \in E_0(K)$ y $P_3 \in E(K)$ tres puntos tales que $P_1 + P_2 + P_3 = \mathcal{O}$. Sea L la recta que pasa por los tres puntos P_1, P_2 y P_3, contandos con multiplicidad. Basta probar que $\tilde{L}$ corta a $\tilde{E}$ en $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ con las mismas multiplicidades, ya que esto implica que $P_3 \in E_0$ y que $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \tilde{\mathcal{O}}$. La prueba no es difícil pero requiere una casuística extensa y no aporta demasiado a desarrollar las ideas principales del trabajo por ello damos la referencia ([10] VII.2.1). ∎

Observación 2.2. El resultado anterior nos se sigue cumpliendo si cambiamos el cuerpo K por cualquier otro cuerpo henseliano (ver A.3).

Bien, notemos ahora que si $v(\Delta) = 0$ entonces $v(\tilde{\Delta}) \neq 0$. En particular, $\tilde{E}$ es no singular. Por tanto, $\tilde{E} = \tilde{E}_{ns}$ y $E_0(K) = E(K)$. En ese caso, la sucesión exacta nos dice que $E(K)$ está hecho de dos piezas, los puntos reducidos y los puntos que se anulan mediante la reducción. El estudio de uno de los pedazos consiste en estudiar la curva sobre k, que habitualmente es un cuerpo finito. En cuanto al otro pedazo, es un objeto conocido como afirma el siguiente resultado.

Proposición 2.9. Sea E/K una curva elíptica dada por una ecuación mínima de Weierstrass, sea $\hat{E}/R$ el grupo formal asociado a la curva y sea $w(z) \in R[\![z]\!]$ la serie que obtuvimos en la proposición 2.6. Entonces,

$$\begin{array}{rcl} \hat{E}(\mathcal{M}) & \longrightarrow & E_1(K) \\ z & \mapsto & \left(\dfrac{z}{w(z)}, -\dfrac{1}{w(z)}\right) \end{array}$$

es un isomorfismo de grupos (se entiende que 0 va a $\mathcal{O}$).

Demostración. En primer lugar, el punto $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$ satisface la ecuación de Weierstrass como serie formal. Además,

$$w(z) = z^3(1 + \cdots) \in R[\![z]\!]$$

por lo que es convergente para todo $z \in \mathcal{M}$. Por tanto, $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) \in E(K)$. Más aún, como $v(-1/w(z)) = -3v(z) < 0$ para $z \in \mathcal{M}$, el punto debe estar en $E_1(K)$. Por tanto, la aplicación está bien definida.

Como la ley de grupo formal se obtiene a partir de la operación de la curva, la aplicación es un homomorfismo de grupos. Además, es inyectivo, ya que $w(z) = 0$ sólo si $z = 0$. Sólo queda ver la sobreyectividad.

Sea $(x, y) \in E_1(K)$, como la reducción de este punto es el punto del infinito $\tilde{O}$, se tiene que cumplir que $v(x), v(y) < 0$. Si tomamos valoración en la ecuación de Weierstrass, obtenemos lo siguiente:

$$3v(x) = 2v(y) = -6r,$$

para algún entero $r \geq 1$. Por tanto, $v(-x/y) = v(x) - v(y) > 0$ y la aplicación,

$$\begin{array}{rcl} E_1(K) & \longrightarrow & \tilde{E}(K) \\ (x, y) & \mapsto & -x/y, \end{array}$$

está bien definida, es homomorfismo de grupos y además es inyectiva. Como las composiciones dan la identidad, hemos probado que es un isomorfismo.

Con esto, podemos dar el siguiente resultado sobre los puntos de orden finito de $E(K)$ que nos será muy útil para entender la reducción.

Proposición 2.10. Sea E/K una curva elíptica y $m \geq 1$ un entero coprimo con $p = \text{char}(k)$. Entonces, se tienen:

a) El subgrupo $E_1(K)$ no tiene puntos no triviales de orden m.
b) Si suponemos que la curva reducida $\tilde{E}/k$ es no singular, entonces la reducción

$$E(K)[m] \longrightarrow \tilde{E}(k)$$

es inyectiva.

Demostración. Por la proposición 2.8, tenemos la sucesión exacta,

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0.$$

El resultado anterior nos dice que $E_1(K) \cong \hat{E}(\mathcal{M})$. Ahora bien, el resultado general de grupos formales que nos da la proposición 1.8 nos dice que $\hat{E}(\mathcal{M})$ no tiene puntos no triviales de orden m. Si además suponemos que $\tilde{E}$ es no singular, entonces $E(K) = E_0(K)$ y $\tilde{E}_{ns}(k) = \tilde{E}(k)$. Por tanto, la m-torsión se inyecta en $\tilde{E}(k)$. ∎

2.4.3 La acción del grupo de inercia

En este apartado, vamos a reinterpretar el resultado de último resultado sobre la inyectividad de la torsión. Por la proposición A.19 tenemos la sucesión exacta

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_{\overline{K}/K_{nr}} & \longrightarrow & G_{\overline{K}/K} & \longrightarrow & G_{K_{nr}/K} & \longrightarrow & 1 \\ & & \| & & & & \| & & \\ & & I_v & & & & G_{\overline{k}/k} & & \end{array}$$

donde I_v denota el grupo de inercia y K_{nr} es la extensión maximal no ramificada. Las igualdades anteriores se tienen por el estudio hecho en las secciones A.4 y A.6, ya que estamos asumiendo que K y k son perfectos.

Definición 2.10. *Sea Σ un conjunto sobre el que actúa el grupo $G_{\overline{K}/K}$. Decimos que Σ es no ramificado con respecto a v si la acción de I_v es trivial.*

Hemos visto que el grupo $G_{\overline{K}/K}$ actúa sobre los subgrupos $E[m]$ y sobre el módulo de Tate $T_l(E)$. El siguiente resultado nos da la ramificación de estos.

Proposición 2.11. Sea E/K una curva elíptica tal que su curva reducida $\tilde{E}/k$ es no singular. Entonces, se tiene:

a) Si $m \geq 1$ es un entero coprimo con $p = \text{char}(k)$, entonces $E[m]$ es no ramificado con respecto a v.
b) Sea l un primo distinto de la característica de k. Entonces, $T_l(E)$ es no ramificado.

Demostración. a) Sea K'/K una extensión finita tal que $E[m] \subset E(K')$, que sabemos que existe porque los puntos de $E[m]$ son finitos. Por hipótesis, la curva reducida es no singular, i.e. si consideramos un modelo de Weierstrass minimal este cumple que $v(\Delta) = 0$. Como la valoración extendida v' restringida a K es un múltiplo (el índice de ramificación) de la valoración v, se tiene que $v'(\Delta) = 0$. Por tanto, el modelo de Weiestrass también es mínimo sobre K' y, por tanto, su curva reducida $\tilde{E}/k$ es minimal. Por el último resultado del apartado anterior sabemos que

$$E[m] \hookrightarrow \tilde{E}(k')$$

Sean $\sigma \in I_v$ y $P \in E[m]$. Sabemos que el grupo de inercia actúa trivialmente sobre $\overline{k}$, por tanto,

$$\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = \tilde{\mathcal{O}}$$

Ahora bien, por la compatibilidad de la acción de Galois con la operación de la curva $\tilde{P}^\sigma - \tilde{P} \in E[m]$. Por la inyectividad de la reducción $E[m] \hookrightarrow \tilde{E}(k')$ tenemos que $P^\sigma - P = \mathcal{O}$.
b) Se deduce directamente del apartado anterior usando la definición del límite inverso.

Este resultado también tiene un recíproco que se conoce como criterio de Néron-Ogg-Shafarevich y que necesitaremos usar más adelante en el trabajo. Para probarlo necesitamos estudiar la curva reducida $\tilde{E}$ más de cerca.

2.4.4 Buena y mala reducción

Una curva E dada por un modelo de Weiestrass con discriminante 0 tiene que estar en uno de los siguientes casos:

a) E tiene un nodo.
b) E tiene una cúspide.

Un estudio de esto se puede encontrar en ([10] III.1.4).

Definición 2.11. *Sea E/K una curva elíptica, y sea $\tilde{E}$ la reducción modulo $\mathcal{M}$ de un modelo mínimo de Weiestrass para E. Se dice que:*

a) E tiene buena reducción (o reducción estable) si $\tilde{E}$ es no singular
b) E tiene reducción multiplicativa (o semiestable) si $\tilde{E}$ tiene un nodo.
c) E tiene reducción aditiva (o inestable) si $\tilde{E}$ tiene una cúspide.

En los dos últimos casos se dice que E tiene mala reducción.

Cuando tenemos una curva elíptica con mala reducción es interesante saber si en alguna extensión la curva pasa a tener buena reducción.

Definición 2.12. *Sea E/K una curva elíptica. Diremos que E/K tiene potencial buena reducción si existe una extensión finita K'/K tal que E tiene buena reducción sobre K'.*

La siguiente proposición nos muestra como se comportan los distintos tipos de reducción cuando tenemos una extensión de cuerpos.

Proposición 2.12 (Teorema de la reducción semiestable). Sea E/K una curva elíptica. Entonces, se tiene que:

a) Sea K'/K una extensión no ramificada. Entonces, el tipo de reducción de E sobre K es el mismo tipo que el de E sobre K'.
b) Sea K'/K una extensión finita. Si E tiene buena reducción o reducción multiplicativa sobre K, entonces tiene el mismo tipo de reducción sobre K'.
c) Existe una extensión finita K'/K tal que E tiene buena reducción o reducción multiplicativa sobre K'.

Demostración. a) Vamos a dar una prueba para $\mathrm{char}(k) \geq 5$, la prueba para cualquier característica se deduce del algoritmo de Tate ([11] IV.9). Si $\mathrm{char}(k) \geq 5$, E tiene una ecuación mínima de Weiestrass sobre K de la forma:

$$E : y^2 = x^3 + Ax + B.$$

Sean R' el anillo de enteros de K', v' la única extensión de v sobre K' y

$$x = (u')^2 x, \quad y = (u')^3 y',$$

un cambio de coordenadas mediante el que obtenemos una ecuación mínima de Weiestrass de E sobre K'. Como K'/K es no ramificada, podemos encontrar un $u \in K$ con $u/u' \in R'^*$. Por tanto, el cambio

$$x = u^2 x', \quad y = u^3 y'$$

también nos da una ecuación mínima de Weiestrass para E/K', pues $v(u^{-12}\Delta) = v'((u')^{-12}\Delta)$. Pero esta nueva ecuación tiene coeficientes en R, luego por la minimalidad de la ecuación original sobre K, $v(u) = 0$. Por tanto, la ecuación original también es minimal sobre K'. Más aún, como $v(\Delta) = v'(\Delta)$ y $v(c_4) = v'(c_4)$, el tipo de reducción de E/K y E/K' es el mismo.

b) Consideramos una ecuación mínima de Weiestrass para E sobre K y sean R' y v' como en la prueba del apartado anterior. Consideramos también un cambio de coordenadas

$$x = u^2 x' + r, \quad y = u^3 y' + s u^2 x' + t,$$

el cual nos da una ecuación mínima de Weiestrass para E sobre K'. Las cantidades Δ' y c_4' asociadas a esta nueva ecuación cumplen:

$$0 \leq v'(\Delta') = v'(u^{-12}\Delta), \quad 0 \leq v'(c_4') = v'(u^{-4} c_4)$$

Por la proposición 2.7 sabemos que $u \in R'$, por tanto,

$$0 \leq v'(u) \leq \text{mín}\left\{ \frac{1}{12} v'(\Delta), \frac{1}{4} v'(c_4) \right\}$$

Si la curva tiene buena reducción (resp. reducción multiplicativa), sabemos que $v(\Delta) = 0$ (resp. $v(c_4) = 0$). Luego $v'(u) = 0$ y, por tanto,

$$v'(\Delta') = v(\Delta) \quad \text{y} \quad v'(c_4') = v'(c_4'),$$

de lo que se deduce que E tiene buena reducción (resp. reducción multiplicativa) sobre K'.

c) Vamos a hacer la prueba para el caso $\text{char}(k) \neq 2$, el caso $\text{char}(k) = 2$ se puede encontrar en ([10] A.1.4). Con esta hipótesis, se puede comprobar ([10] III.1.4.) que toda ecuación de Weierstrass es isomorfa a una de la forma

$$E : y^2 = x(x-1)(x-\lambda) \quad \text{con } \lambda \neq 0, 1.$$

Para curvas de esta forma se tiene que

$$c_4 = 16(\lambda^2 - \lambda + 1) \quad \text{y} \quad \Delta = 16\lambda^2(\lambda - 1)^2.$$

Vamos a considerar tres casos.

Caso 1. $\lambda \in R$ y $\lambda \not\equiv 0, 1 \mod \mathcal{M}$. En este caso $\Delta \in R^*$ y la curva tiene buena reducción.

Caso 2. $\lambda \in R$ y $\lambda \equiv 0$ o $1 \mod \mathcal{M}$. En este caso $\Delta \in \mathcal{M}$ y $c_4 \in R^*$. En este caso, la ecuación tiene reducción multiplicativa.

Caso 3. $\lambda \notin R$. En este caso, existe un $r \geq 1$ tal que $\pi^r \lambda \in R^*$. Entonces, considerando $K(\sqrt{\pi})$ si fuera necesario, el cambio $x = \pi^{-r}x'$ e $y = \pi^{-3r/2}y'$ nos da una ecuación:

$$(y')^2 = x'(x' - \pi^r)(x - \pi^r\lambda).$$

Esta ecuación tiene coeficientes en R y cumple que $\Delta' \in \mathcal{M}$ y $c_4' \in R^*$, por tanto, la curva tiene reducción multiplicativa.

Ya estamos en condiciones de probar el Criterio de Néron-Ogg-Shafarevic que enunciamos a continuación.

Teorema 2.4 (Criterio de Néron-Ogg-Shafarevic). *Sea E/K una curva elíptica. Entonces, los siguientes enunciados son equivalentes:*

a) E tiene buena reducción.
b) $E[m]$ es no ramificado con respecto a v para todos los enteros $m \geq 1$ coprimos con $\mathrm{char}(k)$.
c) El módulo de Tate $T_l(E)$ es no ramificado con respecto a v para l, primo distinto de $p =$ $\mathrm{char}\ k$.
d) $E[m]$ es no ramificado con respecto a v para una cantidad infinita de enteros $m \geq 1$ coprimos con $\mathrm{char}(k)$.

Demostración. La implicación $a) \Rightarrow b)$ ya la hemos visto en la proposición 2.11 y las implicaciones $b) \Rightarrow c) \Rightarrow d)$ son triviales. Por tanto, solo queda probar que $d) \Rightarrow a)$. Para ello, vamos a necesitar el siguiente resultado que daremos sin demostración, pues su prueba requeriría introducir la teoría de esquemas y no aporta mucho a nuestros propósitos.

Proposición 2.13. El grupo $E_0(K)$ tiene índice finito sobre $E(K)$.

Demostración. Una prueba mediante métodos elementales se puede encontrar en ([11] IV.5,IV.6).

Gracias al resultado anterior podemos encontrar un entero $m > \#E(K_{nr})/E_0(K_{nr})$ coprimo con $\mathrm{char}(k)$ tal que $E[m]$ sea no ramificado con respecto a v. Consideramos las sucesiones exactas,

$$0 \longrightarrow E_0(K_{nr}) \longrightarrow E(K_{nr}) \longrightarrow E(K_{nr})/E_0(K_{nr}) \longrightarrow 0$$

$$0 \longrightarrow E_1(K_{nr}) \longrightarrow E_0(K_{nr}) \longrightarrow \tilde{K}_{ns}(\overline{k}) \longrightarrow 0$$

Como $E[m] \subset E(K_{nr})$, tenemos que $E(K_{nr})$ tiene un subgrupo isomorfo a $(\mathbb{Z}/m\mathbb{Z})^2$. Pero como $E(K_{nr})/E_0(K_{nr})$ tiene orden estrictamente menor que m, se sigue de la primera sucesión exacta que existe $l|m$ primo tal que $E_0(K_{nr})$ contiene un subgrupo isomorfo a $(\mathbb{Z}/\mathbb{Z}l)^2$. Ahora bien, en virtud de la proposición 2.10 y de la segunda sucesión exacta tenemos que $\tilde{K}_{ns}(\overline{k})$ contiene un subgrupo isomorfo a $(\mathbb{Z}/\mathbb{Z}l)^2$.
Supongamos que E tiene mala reducción sobre K_{nr}. Si la reducción es multiplicativa entonces

$$\tilde{E}_{ns}(\overline{k}) = \overline{k}^*,$$

En cuyo caso la l-torsión de $\overline{k}^*$ son las l-raíces de la unidad, μ_l que son isomorfas como grupo a $\mathbb{Z}/l\mathbb{Z}$. Luego, E no puede tener reducción multiplicativa. Análogamente, si la reducción es aditiva,

$$\tilde{E}_{ns}(\overline{k}) = \overline{k}^+.$$

y, por tanto, $\tilde{E}_{ns}(\overline{k})$ no tiene l-torsión. Hemos probado que E tiene buena reducción sobre K_{nr}. Ahora bien, como K_{nr} es no ramificada, entonces E tiene buena reducción sobre K, por la proposición 2.12.

2.5 Multiplicación compleja

Para terminar este capítulo, vamos a presentar una propiedad de las curvas elípticas que será fundamental para estudiar como se comporta la representación del grupo de absoluto de Galois de un cuerpo de números asociada a la torsión del grupo de puntos de una curva elíptica. Dicha propiedad se conoce como la *multiplicación compleja* y está relacionada con los endomorfismos de la curva.

Sean E_1/K y E_2/K dos curvas elípticas definidas sobre un cuerpo K. Llamamos $\mathrm{Hom}(E_1, E_2)$ al conjunto de isogenias de E_1 en E_2. Como los puntos de las curvas

elípticas tienen estructura de grupo, $\mathrm{Hom}(E_1, E_2)$ tiene estructura de grupo. El caso que nos interesa es cuando $E_1 = E_2 =: E$. En dicho caso, denotamos por

$$\mathrm{End}(E) := \mathrm{Hom}(E_1, E_2)$$

al anillo de endomorfismos de la curva E, donde el producto viene dado por la composición. Vamos a dar algunos resultados a continuación sobre la estructura de $\mathrm{End}(E)$.

Proposición 2.14. a) Sea E/K una curva elíptica y sea $m \in \mathbb{Z}$ no nulo. Entonces, la aplicación

$$[m] : E \longrightarrow E$$

es no constante.

b) Sea E una curva elíptica. Entonces, el anillo de endomorfismos $\mathrm{End}(E)$ es un anillo (no necesariamente conmutativo) de característica 0 sin divisores de 0.

Demostración. ([10] III.4.2)

Observación 2.3. La proposición anterior nos proporciona la siguiente aplicación inyectiva

$$\begin{aligned} [\cdot] : \mathbb{Z} &\longrightarrow \mathrm{End}(E), \\ m &\longmapsto [m]. \end{aligned}$$

Definición 2.13. *Sea E/K una curva elíptica, si el anillo de endomorfismos de E es estrictamente mayor que $\mathbb{Z}$, diremos que la curva tiene multiplicación compleja.*

El siguiente resultado motiva el nombre que hemos dado a la propiedad anterior.

Proposición 2.15. Sean K un cuerpo de característica 0 y E/K una curva elíptica con multiplicación compleja. Entonces, $\mathrm{End}(E) \simeq \mathbb{Z}\left(\sqrt{D}\right)$ con $D < 0$.

Demostración. ([10] III.9.4)

Vamos a ver ahora como influye la multiplicación compleja en el comportamiento de las representaciones ρ_l.

Sea l un primo y sea E/K una curva elíptica, definida sobre un cuerpo de números K, que supondremos con multiplicación compleja en lo que sigue. Llamemos $\mathcal{O} = \mathrm{End}(E)$. Consideremos la aplicación

$$\begin{aligned} \mathcal{O} &\longrightarrow \mathrm{End}(E[l]) \\ \phi &\longmapsto \phi|_{E[l]}, \end{aligned}$$

donde $\mathrm{End}(E[l])$ es el anillo de endomorfismos de $E[l]$ como grupos abelianos. Notemos que ϕ pertenece al núcleo de esta aplicación si, y sólo si, $\ker[l] \subset \ker \phi$. Ahora bien, se puede probar que esta última condición implica que exisite $g \in \mathrm{End}(E)$ tal que $f = [l] \circ g$ (ver [10] III.4.11). Por tanto, el núcleo de la aplicación anterior son exactamente las isogenias de $[l] \circ \mathcal{O}$, con lo cual tenemos la inclusión

$$\frac{\mathcal{O}}{[l] \circ \mathcal{O}} \hookrightarrow \mathrm{End}(E[l]) \simeq \mathcal{M}(2, \mathbb{F}_l),$$

donde $\mathcal{M}(2, \mathbb{F}_l)$ son las matrices cuadradas 2×2 sobre $\mathbb{F}_l$.

Vamos a suponer en primer lugar que todo $f \in \mathcal{O}$ está definido sobre K, entonces

$$\forall \sigma \in \mathrm{Gal}\left(\overline{K} | K\right), \forall f \in \mathcal{O}, \forall P \in E, \quad \sigma(f(P)) = f(\sigma(P)),$$

lo cual implica que

$$\rho_l\left(\mathrm{Gal}\left(\overline{K} | K\right)\right) \subset \mathcal{Z}\left(\frac{\mathcal{O}}{[l] \circ \mathcal{O}}\right),$$

donde $\mathcal{Z}\left(\frac{\mathcal{O}}{[l] \circ \mathcal{O}}\right)$ es el centralizador de $\frac{\mathcal{O}}{[l] \circ \mathcal{O}}$, i.e. el conjunto de elementos de $\mathcal{M}(2, \mathbb{F}_l)$ que conmutan con todos los de $\frac{\mathcal{O}}{[l] \circ \mathcal{O}}$.

Lema 2.2. Sea $A \in \mathcal{M}(2, \mathbb{F}_l)$ una matriz, entonces $\mathcal{Z}(\{A\})$ tiene dimensión 2 o 4 como espacio vectorial sobre $\mathbb{F}_l$.

Demostración. La prueba de este hecho se deduce de un cálculo directo, aunque tedioso, al imponer que $AX = XA$ para una matriz A fija y una matriz X arbitraria del centralizador de A. ∎

Lema 2.3. El centralizador de $\frac{\mathcal{O}}{[l] \circ \mathcal{O}}$ es $\frac{\mathcal{O}}{[l] \circ \mathcal{O}}$.

Demostración. Llamemos $H = \frac{\mathcal{O}}{[l] \circ \mathcal{O}}$. Se tiene que

$$\mathcal{Z}(H) = \bigcap_{A \in H} \mathcal{Z}(\{A\}).$$

Como la curva tiene multiplicación compleja H tiene dimensión 2 y es un grupo abeliano. Por tanto, $H \subset \mathcal{Z}(\{A\})$, para cada $A \in H$. Además, por el lema anterior $\mathcal{Z}(\{A\})$ tiene dimensión 2, en cuyo caso $H = \mathcal{Z}(\{A\})$ o $\mathcal{Z}(\{A\})$ tiene dimensión 4, en cuyo caso es el espacio entero. Ahora bien, las únicas matrices que conmutan con todas las demás son los múltiplos de la identidad y como H tiene dimensión 2, H debe contener alguna matriz que no sea de este tipo. Por tanto, $H = \mathcal{Z}(H)$. ∎

Los lemas anteriores implican que

$$\rho_l\left(\mathrm{Gal}\left(\overline{K}|K\right)\right) \subset \left(\frac{\mathcal{O}}{[l]\circ\mathcal{O}}\right)^*,$$

ya que $\rho_l(\mathrm{Gal}(\overline{K}|K)) \subset \mathrm{Aut}(E[l])$. Esto es una restricción al tamaño de la imagen del grupo de Galois. Dependiendo del comportamiento de l en $\mathcal{O}$, tenemos la siguiente casuística:

$$\left(\frac{\mathcal{O}}{[l]\circ\mathcal{O}}\right)^* = \begin{cases} \mathbb{F}_l^* \times \mathbb{F}_l^* & \text{si } l \text{ se descompone como producto de primos distintos,} \\ \mathbb{F}_{l^2}^* & \text{si } l \text{ es inerte, i.e. no se descompone,} \\ (\mathbb{F}_l[\varepsilon])^* & \text{si } l \text{ ramifica,} \end{cases}$$

donde ε cumple $\varepsilon^2 = 0$. Los dos primeros casos coinciden con un subgrupo de Cartan escindido y no escindido respectivamente. El tercer caso es un subgrupo de un subgrupo de Borel.

Pasamos ahora a estudiar el caso en que no todos los endomorfismos de E están definidos sobre K. En este caso, tenemos la siguiente aplicación natural dada por la restricción

$$\mathrm{Gal}(\overline{K}|K) \longrightarrow \mathrm{Aut}(\mathcal{O}).$$

Los automorfismos de $\mathcal{O}$ solo pueden ser la identidad o la conjugación compleja. Esto implica que si fijamos $\sigma \in \mathrm{Gal}(\overline{K}|K)$, $f \in \mathcal{O}$ y $P \in E$ se da una de las siguientes ecuaciones:

a) $f(P) = \sigma^{-1}(f(\sigma P))$.
b) $f(P) = \sigma^{-1}\overline{(f(\sigma P))}$.

Por tanto, la imagen del grupo de Galois cumple que

$$\rho_l(\mathrm{Gal}(\overline{K}|K)) \subset \mathrm{Norm}\left[\left(\frac{\mathcal{O}}{[l]\circ\mathcal{O}}\right)^*\right],$$

donde $\mathrm{Norm}[\cdot]$ denota el normalizador. Ya hemos visto qué posibles grupos puede ser $\left(\frac{\mathcal{O}}{[l]\circ\mathcal{O}}\right)^*$, por lo que $\rho_l(\mathrm{Gal}(\overline{K}|K))$ está contenido en el normalizador de un Cartan

o en el normalizador de $\left(\mathbb{F}_l[\varepsilon]\right)^*$ que se comprueba mediante un cálculo directo que es un subgrupo de Borel.

Acabamos de ver como la multiplicación compleja limita el tamaño que puede tener la imagen del grupo de Galois mediante la representación ρ_l. La siguiente pregunta que surge de manera natural es: ¿qué sucede cuando la curva no tiene multiplicación compleja? La respuesta a esta pregunta nos la da el teorema de Serre, el cual nos dice que cuando eliminamos el impedimento de la multiplicación compleja la imagen de ρ_l es tan grande como puede ser para casi todos los primos. En el siguiente capítulo vamos a presentar y desarrollar las herramientas que necesitaremos para presentar la prueba de Serre.

