U F R O

Universidad de La Frontera

CUERPOS DE MÓDULI Y CUERPOS DE DEFINICIÓN

Rubén A. Hidalgo

Departamento de Matemática y Estadística
Universidad de La Frontera

Rubén A. Hidalgo

CUERPOS DE MÓDULI Y CUERPOS DE DEFINICIÓN

Rubén A. Hidalgo
Departamento de Matemática y Estadística, Universidad de La Frontera, Temuco, Chile.
E-mail : ruben.hidalgo@ufrontera.cl
Url : http://dme.ufro.cl/rhidalgo

***Classificación matemática por tema* (2000). —** 14E99, 14A10, 12F10, 30F10, 30F40.

***Palabras claves*. —** Extensión de Galois, Variedades algebraicas, Curvas algebraicas, Automorfismos, Superficies de Riemann.

Esta monografía fué patrocinado por los proyectos Fondecyt 1150003 y ANILLO ACT 1415 PIA-CONICYT.

CUERPOS DE MÓDULI Y CUERPOS DE DEFINICIÓN

Rubén A. Hidalgo

A Betty, Cata y Pucky

INTRODUCCIÓN

Sea $K < L$ una extensión de cuerpos y $X \subset \mathbb{P}^n_L$ una variedad algebraica proyectiva definida sobre L. Denotamos por $\mathrm{Aut}(X)$ al grupo de los automorfsimos birracionales de X definidos sobre L. Denotamos por $[X]$ al conjunto de todas las variedades birracionalmente equivalentes a X. Si X_1 y X_2 son birracionalmente equivalents, entonces esto lo denotamos por $X_1 \cong X_2$.

Dada una variedad algebraica proyectiva $X \subset \mathbb{P}^n_L$, en general no es posible decidir si existe otra variedad algebraica proyectiva $Y \subset \mathbb{P}^m_L$, $Y \cong X$, que esté definida sobre K. En el caso afirmativo, decimos que X es definible sobre K y que K es un cuerpo de definición de X.

No es claro que la intersección de todos los subcuerpos de L sobre los cuales X es definible es también un cuerpo de definición de X.

Si la extensión $K < L$ es de Galois, entonces existe una acción natural del grupo de Galois $\mathrm{Aut}(L/K)$. Para cada $\sigma \in \mathrm{Aut}(L/K)$, se puede definir una nueva variedad algebraica proyectiva $X^\sigma \subset \mathbb{P}^n_L$, la cual satisface los mismos invariantes algebraicos que X, pero que en general (salvo para curvas) no son del mismo tipo topológico. Si $\sigma \in \mathrm{Aut}(L/K)$ y $Y_1 \cong Y_2$, entonces $X^\sigma \cong Y^\sigma$. Así, tenemos la acción transitiva de $\mathrm{Aut}(L/K)$ sobre la órbita $\mathcal{O}_X = \{[X^\sigma] : \sigma \in \mathrm{Aut}(L/K)\}$. El estabilizador, por tal acción, sobre el punto $X \in \mathcal{O}_X$ define un subgrupo $G_X < \mathrm{Aut}(L/K)$, dado por

$$G_X = \{\sigma \in \mathrm{Aut}(L/K) : X^\sigma \cong X\}.$$

El subgrupo G_X tiene asociado un cuerpo fijo, denotado por $M_{L/K}(X)$, donde $K < M_{L/K}(X) < L$. Tal cuerpo es llamado el cuerpo de móduli de X.

Todo cuerpo de definición de X necesariamente contiene el cuerpo $M_{L/K}(X)$. Luego, si $M_{L/K}(X)$ es un cuerpo de definición, entonces este el cuerpo de definición más pequeño de X.

El problema de decidir si $M_{L/K}(X)$ es un cuerpo de definición de X es muy dificil. Existen condiciones necesarias y suficientes (Teorema de Weil) para que $M_{L/K}(X)$ sea un cuerpo de definición. Tales condiciones son dificiles de verificar en la práctica, con la posible excepción de ciertos casos particulares, por ejemplo, cuando $\mathrm{Aut}(X)$ es trivial.

En el caso que X es una curva algebraic proyectiva no-singular, existen varios resultados, tanto negativos como positivos, respecto a la pregunat de si $M_{L/K}(X)$ es cuerpo de definición o no. En este caso, X tiene una estructura de superficie de Riemann compacta y los morfismos algebraicos son funciones holomorfas. Así, uno puede utilizar herramientas propias del análisis complejo para estudiar este tipo de problemas.

Una curva algebraica proyectiva no-singular (o superficie de Riemann compacta) X, definida sobre $\mathbb{C}$, la cual admite una función holomorfa no-constante $f : X \to \mathbb{P}^1_{\mathbb{C}}$ (no necesariamente de Galois) con a lo más tres valores críticos, es llamada una curva de Belyi (la función es llamada una función de Belyi). Un resultado muy impresionante, debido a Belyi, nos dice que toda curva de Belyi está definida sobre $\overline{\mathbb{Q}}$ y viceversa.

Curvas de Belyi se relacionan con los *Dessin's de enfants* (diseños de niños) desarrollado por Grothendieck en su *Esquisse d'un programme* en 1984. Toda función de Belyi produce de manera natural diseños de niños y viceversa cada diseño de niños (sobre una superficie compacta orientable) induce una estructura de superficie de Riemann que resulta ser una curva de Belyi (el diseño de niño induce de manera natural una función de Belyi).

Todo lo anterior permite ver una relación entre combinatoria, superficies de Riemann y Teoría de Galois. Esto ha desarrollado un mundo fascinante para investigar y por ahora una fuente de inspiración de muchos matemáticos.

Estas notas tienen como propósito dar un pequeño recuento de este tema para introducir a estudiantes avanzados y no especialistas de manera rápida en este tema en un lenguage lo más simple posible. Como suele ocurrir cuando se escriben notas, estas irán incrementandose y corrigiendose con el tiempo.

Finalmente, quiero agradecer a Gabino González-Diez, Mauricio Godoy y Sebastián Reyes por su ayuda en la elaboración de estas notas y discusiones de los temas aquí tratados.

Rubén A. Hidalgo
Temuco, Chile, 2017

TABLA DE MATERIAS

CAPÍTULO 1

PRELIMINARES ALGEBRAICOS

En este capítulo recordaremos algunos hechos básico en la teoría de Galois que necesitaremos para el resto de las notas. Los textos de Artin [**1**], Jacobson [**18**] y Stewart [**32**] pueden ser consultados para una mayor comprensión del tema. Daremos la definición de una extensión de Galois general, que en general no es una extensión de Galois, pero que emula parte de la teoría de Galois. Para esto último, la idea es pensar en la extensíon del cuerpo $\mathbb{Q}$ dada por el cuerpo $\mathbb{C}$, lo cual será suficiente para estas notas.

1.1. Cuerpos de extensión

Definición 1.1.1. — Sea K un cuerpo. La **característica** de K es definido como el menor entero positivo n_K (si es que existe) tal que la suma de n_K veces la unidad multiplicativa $1 \in K$ es igual a 0 ; en caso contrario, la característica es definida como 0.

Tarea 1. — *Sea K un cuerpo.*

1. *Si $n_k \neq 0$ es la característica de K, entonces existe un homomorfismo de anillos $\phi : \mathbb{Z}_{n_k} \to K$. Concluir que n_K debe ser un número primo.*
2. *Si la característica de K es un primo p, entonces verificar que existe un subcuerpo de K isomorfo a cuerpo finito $\mathbb{Z}_p$. Este es llamado el cuerpo básico de K.*
3. *Si la característica de K es 0, entonces verificar que existe un subcuerpo de K isomorfo a cuerpo de los racionales $\mathbb{Q}$. Este es llamado el cuerpo básico de K.*

Definición 1.1.2. —

1. Un cuerpo L es llamado una **extensión del cuerpo** K, esto denotado por $K < L$ (la notación clásica es L/K) si K es un subcuerpo de L.
2. Si $K < L$, entonces L es un K-espacio vectorial. La dimensión de L como K-espacio vectorial, $\dim_K L = [L : K]$, es llamado el **grado de la extensión**.
3. Si $K < L$, entonces denotamos por $\mathrm{Aut}(L/K)$ al grupo de los automorfismos del cuerpo L que actúan como la identidad sobre el subcuerpo K.

Tarea 2. — *Verificar que*

$$\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{I\}, \quad \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \langle \sigma(x) = \overline{x} \rangle \cong \mathbb{Z}_2$$

Definición 1.1.3. — Sea $K < L$. Si $A \subset L$, entonces denotaremos por $K(A)$ al subcuerpo más pequeño de L que contiene a K y todo los elementos de A. En el caso particular que $A = \{u\}$, usaremos la notación $K(u)$.

Tarea 3. —

1. *Sea $K < L$, $A \subset L$. Verificar que $K(A)$ es dado por la intersección de todos los subcuerpos de L que contienen a K y A.*
2. *Si $K < N < L$, donde $K < N$ es de grado $[N : K]$ y $N < L$ es de grado $[L : N]$, entonces $K < L$ es de grado $[L : K] = [L : N][N : K]$.*

Proposición 1.1.4. — *Sea $K < L$ una extensión de cuerpos y $\{\sigma_1, ..., \sigma_n\} \subset \mathrm{Aut}(L/K)$ un subconjunto finito no vacío. Si $\lambda_1, ..., \lambda_n \in L$ so tales que, para cada $a \in L$ vale que*

$$\lambda_1\sigma_1(a) + \cdots + \lambda_n\sigma_n(a) = 0,$$

entonces

$$\lambda_1 = \cdots = \lambda_n = 0.$$

Demonstración. — Supongamos que, por el contrario, existen $\lambda_1, ..., \lambda_n \in L$, no todos igual a 0, de manera que, para cada $a \in L$, vale que $\lambda_1\sigma_1(a) + \cdots + \lambda_n\sigma_n(a) = 0$.