3 Representaciones de curvas elípticas sobre un cuerpo local

3.1 Inercia Moderada

En esta sección vamos a seguir la siguiente notación:

a) K será un cuerpo de característica 0 y completo para una valoración discreta v. En particular, K es un cuerpo perfecto, i.e. toda extensión algebraica de K es separable.
b) Denotaremos por R al AVD asociado, por $\mathcal{M}$ al ideal maximal, por U al grupo de unidades y por $k = R/\mathcal{M}$ al cuerpo residual.

Además también supondremos que $\text{char}(k) = p > 0$.

3.1.1 Grupos de Galois

Sea $\overline{K}$ la clausura algebraica de K. La valoración v se extiende de manera única a $\overline{K}$ y el cuerpo residual $\overline{k}$ corresponde a una clausura algebraica de k. Tenemos la siguiente cadena de extensiones,

$$\overline{K} \supset K_t \supset K_{nr} \supset K,$$

donde K_{nr} es la extensión maximal no ramificada de K y K_t es la extensión maximal moderadamente ramificada de K. Hay una identificación canónica entre los cuerpos residuales k_{nr}, k_t y la clausura separable k_s de k en $\overline{k}$. En lo que sigue usaremos la

notación,

$$G := \mathrm{Gal}(\overline{K}|K), \quad I := \mathrm{Gal}(\overline{K}|K_{nr}) \quad \text{y} \quad I_p := \mathrm{Gal}(\overline{K}|K_t)$$

Tenemos $G \supset I \supset I_p$. Sabemos que I (resp. I_p) es el grupo de inercia (resp. el p-grupo de inercia) del grupo de Galois G. Además, sabemos que es un subgrupo normal cerrado y que se tiene la identificación canónica:

$$\mathrm{Gal}(K_{nr}|K) \cong G_k = \mathrm{Gal}(\overline{k}|k)$$

Llamaremos grupo de inercia moderada al cociente $I_t = I/I_p = \mathrm{Gal}(K_t|K_{nr})$, que sabemos que es isomorfo a $\prod_{q\neq p \text{ primo}} \mathbb{Z}_q$. Este grupo jugará un papel esencial en lo que sigue.

3.1.2 Estructura del grupo de inercia moderada

En este apartado vamos a estudiar la estructura del grupo de inercia moderada $I_t = G(K_t|K_{nr})$. En primer lugar, como K es un anillo de valoración discreta y K_{nr} es una extensión no ramificada, K_{nr} también es un anillo de valoración discreta (ver sección A.3). Denotaremos por v a la única extensión a K_{nr} de la valoración de K.

Vamos a construir unas extensiones intermedias

$$K_{nr} \subset K_d \subset K_t,$$

para cada $d \in \mathbb{N}$ coprimo con p. Como veremos más adelante, dichas extensiones generan la extensión $K_t|K_{nr}$.

Sean π un parámetro de uniformización de K_{nr} y $d \geq 1$ un entero coprimo con p. Definimos $K_d = K_{nr}(\pi^{1/d})$. Notemos que dicha extensión no depende de la elección del parámetro de uniformización. En efecto, si π' es otro parámetro de uniformización, existe una unidad ε una unidad del anillo de valoración de K_{nr} tal que $\pi' = \varepsilon\pi$, con lo cual $(\pi')^{1/d} = \varepsilon^{1/d}\pi^{1/d}$. Como $\varepsilon^{1/d}$ es una raíz de $X^d - \varepsilon$ y su polinomio reducido es $X^d - 1$, el cual factoriza en sus factores lineales en k_s. Por tanto, el lema de Hensel (ver A.2) nos garantiza que $\varepsilon^{1/d} \in K_{nr}$. Luego K_d no depende de la elección del parámetro de uniformización.

Lema 3.1. Se verifica

$$K_t = \bigcup_{p\nmid d} K_d.$$

Demostración. Para cada d coprimo con p, se tiene que K_d es una extensión moderadamente ramificada de K_{nr}. Por tanto, $K_d \subset K_t$. Recíprocamente, sea $x \in K_t$, entonces $K_{nr}(x)$ es moderadamente ramificada (ver proposición A.3). Por tanto, por la caracterización de las extensiones moderadamente ramificadas (ver la proposción A.12), tenemos que

$$K(x)K_{nr} = K_{nr}\left(a_1^{1/m_i}, \dots, a_r^{1/m_r}\right),$$

para algunos $a_1, \dots, a_r \in K_{nr}$ y $m_1, \dots, m_r$ enteros coprimos con p. Ahora bien, podemos escribir cada a_i como

$$a_i = \varepsilon_i \pi^{e_i}$$

con π un parámetro de uniformización de K_{nr} y ε_i una unidad. Por tanto, $a_i^{1/m_i} = \varepsilon^{1/m_i}\pi^{e_i/m_i} \in K_{nr}(\pi^{1/m_i})$. En particular,

$$K(x) \subset K_{nr}\left(\pi^{1/m_1}\right) \cdots K_{nr}\left(\pi^{1/m_r}\right).$$

Podemos usar las extensiones K_d para caracterizar el grupo de inercia moderada, ya que el lema anterior implica que

$$I_t = \mathrm{Gal}(K_t|K_{nr}) = \varprojlim_d \mathrm{Gal}(K_d|K_{nr}).$$

Con este propósito, vamos estudiar los grupos de Galois $\mathrm{Gal}(K_d|K_{nr})$. Para ello, necesitamos el siguiente lema que generaliza el criterio de Eisenstein.

Lema 3.2. Sea $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$ un polinomio tal que $a_i \in \mathcal{M}$, para $i = 0, \dots, n-1$, y $a_0 \notin \mathcal{M}^2$, entonces f es irreducible.

Demostración. ([3] I.6.Theorem 1)

Denotemos por μ_d al grupo de las raíces d-ésimas de la unidad, para cada entero d coprimo con p.

Proposición 3.1. La extensión $K_d|K_{nr}$ es de Galois y su grupo de Galois es isomorfo a μ_d.

Demostración. Por definición, $\pi^{1/d}$ cumple la ecuación $X^d - \pi = 0$. Este polinomio es irreducible por lema anterior. Por tanto, $[K_d : K_{nr}] = d$. Además, ya hemos visto que

el polinomio $X^d - \pi$ se descompone completamente en K_d. Luego, $K_d|K_{nr}$ es de Galois.

Consideremos ahora la aplicación

$$\begin{aligned} \theta_d : \mathrm{Gal}(K_d|K_{nr}) &\longrightarrow \mu_d \\ \sigma &\mapsto \theta_d(\sigma), \end{aligned}$$

donde $\theta_d(\sigma)$ es la raíz de la unidad tal que

$$\sigma\left(\pi^{1/d}\right) = \theta_d(\sigma)\,\pi^{1/d}.$$

Esta aplicación no depende de la elección del parámetro de uniformización. En efecto, si $\pi' = \varepsilon\pi$ es otro parámetro de uniformización, tenemos que

$$\sigma\left(\pi'^{1/d}\right) = \sigma\left(\varepsilon^{1/d}\pi^{1/d}\right) = \varepsilon^{1/d}\sigma(\pi) = \varepsilon^{1/d}\theta_d(\sigma)\pi^{1/d} = \theta_d(\sigma)\pi'^{1/d}.$$

Esta aplicación es claramente un homomorfismo inyectivo de grupos. Como $d = \#\mathrm{Gal}(K_d|K_{nr}) = \#\mu_d$, θ_d es un isomorfismo.

Corolario 3.1. Los isomorfismos θ_d inducen un isomorfismo

$$\theta : I_t \longrightarrow \varprojlim \mu_d$$

Demostración. La prueba es inmediata por la propiedad universal del límite inverso.

Observación 3.1. También tenemos el siguiente isomorfismo no canónico:

$$I_t \simeq \varprojlim \mu_d \simeq \varprojlim \mathbb{Z}/d\,\mathbb{Z} \simeq \prod_{q\neq p} \mathbb{Z}_q\,.$$

Podemos refinar el corolario anterior. Sea q una potencia de p y denotemos por $\mathbb{F}_q$ al subcuerpo de k_s con q elementos. Se tiene que $\mathbb{F}_q^* = \mu_{q-1}$, ya que el polinomio $x^{q-1} - 1$ es separable y, por el lema de Hensel, μ_{q-1} son todas las raíces de la unidad.

Los números de la forma $q-1$ son cofinales en el conjunto de los enteros coprimos con p ordenados por divisibilidad. En efecto, si d es un entero de este tipo, sabemos por el teorema de Euler que existe un n tal que $p^n \equiv 1 \mod d$. Así, el sistema proyectivo (μ_d) es equivalente al formado por los $\mathbb{F}_q^*$ y las aplicaciones

$$\begin{aligned} N : \mathbb{F}_{q^m}^* &\longrightarrow \mathbb{F}_q^* \\ \alpha &\mapsto \alpha^{1+q+\cdots+q^{m-1}} \end{aligned}$$

Por tanto, la proposición anterior equivale a:

Proposición 3.2. Los isomorfismos θ_{q-1} inducen un isomorfismo:

$$\theta : I_t \longrightarrow \varprojlim \mathbb{F}_q^*,$$

donde $\mathbb{F}_q$ recorre los subcuerpos finitos de k_s.

Además, este isomorfismo tiene la siguiente propiedad de funtorialidad.

Proposición 3.3. Sea K' un subcuerpo cerrado y no discreto de K. Si llamamos $I_{t,K}$ (resp. $I_{t,K'}$) al grupo de inercia moderada de K (resp. K'). Entonces tenemos el siguiente diagrama conmutativo,

$$\begin{array}{ccc} I_{t,K} & \xrightarrow{\sim} & \varprojlim \mu_d \\ \downarrow & & \downarrow{\scriptstyle e(K/K')} \\ I_{t,K'} & \xrightarrow{\sim} & \varprojlim \mu_d \end{array}$$

Demostración. Sea $d \geq 1$ coprimo con p. Fijamos x y x' parámetros de uniformización de K_{nr} y K'_{nr} respectivamente. Por definición del índice de ramificación $x' = x^e$. Ponemos $K_d = K_{nr}(x^{1/d})$ y $K'_d = K'_{nr}(x^{1/d})$ y llamamos θ_d y θ'_d a los isomorfismos correspondientes. Con esta notación, tenemos la aplicación natural inducida por la restricción

$$r_{K'} : \mathrm{Gal}(K_d|K_{nr}) \longrightarrow \mathrm{Gal}(K'_d|K'_{nr}).$$

De esta manera, si fijamos $s \in \mathrm{Gal}(K_d|K_{nr})$, tenemos que

$$\theta_d(s) = \frac{s(x^{1/d})}{x^{1/d}},$$

y que

$$\theta'_d(r_{K'}(s)) = \frac{r_{K'}(s)(x'^{1/d})}{x'^{1/d}} = \frac{s(x^{e/d})}{x^{e/d}} = \theta_d(s)^e.$$

Por tanto, el diagrama

$$\begin{array}{ccc} \mathrm{Gal}(K_d|K_{nr}) & \xrightarrow{\sim} & \mu_d \\ \downarrow & & \downarrow{\scriptstyle e(K/K')} \\ \mathrm{Gal}(K_d|K_{nr}) & \xrightarrow{\sim} & \mu_d \end{array}$$

es conmutativo para cada $d \geq 1$ coprimo con p. El resultado se deduce ahora de la propiedad universal del límite inverso. ∎

3.1.3 Representaciones de G en característica p

Sea V un espacio vectorial de dimensión finita sobre un cuerpo k_1, de característica p, y sea

$$\rho : G \longrightarrow \mathrm{GL}(V)$$

una representación lineal y continua de G en V, i.e. el kernel es abierto. Así la continuidad de la representación es equivalente a que el núcleo de esta sea abierto.

Definición 3.1. *Sea H un grupo y V un espacio vectorial de dimensión finita. Decimos que una representación $\varphi : H \longrightarrow \mathrm{GL}_r(V)$ es simple si no tiene sub-representaciones no triviales,i.e. no existe ningún subespacio $W \subset V$ tal que $(\varphi|_W, W)$ sea una representación.*

Definición 3.2. *Sea H un grupo y V un espacio vectorial de dimensión finita. Decimos que una representación $\varphi : H \longrightarrow \mathrm{GL}_r(V)$ es semisimple si existen*

$$(\varphi_1, W_1), \dots, (\varphi_n, W_n) \subset V$$

subrepresentaciones tales que $V = W_1 \oplus \cdots \oplus W_n$ y $\varphi = \varphi_1 \oplus \cdots \oplus \varphi_n$.

Proposición 3.4. Si ρ es semisimple, se tiene que $\rho(I_p) = \{1\}$.

Demostración. Basta probar que $\rho(I_p) = \{1\}$ para el caso en que ρ sea simple. En otro caso, basta descomponer la representación en representaciones simples. Así, supongamos que ρ es simple y consideremos

$$V' = \{v \in V : \forall \varphi \in \rho(I_p), \quad \varphi(v) = v\}.$$

Como $\ker \rho$ es un subgrupo normal abierto de G existe una extensión de Galois $L|K$ tal que

$$\mathrm{Gal}(L|K) \cong \rho(G),$$

por el teorema de Galois (ver 1.1). Por tanto,

$$\rho(I_p) \cong I_p/\ker(\rho|_{I_p}) \leq G/\ker(I_p) \cong \mathrm{Gal}(L|K)$$

es un cociente finito de I_p. Esto implica que debe ser un p-grupo finito (A.21). Por tanto, $V' \neq 0$ (una prueba de este hecho se puede encontrar en [8] IX.Teorema 2). Además I_p es normal, por lo que si fijamos $v \in V'$,

$$\forall \sigma \in \rho(G), \forall \varphi \in \rho(I_p) \quad \sigma^{-1}\varphi\sigma(v) = v.$$

Por tanto, $\forall \varphi \in I_p \quad \varphi(\sigma(v)) = \sigma(v)$, de lo que se deduce que $\sigma(v) \in V'$. De esta manera, hemos probado que todo G deja fijo V'. Por la simplicidad de ρ, $V = V'$ como queríamos demostrar. ∎

Supongamos que ρ es semisimple. La proposición anterior nos dice que ρ actúa trivialmente sobre I_p. Por tanto, factoriza a través del grupo de inercia moderada $I_t = I/I_p$. Como $I_t \simeq \prod_{q\neq p} \mathbb{Z}_q$, la imagen de I_t es un grupo cíclico de orden coprimo con p. Si k_1 es suficientemente grande, separablemente cerrado por ejemplo, podemos escribir $\rho(I_t)$ en forma diagonal. Esto es, la restricción ρ_{I_t} viene dada por n caracteres $\psi_i : I_t \longrightarrow k_1^*$. Pasamo ahora a dar explícitamente estos caracteres.

3.1.4 Caracteres de I_t

Pasamos ahora a explícitar el grupo $X = \mathrm{Hom}(I_t, k_s^*)$ de caracteres continuos de I_t en k_s^* (que es isomorfo a $\varprojlim \mu_d$). Lo que haremos será usar los caracteres ya conocidos $\theta_d : I_t \longrightarrow \mathrm{Gal}(K_d|K_{nr})$ para *parametrizar* X.

Comencemos considerando $\mathbb{Q}/\mathbb{Z}$ y llamemos $(\mathbb{Q}/\mathbb{Z})'$ al conjunto de los elementos de $\mathbb{Q}/\mathbb{Z}$ de orden coprimo con p. Es fácil comprobar que todo $\alpha \in (\mathbb{Q}/\mathbb{Z})'$ se escribe de la forma $\alpha = a/d$ con $a, d \in \mathbb{Z}$ tales que $(d, p) = 1$. Comprobamos que,

$$\forall s \in I_t \quad (\theta_d(s))^a = \left(\frac{s(x^{1/d})}{x^{1/d}}\right)^a = \frac{s(x^\alpha)}{x^\alpha}.$$

Por tanto, el carácter θ_d^a solo depende de α y no del representante. Por esto, llamamos $\chi_\alpha := \theta_d^a$.

Proposición 3.5. La aplicación $\alpha \mapsto \chi_\alpha$ es un isomorfismo de grupos entre $(\mathbb{Q}/\mathbb{Z})'$ y X.

Demostración. Por un lado,

$$(\mathbb{Q}/\mathbb{Z})' = \bigcup_{d\in\mathbb{N}\,:\,p\nmid d} \mathbb{Z}\left[\frac{1}{d}\right]/\mathbb{Z}.$$

Por otro lado, I_t es el límite inverso de los μ_d. Por tanto, X es el límite inductivo de $X_d = \mathrm{Hom}(\mu_d, k_s^*)$. De esta manera, basta ver que la aplicación $\alpha \mapsto \chi_\alpha$ es un isomorfismo de $\mathbb{Z}\left[1/d\right]$ en X_d.

Para ver esto, recordemos que μ_d se identifica con las raíces d-ésimas de la unidad que están en k_s. Por tanto, la imagen de todo homomorfismo $\phi : \mu_d \longrightarrow k_s^*$ tiene que estar contenida en las raíces d-ésimas de la unidad de k_s. Por tanto, solo hay d posibles homomorfismos y como θ_d es isomorfismo, sus potencias θ_d^a con $a \in \{0, \dots, d-1\}$ son todos los posibles. ∎

En virtud, de la proposición anterior, si $\psi \in X$, llamaremos invariante de ψ al elemento $\alpha \in (\mathbb{Q}/\mathbb{Z})'$ tal que $\psi = \chi_\alpha$. Por ejemplo el invariante de θ_d es $1/d$.

Observación 3.2. La componente p-primaria de $\mathbb{Q}/\mathbb{Z}$ es $\mathbb{Q}_p/\mathbb{Z}_p$. En efecto, un elemento de la componente p-primaria de $\mathbb{Q}/\mathbb{Z}$ es de la forma a/d con $p|d$ y $(a,d)=1$. Estos números claramente están en $\mathbb{Q}_p/\mathbb{Z}_p$. Recíprocamente, si $x \in \mathbb{Q}_p/\mathbb{Z}_p$ entonces, $x = \varepsilon/p^k$ con $\varepsilon \in \mathbb{Z}_p$ y $k > 0$. Por ser un entero p-ádico,

$$\varepsilon = \sum_{r=0}^{\infty} a_r p^r$$

Por lo que visto en $\mathbb{Q}_p/\mathbb{Z}_p$, $x = \sum_{r=0}^{k} a_{k-r}/p^r$ es una suma finita y, por tanto, lo podemos ver en $\mathbb{Q}/\mathbb{Z}$. Razonando de esta manera, se tienen las descomposiciones

$$\mathbb{Q}/\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p \oplus (\mathbb{Q}/\mathbb{Z})' \quad \text{y} \quad (\mathbb{Q}/\mathbb{Z})' = \oplus_{l\neq p}\mathbb{Q}_l/\mathbb{Z}_l.$$

En particular, tenemos una proyección canónica $\mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow (\mathbb{Q}/\mathbb{Z})'$, cuyo núcleo es $\mathbb{Z}[1/p]$. Por tanto, si $\alpha \in \mathbb{Q}$ podemos denotar por χ_α al carácter $\chi_{\alpha'}$ con α' la imagen de α en $(\mathbb{Q}/\mathbb{Z})'$ y así diremos que el invariante de χ_α es α módulo $\mathbb{Z}[1/p]$.

Ejemplo 3.1 (caracteres fundamentales). Sea $n \geq 1$ y sea $q = p^n$. Llamamos carácter fundamentales de nivel n a todo carácter obtenido al componer el carácter

$$\theta_{q-1} : I_t \longrightarrow \mathbb{F}_{q-1}^*$$

con un automorfismo del cuerpo $\mathbb{F}_{q-1}$. Como los automorfismos de $\mathbb{F}_{q-1}$ forman un grupo cíclico generado por el automorfismo de Frobenius $x \mapsto x^p$, los caracteres fundamentales son:

$$\theta_{q-1}, \theta_{q-1}^p, \dots, \theta_{q-1}^{p^{n-1}}.$$

De esta manera, hay n caracteres fundamentales y sus invariantes son $p^i/(q-1)$ con $i \in \{0, \dots, n-1\}$

3.1.5 Representación de G en $\mathcal{M}_\alpha$ / $\mathcal{M}_\alpha^+$

Sabemos que la valoración discreta v de K se puede prolongar a $\overline{K}$ de manera única (teorema A.3). En particular, $v(\overline{K}^*) = \mathbb{Q}$. Si $\alpha \in \mathbb{Q}$, denotamos

$$\begin{aligned} \mathcal{M}_\alpha &= \{x \in \overline{K} : v(x) \geq \alpha\}, \\ \mathcal{M}_\alpha^+ &= \{x \in \overline{K} : v(x) > \alpha\}. \end{aligned}$$

De esta manera, $V_\alpha := \mathcal{M}_\alpha / \mathcal{M}_\alpha^+$ es un espacio vectorial de dimensión 1 sobre el cuerpo residual $\overline{k}$ de $\overline{K}$. El grupo G actúa sobre V_α de manera natural: para todo $\sigma \in G$ y para todo $x \in \mathcal{M}_\alpha$,

$$x + \mathcal{M}_\alpha^+ \mapsto \sigma(x) + \mathcal{M}_\alpha^+$$

Cabe preguntarse si esta acción respeta la estructura de espacio vectorial de V_α. La respuesta es que no. Sin embargo sí que hay cierta relación entre la acción y la estructura de espacio vectorial. Dicha relación nos la da la siguiente proposición.

Proposición 3.6. Sea $\sigma \in G$, y denotemos por $\overline{\sigma} \in G_k := \mathrm{Gal}(\overline{k}|k)$ a su reducción. Entonces,

$$\forall x + \mathcal{M}_\alpha^+ \in V_\alpha, \forall \lambda \in \overline{k} \quad \sigma(\lambda \cdot (x + \mathcal{M}_\alpha)) = \overline{\sigma}(\lambda) \cdot \sigma(x + \mathcal{M}_\alpha^+)$$

En particular, si $\sigma \in I$, el automorfismo que define sobre V_α es $\overline{k}$-lineal.

Demostración. Escribimos $\lambda = a + \mathcal{M}$ y usando las definiciones anteriores comprobamos que:

$$\begin{aligned} \sigma(\lambda \cdot (x + \mathcal{M}_\alpha^+) &= \sigma(ax + \mathcal{M}_\alpha^+)) = \sigma(ax) + \mathcal{M}_\alpha = \sigma(a)\sigma(x) + \mathcal{M}_\alpha^+ \\ &= (\sigma(a) + \mathcal{M}_\alpha) \cdot (\sigma(x) + \mathcal{M}_\alpha^+) = \overline{\sigma}(\lambda) \cdot \sigma(x + \mathcal{M}_\alpha^+). \end{aligned}$$

Por último, basta recordar que si $\sigma \in I$, entonces $\overline{\sigma}$ es la identidad, por definición del grupo de inercia. ∎

La proposición anterior nos dice que I actúa sobre V_α. Como V_α tiene dimensión 1, la acción viene dada por un carácter $\varphi_\alpha : I \longrightarrow \overline{k}^*$, de manera que

$$\forall \sigma \in I, \forall x \in V_\alpha \quad \sigma(x) = \varphi_\alpha(x)x.$$

Además, la imagen de I_p es trivial. En efecto, por definición,

$$\ker(\varphi_\alpha|_{I_p}) = \{\sigma \in I_p : \forall x \in \mathcal{M}_\alpha, \quad v(\sigma(x) - \varphi_\alpha(\sigma)(x)) > \alpha\}.$$

Este conjunto es cerrado para la topología de Krull, ya que si $\sigma \notin \ker(\varphi_\alpha|_{I_p})$, existe $x \in \mathcal{M}_\alpha$ tal que $v(\sigma(x) - \varphi_\alpha(\sigma)(x)) \leq \alpha$. Elegimos $F|K_t$ una extensión finita tal que $x \in F$ y $\sigma\,\mathrm{Gal}(\overline{K}|F)$ es un entorno abierto de σ disjunto con $\ker(\varphi_\alpha|_{I_p})$. Por tanto, por el teorema de correspondencia de Galois 1.1, $\ker(\varphi_\alpha|_{I_p}) = \mathrm{Gal}(\overline{K}|L)$ para $L|K_t$ una extensión de Galois. De esta manera,

$$I_p/\ker(\varphi_\alpha|_{I_p}) \simeq \mathrm{Gal}(L|K_t)$$

Ahora bien, todo $\sigma \in \mathrm{Gal}(L|K_t)$ de orden finito es de orden una potencia de p, ya que I_p es un límite inverso de p-grupos. Ahora bien, $\varphi_\alpha(I_p) \subset \overline{k}^*$ y, por tanto, por el primer teorema de isomorfía, todos los elementos de $\mathrm{Gal}(L|K_t)$ son de orden finito y como $\overline{k}^*$ no contiene elementos de orden p,

$$\mathrm{Gal}(L|K_t) = \{\mathrm{Id}\}.$$

Lo que equivale a que la imagen de I_p por φ_α sea trivial. Por tanto, el carácter viene determinado por la imagen del grupo de inercia moderada.

Proposición 3.7. El carácter φ_α que viene dado por la acción de I_t sobre V_α es igual al carácter χ_α definido en el apartado 3.1.4.

Demostración. En primer lugar, si $\alpha, \beta \in \mathbb{Q}$ la aplicación,

$$\begin{aligned} \mathcal{M}_\alpha \times \mathcal{M}_\beta &\to \mathcal{M}_{\alpha+\beta} \\ (x, y) &\mapsto xy, \end{aligned}$$

induce un isomorfismo cuando pasamos al cociente entre $V_\alpha \otimes V_\beta$ y $V_{\alpha+\beta}$ que conmuta con la acción de G. Por tanto, $\varphi_{\alpha+\beta} = \varphi_\alpha \varphi_\beta$.

Por otro lado, sea d un entero positivo coprimo con p y sea x una raíz d-ésima de un parámetro de uniformización de K. Sabemos que

$$\forall s \in I_t, \quad s(x) = \theta_d(s)x.$$

Esta ecuación pasa al cociente en $V_{1/d}$ y como $v(x) = 1/d$ la clase de x es distinta de 0. Por lo que $\varphi_{1/d} = \theta_d = \chi_{1/d}$. Si elegimos $\alpha \in \mathbb{Q}$, existe una potencia de q de p tal que $q\alpha = a/d$ con $a \in \mathbb{Z}$ y d coprimo con p. Por la aditividad de φ y θ con respecto a α,

$$\varphi_\alpha^q = \varphi_{a/d} = (\varphi_{1/d})^a = (\chi_{1/d})^a = \chi_\alpha^q,$$

de lo que se deduce que $\varphi = \chi_\alpha$ ya que I_t no tiene p-torsión. ∎

Ejemplo 3.2 (Acción de I_t sobre μ_p). Supongamos que K tiene característica 0. Sea μ_p el grupo de las raíces p-ésimas de la unidad en $\overline{K}$. El grupo G actúa sobre μ_p y esto nos da una representación:

$$\rho : I \to \mathrm{Aut}(\mu_p) = \mathbb{F}_p^*.$$

Como $\mathbb{F}_p^*$ tiene dimensión 1, la representación es simple. Por tanto, $\rho(I_p) = \{\mathrm{Id}\}$. Pasando al cociente, tenemos

$$\chi : I_t \to \mathbb{F}_p^*.$$

Proposición 3.8. El carácter χ es la potencia e-ésima del carácter fundamental θ_{q-1} de nivel 1, con $e = v(p)$.

Demostración. Sea $\alpha = e/(p-1)$. Si $z \in \mu_p$, con $z \neq 1$, se tiene que $v(z^r-1) = v(z-1)$ para $r \leq p-1$. En efecto,

$$\frac{z^r - 1}{z - 1} = \sum_{i=0}^{r} z^i$$

es una unidad y, por tanto, $v(z^r - 1) - v(z - 1) = 0$. De esta manera, consideramos

$$\Phi(x) = \prod_{i=1}^{p-1}(x - z^i) = \sum_{i=0}^{p-1} x^i,$$

ponemos $x = 1$ y tomamos valoraciones,

$$e = v(p) = v(\Phi(1)) = \sum_{i=0}^{p-1} v(1 - z^i) = (p-1)v(z-1).$$

Por tanto, $v(z-1) = e/(p-1) = \alpha$. Esto implica que la aplicación $z \mapsto z-1$ induce un homomorfismo inyectivo de μ_p en V_α que conmuta con la acción de G y, en particular, con la acción de I_t. El resultado se deduce ahora de la proposición 3.7, ya que I_t actúa sobre V_α mediante el carácter $\chi_\alpha = \theta_{p-1}^e$.

Corolario 3.2. Si $e = 1$, entonces $\chi = \theta_{p-1}$.

3.1.6 Representación de G definida por un grupo formal (caso $e = 1$)

En esta sección vamos a suponer que $e = 1$, i.e. que p es un parámetro de uniformización de K. Denotaremos por $\overline{R}$ al anillo de enteros de $\overline{K}$ y a $\overline{\mathcal{M}}$ el ideal maximal de $\overline{R}$.

Consideraremos una ley de grupo formal con coeficientes en R

$$F(X, Y) = X + Y + \sum_{i=1}^{\infty} c_{i,j} X^i Y^j, \quad c_{i,j} \in R.$$

Así, denotamos por,

$$[p](X) = \sum_{i=1}^{\infty} a_i X^i, \quad a_i \in R,$$

a la multiplicación por p con respecto a la ley F. Supondremos además que que F es de altura h, esto es, si ponemos $q = p^h$ la ley F cumple que,

$$a_i \equiv 0 \mod \mathcal{M} \quad \forall i < q \quad \text{y} \quad a_q \not\equiv 0 \mod \mathcal{M}.$$

De esta manera, la reducción módulo $\mathcal{M}$ de $[p]$ comienza por un término en X^q. Denotamos por V al kernel de $[p]$, i.e.

$$V = \{x \in \overline{\mathcal{M}} : [p](x) = 0\}.$$

Así, V es un $\mathbb{F}_p$-espacio vectorial donde la suma viene definida por la operación del grupo formal $\oplus_F$ y el producto escalar viene definido por $a \cdot x := [a]x$. La dimensión de este espacio se puede calcular a partir de la ley de grupo formal. Para ello vamos a necesitar el siguiente resultado.

Teorema 3.1 (de preparación de Weiestrass). *Sea A un anillo local completo. Si $f \in A[\![X]\!]$ es una serie de potencias tal que uno de sus coeficientes es una unidad de A, entonces existe una única unidad $u \in A[\![X]\!]$ y un único polinomio distinguido $g \in A[X]$, i.e. de la forma*

$$a_0 + a_1 X + \cdots + a_{q-1} X^{q-1} + X^q, \text{ con los } a_i \in \mathcal{M},$$

tales que $f = ug$.

Demostración. La prueba se puede encontrar en ([4] IV.2). ∎

Teorema 3.2. *V es un espacio vectorial de dimensión igual a la altura del grupo formal $F(X, Y)$.*

Demostración. Podemos aplicar el teorema de preparación de Weiestrass para R_K. De manera que existen una única unidad $u(X) \in R_K[\![X]\!]$ y un único polinomio distinguido $g(X) \in R_K[X]$ tales que:

$$[p](X) = u(X)g(X).$$

Esto implica que V y $\{x \in \overline{K} : g(x) = 0\}$ coinciden. En efecto, si $x \in \mathcal{M}$ y $[p](x) = 0$, necesariamente $u(x) \cdot g(x) = 0$. Pero $u(x)$ es siempre una unidad R_K pues es la suma del término independiente y de un elemento de $\mathcal{M}$. Luego, $u(x) \neq 0$, y por tanto $g(x) = 0$.

Recíprocamente, sea $x \in \overline{K}$ tal que $g(x) = 0$. Como $g(X)$ es distinguido, es de la forma

$$a_0 + a_1 X + \cdots + a_{q-1} X^{d-1} + X^d, \text{ con los } a_i \in \mathcal{M}.$$

Además, tenemos que $x^d = -(a_{d-1}x^{d-1} + \cdots + a_0) \in \overline{\mathcal{M}}$. Por tanto, $x \in \overline{\mathcal{M}}$. Por otro lado, trivialmente $[p](x) = 0$.

Además, el grado del polinomio $g(X)$ es $p^{\mathrm{ht}(F)}$. En efecto, $p^{\mathrm{ht}(F)}$ es el grado del primer monomio nonulo cuando vemos $[p](X)$ en el cuerpo residual. Como $[p] = ug$ y u es una unidad, al pasar al cociente el primer término no nulo de $[p]$ tiene que coincidir en grado con el primer término no nulo de g, pero g es un polinomio distinguido por lo que dicho término es X^d.

Basta ahora probar que V tiene cardinal $p^{\mathrm{ht}(F)}$. Para ello, basta ver que g tiene $p^{\mathrm{ht}(F)}$ raíces en $\overline{K}$, i.e. g no tiene raíces dobles.

De esta manera, supongamos que $g(x) = 0$, y veamos que $g'(x) \neq 0$. Derivando $[p]'(X) = u'(X)g(X) + u(X)g'(X)$, y, por tanto, tenemos que

$$[p]'(x) = u(x)g'(x).$$

Como $[p]$ es un morfismo de grupos formales,se tiene que

$$[p](F(X,Y)) = F([p](X), [p](Y)).$$

Derivando respecto a Y esta expresión obtenemos,

$$[p]'(F(X,Y))F_Y(X,Y) = F_Y([p](X), [p](Y))[p]'(Y).$$

Ponemos $X = x$ e $Y = 0$ y obtenemos,

$$[p]'(X)F_Y(x,0) = F_Y([p](x), [p](0))[p]'(0).$$

Además, tenemos que $[p](0) = 0$ y, como $g(x) = 0$, $[p](x) = 0$. Por tanto,

$$[p]'(x)F_Y(x,0) = F_Y(0,0)[p]'(0) = [p]'(0) = p \neq 0,$$

luego $[p]'(x) \neq 0$.

De esta manera, podemos dotar a V de una estructura de $\mathbb{F}_p$-espacio vectorial de dimensión h. Además, G actúa de manera natural sobre V, por lo que estamos en la misma situación del apartado 3.1.3.

Proposición 3.9. Existe una estructura para V de $\mathbb{F}_q$-espacio vectorial de dimensión 1 tal que tiene las siguientes propiedades:

a) Sean $\sigma \in G$, $\overline{\sigma} \in \mathrm{Gal}(k_s|k)$ su reducción y $\overline{\sigma}_q$ la restricción de $\overline{\sigma}$ a $\mathbb{F}_q$. El automorfismo de V definido por σ es $\overline{\sigma}_q$-lineal.
b) El grupo I_p actúa trivialmente sobre V y el grupo $I_t = I/I_p$ actúa mediante el carácter fundamental $\theta_{q-1} : I_t \longrightarrow \mathbb{F}_q^*$ de nivel h.

Demostración. Sea x un elemento no nulo de V. Este cumple,

$$p + a_2 x + \cdots + a_q x^{q-1} + \cdots = 0.$$

Además, $v(x) > 0$ y como los $a_i \in R$,

$$\begin{aligned} \forall 1 < i < q, \quad v(a_i) &\geq 1, \\ \forall i \geq q, \quad v(a_i) &= 0. \end{aligned}$$

La valoración del sumando con coeficiente a_q es estrictamente superior a la de los sumandos siguientes. Como la suma es 0 este término debe cancelarse con alguno de los $q-1$ sumandos anteriores anteriores. Ahora bien, el primer sumando tiene una valoración menor que los $q-2$ siguientes, por lo que no puede cancelar con ninguno de ellos. De lo que se deduce que $v(p) = v(a_q x^{q-1})$, ya que en caso contrario $1 = v(p) \geq q v(x)$, lo cual implica $(q-1)v(x) < 1$ y esto es imposible pues entonces el sumando $a_q x^{q-1}$ no cancelaría. Por tanto, $v(x) = 1/q - 1$.

Ponemos ahora $\alpha = 1/q - 1$ y consideramos la aplicación

$$\begin{aligned} V \subset \overline{\mathcal{M}}_\alpha &\longrightarrow V_\alpha = \overline{\mathcal{M}}_\alpha / \overline{\mathcal{M}}_\alpha^+ \\ x &\longmapsto x + \overline{\mathcal{M}}_\alpha^+. \end{aligned}$$

Esta es inyectiva, pues acabamos de ver que si $x \in V$, su valoración es $v(x) = \alpha$. Además, la aplicación es un homomorfismo de grupos, ya que la ley de grupo formal era de la forma

$$F(X, Y) = X + Y + \text{términos de grado} \geq 2.$$

Por tanto, si $x, y \in V$,

$$F(x, y) \equiv x + y \mod \overline{\mathcal{M}}_\alpha^+.$$

Además, se tiene de manera inmediata que este homomorfismo conmuta con la acción de G, por lo que I_p actúa trivialmente sobre V. Así, identificando V con su imagen en V_α la proposición 3.7 nos prueba que I_t actúa sobre V mediante

$$\forall s \in I_t, \forall x \in V \quad s(x) = \theta_{q-1}(s)x.$$

Como $\theta_{q-1} : I_t \longrightarrow \mathbb{F}_q$ es sobreyectiva, V queda fijo mediante la multiplicación por elementos de $\mathbb{F}_q^*$. Por tanto, V es un $\mathbb{F}_q^*$-subespacio vectorial de V_α. Además, sabíamos

que $\#V = q$, por lo que V es de dimensión 1. En esta situación el primer apartado se deduce de 3.6 y el segundo de 3.7.

Corolario 3.3. La imagen de I_t en $\mathrm{GL}(V)$ está formada por las homotecias $\{x \mapsto \lambda x : \lambda \in \mathbb{F}_q^*\}$ y es un grupo cíclico de orden $q-1$

Demostración. Se deduce del resultado anterior y de que $\theta_{q-1} : I_t \longrightarrow \mathbb{F}_q^*$ es sobreyectivo.

Para el siguiente corolario recordamos la definición de aplicación semilineal.

Definición 3.3. *Sea $T : V \longrightarrow W$ una aplicación entre dos F-espacios vectoriales con F un cuerpo. Decimos que T es semilineal si existe $\sigma \in \mathrm{Aut}(F)$ tal que:*

a) $\forall v, v' \in V \quad T(v+v') = T(v) + T(v')$
b) $\forall \lambda \in F, \forall v \in V \quad T(\lambda \cdot v) = \sigma(\lambda) \cdot T(v)$

Corolario 3.4. Supongamos que $k = \mathbb{F}_p$. La imagen de G en $\mathrm{GL}(V)$ está formada por todos los automorfismos semilineales del $\mathbb{F}_q$-espacio vectorial V, es decir, la imagen es el normalizador de un subgrupo de Cartan.

Demostración. Sabemos que $q = p^r$, por la proposición anterior sabemos que si $\sigma \in G$, $x \in V$, $\lambda \in \mathbb{F}_{p^2}$,

$$\sigma(\lambda x) = \overline{\sigma}(\lambda)\sigma(x),$$

donde $\overline{\sigma} \in \mathrm{Gal}(\overline{k}|k)$ es la reducción de σ. Sabemos que los automorfismos de $\mathbb{F}_q$ son el grupo generado por el automorfismo de Frobenius ϕ_q. De manera que si $\sigma \in G$, entonces

$$\sigma(\lambda x) = \lambda^{q^i} x \text{ con } i \in \{1, \dots, r\},$$

con r tal que $p^r = q$. Como la reducción al cuerpo residual es sobreyectiva, hemos terminado.

3.2 Torsión de curvas elípticas sobre un cuerpo local

En esta sección supondremos además que K es un cuerpo de característica 0. Sea E/K una curva elíptica, en esta sección vamos a estudiar la imagen del grupo de inercia por la representación del grupo de Galois sobre los puntos de l-torsión. Para empezar, podemos hacer algunas observaciones generales sin necesidad de suponer que la curva tiene buena reducción.

Como ya vimos en el capítulo 2,

$$E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Por tanto, $E[p]$ es un $\mathbb{F}_p$-espacio vectorial de dimensión 2 sobre el que actúa el grupo G, lo que da lugar a la representación ρ_p. Una primera observación que podemos hacer es la siguiente:

Por la linealidad del pairing de Weil e_p, tenemos que:

$$\forall P, Q \in E[p] \quad e_p\left(\rho_p(\sigma)(P), \rho_p(\sigma)(Q)\right) = e(P,Q)^{\det(\rho_p(\sigma))}.$$

Pero, por la compatibilidad de la acción de G con el pairing de Weil,

$$\forall P, Q \in E[p] \quad \sigma(e_p(P,Q)) = e_p\left(\rho_p(\sigma)(P), \rho_p(\sigma)(Q)\right) = e\,(P,Q)^{\det(\rho_p(\sigma))}$$

El pairing de Weil,

$$e_p : E[p] \times E[p] \longrightarrow \mu_p$$

es sobreyectivo por ser no degenerado. Por tanto, si denotamos por ζ_p a una raíz primitiva p-ésima de la unidad,

$$\sigma(\zeta_p) = \zeta_p^{\det(\rho_p(\sigma))},$$

Por tanto, el carácter dado por la acción natural de G sobre μ_p viene dado por el determinante del pairing de Weil. Si consideramos la restricción de este carácter a I_t, por la proposición 3.8, es la potencia e-ésima de θ_{p-1}, el carácter fundamental de nivel 1.

Añadimos ahora la hipótesis de que E tiene buena reducción sobre R_K. En primer lugar el criterio de Néron-Ogg-Shafarevich (2.11) nos dice que la imagen del grupo de inercia es trivial para las representaciones asociadas los primos $l \neq p$. Por tanto, nos podemos centrar solo en el caso $l = p$. Como la curva tiene buena reducción podemos elegir un modelo de Weiestrass de la forma:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

con $a_i \in R$, y $\Delta = \Delta(a_1, \cdots, a_6) \in R^*$. Como la curva es de buena reducción, tenemos que $E_0 = E$ y $\tilde{E}_{ns}(\overline{k}) = \tilde{E}(\overline{k})$ Recordemos que en estas condiciones, tenemos la sucesión exacta

$$0 \longrightarrow E_1 \longrightarrow E \longrightarrow \tilde{E} \longrightarrow 0.$$

Además esta sucesión exacta es compatible con la acción del grupo de Galois. En efecto, si $[x : y : z] \in E$ cumple que las tres coordenadas están en el anillo de valoración y al menos una es una unidad, el punto $P^\sigma = [\sigma(x) : \sigma(y) : \sigma(z)]$ cumple la misma propiedad, debido a que como K es completo el grupo de Galois respeta la valoración (proposicón A.17). De esta manera, podemos reducir los puntos aplicando la reducción a las coordenas, i.e.

$$\widetilde{P^\sigma} = [\widetilde{\sigma(x)} : \widetilde{\sigma(y)} : \widetilde{\sigma(z)}], \quad \tilde{P} = [\tilde{x} : \tilde{y} : \tilde{z}].$$

Por tanto, si denotamos por $\overline{\sigma} \in G_k$ a la reducción de σ, se tiene que:

$$\widetilde{(P^\sigma)} = \tilde{P}^{\overline{\sigma}}$$

El siguiente resultado nos permite dividir nuestro estudio según si el grupo formal de la curva tiene altura 1 o 2.

Proposición 3.10. Sea K un cuerpo local de característica residual p y E/K una curva elíptica. Si llamamos k al cuerpo residual, se tienen que:

a) Los siguientes son equivalentes
   a) $\tilde{E}([p^r] = 0$ para cada $r \geq 1$.
   b) La altura del grupo $\hat{E}/K$ es 2.

b) Si alguno de los puntos anteriores no se da, entonces

$$\tilde{E}[p^r] \cong \mathbb{Z}/p\mathbb{Z}$$

y el grupo formal $\hat{E}/K$ tiene altura 1.

Demostración. La prueba de este resultado requiere presentar una gran cantidad de herramientas que no vamos a añadir por cuestiones de espacio. La prueba se puede encontrar en ([10] V.3.1). ∎

3.2.1 Representación de G definida sobre una curva elíptica con buena reducción de altura 1

En este apartado supondremos que el grupo formal de la curva tiene altura 1. En este caso, el grupo de puntos de p-torsión de la curva es cíclico de orden p por la proposición 3.11. Vamos a estudiar como actúa el grupo de inercia sobre los puntos de p-torsión se la curva. Sea $\sigma \in I$. Sea $P = (x : y : z) \in E$. Por definición del grupo

de inercia $v(\sigma(x)-x), v(\sigma(y)-y), v(\sigma(z)-z) > 0$. Por tanto, $\widetilde{\sigma(x)} = \tilde{x}, \widetilde{\sigma(y)} = \tilde{y}$ y $\widetilde{\sigma(z)} = \tilde{z}$.

Por otro lado, si el punto P se reduce a $\mathcal{O}$, entonces para cada $\sigma \in G$ el punto P^σ también. En efecto, que P se reduzca al origen significa que $v(x), v(z) > 0$ y $v(y) = 0$. Ahora bien, como K es completo $v(\sigma(x)) = v(x), v(\sigma(y)) = v(y)$ y $v(\sigma(z)) = v(z)$, por la proposición A.17, P^σ también se reduce al punto $\mathcal{O}$. Hemos probado que el grupo de puntos que se reducen al origen es estable por la acción del grupo de Galois.

Podemos restringir la aplicación de reducción a los grupos de p-torsión,

$$E[p] \longrightarrow \widetilde{E}[p].$$

Sin embargo, no es evidente que esta aplicación siga siendo sobreyectiva. El siguiente resultado nos prueba que sí y además nos permitirá entender mucho mejor la acción del grupo de inercia.

Proposición 3.11. Sea K un cuerpo local de característica residual p, y sea E/K una curva elíptica con buena reducción de altura 1. Entonces tenemos una sucesión exacta

$$0 \longrightarrow X_p \longrightarrow E[p] \longrightarrow \widetilde{E}[p] \longrightarrow 0$$

donde $X_p \subset E[p]$ es un grupo (cíclico) de orden p.

Demostración. Es suficiente probar que la aplicación,

$$E[p] \longrightarrow \widetilde{E}[p].$$

es sobreyectiva, ya que en ese caso X_p es el núcleo de esta aplicación. Por reducción al absurdo vamos a suponer que no es sobreyectiva. Como $\tilde{E}[p]$ es cíclico de orden p, todos sus elementos salvo el neutro son generadores. Por tanto, como estamos suponiendo que la reducción no es sobreyectiva, todos los puntos de p-torsión se reducen al punto $\widetilde{\mathcal{O}}$. Tenemos, por tanto, que $E[p] \subset E_1$ (ver la definición 2.1). Ahora bien, sabemos por la proposición 2.9 que $\hat{E}(\mathcal{M}) \cong E_1$. Este isomorfismo induce un isomorfismo entre $E[p]$ y $V = \ker[p] \subset \hat{E}(\mathcal{M})$.

Por tanto, $\#(V) = |E[p]| = p^2$, pero el cardinal de V es p elevado a la altura del grupo, por la proposición 3.2. Por tanto, la altura del grupo formal es 2 y estamos suponiendo que era 1, lo cual es una contradicción. ∎

Este resultado nos permite deducir de manera inmediata los siguientes corolarios.

Corolario 3.5. En las hipótesis de la proposición anterior, se puede elegir una base de $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ de forma que el primer punto de dicha base pertenezca a X_p y la imagen de G por ρ_p está contenida en un subgrupo de la forma:

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

Demostración. Este resultado se deduce de la proposición anterior y de que la acción del grupo de Galois es estable en E_1. En particular si $P \in X_p$, entonces $P^\sigma \in X_p$. ∎

Corolario 3.6. De nuevo, en las hipótesis de la proposición anterior, podemos elegir una base de de $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ de forma que el primer punto de dicha base pertenezca a X_p y la imagen del grupo de inercia por ϕ_p esté contenida en un subgrupo de la forma:

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

Demostración. Este resultado se deduce de que, como hemos visto antes, el grupo de inercia actúa trivialmente sobre $\widetilde{E}(\overline{k})$ y la sucesión exacta nos da que

$$\widetilde{E}(\overline{k}) \cong E[p]/X_p.$$

∎

Por último, también podemos decir algo sobre la imagen del grupo de inercia salvaje I_p.

Corolario 3.7. De nuevo, en las hipótesis de la proposición anterior, podemos elegir una base de de $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ de forma que el primer punto de dicha base pertenezca a X_p y la imagen del grupo de inercia salvaje está contenida en un subgrupo de la forma:

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

Demostración. Como el grupo de inercia salvaje o grupo de ramificación es el único p-grupo de Sylow de I (ver A.21), la imagen por ϕ_p es un p-grupo finito. Sea $\sigma \in I_p$, eligiendo la base como en la hipótesis tenemos que:

$$\rho_p(\sigma) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

y su orden es una potencia de p, de lo que se deduce el resultado inmediatamente. ∎

Acabamos de ver que las imagénes de los grupos G, I e I_p no pueden ser muy grandes. Además, al principio de la sección hemos visto, usando el pairing de Weil, un resultado que nos dice que la imagen no puede ser trivial. De hecho, uniendo los resultados anteriores sabemos que eligiendo adecuadamente una base y suponiendo que $e = v(p) = 1$, tenemos que la imagen del grupo de inercia está contenida en:

$$\begin{pmatrix} \theta_{p-1} & * \\ 0 & 1 \end{pmatrix}.$$

Más aún, bajo estas hipótesis podemos determinar completamente la imagen del grupo de inercia.

Proposición 3.12. Sea E/K una curva elíptica definida sobre un cuerpo local de característica residual p con buena reducción de altura 1. Supongamos además que $v(p) = 1$. Entonces, se tiene una y sólo una de las siguientes posibilidades:

a) I_p actúa trivialmente sobre $E[p]$, y la imagen de I tiene cardinal $p-1$. Eligiendo una base conveniente se tiene que:

$$\rho_p(I) \simeq \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}.$$

b) I_p no actúa trivialmente sobre $E[p]$. Entonces, la imagen de I_p es un grupo cíclico de orden p, que eligiendo una base conveniente se puede representar como:

$$\rho_p(I_p) \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Además, en este caso la imagen de I tiene cardinal $p(p-1)$, y se puede representar como

$$\rho_p(I) \simeq \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Demostración. Supongamos primero que I_p actúa trivialmente. Entonces, $\rho_p(I)$ no tiene elementos de orden p porque I_p es el único p-grupo de Sylow de I. Por lo visto en los corolarios anteriores $|\rho_p(I)|$ divide a $p(p-1)$ y como no tiene elementos de orden p, tiene que dividir a $p-1$. Ahora, bien el determinante de esta representación restringido al grupo de inercia es θ_{p-1} que es sobreyectivo. Por tanto, $|\rho_p(I)|$ tiene orden $p-1$. A partir de esto obtener la expresión matricial es inmediato.

Supongamos ahora que I_p no actúa trivialmente. Por los corolarios anteriores su imagen por ρ_p tiene que ser un grupo de orden p. El hecho de que la imagen del determinante de la representación sea sobreyectivo implica que el orden de la imagen del

grupo de inercia tiene que ser divisible por $p-1$. Por tanto, la imagen del grupo de inercia es todo el grupo:

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

3.2.2 Representación de G definida sobre una curva elíptica con buena reducción de altura 2

Suponemos ahora que la altura del grupo formal de la curva es 2. En este caso, la proposición 3.10 nos dice que $\tilde{E}[p] = 0$. En este caso, el isomorfismo

$$E_1 \longrightarrow \hat{E}(\overline{\mathcal{M}})$$

induce un isomorfismo entre

$$E[p] \longrightarrow V = \ker[p].$$

Además la acción del grupo sobre la curva y el grupo formal es compatible con el isomorfismo. Luego todo lo que sabemos sobre representaciones de un grupo formal lo podemos aplicar aquí. La siguiente proposición encapsula la información que el apartado 3.1.6 nos proporciona.

Proposición 3.13. En las hipótesis de este apartado, si suponemos que $e = v(p) = 1$. Se tiene que:

a) La acción de I_p sobre $E[p]$ es trivial.
b) Existe sobre $E[p]$ una estructura de $\mathbb{F}_{p^2}$-espacio vectorial de dimensión 1 tal que la acción de I_t viene dada por el carácter fundamental de θ_{p^2-1} de nivel 2.
c) La imagen de I en $\mathrm{GL}(E[p])$ es un grupo cíclico C de orden p^2-1 (subgrupo de Cartan no escindido).
d) La imagen de G en $\mathrm{GL}(E[p])$ es igual a C o al normalizador N de C, dependiendo de si k contiene o no contiene a $\mathbb{F}_{p^2}$.

Demostración. El resultado se deduce de la proposición 3.9 y los corolarios 3.3 y 3.4.