De entre todas esas posibles elecciones para λ_1,..., λ_n, escogemos una que minimize la cantidad de valores diferentes de cero ; digamos que el número minimal de tales valores es m. Así, módulo una permutatción de los índices $\{1, 2, ..., n\}$, podemos asumir que

$$\lambda_1\sigma_1(a) + \cdots + \lambda_m\sigma_m(a) = 0, \ \forall a \in L,$$

$$\lambda_j \neq 0, \ j \in \{1, ..., m\}.$$

Es claro que $m \geq 2$, ya que si $m = 1$, tendríamos que $\lambda_1\sigma_1(a) = 0$, para todo $a \in L$. Como $\lambda_1 \neq 0$, esto diría que $\sigma_1(a) = 0$, para todo $a \in L$; una contradicción tomando $a = 1$.

Como $\sigma_1 \neq \sigma_2$, existe algún $b \in L$ tal que $\sigma_1(b) \neq \sigma_2(b)$.

Tenemos las siguientes iguladades :

$$0 = \lambda_1\sigma_1(ab) + \cdots + \lambda_m\sigma_m(ab) = \lambda_1\sigma_1(a)\sigma_1(b) + \cdots + \lambda_m\sigma_m(a)\sigma_m(b)$$

$$0 = \sigma_1(b)(\lambda_1\sigma_1(a) + \cdots + \lambda_m\sigma_m(a)) = \lambda_1\sigma_1(a)\sigma_1(b) + \cdots + \lambda_m\sigma_m(a)\sigma_1(b),$$

de donde se obtiene que

$$0 = \underbrace{\{\lambda_2(\sigma_2(b) - \sigma_1(b))\}}_{\widehat{\lambda_2}}\sigma_2(a) + \cdots + \underbrace{\{\lambda_m(\sigma_m(b) - \sigma_1(b))\}}_{\widehat{\lambda_m}}\sigma_m(a).$$

Como $\widehat{\lambda_2} \neq 0$, obtenemos una contradicción a la minimalidad de m.

□

1.2. Acciones de $\mathrm{Aut}(L/K)$ sobre $L[x_1, ..., x_n]$

Consideremos una extensión $K < L$ y su grupo de automorfismos $\mathrm{Aut}(L/K)$.

Si $P(x_1, ..., x_n) = \sum a_{i_1,...,i_n} x_1^{i_1} \cdots x_n^{i_n} \in L[x_1, ..., x_n]$, y $\sigma \in \mathrm{Aut}(L/K)$, entonces definimos la acción de σ sobre P como

$$P^\sigma(x_1, ..., x_n) = \sum \sigma(a_{i_1,...,i_n}) x_1^{i_1} \cdots x_n^{i_n} \in L[x_1, ..., x_n].$$

Notemos que si $r_1, ..., r_n \in L$, entonces

$$\sigma \circ P \circ \sigma^{-1}(r_1, ..., r_n)) = \sum \sigma(a_{i_1,...,i_n}) r_1^{i_1} \cdots r_n^{i_n} = P^\sigma(r_1, ..., r_n).$$

1.3. Extensiones algebraicas

Definición 1.3.1. — Si $K < L$, entonces un elemento $u \in L$ es llamado **algebraico sobre** K si existe un polinomio $P(x) \in K[x] - \{0\}$ tal que $P(u) = 0$ (visto esto en L) ; en caso contrario, diremos que $u \in L$ es **trascendental sobre** K.

Tarea 4. — *Sea $K < L$ y $u \in L$. Considere la función*

$$\phi : K[x] \to K(u) < L : P(x) \mapsto \phi(P(x)) = P(u).$$

1. *Si u es trascendental sobre K, entonces ϕ induce un isomorfismo $K(x) \cong K(u)$, donde $K(x)$ denota el cuerpo de las funciones racionales con coeficientes en K.*
2. *Sea u algebraico sobre K. Verifique que el núcleo I de ϕ es un ideal principal. Sea $P_u(x) \in K[x]$ el único generador de I que es mónico (este polinomio es llamado el polinomio minimal de u). Ver que $P_u(x)$ es irreducible en $K[x]$ y concluir que I es ideal maximal de $K[x]$. Ver que ϕ induce un isomorphismo entre $K(u)$ y el cuerpo $K[x]/I$.*

Definición 1.3.2. — Una extensión $K < L$ es llamada una **extensión algebraica** si todos los elementos de L son algebraicos sobre K ; en caso contrario decimos que es una extensión trascendental.

Tarea 5. —

1. *Sea $K < L$. Si $\alpha \in L$ es algebraico sobre K, entonces $K(\alpha)$ es una extensión de grado finito sobre K. De manera similar, si $\alpha_1, ..., \alpha_r \in L$ son algebraicos sobre K, entonces $K(\alpha_1, ..., \alpha_r)$ es una extensión de grado finito sobre K.*
2. *Si $K < L$ es una extensión finita (es decir de grado finita), entonces ella es una extensión algebraica.*
3. *Sea $K < N < L$, de manera que la extensión $K < N$ es algebraica sobre K y $N < L$ es algebraica sobre N. Verificar que $K < L$ es algebraica sobre K. Ind. Si $\alpha \in L$, entonces existe un polinomio $Q(x) = a_0 + a_1 x + \cdots a_n x^n \in N[x]$ tal que $Q(\alpha) = 0$. Ahora considere el cuerpo $M = \langle K, a_0, ..., a_n \rangle$. Notar que M es una extension de grado finito sobre K y que $M(\alpha)$ es una extesión de grado finito sobre M. Concluir que $M(\alpha)$ es una extensión de grado finito sobre K.*
4. *Verificar que $\mathbb{R}$ no es una extensión algebraica de $\mathbb{Q}$.*

Definición 1.3.3. —

1. Un cuerpo F es llamado **algebraicamente cerrado** si todo polinomio de grado positivo en $F[x]$ tiene raices en F.
2. Una **clausura algebraica** de un cuerpo K es un cuerpo de extensión $K < L$ que es algebraicamente cerrado y tal que todos los elementos de L son algebraicos sobre K.

Tarea 6. —

1. *Ver que $\mathbb{C}$ es una clausura algebraica de $\mathbb{R}$ pero que no es clausura algebraica de $\mathbb{Q}$.*
2. *Sea $K < L$ una extensión algebraica de K. Verificar que existe una clausura algebraica comun de K y L.*

Teorema 1.3.4. — *Todo cuerpo tiene al menos una clausura algebraica.*

Tarea 7. — *Utilice el Lema de Zorn para probar el Teorema 1.3.4.*

Tarea 8. — *El Teorema 1.3.4 nos dice que cada cuerpo tiene al menos una clausura algebraica. Esta tarea tiene como objetivo verificar que todas ellas son isomorfas como cuerpo.*

1. *Sea $K < L$ y $K < M$, donde L y M son algebraicamente cerrados. Sea $\alpha \in L$ un elemento algebraico sobre K, cuyo polinomio minimal es $P_\alpha(x) \in K[x]$. Sea $\beta \in M$ tal que $P_\alpha(\beta) = 0$. Ver que es posible extender el automorfismo trivial $I : K \to K : k \mapsto k$ a un isomomorfismo $\sigma : K(\alpha) < L \to K(\beta) < M$.*
2. *Verificar que dos clausuras algebraicas del mismo cuerpo son necesariamente isomorfas.*

1.4. Extensiones separables

Definición 1.4.1. — Una extension algebraica $K < L$ es llamada **separable** si para todo $u \in L$ vale que el polinomio minimal $P_u(x) \in K[x]$ tiene todas sus raices simples en una clausura algebraica de K.

Observación 1.4.2. — Existen cuerpos con extensiones algebraicas que no son separables. En particular, para tales cuerpos, una clausura algebraica no es una extensión separable. En estos casos, uno puede considerar sólo las extensiones algebraicas finitas separables y construir (usando el Lema de Zorn) clausuras algebraicas separabales. Estas clausuras algebraicas separables coinciden con las clausuras algebraicas para aquellos cuerpos donde no existe un aextension finita no-separable.

Definición 1.4.3. — Un cuerpo K es llamado un **cuerpo perfecto** si

1. K tiene característica 0 ; o bien
2. K tiene característica finita $p \neq 0$ y cada elemento de K tiene una raíz p-ésima en K (por ejemplo, si K es finito).

Tarea 9. —

1. *Verificar que si K es un cuerpo perfecto y $K < L$ es una extension algebraica, entonces esta es siempre una extensión separable.*

2. *Sea $K < L$, donde K es un cuerpo perfecto y L es una clausura algebraica de K. Sea $\alpha \in L$ un elemento algebraico sobre K, cuyo polinomio minimal es $P_\alpha(x) \in K[x]$ el cual tiene grado d. Ver que e número de extensiones del automorfismo trivial $I : K \to K : k \mapsto k$ a un monomorfismo $\sigma : K(\alpha) \to L$ es exáctamente d.*

1.5. Extensiones de Galois

1.5.1. Extensiones de Galois finita. —

Definición 1.5.1. — Una extensión finita $K < L$ es llamada una **extensión de Galois finita** si
(i) $K < L$ es una extensión separable y
(ii) para todo $u \in L$ vale que su polinomio minimal tiene todas sus raices en L.

1.5.2. Extensiones de Galois infinita. —

Definición 1.5.2. — Una extensión infinita $K < L$ que es la unión de extensiones finitas de Galois de K es llamada una **extension de Galois infinita**. Es decir, tenemos extensiones de Galois finitas $K < E_j$ ($j \in J$), donde $E_j < L$ y $\cup_{j\in J} E_j = L$.

Tarea 10. — *Ver que toda extensión de Galois infinita es una extensión algebraica.*

Observación 1.5.3. — Si K es un cuerpo perfecto y $\overline{K}$ es una clausura algebraica, entonces $\overline{K}$ define una extensión de Galois sobre K.

1.5.3. Topología de Krull. — Supongamos que tenemos una extensión de Galois infinita $K < L$. Por definición, tenemos extensiones de Galois finitas $K < E_j$ ($j \in J$), donde $E_j < L$ y $\cup_{j\in J} E_j = L$.

Tarea 11. — *Si $\sigma \in \mathrm{Aut}(L/K)$, entonces su restricción σ_{E_j} a la extensión de Galois finita E_j induce un elemento de $\mathrm{Aut}(E_j/K)$.*

Por cada $\sigma \in \mathrm{Aut}(L/K)$ podemos considerar sus rectricciones $\sigma_{E_j} \in \mathrm{Aut}(E_j/K)$. De esta manera, tenemos una función

$$\Phi : \mathrm{Aut}(L/K) \to \prod_{j\in J} \mathrm{Aut}(E_j/K)$$
$$\sigma \to \Phi(\sigma) = (\sigma_{E_j})_{j\in J}$$

Tarea 12. — *Verificar que Φ es una función inyectiva.*

Cada grupo de Galois $\mathrm{Aut}(E_j/K)$ es un grupo finito, de orden igual al grado de la extensión $K < E_j$. Dotamos a $\mathrm{Aut}(E_j/K)$ de la topología discreta y consideramos la topología producto en $\prod_{j\in J} \mathrm{Aut}(E_j/K)$. Esta es una topología Hausdorff ya que cada factor lo es.

Consideramos la topología inducida sobre $\Phi(\mathrm{Aut}(L/K))$ y la regresamos por medio de la función inyectiva Φ a $\mathrm{Aut}(L/K)$ (dejando a Φ como un homeomorfismo sobre su imágen). Esta es llamada la **Topología de Krull** en $\mathrm{Aut}(L/K)$. Notamos que con esta topología de Krull, el espacio topológico $\mathrm{Aut}(L/K)$ es Hausdorff.

Notemos que cada $\mathrm{Aut}(E_j/K)$ es un abierto en la topología de Krull. Una base para tal topología es dada por los abiertos de la forma $\sigma\mathrm{Aut}(E/K)$, donde $K < E < L$ y $K < E$ recorre todas las extensiones de Galois finitas.

Teorema 1.5.4. — *Sea $K < L$ una extensión de Galois. Entonces la topología de Krull en $\mathrm{Aut}(L/K)$ es totalmente disconexa.*

Demonstración. — Sea $A \subset \mathrm{Aut}(L/K)$ tal que hay dos puntos diferentes $\sigma_1, \sigma_2 \in A$. Como $\mathrm{Aut}(L/K)$ es Hausdorff, podemos encontrar un subgrupo $\Gamma = \mathrm{Aut}(N/K) < \mathrm{Aut}(L/K)$, donde $K < N$ es extensión de Galois finita, de manera que $\sigma_2 \notin \sigma_1\Gamma$. Notemos que $\sigma_1\Gamma$ es un abierto que contiene a σ_1. También, como $\mathrm{Aut}(L/K) - \sigma_1\Gamma$ es una unión de clases laterales de Γ ; este conjunto también es un abierto y contiene a σ_2. De esta manera, A es unión disjunta de abiertos inducidos, cada uno no vacío : $A = (\sigma_1\Gamma \cap A) \cup ((\mathrm{Aut}(L/K) - \sigma_1\Gamma) \cap A)$.

□

1.5.4. Subgrupos cerrados. — Sea $K < L$ una extensión de Galois y $G < \mathrm{Aut}(L/K)$ un subgrupo.

Si la extensión de Galois es finita, entonces la topología de Krull no es nada más que la topología discreta. En este caso G es un grupo cerrado siempre.

Si la extensión de Galois es infinita, entonces podemos considerar el cuerpo fijo

$$L^G = Fix(G) = \{l \in L : \sigma(l) = l,\ \forall \sigma \in G\}$$

y el subgrupo

$$\overline{G} = \mathrm{Aut}(L/L^G) = \{\sigma \in \mathrm{Aut}(L/K) : \sigma|_{L^G} = I_{L^G}\}.$$

Claramente, $G < \overline{G}$. El grupo $\overline{G}$ es la clausura en la topología de Krull del grupo G. Equivalentemente, el grupo G es cerrado en la topología de Krull si $G = \mathrm{Aut}(L/L^G)$.

1.5.5. Teorema fundamental de la teoría de Galois. — El resultado principal de la teoría de Galois finita es el siguiente.

Teorema 1.5.5 **([1, 18, 32])**. —

1. *Sea $K < L$ una extensión de Galois finita y consideremos las categorías siguientes :*

$$\mathfrak{A} = \{G < \mathrm{Aut}(L/K)\}$$
$$\mathfrak{B} = \{N : K < N < L\}$$

Entonces las funciones

$$\tau_{\mathfrak{A}\mathfrak{B}} : \mathfrak{A} \to \mathfrak{B} : G \mapsto \tau_{\mathfrak{A}\mathfrak{B}}(G) = Fix(G) = \{x \in L : g(x) = x,\ \forall g \in G\}$$
$$\tau_{\mathfrak{B}\mathfrak{A}} : \mathfrak{B} \to \mathfrak{A} : N \mapsto \tau_{\mathfrak{B}\mathfrak{A}}(G) = \{\sigma \in \mathrm{Aut}(L/K) : \sigma(x) = x,\ \forall x \in N\}$$

son una inversa de la otra, en particular, invertibles.

2. *Sea $K < L$ una extensión de Galois infinita y consideremos las categorías siguientes :*

$$\mathfrak{A}_c = \{G < \mathrm{Aut}(L/K)\ \textit{subgrupos cerrados}\}$$
$$\mathfrak{B} = \{K < N < L\}$$

Entonces las funciones

$$\tau_{\mathfrak{A}_c\mathfrak{B}} : \mathfrak{A}_c \to \mathfrak{B} : G \mapsto \tau_{\mathfrak{A}_c\mathfrak{B}}(G) = Fix(G) = \{x \in L : g(x) = x,\ \forall g \in G\}$$
$$\tau_{\mathfrak{B}\mathfrak{A}_c} : \mathfrak{B} \to \mathfrak{A}_c : N \mapsto \tau_{\mathfrak{B}\mathfrak{A}_c}(G) = \{\sigma \in \mathrm{Aut}(L/K) : \sigma(x) = x,\ \forall x \in N\}$$

son una inversa de la otra, en particular, invertibles.

Proposición 1.5.6. — *Sea $K < L$ una extensión de Galois finita, digamos de grado m. Sean $\mathrm{Aut}(L/K) = \{\sigma_1, ..., \sigma_m\}$, donde σ_1 es la identidad, y sea $\{e_1, e_2, ..., e_m\}$ una base de L como espacio vectorial sobre K. Entonces la matriz*

$$A = \begin{bmatrix} e_1 & e_2 & \cdots & e_m \\ \sigma_2(e_1) & \sigma_2(e_2) & \cdots & \sigma_2(e_m) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_m(e_1) & \sigma_m(e_2) & \cdots & \sigma_m(e_m) \end{bmatrix}$$

tiene determinate diferente de cero. Es decir, la transformación L-lineal $A : L^m \to L^m$ es invertible.

Demonstración. — Consideremos la aplicación L-lineal

$$A : L^m \to L^m$$

$$[\lambda_1 \ \cdots \ \lambda_m] \mapsto [\lambda_1 \ \cdots \ \lambda_m]A.$$

Sólo necesitamos ver que el núcleo de esta transformación es trivial. La condición

$$[\lambda_1 \ \cdots \ \lambda_m]A = [0 \ \cdots \ 0]$$

es equivalente a

$$\begin{cases} \lambda_1\sigma_1(e_1) + \cdots + \lambda_m\sigma_m(e_1) &= 0 \\ \lambda_1\sigma_1(e_2) + \cdots + \lambda_m\sigma_m(e_2) &= 0 \\ \vdots & \vdots \ \vdots \\ \lambda_1\sigma_1(e_m) + \cdots + \lambda_m\sigma_m(e_m) &= 0 \end{cases}$$

lo cual es equivalente a tener que

$$\lambda_1\sigma_1(a) + \cdots + \lambda_m\sigma_m(a) = 0, \ \forall a \in L.$$

Como consecuencia de la Proposición 1.1.4, obtenemos que $\lambda_1 = \cdots = \lambda_m = 0$.

□

Ejemplo 1.5.7. —

1. Sea $K = \mathbb{R}$ y $L = \mathbb{C}$. En esta caso, $\mathrm{Aut}(L/K) = \langle \sigma(z) = \overline{z} \rangle \cong \mathbb{Z}_2$. Una base de L sobre K es dada por $\{e_1 = 1, e_2 = i\}$. La matriz A correspondiente es

$$A = \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$$

cuyo determinante es $-2i \neq 0$.

2. Sea $K = \mathbb{Q}$ y $L = \mathbb{Q}(\rho)$, donde $\rho = e^{2\pi i/5}$. En este caso, $\mathrm{Aut}(L/K) = \langle \sigma \rangle \cong \mathbb{Z}_4$, donde

$$\begin{cases} \sigma(\rho) = \rho^3 \\ \sigma(\rho^2) = \rho \\ \sigma(\rho^3) = \rho^4 \\ \sigma(\rho^4) = \rho^2 \end{cases}$$

Una base de L sobre K es dada por $\{e_1 = 1, e_2 = \rho, e_3 = \rho^2, e_4 = \rho^3\}$. La matriz A correspondiente es

$$A = \begin{bmatrix} 1 & \rho & \rho^2 & \rho^3 \\ 1 & \rho^3 & \rho & \rho^4 \\ 1 & \rho^4 & \rho^3 & \rho^2 \\ 1 & \rho^2 & \rho^4 & \rho \end{bmatrix}$$

cuyo determinante es $-5(\rho - \rho^2 - \rho^3 + \rho^4) \neq 0$.

La función traza $\mathrm{Tr} : L \to K : a \mapsto \sum_{\sigma\in\Gamma} \sigma(a)$ se extiende de manera natural al anillo de polinomios $\mathrm{Tr} : L[x_1, ..., x_n] \to K[x_1, ..., x_n] : P \mapsto \sum_{\sigma\in\Gamma} P^\sigma$.

Teorema 1.5.8. — *Sea $K < L$ una extensión de Galois (finita o infinita) y $\Gamma = \mathrm{Aut}(L/K)$. Sea $\{e_1, e_2, ..., e_m\}$ una base para el K-espacio vectorial L.*

1. *Si $P \in L[x_1, ..., x_n]$, entonces $P \in \mathrm{Span}_L(\mathrm{Tr}(e_1P), ..., \mathrm{Tr}(e_mP))$.*
2. *Si $I < L[x_1, ..., x_n]$ es un ideal tal que $\forall\sigma \in \Gamma$ y $\forall P \in I$ vale que $P^\sigma \in I$, entonces I se puede generar (como ideal) por polinomios en $I \cap K[x_1, ..., x_n]$.*

Demonstración. — Sea $P \in I$ y consideremos una extensión de Galois finita $K < M$, donde $M < L$, y tal que $P \in M[x_1, ..., x_n]$. Sea $I_M = I \cap M[x_1, ..., x_n]$. No es dificil ver que I_M es un ideal de $M[x_1, .., x_n]$.