3.2.3 Reducción multiplicativa

En este apartado, E/K será una curva elíptica con mala reducción de tipo multiplicativo. De nuevo, vamos a hacer un estudio de la imagen del grupo de inercia por las representaciones ρ_l con l primo. La técnica que vamos a usar es muy similar a la usada en el caso de que la curva tuviera buena reducción de altura 1. Es decir, vamos a construir una sucesión exacta compatible con la acción de Galois:

$$0 \longrightarrow A_l \longrightarrow E[l] \longrightarrow B_l \longrightarrow 0,$$

donde A_l y B_l serán grupos abelianos de orden l. Para realizar esta construcción vamos a necesitar usar como herramienta la curva de Tate. Sin embargo, las técnicas necesarias para la construcción de la curva de Tate y el desarrollo de sus propiedades es algo que escapa a este trabajo. Por ello, nos limitaremos a dar los resultados que nos serán necesarios sin demostración.

Supongamos que K es un cuerpo local, completo respecto a una valoración v, de característica 0 y característica residual p. Consideramos la norma asociada v definida por

$$|x|_v = \begin{cases} (\#k)^{-v(x)}, & \text{para todo } x \in K^* \\ 0, & \text{si } x = 0 \end{cases} \tag{3.1}$$

Para cada $q \in K$ tal que $|q|_v < 1$ las series de potencias

$$a_4 := \sum_{n\geq 1} \frac{n^3 q^n}{1-q^n} \quad \text{y } a_6 := -\frac{1}{12} \sum_{n\geq 1} \frac{(7n^5+5n^3)q^n}{1-q^n}$$

son convergentes (ya que $|\cdot|_v$ es una norma no arquimediana, tenemos que $\left|\frac{1}{1-q^n}\right|_v = 1$ y $|n|_v \leq 1$ para todo $n \in \mathbb{N}$), y definen elementos $a_4, a_6 \in \mathcal{M}$.

De esta manera, a cada $q \in \mathcal{M}$ le podemos asociar un modelo de Weierstrass

$$E_q : y^2 + xy = x^3 + a_4 x + a_6.$$

Su discriminante es

$$\Delta = q \prod_{n\geq 1} (1-q^n)^2 4$$

Como $|q|_v < 1$, este producto infinito converge a un valor no nulo y, por tanto, esta curva es una curva elípitica. A esta curva se la denomina la curva de Tate asociada a q.

A cada curva elíptica con reducción multiplicativa E/K se puede asociar una curva de Tate E_q que sea isomorfa a ella sobre alguna extensión algebraica de K. El desarrollo de esta correspondencia se puede encontrar en ([11] V.5.3, V.5.4). Los resultados que nos interesan a nosotros sobre las curvas de Tate son los siguientes.

Proposición 3.14. Sea E/K una curva elíptica definida sobre un cuerpo local de característica 0 con mala reducción de tipo multiplicativo. Entonces, existe $q \in \mathcal{M}$ tal que si E_q es la curva de Tate correspondiente y c_4 y c_6 son las cantidades habituales asociadas a un modelo de Weiestrass de E_q, entonces las curvas E y E_q son isomorfas sobre la extensión

$$L = K\left(\sqrt{\frac{-c_4}{c_6}}\right).$$

Además, en caso de que $[L : K] = 2$, la extensión es no ramificada y si denotamos por

$$\varepsilon : G \longrightarrow \mathrm{Gal}(L|K) \simeq \{\pm 1\}$$

al carácter asociado a la extensión $L|K$, entonces existe un isomorfismo $\psi : E \longrightarrow E_q$ tal que

$$\psi(P^\sigma) = \varepsilon(\sigma)\psi(P)^\sigma,$$

para todo $\sigma \in G$ y para todo $P \in E(\overline{K})$.

Demostración. ([11] V.5.3) ∎

Proposición 3.15. Sea K un cuerpo completo respecto a una valoración discreta , y $q \in K^*$ tal que $|q| < 1$. Denotamos por $q^{\mathbb{Z}}$ al subgrupo de K^* generado por las potencias de q. Entonces, la aplicación

$$\begin{array}{rcll} \phi : \overline{K}^*/q^{\mathbb{Z}} & \longrightarrow & E_q(\overline{K}) & \\ u & \mapsto & (x(u,q), y(u,q)) & \text{si } u \notin q^{\mathbb{Z}} \\ u & \mapsto & \mathcal{O} & \text{si } u \in q^{\mathbb{Z}} \end{array}$$

donde

$$\begin{aligned} x(u,q) &= \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{nq^n}{1-q^n} \\ y(u,q) &= \sum_{n\in\mathbb{Z}} \frac{q^{2n}u^2}{(1-q^n u)^3} + \sum_{n\geq 1}\frac{nq^n}{1-q^n}, \end{aligned}$$

está bien definida, y es un isomorfismo de grupos. Además, es compatible con la acción del grupo de Galois (como $q \in K$, los elementos de $\mathrm{Gal}(\overline{K}|K)$ dejan fijo q y, por tanto, actúan sobre el cociente $\overline{K}$):

$$\forall [z] \in K^*/q^{\mathbb{Z}}, \quad \phi\left(\sigma([z])\right) = \sigma(\phi([z])).$$

Pasamos ya a estudiar la imagen del grupo de inercia en este caso. Vamos a estudiar primero los puntos de l-torsión de una curva de Tate. Sea $q \in K^*$ tal que $|q| < 1$, y E_q la curva de Tate asociada. La proposición anterior nos proporciona un isomorfismo

$$\phi : \overline{K}^*/q^{\mathbb{Z}} \longrightarrow E_q(\overline{K}).$$

Por otro lado consideramos la multiplicación por l dentro de la curva,

$$[l] : E_q \longrightarrow E_q,$$

y la siguiente aplicación

$$\psi : \overline{K}^*/q^{\mathbb{Z}} \longrightarrow \overline{K}^*/q^{\mathbb{Z}}$$

consistente en elevar a l, i.e. definida por

$$[z] \mapsto [z^l].$$

De esta manera, ϕ induce un isomorfismo entre $\ker \psi$ y $\ker[l]$. Como consecuencia de esto podemos construir la sucesión exacta que buscábamos

Proposición 3.16. Sean K un cuerpo local de característica 0, $q \in K^*$ un elemento con $|q| < 1$ y E_q/K la correspondiente curva de Tate. Sea l un primo. Entonces, se tiene una sucesión exacta de grupos abelianos

$$0 \longrightarrow \mu_l \longrightarrow E[l] \longrightarrow \mathbb{Z}/l\,\mathbb{Z} \longrightarrow 0,$$

donde μ_l denota el grupo de las raíces l-ésimas de la unidad en $\overline{K}^*$.

Demostración. Consideramos $\mu_l \subset \overline{K}^*$. Como todas las raíces de la unidad tienen valoración cero (equivalentemente norma 1) tenemos que μ_l se inyecta en $\overline{K}^*/q^{\mathbb{Z}} \simeq E[l]$.

Por otro lado, definimos $\psi_2 : E[l] \longrightarrow \mathbb{Z}/l\,\mathbb{Z}$ como sigue. Para cada $[z] \in E[l] \subset \overline{K}^*/q^{\mathbb{Z}}$, se tiene que $z^l \in q^{\mathbb{Z}}$, i.e. existe c tal que $z^l = q^c$ para algún $c \in \mathbb{Z}$. De esta manera, definimos $[z] \mapsto c + l\,\mathbb{Z}$.

Esta aplicación está bien definida, en efecto, si $[z] = [w]$, entonces $w = q^a z$ para algún $a \in \mathbb{Z}$. Entonces, $w^l = q^{la+c}$ y, por tanto, $c + al \equiv c \mod l$.

Es inmediato que esta aplicación es morfismo de grupos y además es sobreyectiva, ya que $z^{c/l} \mapsto c + l\,\mathbb{Z}$.

Solo falta comprobar la exactitud en el centro de la sucesión. La contención $\mathfrak{I}(\phi) \subset \ker \psi_2$ es inmediata del hecho de que si $\zeta \in \mu_l$ entonces $\zeta^l \equiv 1 = q^0$. Recíprocamente, sea $[z] \in \ker(\psi_2)$ entonces $z^l = q^{la}$. Por tanto, existe alguna raíz l-ésima de la unidad ζ tal que $z = \zeta q^a$. Por tanto, $[z] = [\zeta_l]$.

Con la sucesión exacta ya construida, tenemos que ver cómo se comporta con respecto a la acción del grupo de Galois. Por un lado, vimos en la proposición 3.8 que el grupo de Galois actúa sobre μ_l mediante θ^e_{l-1}. Además, G actúa sobre $\overline{K}^*$ de la manera natural. De hecho, se tiene que, para cada $\zeta_l \in \mu_l$,

$$\sigma(\psi_1(\zeta_l)) = \sigma([\zeta_l]) = [\sigma(\zeta_l)] = \psi_1(\sigma(\zeta_l)).$$

Es decir, $\sigma \circ \psi_1 = \psi_1 \circ \sigma$.

Veamos qué sucede con ψ_2. Sean $\sigma \in G$ y $[z] \in E[l]$, supongamos que $z^l = q^c$. Entonces, como $q \in K$, $\sigma(q) = q$ y $\sigma(z)^l = \sigma(z^l) = \sigma(q^c) = q^c$, se tiene que $\psi_2(\sigma([z])) = \psi_2([z])$. Por tanto, si consideramos la acción trivial de G sobre $\mathbb{Z}/l\mathbb{Z}$, el homomorfismo ψ_2 conmuta con la acción de G.

De esta manera, podemos proceder como en el caso de buena reducción de altura 1. Tenemos el siguiente resultado:

Proposición 3.17. Sean K un cuerpo local de característica 0, $q \in K^*$ tal que $|q| < 1$, E_q/K la correspondiente curva de Tate y l primo. Entonces, existe una base de $E[l]$ tal que la imagen de ρ_l está contenida en un subgrupo de la forma

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Demostración. Se deduce directamente de la compatibilidad de la sucesión exacta que nos da la proposición anterior con el grupo de Galois, de que μ_l es es estable por la acción de G y de que G actúa trivialmente sobre $\mathbb{Z}/l\mathbb{Z}$.

Para continuar vamos a dividir en dos casos: cuando $l \neq p$ y cuando $l = p$. En primer lugar, supongamos que $l \neq p$.

Proposición 3.18. En las hipótesis anteriores, $\rho_l(I)$ es o bien trivial o bien cíclico de orden l. El primer caso se dará si, y sólo si, K_{nr} contiene una raíz l-ésima de q. En ambos casos, $\rho_l(I_p)$ es trival.

Demostración. Sean ζ_l una raíz l-ésima de la unidad y $q^{1/l}$ una raíz l-ésima de q. Si tomamos como base $\{[\zeta_l], [q^{1/l}]\}$ de $E[l]$, tenemos que la imagen de ρ_l está contenida

en

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Ahora bien, las raíces l-ésimas de la unidad para $p \neq l$ están en K_{nr} por el lema de Hensel. Por tanto, la imagen del grupo de inercia está contenida en un subgrupo de la forma

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

La imagen del grupo de inercia será trivial si, y sólo si, I deja invariante a $q^{1/l}$. Lo cual es equivalente a que $q^{1/l} \in K_{nr}$. Por último, $\rho_l(I_p)$ tiene que tener orden una potencia de p y, por tanto, tiene que ser trivial.

Pasamos al caso en que $l = p$. Este es análogo al caso de buena reducción de altura 1. En efecto, se tienen los siguientes resultados

Proposición 3.19. Sea K un cuerpo local de característica 0 y característica residual p. Sean $q \in K^*$ un elemento tal que $|q| < 1$ y E_q/K la correspondiente curva de Tate. Entonces, existe una base de manera que la imagen del grupo I_p por ρ_p está contenida en un subgrupo de la forma

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Demostración. La demostración de este resultado es exactamente la misma que la del corolario 3.7.

Proposición 3.20. En las hipótesis de la proposición anterior, si $v(p) = 1$ entonces se da uno, y sólo uno, de los siguientes casos:

a) I_p actúa trivialmente sobre $E_q[p]$ y la imagen de I tiene cardinal $p-1$. Eligiendo una base adecuada,

$$\rho_p(I) \simeq \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}.$$

b) I_p no actúa trivialmente sobre $E_q[p]$. Entonces, $\rho_p(I_w)$ es un grupo cíclico de orden p y eligiendo una base conveniente,

$$\rho_p(I_p) \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Además en este caso $\rho_p(I)$ tiene orden $p(p-1)$ y, eligiendo una base conveniente, se tiene que

$$\rho_p(I) \simeq \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Demostración. La prueba de este resultado es exactamente la misma que la de 3.12. ∎

Con esta proposición termina nuestro análisis de la imagen del grupo de inercia de la representación asociada a la torsión de una curva de Tate. Sea ahora E/K una curva elíptica con reducción multiplicativa. Sabemos que existe $q \in \mathcal{M}$ tal que la curva de Tate E_q y la curva E son isomorfas sobre una extensión cuadrática $L|K$ por la proposición 3.14. Llamamos $\psi : E_q \longrightarrow E$ a ese isomorfismo.

En caso de que E y E_q sean isomorfas sobre K, se comprueba directamente, gracias a que $\psi(P)^\sigma = \psi(P^\sigma)$, que la imagen del grupo de inercia de la representación asociada a los puntos de $E[l]$ es la misma que la de $E_q[l]$.

En caso de que no sean isomorfas sobre K, tenemos que ψ cumple que

$$\forall P \in E_q, \forall \sigma \in G \quad \psi(P^\sigma) = \varepsilon(\sigma)\psi(P)^\sigma,$$

donde

$$\varepsilon : G \longrightarrow \mathrm{Gal}(L|K) \simeq \{\pm 1\}$$

es el carácter asociado a $L|K$. Por tanto, la imagen del grupo de inercia en este caso es la misma que la del caso de E_q, salvo que está multiplicada por $\varepsilon(\sigma)$. Ahora bien, la extensión $L|K$ es no ramificada. Por tanto, $\varepsilon|_I = \mathrm{Id}$. De esta manera, podemos resumir este estudio en los siguientes resultados:

Proposición 3.21. Sea E/K una curva elíptica con reducción multiplicativa. Sea $l \neq p$ un primo. Entonces $\rho_l(I)$ es o bien trivial o bien cíclico de orden l. El primer caso se dará si, y sólo si, K_{nr} contiene una raíz l-ésima de q. En ambos casos, $\rho_l(I_p)$ es trival.

Proposición 3.22. Sea E/K una curva elíptica con reducción multiplicativa, si $v(p) = 1$ entonces se da uno, y sólo uno, de los siguientes casos:

a) I_p actúa trivialmente sobre $E_q[p]$ y la imagen de I tiene cardinal $p-1$. Eligiendo una base adecuada,
$$\rho_p(I) \simeq \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}.$$

b) I_p no actúa trivialmente sobre $E_q[p]$. Entonces, $\rho_p(I_w)$ es un grupo cíclico de orden p y eligiendo una base conveniente,
$$\rho_p(I_p) \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Además en este caso $\rho_p(I)$ tiene orden $p(p-1)$ y, eligiendo una base conveniente, se tiene que

$$\rho_p(I) \simeq \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

4 Resultado Principal

En este capítulo vamos a presentar el resultado principal del artículo [9] de Serre y algunas de las ideas principales de la prueba. Para ello, necesitaremos los algunos resultados auxiliares. En lo que sigue K será un cuerpo de números y E/K será una curva elíptica sin multiplicación compleja. Vamos a probar que las representaciones $\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \mathrm{Aut}(E[l])$ son sobreyectivas salvo para una cantidad finita de primos l.

4.1 Representaciones locales y globales

En esta primera sección vamos a detallar cómo usar los resultados del capítulo anterior sobre cuerpos locales. Lo más importante es que, dado v un lugar finito de K, i.e. una clase de equivalencia de las valoraciones no arquimedianas definidas sobre K, y w una valoración sobre $\overline{K}$ que extienda a v, se tiene una inmersión

$$\mathrm{Gal}(\overline{K_v}/K_v) \hookrightarrow \mathrm{Gal}(\overline{K}/K)$$

Los resultados que vamos a usar en lo que sigue están probados en las secciones A.5 y A.6 del apéndice. Además, vamos a usar la misma notación de la sección A.5. Es decir, denotaremos por v a la extensión canónica de la valoración de K a su completación K_v y por $\overline{v}$ a la única extensión de v desde K_v hasta $\overline{K}_v$.

El teorema de extensión de valoraciones (ver A.6) nos dice que $w = \overline{v} \circ \tau$ para alguna K-inmersión $\tau : \overline{K} \longrightarrow \overline{K}_v$. Dicha inmersión nos da el siguiente diagrama

conmutativo:

$$\begin{array}{ccc} \overline{K} & \xrightarrow{\tau} & \overline{K_v} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\tau} & K_v \end{array}$$

Este diagrama induce un morfismo

$$\begin{aligned} \tau^* : \mathrm{Gal}(\overline{K_v}/K_v) &\longrightarrow \mathrm{Gal}(\overline{K}/K), \\ \sigma &\mapsto \tau^{-1}\sigma\tau. \end{aligned}$$

Se puede probar que esta aplicación es una inclusión. Por tanto, es un isomorfismo con su imagen, la cual coincide con el grupo de descomposición:

$$\mathrm{Gal}(\overline{K_v}/K_v) \simeq G_w(\overline{K}/K) = \left\{ \sigma \in \mathrm{Gal}(\overline{K}/K) : \forall x \in \overline{K}, \quad w(x) = w(\sigma(x)) \right\},$$

donde w es la extensión que induce la inmersión τ.

Vamos a usar la inmersión anterior para relacionar las representaciones sobre los cuerpos locales y sobre los cuerpos de números. Fijemos l un primo, v un lugar finito de K y w una valoración sobre $\overline{K}$ que extiende a v. Entonces, tenemos la representación

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E(\overline{K})[l]).$$

Hemos visto que hay una inmersión

$$\mathrm{Gal}(\overline{K_v}/K_v) \hookrightarrow \mathrm{Gal}(\overline{K}/K).,$$

por tanto podemos restringir la representación a $\mathrm{Gal}(\overline{K_v}/K_v)$ y obtenemos:

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E(\overline{K})[l]).$$

Por otro lado, podemos ver E como una curva elíptica definida sobre K_v. Esto proporciona las representaciones que hemos estudiado en el capítulo anterior y que denotaremos por:

$$\rho'_l : \mathrm{Gal}(\overline{K_v}/K_v) \longrightarrow \mathrm{Aut}(E(\overline{K_v})[l]).$$

La pregunta natural que surge en esta situación es si ρ'_l y $\rho_l|_{\mathrm{Gal}(\overline{K_v}/K_v)}$ coinciden. Denotemos por

$$\tau : \overline{K} \longrightarrow \overline{K_v}$$

a la inmersión que determina la valoración w. Dicha inmersión nos permite definir la aplicación de $E(\overline{K})$ a $E(\overline{K_v})$ que a cada punto $P = (x, y)$ le asocia el punto

$P^\tau = (\tau(x), \tau(y))$. Esta aplicación es inyectiva y se puede restringir a $E(\overline{K})[l]$ y a $E(\overline{K_v})[l]$. Estos dos conjuntos son finitos y tienen el mismo cardinal, por el teorema 2.1. Por tanto, como la aplicación τ es inyectiva necesariamente es un isomorfismo entre $E(\overline{K})[l]$ y $E(\overline{K_v})[l]$. Tenemos, por tanto, el siguiente diagrama:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K) & \xrightarrow{\rho_l} & \mathrm{Aut}(E(\overline{K})[l]) \\ \uparrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ \mathrm{Gal}(\overline{K_v}/K_v) & \xrightarrow[\rho'_l]{} & \mathrm{Aut}(E(\overline{K_v})[l]) \end{array}$$

donde la aplicación vertical de la derecha es un isomorfismo.

Veamos que el diagrama conmuta. Sea $P \in E(\overline{K})[l]$ y $\sigma \in G_w(\overline{K}/K) = \mathrm{Im}(\tau)$ (ver A.6), se tiene que:

$$\rho'_l(\tau\sigma\tau^{-1})(P^\tau) = (\tau(\sigma(x)), \tau(\sigma(y))) = (\sigma(x), \sigma(y))^\tau = \rho_l(\sigma)(P)^\tau,$$

por lo que el diagrama conmuta. Esto nos permite identificar las representaciones ρ'_l y $\rho_l|_{\mathrm{Gal}(\overline{K_v}|K_v)}$, y en lo que sigue así lo haremos. De esta manera, los resultados del capítulo anterior se pueden ver como un estudio de la imagen por las representaciones de ρ_l de ciertos subgrupos de $\mathrm{Gal}(\overline{K}/K)$.

4.2 Reducción al caso semiestable

Todo lo que queda de capítulo será dedicado a dar la prueba del teorema principal de Sere en [9]. En primer lugar, vamos a ver que nos podemos reducir al caso en que la curva tiene reducción semiestable.

Proposición 4.1. Sea K un cuerpo de números y E/K una curva elíptica. Entonces, existe una extensión finita de Galois $L|K$ tal que la curva tiene reducción semiestable sobre L.

Demostración. Como estamos en característica 0, podemos expresar E mediante un modelo de Weierstrass de la forma

$$y^2 = x(x-1)(x-\lambda),$$

con $\lambda \in \overline{\mathbb{Q}}$. Supondremos que $\lambda \in K$, en caso contrario lo añadiremos a la extensión finita que vamos a construir. En primer lugar, notemos que si λ está en $\mathcal{O}_K$, el anillo

de enteros de K y $v(\Delta) = 0$, entonces E tiene buena reducción en v. Esto se debe a que, si vemos la ecuación anterior sobre K_v, esta tiene coeficientes en el anillo de valoración de K_v y como $v(\Delta) = 0$, entonces la curva tiene buena reducción en v.

Veamos cuándo se tiene que $\lambda \in \mathcal{O}_K$ y que $v(\Delta) = 0$. Por un lado, λ se puede escribir como μ/n con $\mu \in \mathcal{O}_K$ y $n \in \mathbb{Z}_{\geq 0}$. Por tanto, si $v(\lambda) < 0$, entonces $v(n) > 0$ y los lugares finitos donde se cumple esto último son una cantidad finita. Por otro lado, el discriminante del modelo de Weiestrass que hemos elegido es $\Delta = 16\lambda^2(\lambda - 1)^2$. Luego, si $\lambda \in \mathcal{O}_K$ tenemos que $v(\Delta) \geq 0$. De nuevo, existe $m \in \mathbb{Z}$ tal que $\lambda/m \in \mathcal{O}_K^*$ y, por tanto, $v(\lambda) = v(m)$. Los lugares finitos en los que m o 2 tienen valoración positiva son solo una cantidad finita. Por tanto, $\lambda \in \mathcal{O}_K$ y $v(\Delta) = 0$ en todos los lugares finitos v de K salvo en una cantidad finita. Luego, en todos los lugares finitos de K salvo en una cantidad finita, la curva E tiene buena reducción. Ahora bien, en cada uno de estos casos la proposición 2.12 nos permite considerar una extensión finita $L|K$ sobre la cual la reducción sea semiestable. Además, como estamos en característica 0 podemos suponer que $L|K$ es de Galois.

Observación 4.1. Notemos que en la prueba anterior hemos usado implícitamente que toda extensión finita de $\mathbb{Q}_p$ es la completación de una extensión finita de $\mathbb{Q}$. Esto es una consecuencia del lema de Krasner, la prueba se puede encontrar en [5] 7.62.

La proposición anterior nos permite reducirnos al caso en que la curva tenga reducción semiestable, pues si $L|K$ es una extensión finita de Galois,

$$\mathrm{Gal}(\overline{\mathbb{Q}}/L) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K),$$

y para probar que ρ_l es sobreyectiva, basta probar que la restricción de ρ_l a $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ es sobreyectiva. Esta es la razón por la cual en el capítulo anterior sólo hemos estudiado curvas sobre cuerpos locales con buena reducción o con reducción multiplicativa.

4.3 Teorema principal

Para empezar, en el capítulo anterior hemos usado como hipótesis que $v(p) = 1$. Sin embargo, si tomamos v una valoración cualquiera sobre K, normalizada, no es cierto en general que $v(p) = 1$ para cada primo. De hecho, esto se da si, y sólo si, el índice de ramificación de la valoración con respecto a la valoración p-ádica en $\mathbb{Q}$ es 1. Ahora bien, sólo una cantidad finita de ideales primos ramifican en la extensión finita

$K|\mathbb{Q}$. Por tanto, si suponemos que el primo p es suficientemente grande, cualquier valoración v que extienda a la valoración p-ádica será no ramificada, i.e. $v(p) = 1$.

Proposición 4.2. Sea E una curva elíptica definida sobre un cuerpo de números K, con reducción semiestable. Sea l un primo ≥ 7 y suficientemente grande según la observación anterior. Entonces, si ρ_l no es sobreyectiva, se verifica una de las dos posibilidades siguientes:

a) $\rho_l(\mathrm{Gal}(\overline{K}|K))$ está contenido en un subgrupo de Borel.
b) $\rho_l(\mathrm{Gal}(\overline{K}|K))$ está contenido en el normalizador de algún subgrupo de Cartan

Demostración. Sea $l \geq 7$ un primo suficientemente grande como en la hipótesis. Se tiene que $\rho_l(\mathrm{Gal}(\overline{K}/K))$ contiene un subgrupo de Cartan o un semisubgrupo de Cartan escindido.

En efecto, si en l hay buena reducción de altura 2, entonces $\rho_l(I_l)$ es un grupo de Cartan no escindido, por la proposición 3.13, y si en l hay reducción de tipo multiplicativa o buena reducción de altura 1, entonces $\rho_l(I_l)$ contiene a un semisubgrupo de Cartan escindido por la proposición 3.22 y la proposición 3.12 respectivamente.

Por último, como $l \geq 7$, podemos aplicar la proposición 1.14 para concluir que la imagen $\rho_l(\mathrm{Gal}(\overline{K}/K))$ está contenido en un subgrupo de Borel o en el normalizador de un subgrupo de Cartan. ∎

Vamos a estudiar si puede darse el segundo caso. En las hipótesis del teorema anterior, supongamos que la imagen de ϕ_l está contenida en el normalizador N de un subgrupo de Cartan C. Podemos considerar la composición:

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\rho_l} N \xrightarrow{\pi} N/C \simeq \{\pm 1\}, \qquad \mathrm{Gal}(\overline{K}/K) \xrightarrow{\varepsilon_l} \{\pm 1\}$$

Si consideramos N y N/C con la topología discreta, todos los morfismos anteriores son continuos. En particular, $\ker(\varepsilon_l)$ es un abierto y por el teorema de correspondencia de Galois (Teorema 1.1) existe una extensión $L|K$ finita y de Galois tal que $\ker(\varepsilon_l) = \mathrm{Gal}(\overline{K}/L)$. Por el primer teorema de isomorfía:

$$\mathrm{Gal}(L/K) \simeq \frac{\mathrm{Gal}(\overline{K}/K)}{\mathrm{Gal}(\overline{K}/L)} \leq N/C \simeq \{\pm 1\}.$$

Por tanto, L es una extensión, a lo más, cuadrática. Además, podemos probar lo siguiente.

Lema 4.1. En las hipótesis anteriores la extensión $L|K$ es no ramificada en todos los lugares finitos de K.

Demostración. Fijemos v un lugar finito de K con característica residual p. Consideramos los siguientes casos:

a) **Caso en que $p \neq l$ y hay buena reducción módulo v.** En este caso por el criterio de Nerón-Ogg-Shafarevich (Teorema 2.4) $\rho_l(I_v) = \{\mathrm{Id}\}$.
b) **Caso en que $p \neq l$ y hay buena reducción multiplicativa en v.** En este caso, la proposición $l \neq p$ nos dice que $\rho_l(I_v)$ es cíclico de orden l o trivial. Ahora bien, el caso en que $\rho_l(I_v)$ sea cíclico no puede darse. En efecto, $\rho_l(I_v) \subset N$. Por tanto, $l|\#N$ y
$$\#N = \begin{cases} 2(l-1)^2 & \text{si } C \text{ es escindido} \\ 2(l^2-1) & \text{si } C \text{ es no escindido.} \end{cases}$$
En ambos casos hemos llegado a una contradicción.
c) **Caso en que $l = p$.** La proposición 3.22 nos dice que $\rho_l(I_v)$ es un subgrupo de Cartan no escindido, un semisubgrupo de Cartan escindido o un subgrupo de matrices de la forma $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. Este último caso no puede darse porque el orden de N es coprimo con l. En los otros casos $\rho_l(I_v) \subset C$. Luego, $\varepsilon_l(I_v) = \{\mathrm{Id}\}$

Observación 4.2. Si K fuera el cuerpo de los números racionales, este lema nos permitiría deducir que la imagen de ρ_l estaría contenida en C, pues no hay ninguna extensión finita de $\mathbb{Q}$ no ramificada en todos los primos (ver [6] teorema 2.18). En el caso de K cuerpo de números, la cantidad de primos l para los que la imagen de ρ_l está contenida en N y no C es finita. Sin embargo, la prueba de este resultado requiere de técnicas en teoría algebraica de números que se escapan al alcance de este trabajo (ver [9] página 296). Terminamos el capítulo dando algunas de las ideas principales de la demostración del Teorema de Serre, en la que usaremos los resultados probados en este capítulo.

Teorema 4.1 (Serre). *Sea E/K una curva elíptica definida sobre un cuerpo de números K, sin multiplicación compleja sobre $\overline{K}$. Entonces, para todo l salvo un número finito, la representación:*
$$\rho_l : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[l])$$
es sobreyectiva.

Demostración. En primer lugar, gracias a la proposición 4.1 podemos suponer que la curva E tiene reducción semiestable en todos los lugares finitos de K.

Procederemos por reducción al absurdo. Supongamos que existen una cantidad infinita de primos l tales que la representación ρ_l asociada a los puntos de l-torsión de E, no es sobreyectiva. Llamamos $\mathcal{P}$ al conjunto formado por dichos primos. De esta manera, si $l \in \mathcal{P}$ entonces, por la proposición 4.2:

a) $\rho_l(\mathrm{Gal}(\overline{K}/K))$ está contenido en un subgrupo de Borel.
b) $\rho_l(\mathrm{Gal}(\overline{K}/K))$ está contenido en el normalizador de un subgrupo de Cartan.

Ahora bien, el lema anterior junto con la observación que lo sigue nos permite suponer, sin pérdida de generalidad (tal vez eliminando una cantidad finita de primos de $\mathcal{P}$), que para todo $l \in \mathcal{P}$ $\rho_l(\mathrm{Gal}(\overline{K}/K))$ está contenido en un subgrupo de Borel o en un subgrupo de Cartan.

En este caso se puede probar que, para todo $l \in \mathcal{P}$, la representación φ_l asociada al módulo de Tate $T_l(E)$ tiene imagen abeliana ([9] 4.2-(e)).

Que la representación φ_l sea abeliana implica que el álgebra de Lie asociada a la imagen de φ_l no es la total. Ahora bien, si esto ocurre E tiene multiplicación compleja ([7] IV.2.2 página IV-11), lo cual es una contradicción. ∎

A | Apéndice

Vamos a dedicar este apéndice a desarrollar en profundidad los conceptos de teoría algebraica de números y teoría de valoraciones que se usan durante todo el trabajo.

A.1 Valoraciones y normas

Al igual que para construir los números reales, completamos $\mathbb{Q}$ con la norma del valor absoluto, podemos generalizar ese procedimiento para otras normas

Definición A.1. *Sea K un cuerpo, decimos que una aplicación*

$$|\cdot| : K \longrightarrow \mathbb{R}$$

es una norma sobre K si se cumplen las condiciones siguientes:

a) $|x| \geq 0$, *con* $|x| = 0 \iff x = 0$.
b) $|xy| = |x| \cdot |y|$.
c) $|x + y| \leq |x| + |y|$.

En lo que sigue excluiremos el caso en que $|\cdot|$ sea constantemente 1 en K^*. Como es habitual, una vez que tenemos una norma definida sobre un cuerpo, podemos definir una distancia

$$d(x, y) = |x - y|.$$

De esta manera damos topología al cuerpo K.

Definición A.2. *Sea K un cuerpo, decimos que dos normas sobre K son equivalentes si definen la misma topología sobre K.*

Proposición A.1. Dos normas $|\cdot|_1$ y $|\cdot|_2$ son equivalentes sobre K si, y sólo si, existe $s \in \mathbb{R}_{>0}$ tal que:

$$|x|_1 = |x|_2^s \quad \forall x \in K.$$

Demostración. Si dos normas cumplen que $|\cdot|_1 = |\cdot|_2^s$, entonces claramente definen la misma topología y, por tanto, son equivalentes. Pasamos a probar el recíproco.

Para cualquier norma $|\cdot|$ sobre K y cualquier $x \in K$, se tiene que:

$$|x| < 1 \iff \{x^n\} \to 0.$$

Por tanto, si $|\cdot|_1$ y $|\cdot|_2$ son equivalentes, entonces

$$\forall x \in K, \quad |x|_1 < 1 \Rightarrow |x|_2 < 1. \tag{1}$$

Fijamos ahora un elemento $y \in K$ tal que $|y|_1 > 1$ y sea $x \in K^*$. Existe un $\alpha \in \mathbb{R}$ tal que $|x|_1 = |y|_1^\alpha$. Consideramos ahora una sucesión decreciente de números racionales $\{m_i/n_i\}$ con $n_i > 0$ tal que converja a α. Por tanto, $|x|_1 = |y|_1^\alpha < |y|_1^{m_1/n_1}$, de lo que se deduce que

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1$$

y, por tanto,

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_2 < 1.$$

De esta manera, $|x|_2 \leq |y|_2^{m_i/n_i}$ y tomando límite $|x|_2 \leq |y|_2^\alpha$. Si tomamos ahora otra sucesión $\{m_i/n_i\}$, esta vez creciente, que converja a α, entonces 1 nos dice que $|x|_2 \geq |y|_2^\alpha$. Como y estaba fijo podemos calcular

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} =: s$$

y obtener que $\forall x \in K, |x|_1 = |x|_2^s$. Además como $|y|_1, |y|_2 > 1$, s tiene que ser positivo. ∎

Observación A.1. En la demostración anterior hemos probado, de hecho, que la equivalencia de las normas $|\cdot|_1$ y $|\cdot|_2$ es equivalente a la condición de que

$$\forall x \in K, \quad |x|_1 < 1 \Rightarrow |x|_2 < 1$$

Lema A.1 (de aproximación). Sean $|\cdot|_1, \ldots, |\cdot|_n$ normas sobre K que no son equivalentes dos a dos y $a_1, \ldots, a_n \in K$. Entonces, para cada $\varepsilon > 0$ existe un $x \in K$ tal que

$$|x - a_i|_i < \varepsilon \quad \forall i \in \{1, \ldots, n\}.$$

Demostración. Por la observación anterior, como $|\cdot|_1$ y $|\cdot|_n$ no son equivalentes existe $\alpha \in K$ tal que $|\alpha|_1 < 1$ y $|\alpha|_n \geq 1$. Razonando exactamente igual podemos encontrar un $\beta \in K$ tal que $|\beta|_n < 1$ y $|\beta|_1 \geq 1$. Poniendo $y = \beta/\alpha$, se tiene que $|y|_1 > 1$ y $|y|_n < 1$.

Probamos ahora por inducción que existe $z \in K$ tal que:

$$|z|_1 > 1 \quad \text{y} \quad |z|_j < 1 \quad \text{para } j = 2, \dots, n.$$

Ya hemos hecho la prueba para $n = 2$. Supongamos que hemos encontrado $z \in K$ tal que

$$|z|_1 > 1 \quad \text{y} \quad |z|_j < 1 \quad \text{para } j = 2, \dots, n-1.$$

Si $|z|_n \leq 1$, podemos multiplicar por y y elegir m suficientemente grande para que $z^m y$ sea el elemento que buscamos. En caso de que $|z|_n > 1$, la sucesión

$$t_m = \frac{z^m}{1 + z^m}$$

converge a 1 con respecto a $|\cdot|_1$ y $|\cdot|_n$ y a 0 con respecto a las demás normas. Por tanto, basta tomar $t_m y$, para m suficientemente grande.

Finalmente, con z construido como antes, la sucesión $\frac{z^m}{1+z^m}$ converge a 1 con respecto a $|\cdot|_1$ y a 0 con respecto a $|\cdot|_2, \dots, |\cdot|_n$. De esta manera, para cada i podemos construir un elemento z_i que esté muy cerca de 1 con respecto a la norma $|\cdot|_i$ y muy cerca de 0 con respecto a la norma $|\cdot|_j$ para $j \neq i$. Por tanto, el elemento

$$x = a_1 z_1 + \cdots + a_n z_n$$

tiene la propiedad que buscábamos. ∎

Definición A.3. *Sea K un cuerpo de característica 0, diremos que una norma definida sobre K es arquimediana si $|\mathbb{N}|$ no está acotado en $\mathbb{R}$. En otro caso, diremos que es no arquimediana.*

Lema A.2. Sean K un cuerpo y $|\cdot|$ una norma. Entonces, $|\cdot|$ es no arquimediana si, y solo si, la norma cumple la siguiente desigualdad triangular fuerte:

$$|x + y| \leq \max\{|x|, |y|\}$$

Demostración. Si se da la desigualdad triangular fuerte, entonces

$$\forall n \in \mathbb{N}, |n| = |1 + \cdots + 1| \leq 1.$$

Recíprocamente, supongamos que existe $N \in \mathbb{R}$ tal que $|n| \leq N$ para cada $n \in \mathbb{N}$. Sean $x, y \in K$ y supongamos, sin pérdida de generalidad, que $|x| \geq |y|$. Entonces, $|x|^\nu |y|^{n-\nu} \leq |x|^n$ para $\nu \geq 0$ y, por tanto,

$$|x+y|^n \leq \sum_{\nu=0}^{n} \binom{n}{\nu} |x|^\nu |y|^{n-\nu} \leq N(n+1)|x|^n,$$

por tanto,

$$|x+y| \leq N^{1/n}(1+n)^{1/n} \operatorname{máx}\{|x|, |y|\}$$

Basta tomar límite ahora para $n \longrightarrow \infty$.

Observación A.2. La desigualdad triangular fuerte implica que

$$|x| \neq |y| \Rightarrow \operatorname{máx}\{|x|, |y|\}.$$

En efecto, supongamos $|x| < |y|$, entonces $|x+y| \leq |y|$. Por otro lado,

$$|y| = |y + x - x| \leq \operatorname{máx}\{|x|, |x+y|\}.$$

Pero como $|x| < |y|$, tenemos que $|y| \leq |x+y|$.

Uno de los principales ejemplos sobre los que aplicamos esta teoría en el trabajo es $\mathbb{Q}$. Sobre este cuerpo el valor absoluto, que aquí denotaremos por $|\cdot|$ o $|\cdot|_\infty$, es un ejemplo de norma arquimediana y las normas p-ádicas $|\cdot|_p$, que definimos a continuación, son normas no arquimedianas.

Definición A.4. *Sean p un primo y $a/b \in \mathbb{Q}$ con $(a,b) = 1$. Existe un número $\nu \in \mathbb{Z}$ tal que*

$$\frac{a}{b} = p^\nu \frac{a'}{b'},$$

con $(a', b') = (a', p) = (b', p) = 1$. Se define la norma p-ádica de a/b como $|a/b|_p = p^{-\nu}$

Es un ejercicio sencillo comprobar que las normas p-ádicas son, en efecto, normas no arquimedianas. El siguiente resultado muestra que no podemos definir otras normas sobre $\mathbb{Q}$ salvo equivalencia de normas.

Proposición A.2. Toda norma sobre $\mathbb{Q}$ es equivalente a $|\cdot|_\infty$ o a $|\cdot|_p$ para algún primo.

Demostración. Sea $||\cdot||$ una norma no arquimediana sobre $\mathbb{Q}$. Entonces, para cada $n \in \mathbb{N}$, se tiene que $||n|| \leq 1$. Además, existe un primo p tal que $||p|| < 1$, porque si no, usando que la factorización en números primos es única y la propiedad de la norma y

el producto, llegaríamos a que $||x|| = 1$ para cada $x \in \mathbb{Q}^*$ y habíamos eliminado este caso. El conjunto

$$\mathfrak{a} = \{a \in \mathbb{Z} : ||a|| < 1\} \neq \mathbb{Z}$$

es un ideal que contiene a $p\mathbb{Z}$. Ahora bien como $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$, $\mathfrak{a} = p\mathbb{Z}$. Tomemos ahora $a \in \mathbb{Z}$, podemos escribir $a = bp^m$ con $p \nmid b$, por tanto, $b \notin \mathfrak{a}$ y $||b|| = 1$. Así, tenemos que

$$||a|| = ||p||^m = |a|_p^s,$$

donde $s = -\log ||p|| / \log p$. Por tanto, hemos probado que $||\cdot||$ es equivalente a $|\cdot|_p$.

Supongamos ahora que $||\cdot||$ es arquimediana. Se tiene que para cualesquiera dos números naturales $m, n > 1$,

$$||m||^{1/\log m} = ||n||^{1/\log n}.$$

En efecto, podemos encontrar

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

con los $a_i \in \{0, 1, \ldots, n-1\}$ y $n^r \leq m$. Notando que $r \leq \log m / \log n$ y $||a_i|| \leq a_i||1|| \leq n$, obtenemos la desigualdad

$$||m|| \leq \sum ||a_i|| \cdot ||a_i||^i \leq \sum ||a_i|| \cdot ||n||^r \leq \left(1 + \frac{\log m}{\log n}\right) n||n||^{\log m/\log n}$$

Si cambiamos ahora m por m^k y tomamos la raíz k-ésima, al tomar límite cuando $k \longrightarrow \infty$, obtenemos

$$||m||^{1/\log(m)} \leq ||n||^{1/\log(n)}$$

Si ahora cambiamos los papeles de m y n, obtenemos la igualdad. Poniendo ahora $c = ||n||^{1/\log n}$ tenemos que $||n|| = c^{\log n}$. Llamamos s al número real tal que $c = e^s$. De esta manera, para cada racional $x = a/b$,

$$||x|| = e^{s\log(x)} = |x|^s.$$

Por tanto, $||\cdot||$ es equivalente a la norma que viene dada por el valor absoluto. ∎

En lo que sigue fijaremos las siguientes convenciones con el símbolo ∞. Si $a \in \mathbb{R}$ ponemos: $a < \infty, a + \infty = \infty, \infty + \infty = \infty$. Vamos a dar ahora un concepto muy

relacionado con las normas. Sea $|\cdot|$ una norma no arquimediana sobre el cuerpo K. Consideramos

$$v(x) = \begin{cases} -\log|x| & \text{si} \quad x \neq 0 \\ \infty & \text{si} \quad x = 0 \end{cases}$$

De esta manera, hemos construido una función

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

que verifica las propiedades:

a) $v(x) = \infty \iff x = 0$.
b) $\forall x, y \in K, \quad v(xy) = v(x) + v(y)$.
c) $v(x + y) \geq \min\{v(x), v(y)\}$.

A las funciones que cumplan estas propiedades las llamaremos valoraciones. Análogamente al caso de las normas, excluiremos el caso en el que la valoración sea constantemente 0 en K^* y valga ∞ en el 0.

Definición A.5. *Diremos que dos valoraciones v_1 y v_2 son equivalentes si existe $s > 0$ tal que*

$$v_1 = sv_2$$

Dada una valoración sobre K podemos definir una una norma sobre K poniendo

$$|x| = q^{-v(x)}$$

con $q > 1$. Además, es inmediato que si cambiamos v por una valoración equivalente las normas inducidas también son equivalentes. Tener una valoración definida sobre un cuerpo nos da mucha información sobre la estructura del mismo. En efecto, es sencillo demostrar el siguiente resultado.

Proposición A.3. Sea K un cuerpo y v una valoración definida sobre él, denotamos por $|\cdot|$ a la norma inducida por la valoración. El subconjunto

$$\mathcal{O} = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$$

es un anillo con grupo de unidades

$$\mathcal{O}^* = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}.$$

Además, su único ideal maximal es

$$\mathfrak{p} = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}.$$

Observación A.3. En las condiciones de la proposición anterior, $\mathcal{O}$ es un dominio de integridad con cuerpo de fracciones K y tiene la propiedad de que, o bien $x \in \mathcal{O}$, o bien $x^{-1} \in \mathcal{O}$. Un anillo de este tipo es lo que se conoce como un anillo de valoración. Su único ideal maximal es $\mathfrak{p} = \{x \in \mathcal{O} : x^{-1} \notin \mathcal{O}\}$, al cuerpo $\mathcal{O}/\mathfrak{p}$ lo llamaremos cuerpo residual de $\mathcal{O}$.

Todo anillo de valoración es íntegramente cerrado. En efecto, sea $x \in K$ entero sobre $\mathcal{O}$. Existe una ecuación polinómica

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

con los $a_i \in \mathcal{O}$. Si $x \notin \mathcal{O}$, entonces $x^{-1} \in \mathcal{O}$ y, por tanto,

$$x = -a_1 - a_2 x^{-1} - \cdots - a_n (x^{-1})^{n-1} \in \mathcal{O}\,.$$

Definición A.6. *Diremos que una valoración es discreta si tiene un valor mínimo $s > 0$. En ese caso, se cumple que:*

$$v(K^*) = s\mathbb{Z}.$$

Decimos que v está normalizada si $s = 1$.

Si una valoración discreta no está normalizada dividir por s no cambia a $\mathcal{O}, \mathcal{O}^*, \mathfrak{p}$. Después de haberla normalizado, a los elementos $\pi \in \mathcal{O}$ tales que

$$v(\pi) = 1$$

los llamaremos parámetros de uniformización. Fijado $\pi \in \mathcal{O}$ un parámetro de uniformización es fácil comprobar que todo $x \in K^*$ admite una representación única como

$$x = u\pi^m$$

con $m \in \mathbb{Z}$ y $u \in \mathcal{O}^*$ ([1] pág. 94).

Definición A.7. *Sea R un dominio de integridad, decimos que es un anillo de valoración discreta (AVD) si es un dominio de ideales principales con un único ideal primo.*

Proposición A.4. Sea K un cuerpo y v una valoración discreta sobre este Entonces,

$$\mathcal{O} = \{x \in K : v(x) \geq 0\}$$

es un anillo de valoración discreta. Supongamos que v está normalizada. Entonces los ideales no nulos de $\mathcal{O}$ vienen dados por

$$\forall n \geq 0, \quad \mathfrak{p}^n = \pi^n \mathcal{O} = \{x \in K : v(x) \geq n\},$$

con π un parámetro de uniformización, i.e. $v(\pi) = 1$. Además se tiene el siguiente isomorfismo

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}.$$

Demostración. Sea $\mathfrak{a} \neq 0$ un ideal de $\mathcal{O}$ y $x \neq 0$ un elemento de dicho ideal con valoración mínima (que existe por ser discreta la valoración). Llamando $n = v(x)$, hemos visto que

$$x = u\pi^n \quad \text{con } u \in \mathcal{O}^*.$$

Por tanto, $\pi^n \mathcal{O} \subset \mathfrak{a}$. Recíprocamente, si $y = \varepsilon\pi^m \in \mathfrak{a}$ con $\varepsilon \in \mathcal{O}^*$ y $m = v(y) \geq n$. Por tanto,

$$y = (\varepsilon\pi^{m-n})\pi^n \in \pi^n \mathcal{O}$$

de forma que $\mathfrak{a} = \pi^n \mathcal{O}$. Por último, el isomorfismo

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}.$$

viene dado por $a\pi^n \mapsto a \mod \mathfrak{p}$. ∎

En un cuerpo K sobre el que tenemos definida una valoración discreta v, tenemos la siguiente cadena de ideales

$$\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \cdots,$$

que forma una base de entornos del elemento cero del cuerpo para la topología que induce la norma inducida por la valoración. En efecto, si $|\cdot| = q^{-v(\cdot)}$, entonces

$$\mathfrak{p}^n = \left\{ x \in K \,:\, |x| < \frac{1}{q^{n-1}} \right\}.$$

De la misma manera, una base de entornos del elemento unidad de K^*, viene dada por la siguiente cadena de subgrupos

$$\mathcal{O}^* = U^{(0)} \supset U^{(1)} \supset U^{(2)} \supset \cdots,$$

donde,

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{ x \in K^* \,:\, |1 - x| < \frac{1}{q^{n-1}} \right\}, \quad \text{para } n > 0.$$

Proposición A.5. Se tienen los isomorfismos

a) $\mathcal{O}^*/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)$, para $n \geq 1$.
b) $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$, para $n \geq 1$.

Demostración. El primer isomorfismo viene inducido por el homomorfismo sobreyectivo

$$\begin{aligned} \mathcal{O}^* &\longrightarrow (\mathcal{O}/\mathfrak{p}^n)^* \\ u &\longmapsto u \mod \mathfrak{p}^n, \end{aligned}$$

cuyo núcleo es $U^{(n)}$. El segundo isomorfismo viene inducido, una vez elegimos un parámetro de uniformización π, por

$$\begin{aligned} U^{(n)} = 1 + \pi^n \mathcal{O} &\longrightarrow \mathcal{O}/\mathfrak{p} \\ 1 + \pi^n a &\longmapsto a \mod \mathfrak{p}, \end{aligned}$$

cuyo núcleo es $U^{(n+1)}$. ∎

Estos resultados nos aportan mucha información acerca de la estructura de los cuerpos sobre los que hemos definido una valoración discreta. En la siguiente sección vamos a usar esta misma herramienta para obtener más información aún gracias a la topología natural de estos cuerpos.

A.2 Completaciones

Sea K un cuerpo sobre el que hemos definido una valoración. El procedimiento por el que se construye $\mathbb{R}$, completando $\mathbb{Q}$ con la norma del valor absoluto, es inmediatamente generalizable al caso que nos ocupa.

Definición A.8. *Sea $\{a_n\} \subset K$ una sucesión. Decimos que es de Cauchy si para cada $\varepsilon > 0$ existe un n_0 tal que*

$$\forall n, m \geq n_0, \quad |a_n - a_m| < \varepsilon.$$

Diremos que K es completo con respecto a su norma si toda sucesión de Cauchy $\{a_n\}$ es convergente, i.e. existe $a \in K$ tal que

$$\lim |a - a_n| = 0.$$

En general, dado un cuerpo K con una valoración asociada siempre podemos construir su completación, que denotaremos $\widehat{K}$. Este es el cuerpo completo más pequeño que contiene a K, respetando su norma.

La construcción del cuerpo $\widehat{K}$ es completamente análoga a la construcción del cuerpo de los números reales. Se considera el anillo R de todas las sucesiones de Cauchy sobre K y el ideal maximal $\mathfrak{m}$ de las sucesiones de Cauchy con límite 0. Ponemos así,

$$\widehat{K} = R/\mathfrak{m}.$$

Podemos incluir K en $\widehat{K}$ mediante la aplicación que manda $a \in K$ a la sucesión constante $\{a, a, a, a, a, \dots\}$. Si $a = \{a_n\} \in \widehat{K}$, la norma se extiende como

$$|a| = \lim_n |a_n|.$$

Se puede comprobar que este procedimiento hace que $\widehat{K}$ sea completo y la norma anterior extiende a la de partida. Además, esta construcción es única salvo isomorfismo.

Observación A.4. En el caso de que consideremos la completación de $\mathbb{Q}$ con la norma p-ádica denotaremos por $\mathbb{Q}_p$ a $\widehat{\mathbb{Q}}$ y lo llamaremos el cuerpo de los números p-ádicos.

Los primeros ejemplos en los que se piensa cuando a hablamos de cuerpos completos son $\mathbb{R}$ y $\mathbb{C}$. De hecho, son los únicos cuerpos completos con una norma arquimediana.

Teorema A.1 (Ostrowski). *Sea K un cuerpo completo con respecto a una norma arquimediana $|\cdot|$. Entonces existe un isomorfismo σ de K a $\mathbb{R}$ o a $\mathbb{C}$ tal que*

$$|a| = |\sigma a|^s \quad \forall a \in K,$$

para algún $s \in (0, 1]$ fijo.

Demostración. ([6] II.4.2)

Habida cuenta de este teorema, nos centraremos en estudiar los cuerpos completos cuya norma sea no arquimediana. Los principales ejemplos en este caso son los cuerpos p-ádicos.