Consideremos una base de M como espacio vectorial sobre K, digamos $\{e_1, e_2, ..., e_m\}$ y denotemos por $\Gamma_M = \mathrm{Aut}(M/K) = \{\sigma_1, ..., \sigma_m\}$, donde σ_1 es la identidad.

Como cada $\tau \in \Gamma_M$ puede ser visto como la restricción de algún $\sigma \in \Gamma$, notamos que $P^\tau = P^\sigma \in I$, luego $P^\tau \in I_M$.

Consideremos los siguientes polinomios de $M[x_1, ..., x_n]$

$$\begin{cases} Q_1 &= \mathrm{Tr}(e_1P) = e_1P + \sigma_2(e_1)P^{\sigma_2} + \cdots + \sigma_m(e_1)P^{\sigma_m} \\ Q_2 &= \mathrm{Tr}(e_2P) = e_2P + \sigma_2(e_2)P^{\sigma_2} + \cdots + \sigma_m(e_2)P^{\sigma_m} \\ \vdots &\vdots \quad \vdots \\ Q_m &= \mathrm{Tr}(e_mP) = e_mP + \sigma_2(e_m)P^{\sigma_2} + \cdots + \sigma_m(e_m)P^{\sigma_m} \end{cases}$$

Observamos que $Q_1, ..., Q_m \in I_M$. Además, por la construcción, para cada $\tau \in \Gamma_M$ vale que $Q_1^\tau = Q_1$,..., $Q_m^\tau = Q_m$, es decir, $Q_1, ..., Q_m \in K[x_1, ..., x_n]$. De esta manera, $Q_1, ..., Q_m \in I_M \cap K[x_1, ..., x_n] < I \cap K[x_1, ..., x_n]$.

Por la Proposición 1.5.6, tenemos que la matriz

$$A = \begin{bmatrix} e_1 & e_2 & \cdots & e_m \\ \sigma_2(e_1) & \sigma_2(e_2) & \cdots & \sigma_2(e_m) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_m(e_1) & \sigma_m(e_2) & \cdots & \sigma_m(e_m) \end{bmatrix}$$

es invertible, es decir, la transformación lineal $A : M^m \to M^m$ es invertible, donde a M^m lo pensamos como el espacio de columnas de longitud m con coeficientes en M. Esto nos asegura la existencia de valores $\lambda_1, ..., \lambda_m \in M$ tales que $A\lambda = E$, donde $\lambda = {}^t[\lambda_1\ \lambda_2\ \cdots\ \lambda_m]$ y $E = {}^t[1\ 0\ \cdots\ 0]$. Luego, $P = \lambda_1Q_1 + \lambda_2Q_2 + \cdots + \lambda_mQ_m$.

□

Ejemplo 1.5.9. — Consideremos el caso $K = \mathbb{R}$ y $L = \mathbb{C}$. En este caso $\Gamma = \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \langle\sigma(z) = \overline{z}\rangle \cong \mathbb{Z}_2$. Si $I < \mathbb{C}[x_1, ..., x_n]$ es un ideal con la propiedad de que para cada $P \in I$ vale que $P^\sigma \in I$, entonces el Teorema 1.5.8 nos dice que I se puede generar por polinomios en $I \cap \mathbb{R}[x_1, ..., x_n]$. De hecho, si consideramos la base $\{e_1 = 1, e_2 = i\}$ de $\mathbb{C}$ sobre $\mathbb{R}$, entonces si $P \in I$, tenemos que

$$Q_1 = P + P^\sigma,\ Q_2 = iP - iP^\sigma,$$

de donde obtenemos que

$$P = \frac{1}{2}Q_1 - \frac{i}{2}Q_2.$$

1.6. Extensiones de Galois general

Muchos de los resultados que veremos en esta monografía serán válidos no tan sólo para el caso de extensiones de Galois ; estos serán válidos también para otros tipos de extensiones : estas serán extensiones algebraicamente cerradas en característica cero. Primero partiremos con una definición que indica la propiedad más importante de estas extensiones.

Definición 1.6.1. — Diremos que una extensión $K < L$ es una **extensión de Galois general de** K si para todo cuerpo N, donde $K < N < L$, se tiene que $Fix(\mathrm{Aut}(L/N)) = N$.

Tarea 13. —

1. *Toda extensión de Galois es una extensión de Galois general.*
2. *El caso $K = \mathbb{Q}$ y $L = \mathbb{C}$ nos da un ejemplo de una extensión de Galois general que no es una extensión de Galois.*
3. *El caso $K = \mathbb{Q}$ y $L = \mathbb{R}$ no es una extensión de Galois general.*

El resultado siguiente determina las extensiones de Galois general.

Teorema 1.6.2. — *Sea $K < F$ es una extensión de cuerpos.*

1. *Si F es algebraicamente cerrado de caracterísitica cero, entonces $K < F$ es una extensión de Galois general.*
2. *Si $K < L$ una extensión de Galois general en característica $p \neq 0$, entonces ella es una extensión de Galois.*

1.6.1. Prueba del Teorema 1.6.2. — Primero describiremos algunos lemas necesarios para la demostración de la primera parte del Teorema

Lema 1.6.3. — *Sea $K < L < F$, donde F es algebraicamente cerrado y sea $\overline{L}$ la clausura algebraica de L en F. Si $\sigma \in \mathrm{Aut}(F/L)$, then σ define un automorfismo del cuerpo $\overline{L}$ y luego $\sigma \in \mathrm{Aut}(\overline{L}/L)$.*

Demonstración. — Sea $\sigma \in \mathrm{Aut}(F/L)$ y $a \in \overline{L}$. Como σ actúa como la identidad sobre L, se tiene que $\sigma(a)$ es cero del polinomio irreducible $Irr(a, L) \in L[x]$. Luego $\sigma(a) \in \overline{L}$. □

Lema 1.6.4. — *Sea $K < L < F$, donde F es algebraicamente cerrado y sea $\overline{L}$ la clausura algebraica de L en F. Entonces, para cada $\sigma \in \mathrm{Aut}(\overline{L}/L)$ existe una extensión $\eta \in \mathrm{Aut}(F/L)$.*

Demonstración. — Sea $\mathcal{F} = \{(M, \rho) : \overline{L} < M < F, \rho \in \mathrm{Aut}(M/L), \rho|_{\overline{L}} = \sigma\}$. Definimos la relación de orden parcial $\leq$ definida por

$$(M_1, \rho_1) \leq (M_2, \rho_2) \iff M_1 < M_2,\ \rho_2|_{M_1} = \rho_1.$$

Si consideramos una cadena

$$(M_1, \rho_1) \leq (M_2, \rho_2) \cdots,$$

entonces definimos

$$M = \cup_{j=1}^{\infty} M_j$$
$$\rho|_{M_j} = \rho_j$$

Como $M_1 < M_2 < \cdots$, se tiene que M es un cuerpo y satisface que $\overline{L} < M < F$. Ya que $\rho_j|_{M_k} = \rho_k$, para $k \leq j$, se tiene que ρ está bien definida y es de hecho un elemento de $\mathrm{Aut}(M/L)$ que es extensión de σ. De esta manera, $(M, \rho) \in \mathcal{F}$ y obtenemos que cada cadena tiene un elemento maximal.

Ahora podemos usar el Lema de Zorn para verificar la existencia de un elemento maximal $(M_\infty, \rho_\infty) \in \mathcal{F}$.
Ya que para cualquier extensión simple de M_∞ se puede escoger una extensión de ρ_∞, se tiene que $M_\infty = F$. □

Lema 1.6.5. — *Sea $K < F$, donde F es algebraicamente cerrado y suponga que todo cuerpo L, donde $K < L < F$, es perfecto. Entonces, la extensión $K < F$ es Galois general.*

Demonstración. — Sea $K < L < F$. Queremos verificar que $Fix(\mathrm{Aut}(F/L)) = L$. Es claro, por la definición, que $L < Fix(\mathrm{Aut}(F/L))$. Supongamos que existe algún $\alpha \in Fix(\mathrm{Aut}(F/L)) - L$.

Si $\alpha \in \overline{L}$, entonces (al ser L perfecto) podemos tomar un cero $\beta \in \overline{L}$ de $Irr(\alpha, L) \in L[x]$, $\beta \neq \alpha$. Luego, es posible encontra algún $\sigma \in \mathrm{Aut}(\overline{L}/L)$ tal que $\sigma(\alpha) = \beta$. Por el Lema 1.6.4, podemos extender a un $\eta \in \mathrm{Aut}(F/L)$ tal que $\eta(\alpha) = \beta \neq \alpha$, una contradicción.

Si $\alpha \notin \overline{L}$, entonces α y $\alpha + 1$ son ambos trascendentales sobre L. Luego, existe algún $\sigma \in \mathrm{Aut}(\overline{L}/L)$ tal que $\sigma(\alpha) = \alpha + 1$ y procedemos como arriba para obtener $\eta \in \mathrm{Aut}(F/L)$ con $\eta(\alpha) \neq \alpha$, una contradicción.

□

1.6.1.1. Prueba de la primera parte. — Ahora, la primera parte delTeorema 1.6.2 es consecuencia del lemma 1.6.5 y del hecho que todo cuerpo de característica cero es perfecto.

1.6.1.2. Prueba de la segunda parte. — Veamos que $K < L$ es una extension algebraica. Supongamos que existe $\gamma \in L$ que sea trascendental sobre K. Entonces $K(\gamma)$ es isomorfo al cuerpo de funciones racionales en una variable con coeficientes en K. En particular, se tiene que $K(\gamma^p) \neq K(\gamma)$. Como estamos en característica p, tenemos que

$$Q(x) = x^p - \gamma^p = (x - \gamma)^p \in L[x].$$

Ahora, si $\sigma \in \mathrm{Aut}(L/K)$ es tal que $\sigma(\gamma^p) = \gamma^p$, entonces $Q^\sigma(x) = x^p - \sigma(\gamma^p) = Q(x)$, de donde obtenemos que $\sigma(\gamma) = \gamma$, al ser γ la única raiz de Q. Pero esto nos asegura que $\mathrm{Fix}(\mathrm{Aut}(L/K(\gamma^p))) \neq K(\gamma^p)$, una contradicción.