Sea v una valoración no arquimediana sobre un cuerpo K. Dicha valoración se prolonga canónicamente a una valoración $\widehat{v}$ sobre $\widehat{K}$ poniendo

$$\widehat{v}(a) = \lim_n v(a_n),$$

con los $a_n \in K$ tales que $a_n \longrightarrow a \in \widehat{K}$. Una primera observación interesante es que la sucesión $\{v(a_n)\}$ es estacionaria. En efecto, para un $n \geq n_0$ se tiene que $\widehat{v}(a_n - a) > \widehat{v}(a)$, por tanto,

$$v(a_n) = \widehat{v}(a_n - a + a) = \min\{\widehat{v}(a_n - a), \widehat{v}(a)\} = \widehat{v}(a).$$

De esto se sigue que

$$v(K^*) = \widehat{v}\left(\widehat{K}^*\right).$$

En particular, si v es discreta y normalizada su prolongación también lo es. Más aún, para probar que una sucesión es $\{a_n\}$ es de Cauchy basta probar que $a_n - a_{n+1}$ tiende a cero, ya que

$$v(a_n - a_m) \geq \min\{v(a_{i+1} - a_i)\}.$$

En particular, tenemos que

$$\sum a_n \text{ converge} \iff a_n \to 0.$$

Proposición A.6. Sean (K, v) y $(\widehat{K}, \widehat{v})$ un cuerpo y su completación. Denotamos por $\mathcal{O} \subset K$ y $\widehat{\mathcal{O}} \subset \widehat{K}$ los anillos de valoración con respecto a v y $\widehat{v}$ respectivamente. De la misma manera, llamamos $\mathfrak{p}$ y $\widehat{\mathfrak{p}}$ a los ideales maximales correspondientes. Entonces, se tiene

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}.$$

Si además v es discreta, también tenemos que:

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n \quad \text{para } n \geq 1.$$

Demostración. Consideramos la aplicación,

$$\begin{array}{ccc} \mathcal{O} & \to & \widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \\ x & \mapsto & x \mod \widehat{\mathfrak{p}}. \end{array}$$

Es inmediato que el núcleo de esta aplicación es $\mathfrak{p}$, de manera que basta comprobar que es sobreyectiva para comprobar que existe el isomorfismo deseado. Sea $[a] \in \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ con $a \in \widehat{\mathcal{O}}$. Como K es denso en $\widehat{K}$, por continuidad, existe $x \in \mathcal{O}$ tal que $|x - a| < 1$, i.e. $x - a \in \widehat{\mathfrak{p}}$. De manera que

$$x \equiv a \mod \widehat{\mathfrak{p}}$$

Por tanto, la aplicación es sobreyectiva. El otro isomorfismo para el caso en que la valoración sea discreta, se construye de manera análoga. ∎

En lo que sigue K será un cuerpo sobre el que tenemos definida una valoración discreta v y $(\widehat{K}, \widehat{v})$ su completación

Proposición A.7. Sea R un sistema de representantes de $k = \mathcal{O}/\mathfrak{p}$ tal que $0 \in R$, y sea $\pi \in \mathcal{O}$ un parámetro de uniformización. Entonces para cada $x \neq 0$ en $\widehat{K}$ hay una única serie convergente:

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

con $a_i \in R, a_0 \neq 0, m \in \mathbb{Z}$.

Demostración. Sea $x = \pi^m u$ con $u \in \widehat{\mathcal{O}}^*$. Como $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$, la clase de $u + \widehat{\mathfrak{p}}$ tiene un único representante $a_0 \in R$. De esta manera,

$$u = a_0 + \pi b_1$$

para algún $b_1 \in \widehat{\mathcal{O}}$. Supongamos ahora que tenemos $a_0, \dots, a_{n-1} \in R$, tales que

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \pi^n b_n.$$

para algún $b_n \in \widehat{\mathcal{O}}$, de manera que la ecuación anterior los determina de manera única. En esas condiciones el representante $a_n \in R$ de $b_n + \widehat{\mathfrak{p}}$ también está determinado de manera única. Tenemos, por tanto, $b_n = a_n + \pi b_{n+1}$, para algún $b_{n+1} \in \widehat{\mathcal{O}}$. Sustituyendo esto en la ecuación anterior:

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + \pi^{n+1} b_{n+1}.$$

La serie construida de esta manera es única y converge porque el término general tiende a 0. ∎

El resultado anterior recuerda a la estructura de los enteros p-ádicos $\mathbb{Z}_p$, que se pueden escribir como series de potencias en p con coeficientes en $\{0, 1, \dots, p-1\}$. Los enteros p-ádicos también se pueden identificar con el límite inverso $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, y esta construcción se puede hacer en un contexto más general. Para aliviar la notación vamos a suponer que K es completo. Tenemos los morfismos canónicos,

$$\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}^n$$

que son compatibles con los morfismos:

$$\mathcal{O}/\mathfrak{p} \xleftarrow{\lambda_1} \mathcal{O}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \mathcal{O}/\mathfrak{p}^3 \xleftarrow{\lambda_3} \cdots$$

La propiedad universal del límite inverso nos da un morfismo

$$\mathcal{O} \longrightarrow \varprojlim_n \mathcal{O}/\mathfrak{p}^n.$$

Proposición A.8. La aplicación canónica

$$\mathcal{O} \longrightarrow \varprojlim \mathcal{O}/\mathfrak{p}^n$$

es un isomorfismo de anillos y un homeomorfismo.

Demostración. La aplicación canónica viene dada por mandar al cociente en cada coordenada. Por tanto, el núcleo de esa aplicación es $\bigcap_n \mathfrak{p}^n = \{0\}$, de lo que se deduce que la aplicación es inyectiva. Para ver la sobreyectividad, fijamos un parámetro de uniformización π y R unos representantes de cada elemento de $\mathcal{O}/\mathfrak{p}$. Todo elemento de $\mathcal{O}/\mathfrak{p}^n$ se puede escribir de manera única de la forma

$$a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}.$$

con los $a_i \in R$. De esta manera, dado un elemento en el límite, el elemento $x = \sum_{i=0}^{\infty} a_i\pi^i$ es su preimagen.

Para ver que es homeomorfismo, la aplicación es continua porque respeta los límites de las sucesiones y, además, es abierta. Esto último se comprueba gracias a que la aplicación manda la base de entornos $\{\mathfrak{p}^n\}$ de 0 a la base de entornos de 0 en el límite que consiste en

$$\left\{ \prod_{n>\nu} \mathcal{O}/\mathfrak{p}^n \cap \varprojlim \mathcal{O}/\mathfrak{p}^n \right\}.$$

Por tanto, la aplicación es un isomorfismo y un homeomorfismo. Además, induce otro homeomorfismo e isomorfismo en el grupo de las unidades:

$$\mathcal{O}^* \cong \left(\varprojlim \mathcal{O}/\mathfrak{p}^n\right)^* \cong \varprojlim (\mathcal{O}/\mathfrak{p}^n)^* \cong \varprojlim \left(\mathcal{O}^*/U^{(n)}\right).$$

En este trabajo nos interesa particularmente el estudio de las raíces y factorización de polinomios sobre cuerpos completos con respecto a una valoración. Para ello, una herramienta fundamental es el lema de Hensel. Para enunciarlo necesitamos la siguiente definición que generaliza un concepto ya conocido.

Definición A.9. *Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{O}[x]$ un polinomio. Decimos que es primitivo si $f(x) \not\equiv 0 \mod \mathfrak{p}$, i.e. si*

$$|f| := \max\{|a_0|, \ldots, |a_n|\} = 1.$$

Teorema A.2 (Lema de Hensel). *Sea $f \in \mathcal{O}[x]$ un polinomio primitivo tal que admite una factorización en el cuerpo residual,*

$$f(x) \equiv \tilde{g}(x)\tilde{h}(x) \mod \mathfrak{p},$$

en polinomios $\tilde{g}(x), \tilde{h}(x) \in k$ coprimos entre sí. Entonces, f admite una factorización

$$f(x) = g(x)h(x)$$

con $g, h \in \mathcal{O}[x]$ *tales que* $\deg(g) = \deg(\tilde{g})$ *y*

$$g(x) \equiv \tilde{g}(x) \mod \mathfrak{p}, \quad h(x) \equiv \tilde{h}(x) \mod \mathfrak{p}$$

Demostración. Pongamos $d = \deg(f)$ y $m = \deg(\tilde{g})$. Por hipótesis, $d - m \geq \deg(\tilde{h})$. Vamos a construir una sucesión de polinomios en $\mathcal{O}[x]$ y los límites van a ser los polinomios que buscamos.

Comenzamos con $g_0, h_0 \in \mathcal{O}[x]$ unos polinomios que cumplan que

$$g_0 \equiv \tilde{g} \mod \mathfrak{p} \quad h_0 \equiv \tilde{h} \mod \mathfrak{p}$$

y tales que $\deg(g_0) = m$ y $\deg(h_0) \leq d - m$. Por otro lado, como $k[x]$ es un dominio euclídeo, y $(\tilde{g}, \tilde{h}) = 1$ tenemos identidad de Bezout, esto es, existen polinomios $a(x), b(x) \in \mathcal{O}[x]$ tales que

$$ag_0 + bh_0 \equiv 1 \mod \mathfrak{p}$$

De esta manera, los polinomios $f - g_0 h_0$ y $ag_0 + bh_0 - 1 \in \mathfrak{p}[x]$. Llamamos π al coeficiente de menor valoración de los polinomios anteriores. La estrategia de la prueba consiste en buscar polinomios g y h de la forma

$$\begin{aligned} g &= g_0 + g_1\pi + g_2\pi^2 + \cdots, \\ h &= h_0 + h_1\pi + g_2\pi^2 + \cdots \end{aligned}$$

con los $p_i, g_i \in \mathcal{O}[x]$ polinomios de grado $< m$ y $\leq d - m$ respectivamente. Para hacer esto, vamos a construir unos polinomios

$$\begin{aligned} g_{n-1} &= g_0 + g_1\pi + g_2\pi^2 + \cdots + p_{n-1}\pi^{n-1}, \\ h_{n-1} &= h_0 + h_1\pi + g_2\pi^2 + \cdots + q_{n-1}\pi^{n-1}, \end{aligned}$$

de manera que,

$$f \equiv g_{n-1}h_{n-1} \mod \pi^n.$$

Así al tomar límite vamos a obtener polinomios con coeficientes en $\mathcal{O}$ tales que $f = gh$. De esta manera, hemos visto que si somos capaces de construir una sucesión en las condiciones anteriores hemos probado el teorema. Procedemos a construir la sucesión por inducción.

Para $n \geq 1$ se cumple la congruencia por la elección que hemos hecho de π. Supongamos ahora que la congruencia se cumple para algún $n \geq 1$. De esta manera, ponemos

$$g_n = g_{n-1} + p_n\pi^n, \quad h_n = h_{n-1} + q_n\pi^n,$$

donde tenemos que elegir p_n y q_n. Las condiciones que hay que imponer sobre estos polinomios se reducen a

$$f - g_{n-1}h_{n-1} \equiv \pi^n(g_{n-1}q_n + h_{n-1}p_n) \mod \pi^{n+1}.$$

Dividiendo por π^n, esto se traduce a

$$g_{n-1}q_n + h_{n-1}p_n \equiv g_0h_n + h_0p_n \equiv f_n \mod \pi,$$

donde $f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}[x]$. Como $g_0a + bh_0 \equiv 1 \mod \pi$, tenemos que

$$g_0af_n + bh_0f_n \equiv f_n \mod \pi.$$

Ahora tenemos la tentación de poner $q_n = af_n$ y $p_n = bf_n$, pero los grados podrían salir demasiado grandes. Por ello dividimos,

$$b(x)f_n(x) = q(x)h_0(x) + p_n(x)$$

con $\deg(p_n) < m$. Como $g_0 \equiv \tilde{g} \mod \mathfrak{p}$ y $\deg(g_0) = m$, el coeficiente líder de g_0 es una unidad y, por tanto, $q(x) \in \mathcal{O}[x]$. Sustituyendo en la congruencia que teníamos llegamos a que:

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \mod \pi.$$

Si ahora quitamos de $af_n + h_0q$ los monomios con coeficientes divisibles por π, obtenemos un polinomio q_n tal que

$$g_0q_n + h_0p_n \equiv f_n \mod \pi$$

con grado $\leq d - m$. Esto último se deduce de que $\deg(f_n) \leq d, \deg(g_0) = m$ y $\deg(h_0p_n) < d - m + m$.

Ejemplo A.1. El polinomio $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ tiene todas sus raíces en $\mathbb{F}_p$ y, por tanto, factoriza en factores lineales. Aplicando reiteradamente el lema de Hensel, llegamos a que $\mathbb{Q}_p$ contiene a las raíces $(p-1)$-ésimas de la unidad.

Corolario A.1. Todo polinomio irreducible $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ tal que $a_0a_n \neq 0$, cumple que

$$\max\{|a_0|, |a_n|\} = |f|.$$

En particular, si $a_n = 1$ y $a_0 \in \mathcal{O}$, entonces necesariamente $f \in \mathcal{O}[x]$.

Demostración. Después de multiplicar por un elemento apropiado de K podemos asumir que $f \in \mathcal{O}[x]$ y que $|f| = 1$. Sea a_r el primer coeficiente tal que $|a_r| = 1$, i.e. $|a_i| < 1$ para $i \leq r - 1$. Tenemos que

$$f(x) \equiv x^r\left(a_r + a_{r+1}x + \cdots + a_nx^{n-r}\right) \mod \mathfrak{p}.$$

Si tuvieramos $\max\{|a_0|, |a_n|\} < 1$, entonces $0 < r < n$ y la congruencia anterior junto a la irreducibilidad de f contradiría el lema de Hensel.

Ahora estamos en condiciones de probar el siguiente teorema de extensión de valoraciones, para el que necesitaremos algunos conceptos procedentes de la teoría de enteros algebraicos.

Definición A.10. *Sea $L|K$ una extensión de cuerpos y sea $x \in L$. Definimos el siguiente endomorfismo de K-e.v.,*

$$T_x : L \longrightarrow L, \quad T_x(\alpha) = x\alpha,$$

y la traza y la norma de x como

$$\mathrm{tr}_{L|K}(x) = \mathrm{tr}(T_x), \quad N_{L|K}(x) = \det(T_x).$$

Teorema A.3. *Sean K un cuerpo completo con respecto a una norma $|\cdot|$ y $L|K$ una extensión algebraica (posiblemente infinita). Entonces, $|\cdot|$ se extiende de manera única a L. En caso de que L sea una extensión de grado $n < \infty$, la extensión de la valoración viene dada por*

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|}.$$

Además, en este caso la extensión es completa.

Demostración. El caso de que la norma sea arquimediana, se restringe a los casos $\mathbb{R}$ y $\mathbb{C}$ por el teorema de Ostrowski. En estas condiciones, el único caso no trivial es

$$N_{\mathbb{C}|\mathbb{R}}(z) = z\overline{z} = |z|^2,$$

lo cual es un resultado conocido de análisis. Suponemos entonces que $|\cdot|$ es no arquimediana. Como toda extensión algebraica es la unión de sus subextensiones finitas, podemos asumir que $L|K$ es finita de grado n.

Comenzamos probando que la norma se puede extender. Denotaremos por $\mathcal{O}_K$ y $\mathcal{O}_L$ al anillo de valoración de K (su anillo de enteros) y a la clausura entera de $\mathcal{O}_K$ sobre L. Se tiene que

$$\mathcal{O}_L = \left\{\alpha \in L : N_{L|K}(\alpha) \in \mathcal{O}_K\right\}. \tag{2}$$

La contención de izquierda a derecha es un resultado sencillo de teoría algebraica de números ([6] I,pág 12). Recíprocamente, sea $\alpha \in L^*$ tal que $N_{L|K}(\alpha) \in \mathcal{O}_K$. Consideramos

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$$

el polinomio mínimo de α sobre K. Entonces, $N_{L|K}(\alpha) = \pm a_0^m \in \mathcal{O}_K$ ([6] I.2.6). Por tanto, $|a_0| \leq 1$, i.e. $a_0 \in \mathcal{O}_K$. El corolario anterior implica que $f(x) \in \mathcal{O}_K[x]$, i.e.

$\alpha \in \mathcal{O}_L$.

Vamos a comprobar que la norma que nos da el teorema, efectivamente es una norma sobre L y extiende a la de K. En primer lugar, las condiciones

$$\alpha = 0 \iff |\alpha| = 0 \quad y \quad |\alpha\beta| = |\alpha||\beta|$$

son triviales. La desigualdad triangular fuerte

$$|\alpha + \beta| \leq \text{máx}\{|\alpha|, |\beta|\}$$

se reduce, dividiendo por α o β, a probar la implicación

$$|\alpha| \leq 1 \Rightarrow |\alpha + 1| \leq 1.$$

Ahora bien, esto equivale a la implicación $\alpha \in \mathcal{O}_L \Rightarrow \alpha + 1 \in \mathcal{O}_L$, lo cual es trivialmente cierto, por (2). La restricción de esta norma a K es la norma $|\cdot|$ y el anillo de valoración de la norma extendida es $\mathcal{O}$.

Pasamos a probar la unicidad, sea $|\cdot|'$ otra extensión de la valoración con anillo de valoración $\mathcal{O}'_L$. Sean $\mathfrak{p}$ y $\mathfrak{p}'$ los ideales maximales de los anillos de valoración $\mathcal{O}_L$ y $\mathcal{O}'_L$ respectivamente. Vamos a probar que $\mathcal{O}_L \subset \mathcal{O}'_L$. Por reducción al absurdo, supongamos que existe $\alpha \in \mathcal{O}_L \setminus \mathcal{O}'_L$ y sea

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$$

el polinomio mínimo de α sobre K. Por definición de $\mathcal{O}_L$, se cumple que $a_1, \ldots, a_d \in \mathcal{O}_K$. Además, como $\mathcal{O}'$ es un anillo de valoración $\alpha^{-1} \in \mathfrak{p}'$, de lo que se deduce que $1 = -a_1\alpha^{-1} - \cdots - a_d(\alpha^{-1})^d \in \mathfrak{p}'$ y esto es una contradicción. Por tanto, $\mathcal{O} \subset \mathcal{O}'$. Dicho de otra forma hemos probado que:

$$|\alpha| \leq 1 \Rightarrow |\alpha|' \leq 1.$$

Esto implica que las normas son equivalentes, ya que si no lo fueran el lema de aproximación (A.1) nos permite encontrar $\alpha \in L$ tal que $|\alpha| \leq 1$ y $|\alpha|' > 1$. Además, $|\cdot|$ y $|\cdot|'$ son iguales porque ambas coinciden en K, que es denso. ∎

Este teorema también nos dice que dado un cuerpo K completo con respecto a una valoración v y $L|K$ una extensión algebraica, la valoración se extiende de manera única a una valoración w sobre L. Además, la extensión viene dada por

$$w(\alpha) = \frac{1}{n} v\left(N_{L|K}(\alpha)\right)$$

si $n = [L : K] < \infty$.

A.3 Cuerpos henselianos

Muchos de los resultados sobre cuerpos sobre los que tenemos definida una valoración se pueden deducir del lema de Hensel, sin necesidad de usar la completitud. Dicho lema es cierto en una clase mucho más amplia de cuerpos que los cuerpos completos. Un caso que nos será de particular interés es el siguiente:

Sean (K, v) un cuerpo con una valoración no arquimediana y $(\widehat{K}, \widehat{v})$ su completación. Consideramos K_v la clausura separable de K y $\mathcal{O}_v$ y $\mathfrak{p}_v$ su anillo de valoración e ideal de valoración, asociados a la restricción de $\widehat{v}$ a K_v, respectivamente. Tenemos así,

$$K \subset K_v \subset \widehat{K}, \quad \mathcal{O} \subset \mathcal{O}_v \subset \widehat{\mathcal{O}}.$$

En este caso, el lema de Hensel se cumple en $\mathcal{O}_v$ de la misma manera que sucedía en $\widehat{\mathcal{O}}$ sin que sea completo necesariamente. En efecto, por la proposición A.6 se tiene que:

$$\mathcal{O}/\mathfrak{p} = \widehat{\mathcal{O}}/\widehat{\mathfrak{p}} = \mathcal{O}_v/\mathfrak{p}_v.$$

Luego si $f \in \mathcal{O}_v[x]$ factoriza en factores coprimos $\overline{g}(x), \overline{h}(x)$ sobre $\mathcal{O}_v/\mathfrak{p}_v$, por el lema de Hensel (A.2) tenemos una factorización en $\widehat{\mathcal{O}}$

$$f(x) = g(x)h(x)$$

tal que $g \equiv \overline{g} \mod \widehat{\mathfrak{p}}$, $h \equiv \overline{h} \mod \widehat{\mathfrak{p}}$ y $\deg(g) = \deg(\widehat{g})$. Por la proposición A.6 podemos elegir el coeficiente de grado más alto de g para que esté en $\mathcal{O}_v^*$. De esta manera, como los coeficientes de f son algebraicos sobre K, los de g y h tienen que estar en $\mathcal{O}_v$.

Al cuerpo K_v también se le suele llamar la henselianización de K con respecto a v. Este cuerpo tiene muchas de las ventajas algebraicas de la completación, pero además es una extensión algebraica de K y no necesitamos usar análisis para construirlo.

Definición A.11. *Un cuerpo henseliano es un cuerpo sobre el que hay definida una valoración no arquimediana cuyo anillo de valoración $\mathcal{O}$ cumple la propiedad de de Hensel, en el sentido de que se satisface el lema A.2.*

Teorema A.4. *Sean K un cuerpo henseliano con respecto a una norma $|\cdot|$ y $L|K$ una extensión algebraica (posiblemente infinita). Entonces, $|\cdot|$ se extiende de manera única a L. En caso de que L sea una extensión de grado $n < \infty$, la extensión de la valoración viene dada por*

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|}.$$

En todo caso, el anillo de valoración de la extensión es la clausura entera del anillo de valoración de K en L.

Demostración. La prueba de este teorema es exactamente la misma que la del teorema A.3, ya que la completitud solo se usa para aplicar el lema de Hensel. ∎

Se puede probar que la propiedad anterior caracteriza a los cuerpos henselianos.

Teorema A.5. *Sea K un cuerpo sobre el que hay definida una norma $|\cdot|$ no arquimediana. Entonces, K es henseliano si, y sólo si, la norma $|\cdot|$ se puede extender de manera única a cualquier extensión algebraica de K.*

Demostración. ([6] II.6.6) ∎

Sea K un cuerpo henseliano con respecto a una valoración v. Si $L|K$ es una extensión finita de grado n, entonces v se extiende de manera única a una valoración w sobre L. De hecho, sabemos que:

$$\forall x \in L, \quad w(x) = \frac{1}{n} v\left(N_{L|K}(x)\right).$$

Si llamamos k al cuerpo residual de K y λ al de L, se tienen las siguientes inclusiones:

$$v(K^*) \subset v(L^*) \quad \text{y} \quad k \subset \lambda.$$

Definición A.12. *Sea $L|K$ una extensión en las condiciones anteriores. Se llama índice de ramificación de la extensión al índice*

$$e = e(w|v) := (w(L^*) : v(K^*))$$

y se llama grado de inercia de la extensión al grado

$$f = f(w|v) := [\lambda : k].$$

Observación A.5. Si v es una valoración discreta sobre K y $L|K$ es una extensión, entonces la valoración extendida

$$w = \frac{1}{n} v \circ N_{L|K}$$

es discreta. Si llamamos $\mathcal{O}_K, \mathfrak{p}_K, \pi$ (resp. $\mathcal{O}_L, \mathfrak{p}_L, \pi_L$) al anillo de valoración, al ideal de valoración y a un parámetro de uniformización de K (resp. de L), entonces se tiene que

$$e = \left(w(\pi_L)\mathbb{Z} : v(\pi_L)\mathbb{Z}\right),$$

lo cual implica que $v(\pi_K) = ew(\pi_L)$, i.e.

$$\pi_K = \varepsilon \pi_L^e,$$

para alguna unidad $\varepsilon \in \mathcal{O}^*$. Esta es la interpretación habitual del índice de ramificación.

Proposición A.9. En las condiciones anteriores, se tiene que $[L : K] \geq ef$ y se da la igualdad si v es discreta y $L|K$ es separable.

Demostración. Sean $\omega_1, \dots, \omega_f$ representates de una base de $\lambda|k$ y sean $\pi_0, \dots, \pi_{e-1} \in L^*$ representantes de las clases de equivalencia de $w(L^*)/v(K^*)$. Si v es discreta, podemos elegir $\pi_i = \pi_L^i$. Veamos que los elementos

$$\omega_j \pi_i, \quad j = 1, \dots, f, \quad i = 1 \dots, e-1,$$

son linealmente independientes sobre K y que en el caso discreto forman una base. Consideramos una combinación lineal

$$\sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{ij} \omega_j \pi_i = 0$$

con $a_{ij} \in K$. Por reducción al absurdo supongamos que no son todos 0. Como la reducción de los ω_j son base tiene que haber alguna suma de la forma

$$s_i = \sum_{j=1}^{f} a_{ij} \omega_j$$

distinta de 0. De hecho, si $s_i \neq 0$ entonces $w(s_i) \in v(K^*)$. En efecto, si dividimos s_i por el coeficiente de mínima valoración a_{iv}, obtenemos una combinación lineal de $\omega_1, \dots, \omega_f$ con coeficientes en el anillo de valoración $\mathcal{O}_K$ y uno de los coeficientes igual a 1. Esta combinación lineal es no nula módulo $\mathfrak{p}_L$, ya que $w(s_i) = w(a_{iv}) \in v(K^*)$.

La combinación lineal $\sum_{i=0}^{e-1} s_i \pi_i$ debe tener al menos dos sumandos con la misma valoración, i.e. existen $i \neq j$ tales que $w(s_i \pi_i) = w(s_j \pi_j)$, ya que en otro caso la combinación lineal no podría ser 0. Esto es consecuencia de $w(x) \neq w(y) \Rightarrow w(x + y) = \min\{w(x), w(y)\}$. Deducimos, por tanto, que

$$w(\pi_i) = w(\pi_j) + w(s_j) - w(s_i) \equiv w(\pi_j) \mod v(K^*)$$

y esto es una contradicción. De esta manera, hemos probado la independencia lineal de los $\omega_j \pi_i$. En particular, tenemos que $ef \leq [L : K]$.

Supongamos ahora que v es discreta, y por tanto lo es w, y que π_L es un parámetro de uniformización del anillo de valoración $\mathcal{O}_L$ asociado a w. Consideramos el $\mathcal{O}_L$-módulo

$$M = \sum_{i=0}^{e-1} \sum_{j=1}^{f} \mathcal{O}_K \, \omega_j \pi_i$$

con $\pi_i = \pi_L^i$. Vamos a probar que $M = \mathcal{O}_L$, i.e. $\{\omega_j \pi_i\}$ es una base entera de $\mathcal{O}_L$ sobre $\mathcal{O}_K$. Ponemos

$$N = \sum_{j=1}^{f} \mathcal{O}_K \, \omega_j,$$

de manera que $M = N + \pi_L N + \cdots + \pi_L^{e-1} N$. Por otro lado como los $\{\omega_i \mod \pi_L \mathcal{O}_L\}$ son una base de λ sobre k tenemos que

$$\mathcal{O}_L = N + \pi_L \mathcal{O}_L$$

Esto implica que:

$$\mathcal{O}_L = N + \pi_L(N + \pi_L \mathcal{O}_L) = \cdots = N + \pi_L N + \cdots + \pi_L^{e-1} N + \pi_L^e \mathcal{O}_L \, .$$

Por tanto, $\mathcal{O} = M + \mathfrak{p}^e = M + \mathfrak{p}\mathcal{O}_L$. Como $L|K$ es separable, $\mathcal{O}_L$ es finitamente generado como $\mathcal{O}_K$-módulo (una prueba de esto se puede encontrar en ([6] I.2.11)). Luego, por lema de Nakayama $\mathcal{O} = M$ como queríamos demostrar.