Veamos ahora que $K < L$ es una extensión separable. Si no fuese así, existiría algún $\alpha \in L - K$ con $Q(x) = \mathrm{Irr}(\alpha, K)(x) \in K[x]$ satisfaciendo que, en $L[x]$,

$$Q(x) = (x - \alpha_1)^N \cdots (x - \alpha_n)^N \widehat{Q}(x) \in L[x],$$

donde $\alpha = \alpha_1$, $N \geq 2$, $\alpha_i \neq \alpha_j$ para $i \neq j$, y $\widehat{Q}(x)$ sin raices en L (podría ser una contante no cero).

Si $\sigma \in \mathrm{Aut}(L/K)$, entonces ella fija cada polinomio simétrico en α_1,..., α_n. Como $\mathrm{Fix}(\mathrm{Aut}(L/K)) = K$, esto nos dice que $(x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$, con lo que obtendríamos una contradicción con la propiedades de $Q(x)$.

Veamos ahora que $K < L$ es un cuerpo de descomposición. El argumento es similar al anterior. Supongamos que no fuese el caso, entonces existe $\alpha \in L - K$ con $Q(x) = \mathrm{Irr}(\alpha, K)(x) \in K[x]$ satisfaciendo que, en $L[x]$,

$$Q(x) = (x - \alpha_1) \cdots (x - \alpha_n) \widehat{Q}(x) \in L[x],$$

donde $\alpha = \alpha_1$, $\alpha_i \neq \alpha_j$ para $i \neq j$, y $\widehat{Q}(x)$ sin raices en L pero de grado al menos 2. Si $\sigma \in \mathrm{Aut}(L/K)$, entonces ella fija cada polinomio simétrico en α_1,..., α_n. Luego, $(x-\alpha_1) \cdots (x-\alpha_n) \in K[x]$, otra vez obteniendo una contradicción a las propiedades de Q y $\widehat{Q}$.

CAPÍTULO 2

CUERPOS DE MÓDULI Y DE DEFINICIÓN

2.1. Variedades algebraicas proyectivas

Consideremos un cuerpo L y denotemos por $\mathbb{P}^n_L$ el espacio proyectivo de dimensión n sobre el cuerpo L. En toda este capítulo, denotaremos por $\mathcal{C}$ a un cuerpo algebraicamente cerrado.

Teorema 2.1.1 **(Teorema de la base de Hilbert [13])**. — *Sea L un cuerpo. Todo ideal de $L[x_1, ..., x_n]$ es finitamente generado.*

El Teorema de la base de Hilbert permite dar la siguiente definición de variedad algebraica proyectiva.

Definición 2.1.2. — Sea $\mathcal{C}$ un cuerpo algebraicamente cerrado. Una **variedad algebraica proyectiva** $X \subset \mathbb{P}^n_{\mathcal{C}}$ es dado como los ceros comunes de una colección finita de polinomios homogéneos $P_1, ..., P_r \in \mathcal{C}[x_0, ..., x_n]$, donde los puntos de $\mathbb{P}^n_{\mathcal{C}}$ son denotados por $[x_0 : x_1 : \cdots : x_n]$.

Consideremos la función

$$F : \mathcal{C}^{n+1} - \{0\} \to \mathcal{C}^r$$

definida por

$$F(x_0, ..., x_n) = (P_1(x_0, ..., x_n), ..., P_r(x_0, ..., x_n))$$

y la proyección natural

$$\pi : \mathcal{C}^{n+1} - \{0\} \to \mathbb{P}^n_{\mathcal{C}}.$$

Si $X \subset \mathbb{P}^n_{\mathcal{C}}$ y $\widehat{X} = F^{-1}(0)$, entonces $\pi(\widehat{X}) = X$.

Definición 2.1.3. — Sea $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica. Diremos que un punto $\pi(p) \in X$ es un punto singular si $DF(p)$ no tiene rango maximal. Si X no tiene puntos singulares, entonces diremos que X es **no-singular (suave)**.

Definición 2.1.4. — Diremos que dos variedades algebraicas proyectivas, digamos $X \subset \mathbb{P}^n_{\mathcal{C}}$ y $Y \subset \mathbb{P}^m_{\mathcal{C}}$ son **equivalentes** si existe una función birracional entre ellas definida sobre $\mathcal{C}$; esto lo denotaremos por el símbolo $X \cong Y$.

Definición 2.1.5. — Sea $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica y $\mathcal{U}$ un subcuerpo de $\mathcal{C}$. Diremos que X está definida sobre $\mathcal{U}$ si existen polinomios homogéneso $Q_1, ...Q_s \in \mathcal{U}[x_0 : ... : x_n]$ tales que X es dado como los ceros comunes a ellos.

Definición 2.1.6. — Consideremos una variedad algebraica $X \subset \mathbb{P}^n_C$ y $\mathcal{U}$ un subcuerpo de $\mathcal{C}$. Diremos que un punto $p = [a_0 : a_1 : \cdots : a_n] \in X$ es $\mathcal{U}$-racional si $p = [\sigma(a_0) : \sigma(a_1) : \cdots : \sigma(a_n)]$ para cada $\sigma \mathrm{Aut}(\mathcal{C}/\mathcal{U})$.

La busqueda de puntos $\mathcal{U}$-racionales en una variedad algebraica $X \subset \mathbb{P}^n_{\mathcal{C}}$, donde $\mathcal{U} < \mathcal{C}$, es muy dificil de hacer. Inclusive esto es dificil en el caso $\mathcal{C} = \mathcal{U}$. En algunos casos particulares esto es posible.

Definición 2.1.7. — Sea L un cuerpo y $\mathcal{C}$ una clausura algebraica de L. Consideremos una curva algebraica $C \subset \mathbb{P}^n_{\mathcal{C}}$. Diremos que un divisor $D = p_1 + \cdots + p_r$ de C es L-racional si para cada $\sigma \in \mathrm{Aut}(\mathcal{C}/L)$ se tiene que $D^\sigma = \sigma(p_1) + \cdots \sigma(p_r) = D$.

Proposición 2.1.8 (**[15, 16]**). — *Sea L un cuerpo y $\mathcal{C}$ una clausura algebraica de L. Sea $C \subset \mathcal{C}$ una curva algebraica de género 0 definida sobre el cuerpo L. Si C tiene un divisor L-racional de grado impar, entonces C tiene un punto L-racional.*

Demonstración. — Sea K_C un divisor canónico sobre C, luego definido sobre L. Como C es degénero 0, el grado de K_C es -2. Sumando al divisor D multiplos enteros de K_C, podemos obtener un nuevo dividor E de grado 1 y que sigue siendo L-racional. Como consecuencia del Teorema de Riemann-Roch, se tiene que $l(E) \geq 2$. Esto nos dice que existe una función racioanl, definida sobre L, digamos f, de manera que $F = E + (f) \geq 0$. Es claro que el divisor F es L-racional, positivo y de grado 1 ; en particular, $F = p$, donde $\sigma(p) = p$, para todo $\sigma \in \mathrm{Aut}(\overline{L}/L)$. En consecuencia, $p \in C$ es un punto L-racional. □

Corolario 2.1.9 (**[15, 16]**). — *Sea $K < L$ una extensión separable de grado impar. Sea C una curva de género 0 definida sobre K. Si C tiene un punto L-racional, entonces también tiene un punto K-racional.*

Demonstración. — Sea n el grado de la extensión $K < L$, el cual estamos asumiendo impar. Sea $q \in C$ un punto L-racioanl y sean $\sigma_1, ..., \sigma_n : L \to \overline{L}$ las diferentes incrustaciones de L en una clausura algebraica $\overline{L}$ de L (que hemos fijado) con $\sigma_j(k) = k$ para todo $k \in K$. El divisor $D = \sigma_1(q) + \cdots + \sigma_n(q)$ es claramente un divisor K-racional de grado impar. Luego, la Proposición 2.1.8 nos asegura la existencia de un punto K-racional en C. □

Tarea 14. — *Si $K < L$ es una extensión de Galois y $\Gamma = \mathrm{Aut}(L/K)$.*

1. *Si $\sigma \in \Gamma$, entonces verificar que*
$$\widehat{\sigma} : \mathbb{P}^n_L \to \mathbb{P}^n_L$$
$$\widehat{\sigma}([a_0 : \cdots : a_n]) = [\sigma(a_0) : \cdots : \sigma(a_n)]$$
está bién definida y define una biyección del espacio proyectivo $\mathbb{P}^n_L$.
2. $\widehat{\sigma}^{-1} = \widehat{\sigma^{-1}}$.
3. *Sea $r \in \{0, 1, ..., n\}$ y $U_r = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n_L : x_r = 1\}$. Verificar que, para cada $\sigma \in \Gamma$, vale que $\widehat{\sigma}(U_r) = U_r$. Denote por $\pi_r : U_r \to \mathbb{L}^n$ la proyección dada por $\pi_r([x_0 : \cdots : x_n]) = (x_0, ..., x_{r-1}, x_{r+1}, ..., x_n)$. Verificar que, si*
$$\widetilde{\sigma} : L^n \to L^n$$
$$\widetilde{\sigma}(b_1, ..., b_n) = (\sigma(b_1), ..., \sigma(b_n))$$
entonces
$$\pi_r \circ \widehat{\sigma} = \widetilde{\sigma} \circ \pi_r.$$

Si tenemos una extensión de Galois $K < L$, entonces podemos considerar una clausura algebraica $\mathcal{C}$ de L. Entonces tenemos un homomorfismo sobreyectivo natural

$$\rho : \mathrm{Aut}(\mathcal{C}/K) \to \mathrm{Aut}(L/K)$$

definido por restricción.

Sea $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva definida sobre L, es decir, como los ceros comunes de una colección de polinomios homogeneos $P_1, ..., P_r \in L[x_0, ..., x_n]$.

Sean $\eta_1, \eta_2 \in \mathrm{Aut}(\mathcal{C}/K)$ tales que $\rho(\eta_1) = \rho(\eta_2) = \sigma$. Entonces se puede ver que $\widehat{\eta_1}(X) = \widehat{\eta_2}(X) = X^\sigma$ es la variedad algebraica proyectiva definida como los ceros comunes de los polinomios P_1^σ,..., P_r^σ.

Teorema 2.1.10. — *Sea $K < L$ una extensión de Galois (finita o infinita), $\Gamma = \mathrm{Aut}(L/K)$ y $\mathcal{C}$ una clausura algebraica de L. Sea $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva. Si $\forall \sigma \in \Gamma$ vale que $X^\sigma = X$, entonces X está definida sobre K.*

Demonstración. — Supongamos que las coordenadas proyectivas de $\mathbb{P}^n_L$ son dadas por $[x_0 : x_1 : \cdots : x_n]$. Tomando $x_0 = 1$, podemos considerar la variedad afín $X_0 \subset L^n$ de X.

Sea $\sigma \in \Gamma$ y $\eta \in \mathrm{Aut}(\mathcal{C}/K)$ tal que $\rho(\eta) = \sigma$. Nuestra hipótesis nos asegura que $\widetilde{\eta}(X_0) = X_0$.

Consideremos el ideal $I < \mathcal{C}[x_1, ..., x_n]$ asociado a la variedad X_0, es decir, el ideal de todos los polinomios $P \in \mathcal{C}[x_1, ..., x_n]$ tales que $P(b_1, ..., b_n) = 0$ para cada $(b_1, ..., b_n) \in X_0$.

Sea $P \in I$. Notemos que, para $(b_1, ..., b_n) \in X_0$ vale que

$$0 = \widetilde{\eta}(P(b_1, ..., b_n)) = P^\sigma(\eta(b_1), ..., \eta(b_n)) = P^\sigma \circ \widetilde{\eta}(b_1, ..., b_n).$$

Como $\widetilde{\eta} : X_0 \to X_0$ es una biyección, lo anterior dice que $P^\sigma(c_1, ..., c_n) = 0$ para cada $(c_1, ..., c_n) \in X_0$. Esto nos asegura que $P^\sigma \in I$.

Ahora, el Teorema 1.5.8 dice que I se puede generar (como ideal) por polinomios en $I \cap K[x_1, .., x_n]$; de donde obtenemos que X_0 está definida sobre K. Por el proceso de homogenización vemos que esto también es válido para X.

□

2.2. Cuerpos de definición de variedades

Definición 2.2.1. — Sea $K < L$ una extensión de cuerpos, $\mathcal{C}$ una clausura algebraica de L y $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva definida sobre L (es decir, una variedad algebraica proyectiva definida por polinomios homogéneos con coeficientes en L). Un **cuerpo de definición** de X, con respecto a la extensión $K < L$, es cualquier cuerpo N, $K < N < L$, tal que existe una variedad algebraica proyectiva $Y \cong X$ (isomorfismo birracional definido sobre L) definida sobre N.

Tarea 15. — *Sea $K < N < J < L$ tal que N es un cuerpo de definición de X. Entonces, J es también un cuerpo de definición de X.*

Observación 2.2.2. — Si tenemos $K < N < L$ donde N es un cuerpo de definición de X, no es muy claro determinar si es posible encontrar un cuerpo U, donde $K < U < N$, que también sea un cuerpo de definición de X.

2.3. Cuerpo de módulo de variedades

Definición 2.3.1. — Sea $K < L$ una extensión de cuerpos, $\mathcal{C}$ una clausura algebraica de L, y $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva definida sobre L, digamos definida por los polinomios homogéneos $P_1, ..., P_r \in L[x_0, ..., x_n]$.

1. Si $\sigma \in \mathrm{Aut}(L/K)$, entonces σ actúa sobre cada coeficiente del polinomio P_j. De esta manera, obtenemos polinomios homogéneos P_j^σ. Esta acción permite obtener una nueva variedad algebraica proyectiva X^σ, obtenida como los ceros comunes de los polinomios $P_1^\sigma, ..., P_r^\sigma \in L[x_0, ..., x_n]$.
2. $L_K(X) := \{\sigma \in \mathrm{Aut}(L/K) : X \cong X^\sigma\}$. Los isomorfismos birracionales están definidos sobre L.
3. Se define el **cuerpo de móduli** $M_{L/K}(X)$ de X, respecto a la extensión $K < L$, como el cuerpo fijo del subgrupo $L_K(X)$.

Observación 2.3.2. — Consideremos la extensión de Galois de grado dos dada por $\mathbb{Q} < \mathbb{Q}(\sqrt{3})$ y la curva algebraica

$$C : \left\{ \begin{array}{rcl} y^4 & = & (x^2-3)(x^2-1) \\ z^4 & = & x - \sqrt{3} \end{array} \right.$$

En este caso tenemos que $\mathrm{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \langle\tau\rangle \cong \mathbb{Z}_2$, donde $\tau(\sqrt{3}) = -\sqrt{3}$. Ahora, se tiene que

$$C^\tau : \left\{ \begin{array}{rcl} y^4 & = & (x^2-3)(x^2-1) \\ z^4 & = & x + \sqrt{3} \end{array} \right.$$

Se puede verificar que no existe un isomorfismo $h : C \to C^\tau$ definido sobre $\mathbb{Q}(\sqrt{3})$; con lo cual se obtiene que $\mathbb{Q}(\sqrt{3})_{\mathbb{Q}}(C) = \{I\}$, es decir, $M_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(C) = \mathbb{Q}(\sqrt{3})$.

Por otro lado, si consideramos la extensión de Galois $\mathbb{Q} < \overline{\mathbb{Q}}$, obtenemos que para cada $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ vale que $\sigma(\sqrt{3}) = \sqrt{3}$ (en cuyo caso $C^\sigma \cong C$) o bien vale que $\sigma(\sqrt{3}) = -\sqrt{3}$ (en cuyo caso $C^\sigma = C^\tau$). Pero en este último caso, tenemos un isomorfismos $h : C \to C^\sigma$ definido sobre $\overline{\mathbb{Q}}$, dado por $h(x, y, z) = (-x, y, \rho z)$, donde $\rho^4 = -1$. Así, se obtiene que $\overline{\mathbb{Q}}_{\mathbb{Q}}(C) = \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$, es decir, $M_{\overline{\mathbb{Q}}/\mathbb{Q}}(C) = \mathbb{Q}$.

Este ejemplo nos dice que el cuerpo de moduli depende de la extensión.

Tarea 16. — *Sea $K < L$ una extensión de cuerpos y $\mathcal{C}$ una clausura algebraica de L. Sea $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva definida sobre. Supongamos que X está definida por los polinomios homogéneos $P_1, ..., P_r \in L[x_0, ..., x_n]$.*

1. *Verificar que $L_K(X)$ es un subgrupo de $\mathrm{Aut}(L/K)$.*
2. *Sea $\sigma \in \mathrm{Aut}(L/K)$. Ver que $[x_0 : \cdots : x_n] \in X$ es un punto singular de X sí y sólo si $[\sigma(x_0) : \cdots : \sigma(x_n)] \in X^\sigma$ es punto singular de X^σ. Concluir que X es no-singular sí y sólo si X^σ es no-singular.*
3. *Verificar que $K < M_{L/K}(X) < L$.*
4. *Si $P_1, ..., P_r \in K[x_0, ..., x_n]$ y $K < L$ es una extensión de Galois general, entonces $M_{L/K}(X) = K$.*
5. *Si $K < N < L$, entonces $L_N(X) < L_K(X)$. Concluir que $M_{L/K}(X) < M_{L/N}(X)$.*
6. *Dar un ejemplo $K < N < L$ de manera que $M_{L/K}(X) \neq M_{L/N}(X)$.*
7. *Si $K < L$ es una extensión y $N = M_{L/K}(X)$, entonces $M_{L/N}(X) = M_{L/K}(X)$. Indicación : Notar que para $N = M_{L/K}(X)$ vale que $L_K(X) = L_N(X)$.*
8. *Si $X \cong Y$, entonces $M_{L/K}(X) = M_{L/K}(Y)$.*

Teorema 2.3.3 **(Dèbes-Emsalem [6])**. — *Si $K < L$ es una extensión de Galois, entonces $L_K(X)$ es un subgrupo cerrado de $\mathrm{Aut}(L/K)$ en la topología de Krull, es decir, $L_K(X) = \mathrm{Aut}(L/M_{L/K}(X))$.*

Demonstración. — Si $K < L$ es una extensión de Galois finita, entonces no hay nada que probar. Supongamos que estamos con una extensión de Galois infinita. Como $L_K(X) < \mathrm{Aut}(L/M_{L/K}(X))$, sólo nos resta ver la contensión $\mathrm{Aut}(L/M_{L/K}(X)) < L_K(X)$. Lo que si sabemos es que $\mathrm{Aut}(L/M_{L/K}(X))$ es la clausura de $L_K(X)$ en la topología de Krull.

Sea $\sigma \in \mathrm{Aut}(L/M_{L/K}(X))$.

Es claro que podemos encontrar una extensión de Galois finita $K < N$, donde $N < L$ y X está definida sobre N. Tenemos que $\mathrm{Aut}(L/N)$ es un subgrupo normal de $\mathrm{Aut}(L/K)$ de índice finito. Esto nos asegura que $\sigma\mathrm{Aut}(L/N)$ es un abierto que contiene a σ. Luego, $L_K(X) \cap \sigma\mathrm{Aut}(L/N) \neq \emptyset$. De aquí vemos que existe $\eta \in L_K(X)$ tal que $\sigma^{-1}\eta \in \mathrm{Aut}(L/N)$. Como X está definida sobre N, se tiene que $X^{\sigma^{-1}\eta} = X$, es decir, $X^\sigma = X^\eta \cong X$; de donde tenemos que $\sigma \in L_K(X)$, como deseabamos verificar.