A.4 Extensiones no ramificadas y moderadamente ramificadas

En esta sección vamos a fijar un cuerpo base K que será henseliano con respecto a una determinada valoración no arquimediana v. Al igual que en la sección anterior, $\mathcal{O}_K, \mathfrak{p}, k$ denotarán el anillo de valoración, su ideal maximal y el cuerpo residual. Si $L|K$ es una extensión algebraica denotaremos por $\mathcal{O}_L, \mathfrak{p}_L, \lambda$ a los correspondientes invariantes. En esta sección vamos a estudiar como el índice de ramificación y el grado de inercia determinan el comportamiento de las extensiones.

Definición A.13. *Sea $L|K$ una extensión finita. Decimos que es una extensión no ramificada si la extensión $\lambda|k$ es separable y se tiene que:*

$$[L : K] = [\lambda : k].$$

Una extensión algebraica $L|K$, posiblemente infinita, se dice no ramificada si es unión de extensiones finitas no ramificadas.

Proposición A.10. Sean $L|K$ y $K'|K$ dos extensiones dentro de una clausura algebraica $\overline{K}|K$ y sea $L' = LK'$. Entonces, tenmos que

$$L|K \text{ es no ramificada } \Rightarrow L'|K' \text{ es no ramificada.}$$

Es decir, cada subextensión de una extensión no ramificada es no ramificada.

Demostración. Por definición de extensión no ramificada podemos suponer que la extensión $L|K$ es finita. En ese caso, la extensión $\lambda|k$ también es finita, como además es separable podemos aplicar el teorema del elemento primitivo, i.e. existe un elemento $\overline{\alpha} \in \lambda$ tal que $\lambda = k[\overline{\alpha}]$. Sea $\alpha \in L$ un representante y $f(x) \in \mathcal{O}_K[x]$ (aquí hemos usado la propiedad de Hensel gracias al teorema A.5) un polinomio mínimo de α. Llamamos $\overline{f}(x) = f(x) \mod p \in k[x]$. Como

$$[\lambda : k] \leq \deg(\overline{f}) = \deg(f) = [K(\alpha) : K] \leq [L : K] = [\lambda : k],$$

Se tiene que $L = K(\alpha)$ y $\overline{f}(x)$ es el polinomio mínimo de $\overline{\alpha}$ sobre k.

Tenemos que $L' = K'[\alpha]$. Sea $g(x) \in \mathcal{O}_{K'}$ el polinomio mínimo de α sobre K' y $\overline{g}(x) = g(x) \mod \mathfrak{p}_{K'} \in k'[x]$. Como $\overline{g}(x)$ es un factor de $\overline{f}(x)$, entonces $\overline{g}$ es separable. Además, $\overline{g}$ tiene que ser irreducible porque en caso contrario el lema de Hensel contradeciría la irreducibilidad de g. De esta manera, tenemos

$$[\lambda' : k'] \leq [L' : K'] = \deg g = \deg \overline{g} = [k'[\alpha] : k'] \leq [\lambda : k'].$$

Por tanto, $[L' : K'] = [\lambda' : k']$ es no ramificada. En particular, si $L|K$ es una subextensión de una extensión no ramificada $L'|K$, se sigue de lo que hemos probado que $L'|L$ es no ramificada. Por lo que gracias a la fórmula del grado $L|K$ es no ramificada.

Corolario A.2. La extensión generada por otras dos extensiones no ramificadas (el composite) es no ramificada.

Demostración. Podemos suponer que $L|K$ y $L'|K$ son extensiones finitas y no ramificadas. Por el resultado anterior, tenemos que $LL'|L'$ es una extensión no ramificada. El resultado se sigue ahora de que la separabilidad es transitiva y el grado de las distintas extensiones es multiplicativo.

Definición A.14. *Sea $L|K$ una extensión algebraica. Entonces, la unión $T|K$ de todas las subextensiones no ramificadas se denomina la subextensión maximal no ramificada de $L|K$.*

Proposición A.11. En las condiciones de la definición anterior, el cuerpo residual de la extensión T es la clausura separable λ_s de k en la extensión residual $\lambda|k$ de $L|K$. Además, la imagen de la valoración en T es igual a la imagen de la valoración en K.

Demostración. Sea λ_0 el cuerpo residual de $T|K$ y supongamos que $\overline{\alpha} \in \lambda$ es separable sobre k. Vamos a ver que $\overline{\alpha} \in \lambda_0$. Sea $\overline{f}(x) \in [x]$ el polinomio mínimo de $\overline{\alpha}$ y $f(x) \in \mathcal{O}_K$ un polinomio mónico tal que $\overline{f}(x) \equiv f(x) \mod \mathfrak{p}_K$. El polinomio $f(x)$ es irreducible y por el lema de Hensel existe $\alpha \in L$ tal que $f(\alpha) = 0$ y $\overline{\alpha} \equiv \alpha \mod \mathfrak{p}_K$. En particular, $[K(\overline{\alpha}) : K] = [\lambda : k]$. Esto implica que $K(\alpha)|K$ es no ramificada. Luego, $K(\alpha) \subset T$ y, por tanto, $\alpha_0 \in \lambda_0$.

Para probar que $w(T^*) = v(K^*)$ podemos suponer que $L|K$ es finita. En ese caso,

$$[T : K] \geq (w(T^*) : v(K^*))[\lambda_0 : k] = (w(T^*) : v(K^*))[T : K],$$

de lo que se sigue que $w(T^*) = v(K^*)$. ∎

La unión de todas las extensiones no ramificadas dentro de una clausura algebraica $\overline{K}$ de K se denomina la extensión maximal no ramificada $K_{nr}|K$ de K. Su cuerpo residual es la clausura separable $\overline{k}_s$ de k. Además, K_{nr} contiene a todas las raíces de la unidad de orden m con m coprimo con la característica de k, ya que el polinomio $x^m - 1$ factoriza sobre $\overline{k}_s$ y, por el lema de Hensel, sobre K_{nr}. Además, en el caso en que k sea un cuerpo finito, la extensión $K_{nr}|K$ está generada por estas raíces de la unidad, ya que este es el caso de $\overline{\lambda}_s|k$.

Pasamos ahora a estudiar un segundo tipo de extensiones donde permitimos cierta ramificación.

Definición A.15. *Una extensión algebraica $L|K$ se dice que es moderadamente ramificada si la extensión $\lambda|k$ es separable y $([L : T], p) = 1$, donde T es la subextensión maximal no ramificada de $L|K$. En caso de que $[L : T] = \infty$, la condición anterior quiere decir que el grado de cada subextensión finita de $L|T$ sea coprimo con $p = \mathrm{char}(k)$.*

Observación A.6. En el caso de que se cumpla la identidad $ef = [L : K]$ y que $\lambda|k$ sea separable, decir que la extensión $L|K$ es no ramificada, resp. moderadamente ramificada, es equivalente a decir que el índice de ramificación es $e = 1$, resp. $(e, p) = 1$.

Proposición A.12. Sea $L|K$ una extensión finita. Dicha extensión es moderadamente ramificada si, y sólo si, la extensión $L|T$ es de la forma

$$L = T\left(a_1^{1/m_1}, \dots, a_r^{1/m_r}\right)$$

con $(m_i, p) = 1$ para todo i. En dicho caso, siempre se da la igualdad

$$[L : K] = ef$$

Demostración. Podemos suponer que $K = T$ porque $L|K$ es moderadamente ramificada si, y sólo si, $L|T$ es moderadamente ramificada. Además, en este último caso, la proposición A.11 nos dice que $[T : K] = [\lambda : k] = f$.

De esta manera, supongamos que $L|K$ es una extensión moderadamente ramificada con $K = T$. En particular, tenemos que $\lambda = k$ y que $([L : K], p) = 1$. En primer lugar, vamos a probar que $e = 1$ implica que $L = K$. Sea $\alpha \in L \setminus K$, llamamos $\alpha = \alpha_1, \dots, \alpha_m$ a los conjugados de α, $a := \mathrm{tr}(\alpha) = \sum_{i=1}^m \alpha_i$ y $\beta := \alpha - \frac{1}{m}a \in L \setminus K$. Notemos que,

$$\mathrm{tr}(\beta) = a - \frac{1}{m}\sum_{i=1}^m \mathrm{tr}(\alpha_i) = a - a = 0.$$

Como $v(K^*) = w(L^*)$, podemos encontrar un $b \in K^*$ tal que $v(b) = w(\beta)$. De esta manera, $\varepsilon := \beta/b \in L \setminus K$ es una unidad con traza $\sum_{i=1}^m \varepsilon_i = 0$. Ahora bien, los conjugados ε_i tienen todos la misma clase residual, pues estamos suponiendo que $\lambda = k$. Reduciendo la ecuación $\sum_{i=1}^m \varepsilon_i = 0$ obtenemos:

$$0 = \sum_{i=1}^m \overline{\varepsilon}_i = m\overline{\varepsilon}.$$

Como ε es una unidad, esto implica que $p|m$, pero $m|[L : K]$ lo cual contradice que la extensión sea moderadamente ramificada.

Sean ahora $\omega_1, \dots, \omega_r \in \omega(L^*)$ un sistema de representantes para el grupo cociente $w(L^*)/v(K^*)$ y m_i el orden de $\omega_i \mod v(K^*)$. Si llamamos $n = [L : K]$, tenemos que

$$w(L^*) = \frac{1}{n}v(N_{L|K}(L^*)) \subset \frac{1}{n}v(K^*).$$

Por tanto, $m_i|n$, lo cual implica que $(m_i, p) = 1$. Sea $\gamma_i \in L^*$ tal que $w(\gamma_i) = \omega_i$, por definicón de los m_i tenemos que $w(\gamma_i^{m_i}) = c_i$ con los $c_i \in K$. Tenemos, por tanto, que $\gamma_i^{m_i} = c_i\varepsilon_i$ para alguna unidad $\varepsilon_i \in L$. Como $\lambda = k$ podemos escribir $\varepsilon_i = b_i u_i$

con $b_i \in K$ y u_i una unidad de L que se reduce a 1 en λ. Aplicando ahora el lema de Hensel a la ecuación $x^{m_i} - u_i = 0$ obtenemos $\beta_i \in L$ una solución para dicha ecuación. Poniendo $\alpha_i = \gamma_i \beta_i^{-1} \in L$, tenemos que $w(\alpha_i) = \omega_i$ y que:

$$\alpha^{m_i} = a_i, \quad i = 1, \dots, r,$$

donde, los $a_i = c_i b_\in K$, i.e. tenemos que $K\left(a_1^{1/m_1}, \dots, a_r^{1/m_r}\right) \subset L$. Ahora bien, el índice de ramificación de esta última extensión es 1 por construcción. Así que como vimos al principio de la prueba tenemos que

$$L = K\left(a_1^{1/m_1}, \dots, a_r^{1/m_r}\right).$$

La igualdad $[L : K] = e$ la probaremos por inducción en r usando que sabemos que $[L : K] \geq e$. Sea $L_1 = K\left(a_1^{1/m_1}\right)$, entonces $\omega_1 \in w(L_1^*)$. Luego,

$$e(L_1|K) = (w(L_1^*) : v(K^*)) \geq m_1 \geq [L_1 : K]$$

Además, $e(L|L_1) \geq [L : L_1]$, ya que $w(L^*)/w(L_1^*)$ está generado por $\omega_2, \dots, \omega_r$. Entonces,

$$e = e(L|L_1)e(L_1|K) \geq [L : L_1][L_1 : K] = [L : K].$$

Recíprocamente, vamos a probar que la extensión $L = K\left(a_1^{1/m_1}, \dots, a_r^{1/m_r}\right)$ es moderadamente ramificada. Para ello, basta probarlo para $r = 1$ y aplicarlo iterativamente. Además, nos podemos reducir al caso en que el cuerpo residual es separablemente cerrado. En efecto, si consideramos $K_1 = K_{nr}$, cuyo cuerpo residual es $k_1 = \overline{k}_s$ la clausura separable de k. Obtenemos, así el siguiente diagrama:

$$\begin{array}{ccc} L & \text{———} & L_1 \\ | & & | \\ K & \text{———} & K_1 \end{array}$$

donde $L \cap K_1 = T = K$ y $L_1 = K_1\left(a^{1/m}\right)$. Si suponemos que $L_1|K_1$ es moderadamente ramificada, entonces $\lambda_1|k_1$ es separable, luego $\lambda_1 = k_1$ y $p \nmid [L_1 : K_1] = [L : K] = [L : T]$. Por tanto, $L|K$ también es moderadamente ramificada.

Sea ahora $\alpha = a^{1/m}$. Podemos suponer que $[L : K] = \left[K\left(a^{1/m}\right) : K\right] = m$. En efecto, si d es el mayor divisor de m tal que $a = a'^d$ para algún $a' \in K^*$, y si $m' = m/d$,

entonces $\alpha = a'^{1/m'}$ y $\left[K(a'^{1/m'}) : K\right] = m'$.

Pongamos $n = \text{ord}(w(\alpha) \mod v(K^*))$. Como $mw(\alpha) = v(a) \in v(K^*)$, podemos escribir $m = nd$. Por otro lado, existe $b \in K^*$ tal que $w(\alpha^n) = v(b)$. Además, $v(b^d) = w(\alpha^m) = v(a)$, de lo que se deduce que existe una unidad ε de K tal que:

$$\alpha^m = a = \varepsilon b^d.$$

Como $(d, p) = 1$, la ecuación $x^d - \overline{\varepsilon} = 0$ tiene todas sus raíces en k, por ser separablemente cerrado. Por tanto, por el lema de Hensel la ecaución $x^d - \varepsilon = 0$ también tiene todas sus raíces sobre K. Por tanto, podemos elegir $b \in K^*$ de manera que $\alpha^m = b^d = a$. Como $x^m - a$ es irreducible, tenemos que $d = 1$, y, por tanto, $m = n$. Luego,

$$e \geq n = [L : K] \geq ef \geq e.$$

Es decir, $f = 1$, luego $\lambda = k$ y $p \nmid n = e$. Por tanto, $L|K$ es moderadamente ramificada.

Corolario A.3. Sea $L|K$ y $K'|K$ dos extensiones dentro de la clausura algebraica $\overline{K}|K$, y $L' = LK'$. Entonces,

$$L|K \text{ es moderadamente ramificada } \Rightarrow L'|K' \text{ es moderadamente ramificada.}$$

En particular, toda subextensión de una extensión moderadamente ramificada es moderadamente ramificada.

Demostración. Sin pérdida de generalidad, podemos suponer que la extensión $L|K$ es finita. Consideramos el diagrama

$$\begin{array}{ccc} L & \text{——} & L' \\ | & & | \\ T & \text{——} & T' \\ | & & | \\ K & \text{——} & K' \end{array}$$

donde la inclusión $T \subset T'$ se deduce de la proposición A.10. Si $L|K$ es moderadamente ramificada, entonces $L = T\left(a_1^{1/m_1}, \ldots, a_r^{1/m_r}\right)$ con $(m_i, p) = 1$. Por tanto, $L' = LK' = LT' = T'\left(a_1^{1/m_1}, \ldots, a_r^{1/m_r}\right)$. Luego el resultado anterior nos dice que $L'|K'$ es moderadamente ramificada.

La afirmación relacionada con las subextensiones se prueba igual que en el caso no ramificado.

Corolario A.4. La extensión generada por otras dos extensiones moderadamente ramificadas (el composite) es moderadamente ramificada.

Demostración. De nuevo, la prueba es análoga al caso no ramificado. ∎

Definición A.16. *Sea $L|K$ una extensión algebraica. Entonces, la unión $V|K$ de todas las subextensiones moderadamente ramificadas se denomina la subextensión maximal moderadamente ramificada de $L|K$.*

Denotemos por $w(L^*)^{(p)}$ al subgrupo de los elementos $\omega \in w(L^*)$ tal que $m\omega \in v(K^*)$ para algún m coprimo con p. De esta manera, el cociente $w(L^*)^{(p)}/v(K^*)$ son los elementos de $w(L^*)/v(K^*)$ de orden coprimo con p. Se tiene el siguiente resultado:

Proposición A.13. La extensión maximal moderadamente ramificada $V|K$ de $L|K$ cumple que $w(V^*) = w(L^*)^{(p)}$ y que su cuerpo residual es igual a la clausura separable λ_s de k en $\lambda|k$.

Demostración. Nos podemos restringir al caso en que $L|K$ es una extensión finita. Pasando de K a la subextensión maximal no ramificada, podemos suponer que $\lambda_s = k$. Como $p \nmid e(V|K) = \#w(V^*)/v(K^*)$, tenemos que $w(V^*) \subset w(L^*)^{(p)}$. Recíprocamente, si seguimos la prueba de la proposición A.12, dado $\omega \in w(L^*)^{(p)}$ podemos ecntrar $\alpha = \sqrt[n]{a} \in L$ tal que $a \in K$, $(m, p) = 1$ y $w(\alpha) = \omega$. Como $\alpha \in V$, hemos acabado. ∎

Los resultados obtenidos en esta sección se pueden resumir como sigue:

$$\begin{array}{ccccccc} K & \subset & T & \subset & V & \subset & L \\ k & \subset & \lambda_s & = & \lambda_s & \subset & \lambda \\ v(K^*) & = & w(T^*) & \subset & w(L^*)^{(p)} & \subset & w(L^*) \end{array}$$

Si $L|K$ es una extensión finita y $e = e'p^a$ con $(e', p) = 1$, entonces $[V : T] = e'$. Diremos que la extensión $L|K$ es totalmente ramificada si $T = K$ y salvajemente ramificada si no es moderadamente ramificada, i.e. $V \neq L$.

Aunque, hasta ahora hemos desarrollado la teoría en un contexto muy general, el caso que nos interesa es el de K un cuerpo completo con respecto a una valoración con cuerpo residual finito, i.e $k = \mathbb{F}_q$ con $q = p^r$.

Proposición A.14. Sea ζ una raíz n-ésima de la unidad. Pongamos $L = K(\zeta)$ y sean $\mathcal{O}_L \mid \mathcal{O}_K$, resp. $\lambda|k$, la extensión de anillos de valoración, resp. de cuerpos residuales, de $L|K$. Supongamos que $(n, p) = 1$. Entonces, se tienen:

a) La extensión $L|K$ es no ramificada de grado f, con f el menor numero natural tal que $q^f \equiv 1 \mod n$.

b) El grupo de Galois $\mathrm{Gal}(L|K)$ es canónicamente isomorfo a $\mathrm{Gal}(\lambda|k)$ y está generado por el automorfismo $\varphi : \zeta \mapsto \zeta^q$.
c) $\mathcal{O}_L = \mathcal{O}_K[\zeta]$.

Demostración. Sea $\phi(x)$ el polinomio mínimo de ζ sobre K. La reducción $\overline{\phi}(x)$ es el polinomio mínimo de $\overline{\zeta} \equiv \zeta \mod \mathfrak{p}_K$ sobre k. En efecto, el $\overline{\phi}(x)$ tiene que ser un divisor del polinomio $x^n - 1$ y, como $(n, p) = 1$, dicho polinomio tiene que ser separable. Si $\overline{\phi}(x)$ no es irreducible, $\phi(x)$ tampoco, por el lema de Hensel, lo cual es una contradicción. Por tanto, ϕ y $\overline{\phi}$ tienen el mismo grado, de lo que deducimos que $[L : K] = [K(\zeta) : K] = [\lambda : k] = f$. Luego, $L|K$ es no ramificada.

El polinomio $x^n - 1$ se descompone en sus factores lineales sobre $\mathcal{O}_L$ y, por tanto, sobre λ, por ser separable. Por tanto, $\lambda = \mathbb{F}_{q^f}$ está contiene a μ_n el grupo de raíces de la unidad y está generado por ellas. Por tanto, f es el menor entero tal que $\mu_n \subset \mathbb{F}_{q^f}$. De esto se deducen los dos primeros puntos.

Como $L|K$ es no ramificado, tenemos que $\mathfrak{p}_K \mathcal{O} = \mathfrak{p}_L$ y como $1, \zeta, \ldots, \zeta^{f-1}$ es una base de $\lambda|k$, tenemos que $\mathcal{O}_L = \mathcal{O}_K[\zeta] + \mathfrak{p}_K \mathcal{O}$. Luego, $\mathcal{O}_L = \mathcal{O}_K[\zeta]$ por el lema de Nakayama. ∎

A.5 Extensión de Valoraciones

En la sección anterior hemos visto que si K es un cuerpo henseliano la valoración se extiende de manera única a toda extensión algebraica. En esta sección vamos a estudiar el problema de extender una valoración v sobre un cuerpo K a una extensión algebraica de este en general.

Para cada valoración v de K, denotaremos por K_v a la completación de K con respecto a v y por $\overline{K}_v$ a la clausura algebraica de K_v. A la extensión canónica de v desde K a K_v, la seguiremos denotando por v, mientras que a la extensión única de v desde K_v hasta $\overline{K}_v$ la denotaremos por $\overline{v}$.

Sea $L|K$ una extensión algebraica. Si elegimos una K-inmersión

$$\tau : L \longrightarrow \overline{K}_v,$$

podemos restringir la valoración $\overline{v}$ a τL, para obtener una extensión de v a L. Si llamamos w a dicha extensión, esta viene definida por

$$w = \overline{v} \circ \tau.$$

Con respecto a estas valoraciones, la inmersión

$$\tau : L \longrightarrow \overline{K}_v$$

es continua por construcción. Si la extensión $L|K$ es finita, entonces τ se extiende de manera única a un homomorfismo

$$\tau : L_w \longrightarrow \overline{K}_v.$$

Dicha extensión se hace por continuidad y está bien definida porque la completación de τL es una extensión finita de K_v y, por tanto, está contenida en $\overline{K}_v$. En el caso en que la extensión $L|K$ sea infinita, también podemos extender la inmersión a

$$\tau : L_w \longrightarrow \overline{K}_v.$$

Sin embargo, en este caso L_w no denota la completación de L con respecto a w, ya que en ese caso la aplicación anterior no está bien definida. El objeto apropiado para definir la extensión anterior es

$$L_w = \bigcup_i L_{i,w},$$

donde $L_{i,w}$ recorre las completaciones de las subextensiones finitas de $L|K$. Esta unión se denomina la localización de L en w. De esta manera, tenemos el siguiente diagrama compatible con la extensión de valoraciones:

$$\begin{array}{ccc} L & \longrightarrow & L_w \\ \big| & & \big| \\ K & \longrightarrow & K_v \end{array}$$

Este diagrama es de vital importancia en teoría de números. En cierta forma, representa el principio local-global, es decir, nos permite pasar problemas en extensiones globales $L|K$ a extensiones locales $L_w|K_v$. En la siguiente sección veremos como relacionar las extensiones locales con las globales mediante los grupos de Galois.

Acabamos de ver que cada K-inmersión $\tau : L \longrightarrow \overline{K}_v$ nos da una extensión $w = \overline{v} \circ \tau$

de la valoración v de K. Para cada $\sigma \in \mathrm{Gal}(\overline{K})$, tenemos una nueva K-inmersión dada por la composición

$$L \xrightarrow{\tau} \overline{K}_v \xrightarrow{\sigma} \overline{K}_v,$$

es decir, $\tau' = \sigma \circ \tau$. Llamaremos conjugadas a las K-inmersiones que están relacionadas por un K-automorfismo de $\overline{K}_v$. El siguiente resultado nos da una descripción completa de las extensiones de v a L.

Teorema A.6 (de extensión de valoraciones). *Sea $L|K$ una extensión algebraica de cuerpos y v una valoración definida sobre K. Entonces, tenemos que:*

i) Cada extensión w de la valoración v es de la forma $w = \overline{v} \circ \tau$ para alguna inmersión $\tau : L \longrightarrow \overline{K}_v$.
ii) Dos extensiones $\overline{v} \circ \tau$ y $\overline{v} \circ \tau'$ son iguales si, y sólo si, τ y τ' son conjugados.

Demostración. i) Sea w una extensión de v a L y sea L_w la localización de L con respecto a w. A la extensión canónica de w a L_w, la seguiremos denotando w. Por el teorema A.3, hay una única extensión de v desde K_v a L_w. Si elegimos $\tau : L_w \longrightarrow \overline{K}_v$ una K_v-inmersión cualquiera, la cual existe porque $L_w|K_v$ es una extensión algebraica, tenemos que $\overline{v} \circ \tau$ debe coincidir con w por la unicidad. Ahora bien, la restricción $\tau : L \longrightarrow \overline{K}_v$ es una K-inmersión que cumple $w = \overline{v} \circ \tau$.

ii) Sean τ y $\sigma\tau$ dos K-inmersiones de L conjugadas, con $\sigma \in \mathrm{Gal}(\overline{K}_v|K_v)$. Como $\overline{v}$ es la única extensión de v desde K_v a $\overline{K}_v$, se tiene que $\overline{v} = \overline{v} \circ \sigma$ y, por tanto, $\overline{v} \circ \tau = \overline{v} \circ (\sigma \circ \tau)$. Por tanto, las extensiones de v inducidas por τ y $\sigma \circ \tau$ son la misma.

Recíprocamente, sea $\tau, \tau' : L \longrightarrow \overline{K}_v$ dos K-inmersiones tales que $\overline{v} \circ \tau = \overline{v} \circ \tau'$. Sea $\sigma : \tau L \longrightarrow \tau' L$ el K-isomorfismo dado por $\sigma = \tau' \circ \tau^{-1}$. Este isomorfismo se puede extender a un K_v-isomorfismo

$$\sigma : \tau L \cdot \overline{K}_v \longrightarrow \tau' L \cdot \overline{K}_v$$

por continuidad, ya que τL es denso en $\tau L \cdot \overline{K}_v$. Extendiendo ahora σ a un $\widetilde{\sigma} \in \mathrm{Gal}(\overline{K}_v|K_v)$, tenemos que $\tau = \widetilde{\sigma} \circ \tau$, como queríamos demostrar.