□

2.4. Cuerpos de móduli versus cuerpos de definición

Teorema 2.4.1. — *Sea $K < L$ una extensión de Galois general, $\mathcal{C}$ una clausura algebraica de L y $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva definida sobre L. Entonces, todo cuerpo de definición de X respecto a la extensión $K < L$ contiene al cuerpo de móduli de X.*

Demonstración. — Sea $K < N < L$, donde N es un cuerpo de definición de X. Podemos asumir que X está definida por polinomios homogéneos con coeficientes en N. Sea $\sigma \in \mathrm{Aut}(L/N) < \mathrm{Aut}(L/K)$. Entonces, tenemos que $X^\sigma = X$, es decir, $\sigma \in L_K(X)$. Esto nos asegura la contención $\mathrm{Aut}(L/N) < L_K(X)$. Luego, $M_{L/K}(X) = Fix(L_k(X)) < Fix(\mathrm{Aut}(L/N)) = N$.

□

Dado el resultado anterior, podemos preguntarnos por la intersección de todos los cuerpos de definicion N, $K < N < L$, de una variedad algebraica proyectiva $X \subset \mathbb{P}^n_{\mathcal{C}}$ definida sobre L, donde $\mathcal{C}$ es una clausura algebraica de L.

Teorema 2.4.2. — [**22**] *Sea K un cuerpo de característica $p \neq 2$ y sea $K < L$ una extensión de Galois general. Sea $\mathcal{C}$ una clausura algebraica de L y $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad Abeliana polarizada o bien una curva algebraica proyectiva no-singular definida sobre L. Entonces :*

1. $\mathrm{Aut}(L/M_{L/K}(X)) = \{\sigma \in \mathrm{Aut}(L/K) : X^\sigma \cong X\}$.
2. *Si estamos en característica cero (luego $L = \mathcal{C}$) y además en L hay elementos trascendentales sobre K, entonces $M_{L/K}(X)$ es igual a la intersección de todos los cuerpos de definición de X en L.*
3. *Existe un cuerpo de definición de X de grado finito sobre $M_{L/K}(X)$.*

Observación 2.4.3. — Es importante notar el punto 2., en el teorema anterior, la condición de la existencia de trascendentales. Si, por ejemplo, tenemos la extensión de Galois $\mathbb{R} < \mathbb{C}$ (en el cual no hay trascendentales sobre $\mathbb{R}$), entonces cualquier curva que tenga cuerpo de moduli $\mathbb{R}$ y que no se pueda definir sobre $\mathbb{R}$ será un contra-ejemplo.

En el caso de curvas algebraicas no-singulares, el resultado anterior se puede ver en [**11**], generalizando un resultado de J. Wolfart [**35**] para característica 0.

Teorema 2.4.4. — [**11**] *Sea L un cuerpo algebraicamente cerrado y $X \subset \mathbb{P}^n_L$ una curva algebraica proyectiva no-singular. Sea K el cuerpo básico de L. Entonces, existe un cuerpo de definición de X en L que es extensión finita del cuerpo de móduli $M_{L/K}(X)$.*

Notemos que el Teorema 2.4.4 vale para curvas algebraicas proyectivas no-singulares definidas sobre el cuerpo de los números complejos $L = \mathbb{C}$, en cuyo caso $K = \mathbb{Q}$.

El siguiente resultado nos dice que siempre podemos asumir que tenemos una extensión $K < L$, donde $L = \overline{K}$, una clausura algebraica de K, y que $K = M_{L/K}(X)$.

Teorema 2.4.5. — *Sea $K < L$ una extensión, donde L es un cuerpo algebraicamente cerrado. Sea $X \subset \mathbb{P}^n_L$ una variedad algebraica proyectiva. Sea $\overline{M_{L/K}} < L$ la clausura algebraica del cuerpo de móduli $M_{L/K}(X)$. Entonces*

$$M_{L/K}(X) = M_{\overline{M_{L/K}(X)}/M_{L/K}(X)}(X).$$

Demonstración. — Sean $F_X = \{\sigma \in \mathrm{Aut}(L/K) : X^\sigma \cong X\}$ y $M_{L/K}(X) = Fix(F_X)$. Denotemos por $\overline{M_{L/K}(X)}$ la clausura algebraica de $M_{L/K}(X)$ en L. Similarmente, sean $\widehat{F_X} = \{\sigma \in \mathrm{Aut}(\overline{M_{L/K}(X)}/M_{L/K}(X)) : X^\sigma \cong X\}$ y $M_{\overline{M_{L/K}(X)}/M_{L/K}(X)}(X) = Fix(\widehat{F_X})$.

Si $\sigma \in F_X$, entonces como σ actúa como la identidad sobre $M_{L/K}(X)$, este define un elemento de $\mathrm{Aut}(\overline{M_{L/K}(X)}/M_{L/K}(X))$ (por restricción) y luego un elemento de $\widehat{F_X}$. Esto nos dice que

$$M_{\overline{M_{L/K}(X)}/M_{L/K}(X)}(X) < M_{L/K}(X).$$

Como $M_{L/K}(X) < M_{\overline{M_{L/K}(X)}/M_{L/K}(X)}(X)$, se obtiene la igualdad deseada.

□

La noción de cuerpos de móduli para variedades Abelianas polarizadas fué introducida por T. Matsusaka en [**24**] y luego definida por G. Shimura en [**30**]. Para este caso de variedades, se tiene la siguiente información.

Teorema 2.4.6. — [**31**] *Sea K un cuerpo de característica 0 y $\overline{K}$ una clausura algebraica de K. Sea X una variedad Abeliana polarizada X definida sobre $\overline{K}$ de dimensión n genérica, es decir, su cuerpo de móduli $M_{\overline{K}/K}(X)$ tiene grado de trascendencia $n(n+1)/2$ sobre K.*

1. *Si X es de dimensión impar, entonces X se puede definir sobre su cuerpo de móduli $M_{\overline{K}/K}(X)$.*
2. *Si X es principalmente polarizada de dimensión par, entonces X no se puede definir sobre su cuerpo de móduli $M_{\overline{K}/K}(X)$.*

2.5. Cuerpo de móduli de morfismos entre curvas algebraicas

Sea $K < L$ una extensión de cuerpos y $\mathcal{C}$ una clausura algebraica de L donde estarán definidos todos nuestros objetos.

Sean X e Y curvas algebraica proyectiva no-singulares, donde X está definida sobre L e Y está definida sobre $M_{L/K}(X)$. Sea $P : X \to Y$ un morfismo algebraico de grado finito definido sobre L.

2.5.1. Cada $\sigma \in \mathrm{Aut}(L/K)$ produce un morfismo algebraico natural $P^\sigma : X^\sigma \to Y^\sigma$. Por otro lado, como Y está definida sobre $M_{L/K}(X)$, tenemos $Y^\sigma = Y$ y luego $P^\sigma : X^\sigma \to Y$.

Definición 2.5.1. — En las notaciones anteriores.

1. Decimos que $P : X \to Y$ es equivalente a $P^\sigma : X^\sigma \to Y$, lo que denotamos por $\{P : X \to Y\} \cong \{P^\sigma : X^\sigma \to Y\}$, si existe un isomorphismo $f_\sigma : X \to X^\sigma$, definido sobre L, tal que $P^\sigma \circ f_\sigma = P$.
2. $L_K(P : X \to Y) := \{\sigma \in \mathrm{Aut}(L/K) : \{P : X \to Y\} \cong \{P^\sigma : X^\sigma \to Y\}\}$.

3. Se define el **cuerpo de móduli** $M_{L/K}(P : X \to Y)$ de $P : X \to Y$, respecto a la extensión $K < L$, como el cuerpo fijo del subgrupo $L_K(P : X \to Y)$.

De la definición, se observa que $M_{L/K}(X) < M_{L/K}(P : X \to Y)$. Pero en general puede ocurrir que esos cuerpos son diferentes.

Tarea 17. — *Dar un ejemplo donde* $M_{L/K}(X) \neq M_{L/K}(P : X \to Y)$.

Más a delante veremos que es posible escoger un **modelo canónico** B de Y, el cual se puede definir sobre $M_{L/K}(X)$, y un isomorphismo $Q : Y \to B$, de manera que $M_{L/K}(X) = M_{L/K}(Q \circ P : X \to B)$. Este es un resultado debido a Pierre Dèbes y Michel Emsalem [**6**].

2.5.2. Cubrientes de Galois. — En el caso que el morfismo $P : X \to Y$ es de Galois, es decir, definido por la acción de un grupo finito $G < \mathrm{Aut}(X)$. En este caso, escribiremos $L_K(P : X \to Y) = L_K(P : X \to Y, G)$ y $M_{L/K}(P : X \to Y) = M_{L/K}(P : X \to Y, G)$ para hacer referencia al grupo G.

Por cada $\sigma \in \mathrm{Aut}(L/K)$, podemos también mirar el grupo $G^\sigma = \{\gamma^\sigma : \gamma \in G\}$. Notemos que si $\sigma \in L_K(P : X \to Y)$ y $f_\sigma : X \to X^\sigma$ es un isomorfismo birracional, entonces la condición $P^\sigma \circ f_\sigma = P$ nos asegura que $f_\sigma G f_\sigma^{-1} = G^\sigma$. Por otro lado, si $\sigma \in L_K(X)$ y $f_\sigma : X \to X^\sigma$ es un isomorfismo birracional, entonces puede ocurrir que $f_\sigma G f_\sigma^{-1} \neq G^\sigma$.

Supongamos que el grupo G es único en $\mathrm{Aut}(X)$ (por ejemplo, si G es un subgrupo característico de $\mathrm{Aut}(X)$) o bién si $G = \mathrm{Aut}(X)$). En este caso tenemos que el grupo G^σ es único en $\mathrm{Aut}(X^\sigma)$ para cada $\sigma \in \mathrm{Aut}(L/K)$. La unicidad de G nos asegura que si $\sigma \in L_K(X)$ y $f_\sigma : X \to X^\sigma$ es un isomorfismo birracional, entonces $f_\sigma G f_\sigma^{-1} = G^\sigma$, en particular, que vale la igualdad $P^\sigma \circ f_\sigma = P$. Esto permite concluir el siguiente resultado.