A.6 Teoría de Galois de valoraciones

En esta sección vamos a considerar $L|K$ una extensión de Galois y vamos a estudiar como el grupo de Galois actúa sobre las valoraciones w que extienden a v. Para hacer este estudio vamos a necesitar usar los resultados principales de la teoría de Galois, no solo finita , sino también la infinita. Por ello, comenzaremos la sección dando los principales resultados de esta

A.6.1 Inercia y ramificación

Sea $L|K$ una extensión de Galois arbitraria con grupo de Galois $G = \mathrm{Gal}(L|K)$. Si v es una valoración sobre v y w es una valoración sobre L que extiende a v, entonces $w\circ\sigma$ también extiende a v, para cada $\sigma \in G$. Por tanto, el grupo G actúa sobre el conjunto de extensiones $w|v$.

Proposición A.15. El grupo G actúa transitivamente sobre el conjunto de las extensiones $w|v$, i.e. dos extensiones cualesquiera son conjugados.

Demostración. Sean w y w' dos extensiones de v sobre L. En primer lugar, supongamos que $L|K$ es finita. Si w y w' no son conjugados, entonces los conjuntos

$$\{w\circ\sigma : \sigma \in G\} \quad \text{y} \quad \{w'\circ\sigma : \sigma \in G\}$$

son disjuntos. Por el lema de aproximación (lema A.1), existe $x \in L$ tal que

$$|\sigma x|_w < 1 \quad \text{y} \quad |\sigma x|'_w > 1$$

para todo $\sigma \in G$. Si ponemos ahora

$$\alpha := N_{L|K}(x) = \prod_{\sigma\in G} \sigma x,$$

entonces,

$$|\alpha|_v = \prod_{\sigma\in G} |\sigma x|_w < 1.$$

De manera análoga, podemos probar que $|\alpha|_v > 1$, lo cual es una contradicción.

Supongamos ahora que $L|K$ es infinita y consideremos los conjuntos

$$X_M = \{\sigma \in G : w\circ\sigma_{|M} = w'_{|M}\}$$

con $M|K$ variando entre las extensiones finitas de Galois. Ya hemos visto que los X_M son no vacíos. Además, son cerrados, ya que si $\sigma \in G \setminus X_M$ entonces, el entorno abierto $\sigma\,\mathrm{Gal}(L|M) \subset G \setminus X_M$. Además, $\bigcap X_M \neq \emptyset$, pues en caso contrario, por la compacidad de G tendríamos que $\bigcap_{i=1}^{r} X_{M_i} = \emptyset$ para una cantidad finita de M_i. Sin embargo, esto es una contradicción, ya que $X_M = \bigcap_{i=1}^{r} X_{M_i}$ con $M = M_1 \cdots M_r$. Por tanto, hemos probado que existe $\sigma \in G$ tal que $w \circ \sigma = w'$.

Definición A.17. *El grupo de descomposición de una extensión w de v sobre L se define como*

$$G_w = G_w(L|K) = \{\sigma \in \mathrm{Gal}(L|K) : w \circ \sigma = w\}.$$

En caso de que v sea una valoración no arquimediana, podemos encontrar dos subgrupos canónicos más. Recuperamos la notación $\mathcal{O}_v, \mathfrak{p}_v, k, \mathcal{O}_w, \mathfrak{p}_w, \lambda$.

Definición A.18. *El grupo de inercia de $w|v$ se define como*

$$I_w = I_w(L|K) = \left\{\sigma \in G_w : \forall x \in \mathcal{O}_w, \quad \sigma x \equiv x \mod \mathfrak{p}_w\right\}$$

y el grupo de ramificación se define como

$$R_w = R_w(L|K) = \left\{\sigma \in G_w : \forall x \in L^*, \quad \frac{\sigma x}{x} \equiv 1 \mod \mathfrak{p}_w\right\}.$$

Observación A.7. Es importante notar que si $\sigma \in G_w$, la igualdad $w \circ \sigma = w$ implica que $\sigma\,\mathcal{O}_w = \mathcal{O}_w$ y $\forall x \in L^*, \sigma x/x \in \mathcal{O}_w$. Además, se tiene que

$$R_w \subset I_w \subset G_w.$$

Los subgrupos G_w, I_w, R_w de $G = \mathrm{Gal}(L|K)$ son canónicos en el sentido de que son cerrados para la topología de Krull. La prueba de esto es rutinaria. Vamos a dar la prueba para el grupo de descomposición para ilustrar el tipo de argumentos que se usan.

Sea $\sigma \in \mathrm{Gal}(L|K)$ un elemento en la clausura de G_w. Esto quiere decir que para cada $M|K$ subextensión finita de Galois de $L|K$ el entorno $\sigma \in \mathrm{Gal}(L|M)$ contiene algún elemento $\sigma_M \in G_w$. Como $\sigma_M \in \sigma\,\mathrm{Gal}(L|M)$, se tiene que $\sigma_M|_M = \sigma|_M$, y $w \circ \sigma_M = w$ implica que

$$w \circ \sigma|_M = w \circ \sigma_M|_M = w|_M$$

Como L es la unión de todos los M, hemos probado que $w \circ \sigma = w$ y, por tanto, $\sigma \in G_w$.

Los subgrupos G_w, I_w, R_w contienen mucha información acerca de cómo se extiende la valoración v de K a L. Sin embargo, antes de adentrarnos en esto vamos a ver las propiedades funtoriales de estos grupos.

Consideremos dos extensiones de Galois $L|K$ y $L'|K'$ y un diagrama conmutativo de la forma:

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\tau} & K' \end{array}$$

con τ un homomorfismo. Esta situación induce un homomorfismo

$$\begin{aligned} \tau^* : \mathrm{Gal}(L'|K') &\longrightarrow \mathrm{Gal}(L|K) \\ \sigma' &\longmapsto \tau(\sigma') = \tau^{-1}\sigma'\tau \end{aligned}$$

Notemos que como la extensión $L|K$ es normal, la extensión $\tau L|\tau K$ también lo es. Por tanto, $\sigma'\tau L \subset \tau L$. Luego la definición anterior tiene sentido.

Proposición A.16. Sea w' una valoración sobre L' y w una valoración sobre L tales que $v' = w'|_K$, $v = w|_K$ y $w = w' \circ \tau$. Entonces, τ^* induce homomorfismos:

$$\begin{aligned} G_{w'}(L'|K') &\longrightarrow G_w(L|K) \\ I_{w'}(L'|K') &\longrightarrow I_w(L|K) \\ R_{w'}(L'|K') &\longrightarrow R_w(L|K), \end{aligned}$$

donde, en los dos últimos casos, estamos suponiendo que v es no arquimediana.

Demostración. Sean $\sigma' \in G_{w'}(L'|K')$ y $\sigma = \tau^*(\sigma')$. Si $x \in L$, entonces se tiene que:

$$|x|_{w\circ\sigma} = |\sigma x|_w = |\tau^{-1}\sigma'\tau x|_w = |\sigma'\tau x|_{w'} = |\tau x|_{w'} = |x|_w.$$

Por tanto, $\sigma \in G_w(L|K)$. Supongamos ahora que $\sigma' \in I_{w'}(L'|K')$ y $x \in \mathcal{O}_L$, entonces

$$w(\sigma x - x) = w(\tau^{-1}(\sigma'\tau x - \tau x)) = w'(\sigma'(\tau x) - (\tau x)) > 0,$$

luego $\sigma \in I_w(L|K)$.

Por último supongamos que $\sigma' \in R_w(L|K)$ y $x \in L^*$, entonces

$$w\left(\frac{\sigma x}{x} - 1\right) = w(\tau^{-1}(\frac{\sigma'\tau x}{\tau x} - 1)) = w'(\frac{\sigma'\tau x}{\tau x} - 1) > 0.$$

Por tanto $\sigma \in R_w(L|K)$. ∎

Si los dos morfismos $\tau : L \longrightarrow L'$ y $\tau : K \longrightarrow K'$ son isomorfismos, entonces los morfismos inducidos anteriores son isomorfismos. Si además $K = K'$ y $L = L'$, tenemos que para cada $\tau \in \mathrm{Gal}(L|K)$:

$$G_{w\circ\tau} = \tau^{-1} G_w \tau, \quad I_{w\circ\tau} = \tau^{-1} I_w \tau, \quad R_{w\circ\tau} = \tau^{-1} R_w \tau,$$

i.e. los grupos de descomposición, inercia y ramificación de valoraciones conjugadas son conjugados.

Otro caso interesante aparece cuando tenemos una extensión intermedia M de $L|K$. En dicho caso el diagrama es

$$\begin{array}{ccc} L & = & L \\ | & & | \\ K & \hookrightarrow & M \end{array}$$

En este caso, el homomorfismo inducido es la inclusión $\tau^* : \mathrm{Gal}(L|M) \longrightarrow \mathrm{Gal}(L|K)$, y obtenemos el siguiente corolario

Corolario A.5. Consideramos extensiones $K \subset M \subset L$, entonces tenemos

$$\begin{aligned} G_w(L|K) &= G_w(L|K) \cap \mathrm{Gal}(L|M) \\ I_w(L|K) &= I_w(L|K) \cap \mathrm{Gal}(L|M) \\ R_w(L|K) &= R_w(L|K) \cap \mathrm{Gal}(L|M) \end{aligned}$$

Otro caso muy importante es el del diagrama

$$\begin{array}{ccc} L & \text{———} & L_w \\ | & & | \\ K & \text{———} & K_v \end{array}$$

donde $w|v$ es una extensión de valoraciones, K_v es la completación de K con respecto a v y L_w es la localización de L con respecto a w en el sentido de la sección anterior. Como la extensión de valoraciones de $L_w|K_v$ es única, por el teorema A.3, denotaremos a sus grupos de descomposición, inercia y ramificación por $\mathrm{Gal}(L_w|K_v)$, $I(L_w|K_v)$, $R(L_w|K_v)$. En este caso, el homorfismo inducido es la aplicación restricción

$$\begin{aligned} \mathrm{Gal}(L_w|K_v) &\longrightarrow \mathrm{Gal}(L|K) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

De hecho, se tiene el siguiente resultado

Proposición A.17. Son isomorfos los siguientes grupos:

$$\begin{aligned} G_w(L|K) &\cong \mathrm{Gal}(L_w|K_v) \\ I_w(L|K) &\cong I(L_w|K_v) \\ R_w(L|K) &\cong R(L_w|K_v) \end{aligned}$$

Demostración. La proposición se deduce del hecho de que el grupo de descomposición $G_w(L|K)$ son precisamente los elementos $\sigma \in \mathrm{Gal}(L|K)$ tales que son continuos con respecto a w. En efecto, si $\sigma \in G_w(L|K)$ la continuidad es trivial. Recíprocamente, si σ es un automorfismo arbitrario continuo, se tiene que

$$|x|_w < 1 \Rightarrow |\sigma x|_w = |x|_{w\circ\sigma} < 1,$$

porque $|x|_w < 1$ implica que la sucesión $\{x^n\}$ tiende a 0 con respecto a w y, por tanto, σx^n también, i.e. $|\sigma x| < 1$. Por la observación A.1 esto implica que las valoraciones w y $w\circ\sigma$ son equivalentes. Ahora bien, como $w|_K = w\circ\sigma|_K$, necesariamente son iguales, i.e. $\sigma \in G_w(L|K)$.

Como L es denso en L_w, todo K-automorfismo $\sigma \in G_w(L|K)$ se extiende de manera única a un K_v-automorfismo $\widehat{\sigma}$ de L_w, con esto hemos probado la biyectividad de la aplicación de la que se deducen todos los isomorfismos.

Gracias al estudio que acabamos de hacer podemos identificar los los grupos de descomposición, inercia y ramificación de una extensión con los de sus completaciones, una vez hemos dado la extensión de valoraciones. Pasamos ahora a estudiar qué papel juegan estos grupos.

El grupo de descomposición lo forman, como hemos visto en la prueba del resultado anterior, los automorfismos continuos con respecto a w.

Definición A.19. *El cuerpo fijo de G_w,*

$$Z_w = \{x \in L : \forall x \in G_w, \quad \sigma x = x\}$$

se denomina el cuerpo de descomposición de w sobre K.

El papel que juega este cuerpo viene dado por la siguiente proposición.

Proposición A.18. Se tienen los siguientes resultados:

a) La restricción w_Z de w a Z_w se extiende de manera única a L.
b) Si v es no arquimediana, w_Z tiene el mismo cuerpo residual e imagen que v.
c) $Z_w = L \cup K_v$.

Demostración. En primer lugar, sea w' una extensión de w_Z a L. Por la proposición A.15, w y w' son conjugadas, i.e. $w' = w \circ \sigma$ para algún $\sigma \in \mathrm{Gal}(L|Z_w) = G_w$, i.e. $w' = w$. Por otro lado, la igualdad $Z_w = L \cap K_v$ es inmediata del hecho de que $G_w(L|K) \cong \mathrm{Gal}(L_w|K_v)$. Por último, como K_v tiene el mismo cuerpo residual que K y $\widehat{v}$ tiene la misma imagen que v, esto sigue siendo cierto para $Z_w = L \cap K_v$. ∎

En lo que sigue, supondremos que v y w son no arquimedianas. En este caso, podemos hablar de los grupos de inercia y ramificación. El grupo I_w es el kernel de un homomorfismo canónico de G_w que describiremos a continuación.

Consideramos $\mathcal{O}_w$ el anillo de valoración de w y $\mathfrak{p}_w$ su ideal maximal. Para cada $\sigma \in G_w$, se tiene que $\sigma\mathcal{O}_w = \mathcal{O}_w$ y $\sigma\mathfrak{p}_w = \mathfrak{p}_w$. Por tanto, cada $\sigma \in G_w$ induce un k-automorfismo

$$\overline{\sigma} : \mathcal{O}_w/\mathfrak{p}_w \longrightarrow \mathcal{O}_w/\mathfrak{p}_w, \quad x \mod \mathfrak{p}_w \mapsto \sigma x \mod \mathfrak{p}_w$$

de λ. De manera, que tenemos un homorfismo

$$G_w \longrightarrow \mathrm{Aut}(\lambda)$$

de núcleo I_w.

Proposición A.19. Si $L|K$ es una extensión de Galois, entonces $\lambda|k$ es normal y se tiene la siguiente sucesión exacta

$$1 \longrightarrow I_w \longrightarrow G_w \longrightarrow \mathrm{Gal}(\lambda|k) \longrightarrow 1$$

Para la prueba vamos a ver primero el siguiente lema

Lema A.3. Si $L|K$ es una extensión finita de Galois, entonces la extensión $\lambda|k$ es normal y el homomorfismo $G_w \longrightarrow \mathrm{Gal}(\lambda|k)$ es sobreyectivo.

Demostración. Como Z_w tiene el mismo cuerpo residual que K, podemos suponer que $K = Z_w$ y, por tanto, $G_w = G$. Sea $\theta \in \mathcal{O}_K$ un representante de $\overline{\theta} \in k$ y $f(X)$, resp. $\overline{g}(X)$, el polinomio mínimo de θ sobre K, resp. de $\overline{\theta}$ sobre k. Entonces, $\overline{\theta} = \theta \mod \mathfrak{p}_w$ es un cero de $\overline{f}(X) = f(X) \mod \mathfrak{p}_w$. Por tanto, $\overline{g}(X)|\overline{f}(X)$. Como $L|K$ es normal f se descompone en sus factores lineales sobre $\mathcal{O}$. Por tanto, $\overline{f}(X)$ también

factoriza en sus factores lineales sobre k y, por tanto, $\overline{g}(X)$ también. Luego $\lambda|k$ es una extensión normal.

Sea ahora $\overline{\theta}$ un elemento primitivo para la subextensión maximal separable de $\lambda|k$ y fijamos

$$\overline{\sigma} \in \mathrm{Gal}(\lambda|k) = \mathrm{Gal}(k(\overline{\theta})|k).$$

Entonces, $\overline{\sigma}\overline{\theta}$ es una raíz de $\overline{g}(X)$ y, por tanto, de $\overline{f}(X)$. Es decir, existe θ' una raíz de f. Luego, θ y θ' son conjugados, i.e. existe $\sigma \in \mathrm{Gal}(L|K)$ tal que $\sigma\theta = \theta'$. Como $\overline{\theta}$ es un elemento primitivo y $\overline{\sigma}\overline{\theta} \equiv \sigma\theta \mod \mathfrak{p}_w$, $\overline{\sigma}$ es la imagen por el homomorfismo de la hipótesis de σ.

Pasámos ahora con la prueba del resultado para el caso general.

Demostración (de la proposición A.19). El lema anterior prueba el caso en que $L|K$ sea una extensión finita. Si $L|K$ es una extensión finita, el lema anterior nos dice que $\lambda|k$ es una unión de extensiones normales finitas. Luego, $\lambda|k$ es normal.

Para probar la sobreyectividad de $f : G_w \longrightarrow \mathrm{Gal}(\lambda|k)$, basta probar que $f(G_w)$ es denso en la imagen, pues como f es continua (esto es una propiedad general de los grupos profinitos, ver [6] IV sección 2) y G_w es un compacto, entonces $f(G_w)$ es compacto en un cerrado y, por tanto, cerrado.

Sea $\overline{\sigma} \in \mathrm{Gal}(\lambda|k)$ y $\overline{\sigma}\,\mathrm{Gal}(\lambda|\mu)$ un entorno de $\overline{\sigma}$, con $\mu|k$ una subextensión finita de Galois de $\lambda|k$. Vamos a probar que este entorno contien algún elemento de de la forma $f(\tau)$ para algún $\tau \in G_w$. Como el cuerpo residual de Z_w es k, existe una subextensión finita de Galois $M|Z_w$ de $L|Z_w$ con cuerpo residual $\overline{M}$ que contenga a μ. Por el lema anterior $\mathrm{Gal}(M|Z_w) \longleftarrow \mathrm{Gal}(\overline{M}|k)$ es sobreyectiva. Por tanto, la composición

$$G_w = \mathrm{Gal}(L|Z_w) \longrightarrow \mathrm{Gal}(M|Z_w) \longrightarrow \mathrm{Gal}(\overline{M}|k) \longrightarrow \mathrm{Gal}(\mu|k)$$

también es sobreyectiva y si $\tau \in G_w$ va a $\overline{\sigma}|_\mu$, entonces $f(\tau) \in \overline{\sigma}\,\mathrm{Gal}(\lambda|k)$.

Definición A.20. *El cuerpo fijo*

$$T_w = T_w(L|K) = \left\{x \in L : \forall \sigma \in I_w, \quad \sigma x = x\right\}$$

se denomina cuerpo de inercia.

La proposición A.19 nos da el isomorfismo

$$\mathrm{Gal}(T_w|Z_w) \cong \mathrm{Gal}(\lambda|k).$$

Además, el siguiente resultado nos relaciona I_w con alguien a quien ya conocíamos.

Proposición A.20. La extensión $T_w|Z_w$ es la subextensión maximal no ramificada de $L|Z_w$.

Demostración. Llamamos $K = Z_w$. Por la proposición A.17 podemos asumir que K es henseliano. Sea $T|K$ la subextensión maximal no ramificada de $L|K$. Es una extensión de Galois porque sus extensiones conjugadas también son no ramificadas. Por la proposición A.11, T tiene por cuerpo residual λ_s. Además, la aplicación

$$\mathrm{Gal}(T|K) \longrightarrow \mathrm{Gal}(\lambda_s|k)$$

es un isomorfismo. La sobreyectividad se deduce del resultado anterior y la inyectividad se deduce de que $T|K$ es no ramificada: el grado de cada subextensión finita de Galois es el grado de la extensión de cuerpos residuales. Por tanto, un elemento $\sigma \in \mathrm{Gal}(L|K)$ induce la identidad en λ_s si, y sólo si, pertenece a $\mathrm{Gal}(L|T)$. Luego $\mathrm{Gal}(L|T) = I_w$, con lo cual $T = T_w$. ∎

Si, en particular, K es un cuerpo henseliano y $\overline{K}_s|K$ es su clausura separable, entonces el cuerpo de inercia de esta extensión es la extensión maximal no ramificada $T|K$ y tiene cuerpo residual $\overline{k}_s|k$. El isomorfismo

$$\mathrm{Gal}(T|K) \cong \mathrm{Gal}(\overline{k}_s|k)$$

nos da una correspondencia $1-1$ de la extensiones no ramificadas de K y las separables de k.

Al igual que el grupo de inercia, el grupo de ramificación R_w es el núcleo de otro homomorfismo canónico

$$I_w \longrightarrow \chi(L|K)$$

donde

$$\chi(L|K) = \mathrm{Hom}(\Delta/\Gamma, \lambda^*),$$

donde $\Delta = w(L^*)$ y $\Gamma = v(K^*)$. Si $\sigma \in I_w$, entonces el homomorfismo asociado

$$\chi_\sigma : \Delta/\Gamma \longrightarrow \lambda^*$$

viene dado por $\overline{\delta} = \delta \mod \Gamma \in \Delta/\Gamma$, elegimos $x \in L^*$ tal que $w(x) = \delta$ y ponemos

$$\chi_\sigma(\overline{\delta}) = \frac{\sigma x}{x} \mod \mathfrak{p}_w$$

Esta definición no depende del representante $\delta \in \overline{\delta}$ ni del $x \in L^*$ elegidos. En efecto, si $x' \in L^*$ es un elemtento tal que $w(x') \cong w(x) \mod \Gamma$, entonces $w(x') = w(xa)$ con

$a \in K^*$. Por tanto, $x' = xau$, con $u \in \mathcal{O}_w^*$ y, como $\sigma u \equiv u \mod \mathfrak{p}_w$(porque $\sigma \in I_w$), tenemos que $\sigma x'/x' \equiv \sigma x/x \mod \mathfrak{p}_w$.

Es inmediato comprobar que la aplicación así definida $\sigma \mapsto \chi_\sigma$ es un homomorfismo de núcleo R_w.

Proposición A.21. R_w es el único p-subgrupo de Sylow de I_w.

Observación A.8. Si $L|K$ es una extensión finita, el enunciado de la proposición tiene perfecto sentido. En caso de que $L|K$ sea una extensión infinita, entenderemos dicho enunciado en el sentido de los grupos profinitos. Es decir, todos los cocientes finitos del grupo R_w, resp. I_w/R_w, por subgrupos normales cerrados tienen por orden una potencia de p, resp. orden coprimo con p.

Demostración. ([6] 9.12)

Definición A.21. *EL cuerpo fijo de* R_w,

$$V_w = V_w(L|K) = \left\{x \in L : \forall x \in R_w, \quad \sigma x = x\right\}$$

se denomina cuerpo de ramificación.

Proposición A.22. La extensión $V_w|Z_w$ es la subextensión maximal moderadamente ramificada de $L|K$.

Demostración. Como la imagen de la valoración y el cuerpo residual no cambian en Z_w y gracias la proposición A.17, podemos suponer que el cuerpo $K = Z_w$ es henseliano. Como R_w es el p-grupo de Sylow de I_w, su cuerpo fijo V_w es la unión de todas las subextensiones de $L|K$ de grado coprimo con p. Por tanto, V_w contiene a la extensión maximal moderadamente ramificada V de T (y de Z_w). Como el grado de cada subextensión finita $M|V$ de $V_w|V$ no es divisible por p su cuerpo residual es separable. Por tanto, $V_w|V$ es moderadamente ramificada, con lo cual $V = V_w$.

Corolario A.6. Se tiene la sucesión exacta

$$1 \longrightarrow R_w \longrightarrow I_w \longrightarrow \chi(L|K) \longrightarrow 1$$

Demostración. Al igual que en las demostraciones anteriores la proposición A.17 nos permite suponer que el cuerpo K es henseliano. Vamos a probar el caso en que la extensión $L|K$ es finita. Para el caso infinito se procede con en la prueba de la proposición A.19. Ya hemos visto que R_w es el núcleo de la flecha de la derecha. Basta probar que

$$(I_w : R_w) = [V_w : T_w] = \#\chi(L|K).$$

Como $T_w|K$ es la subextensión maximal no ramificada de $V_w|K$, $V_w|T_w$ tiene grado de inercia 1. Por tanto, por el teorema A.12 se cumple la igualdad

$$[V_w : T_w] = \#(w(V_w^*)/w(T_w^*)).$$

También sabemos que $w(T_w) = v(K^*) =: \Gamma$. Si ahora llamamos $\Lambda = w(L^*)$, también hemos probado que

$$w(V_w^*)/v(K^*) \cong \Delta^{(p)}/\Gamma \leq \Delta/\Gamma.$$

Luego,

$$[V_w : T_w] = \#(\Delta^{(p)}/\Gamma).$$

Como λ^* no tiene elementos de orden divisible por p, tenemos que

$$\chi(L|K) = \mathrm{Hom}(\Delta/\Gamma, \lambda^*) = \mathrm{Hom}(\Delta^{(p)}/\Gamma, \lambda^*).$$

Además, λ^* contiene una raíz m-ésima siempre que $\Delta^{(p)}/\Gamma$ contenga un elemento de orden m, ya que en ese caso hay una subextensión de Galois de $V_w|T_w$ de la forma $T_w(\sqrt[m]{a})|T_w$ por el teorema A.12. Por tanto,

$$[V_w : T_w] = \#(\Delta^{(p)}/\Gamma) = \chi(L|K).$$

Bibliografía

[1] Michael F. Atiyah; Ian G. Mcdonald , 'Introducción al Álgebra Conmutativa'. *Reverté* (1978).

[2] Sara Arias-de-Reyna 'DEA: Representaciones de Galois asociadas a los puntos de torsión de una curva' elíptica'. Barcelona (Spain), (Junio 2006).

[3] J.W.S. Cassels, A. Frölich 'Algebraic Number Theory'. *Thompson Book Company INC* (1967).

[4] A. Frölich 'Formal groups'. *Springer* (1968).

[5] J.S. Milne 'Algebraic Number Theory'. Material autoeditado (2020) `https://www.jmilne.org/math/CourseNotes/ANT.pdf`

[6] Jürgen Neukirch, 'Algebraic Number Theory'. *Springer* 2nd Edition (1999).

[7] J-P. Serre, 'Abelian l-Adic Representations and Elliptic Curves'. *McGRaw-Hill* (1968).

[8] J-P. Serre, 'Local Fields'. *Springer* (1995).

[9] J-P. Serre,, 'Proprietes galoisiénnés des points d'ordre fini des courbes elliptiques', Inventiones Math. 15, 259–331 (1972).

[10] Joseph H. Silverman, 'The Arithmetic of Elliptic Curves'. *Springer* 2nd Edition (1986).

[11] Joseph H. Silverman, 'Advanced Topics in the Arithmetic of Elliptic curves'. *Springer* (1994).