Teorema 2.5.2. — *Sean X una variedad algebraica proyectiva no-singular, $G < \mathrm{Aut}(X)$ un grupo finito de automorfismos birracionales de X y $P : X \to Y$ un morfismo algebraico definido por la acción de G. Si el grupo G es único en $\mathrm{Aut}(X)$, entonces*

$$L_K(X) = L_X(P : X \to Y) = L_X(P : X \to Y, G)$$
$$M_{L/K}(X) = M_{L/K}(P : X \to Y) = M_{L/K}(P : X \to Y, G).$$

CAPÍTULO 3

TEOREMA DE WEIL

En general el cuerpo de móduli no es un cuerpo de definición. El resultado más importante respecto a este punto es el siguiente debido a A. Weil que nos da condiciones necesarias y suficientes para que el cuerpo de móduli sea un cuerpo de definición. En este capítulo recordaremos este famoso teorema y daremos una demostración existencial y otro computacional de este.

3.1. Teorema de Weil

Sea $K < L$ una extensión general de Galois, con L algebraicamente cerrado, y sea $\overline{K}$ la clausura algebraica de K en L. Si $\sigma \in \mathrm{Aut}(L/K)$, entonces tenemos que (por restricción) $\sigma \in \mathrm{Aut}(\overline{K}/K)$.

Lema 3.1.1. — *Sea $K < L$ una extensión general de Galois, con L algebraicamente cerrado. Sea $X \subset \mathbb{P}^n_L$ una variedad algebraica proyectiva definida sobre L. Si X se puede definir sobre K, entonces para cada $\sigma \in \mathrm{Aut}(L/K)(= L_K(X))$ existe un isomorfismo birracional $f_\sigma : X \to X^\sigma$, definido sobre L, tal que para cada par $\sigma, \tau \in \mathrm{Aut}(L/K)$ vale la igualdad $f_{\sigma\tau} = f_\tau^\sigma \circ f_\sigma$.*

Demonstración. — Si X se puede definir sobre K, entonces existe un isomorfsimo birracional $R : X \to Y$, definida sobre L, donde Y es una variedad algebraica definida sobre K. Si $\sigma \in \mathrm{Aut}(L/K)$, entonces, como $Y^\sigma = Y$, podemos definir el isomorfismo birracional

$$f_\sigma = (R^\sigma)^{-1} \circ R : X \to X^\sigma.$$

Si $\sigma, \tau \in \mathrm{Aut}(L/K)$, entonces tenemos que

$$f_\tau^\sigma \circ f_\sigma = ((R^\tau)^{-1} \circ R)^\sigma \circ (R^\sigma)^{-1} \circ R = (R^{\sigma\tau})^{-1} \circ R^\sigma \circ (R^\sigma)^{-1} \circ R = (R^{\sigma\tau})^{-1} \circ R = f_{\sigma\tau}.$$

□

Observación 3.1.2. — Sea $X \subset \mathbb{P}^n_L$ es una variedad algebraica proyectiva definida sobre $\overline{K}$, donde $K = M_{L/K}(X)$.

1. Si $\sigma \in \mathrm{Aut}(L/K)$, entonces σ define por restricción un elemento de $\mathrm{Aut}(\overline{K}/K)$. Así, podemos notar que $M_{L/K}(X) = M_{\overline{K}/K}$. Más aún, si X está definida sobre una extensión de Galois $K < N$, $N < L$, entonces $M_{L/K}(X) = M_{N/K}$.
2. Como X está definida por un número finito de polinomios con coeficientes en $\overline{K}$, entonces sólo tenemos una cantidad finita de variedades X^σ que son birracionalmente equivalentes con X. Esto último debido a que podemos encontrar una extensión de Galois finita $K < N$, $N < L$, que contiene a todos los coeficientes de tales polinomios. Si además los isomorfismos birracionales $f_\sigma : X \to X^\sigma$ se pueden definir sobre $\overline{K}$, entonces podemos asumir que ellos también están definidas sobre la extensión de Galois finita $K < N$.

3. Si X se puede definir sobre K, entonces en la demostración del Lema 3.1.1 se puede escoger que $R : X \to Y$ sea definida sobre $\overline{K}$. De esta manera, como σ preserva $\overline{K}$, se tiene que los isomorfismos birracionales $f_\sigma : X \to X^\sigma$ están necesariamente definidos sobre $\overline{K}$. De esta manera, por el punto 2., existe una extensión de Galois finita $K < N$, $N < L$, de manera que las variedades algebraicas X^σ birracionalmente equivalentes con X y los isomorfismos birracionales $f_\sigma : X \to X^\sigma$ están todas definidas en N.

Teorema 3.1.3 **(Teorema de Weil [33])**. — *Sea $K < L$ una extensión general de Galois, L algebraicamente cerrado, y $X \subset \mathbb{P}^n_L$ una variedad algebraica proyectiva definida sobre $\overline{K}$, donde $K = M_{L/K}(X)$. Supongamos que para cada $\sigma \in \mathrm{Aut}(L/K)(= L_K(X))$ existe un isomorfismo birracional $f_\sigma : X \to X^\sigma$, definido sobre $\overline{K}$, tal que para cada par $\sigma, \tau \in \mathrm{Aut}(L/K)$ vale la igualdad $f_{\sigma\tau} = f^\sigma_\tau \circ f_\sigma$. Entonces vale lo siguiente.*

1. *(Existencia) Existe una variedad algebraica proyectiva Y, definida sobre K, y existe un isomorfismo birracional $R : X \to Y$, definido sobre $\overline{K}$, de manera que, para todo $\sigma \in \mathrm{Aut}(L/K)$, vale la igualdad $R^\sigma \circ f_\sigma = R$. Si, además, los isomorfismos birracionales f_σ son todos isomorfismos biregulares, entonces se puede asumir que el isomorfismo $R : X \to Y$ es también biregular.*
2. *(Unicidad) Más aún, si el par $(\widehat{R}, \widehat{Y})$ es otra solución al problema anterior, entonces existe un isomorfismo birracional $F : Y \to \widehat{Y}$, definido sobre K, de manera que $\widehat{R} = F \circ R$.*

Como consecuencia de la Observación 3.1.2, el Teorema de Weil es consecuencia de la siguiente versión finita.

Teorema 3.1.4 **(Versión finita del Teorema de Weil [33])**. — *Sea $K < L$ una extensión de Galois de grado finito, $\mathcal{C}$ una clasusura algebraica de L y $X \subset \mathbb{P}^n_{\mathcal{C}}$ una variedad algebraica proyectiva definida sobre L, donde $K = M_{L/K}(X)$. Supongamos que para cada $\sigma \in \mathrm{Aut}(L/K)(= L_K(X))$ existe un isomorfismo birracional $f_\sigma : X \to X^\sigma$, definido sobre L, tal que para cada par $\sigma, \tau \in \mathrm{Aut}(L/K)$ vale la igualdad $f_{\sigma\tau} = f^\sigma_\tau \circ f_\sigma$. Entonces vale lo siguiente.*

1. *(Existencia) Existe una variedad algebraica proyectiva Y, definida sobre K, y existe un isomorfismo birracional $R : X \to Y$, definido sobre L, de manera que, para todo $\sigma \in \mathrm{Aut}(L/K)$, vale la igualdad $R^\sigma \circ f_\sigma = R$. Si, además, los isomorfismos birracionales f_σ son todos isomorfismos biregulares, entonces se puede asumir que el isomorfismo $R : X \to Y$ es también biregular.*
2. *(Unicidad) Más aún, si el par $(\widehat{R}, \widehat{Y})$ es otra solución al problema anterior, entonces existe un isomorfismo birracional $F : Y \to \widehat{Y}$, definido sobre K, de manera que $\widehat{R} = F \circ R$.*

Observación 3.1.5. — Notemos que la condición $f_{\sigma\tau} = f^\sigma_\tau \circ f_\sigma$, en el Teorema de Weil, asegura que $f_e = I$, el automorfismo identidad de X, donde $e \in \mathrm{Aut}(L/K)$ es la identidad. Para esto, basta asumir $\tau = \sigma = e$. Originalmente, en las hipótesis del Teorema de Weil en [**33**] sólo se asume que la extensión $K < L$ sea una extensión separable de grado finito.

Corolario 3.1.6. — *Sea $K < L$ una extensión de Galois de grado finito y $X \subset \mathbb{P}^n_L$ una variedad algebraica proyectiva sin automorfismos biracionales, salvo la identidad. Entonces $M_{L/K}(X)$ es cuerpo de definición de X.*

Observación 3.1.7. —

1. En general, una curva algebraica no tienen automorfismos biracionales (diferentes del trivial). Luego, en el caso genérico se tienen que el cuerpo de móduli es un cuerpo de definición.

2. Si X e Y son curvas algebraicas no-singulares, entonces cualquier isomorfismo birracional $f : X \to Y$ es biregular.

3.2. Demostración de la unicidad

Supongamos que tenemos $R : X \to Y$ y $\widehat{R} : X \to \widehat{Y}$ isomorfismos birracionales definidos sobre L, donde Y y $\widehat{Y}$ son variedades definidas sobre K, de manera que, para todo $\sigma \in \mathrm{Aut}(L/K)$, valen las igualdades $R^\sigma \circ f_\sigma = R$ y $\widehat{R}^\sigma \circ f_\sigma = \widehat{R}$. Entonces $F = \widehat{R} \circ R^{-1} : Y \to \widehat{Y}$ es un isomorfismo birracional, definido sobre L. Para cada $\sigma \in \mathrm{Aut}(L/K)$ se tiene que

$$F^\sigma = (\widehat{R} \circ R^{-1})^\sigma = \widehat{R}^\sigma \circ (R^\sigma)^{-1} = (\widehat{R} \circ f_\sigma^{-1}) \circ (R \circ f_\sigma^{-1})^{-1} = \widehat{R} \circ R^{-1} = F,$$

de donde se obtiene que F está realmente definido sobre K.

3.3. Primera demostración de la existencia : version finita

3.3.1. Existencia : caso birracional. — Denotemos por $L(X)$ el cuerpo de funciones racionales de X, definidas sobre L. Por el Lema de Normalización de Noether [**27**], $L(X)$ es finitamente generada sobre L.

Si $\sigma \in \mathrm{Aut}(L/K)$ y $\phi \in L(X)$, entonces tenemos $\phi^\sigma = \sigma \circ \phi \circ \sigma^{-1} \in L(X^\sigma)$. Como $f_\sigma : X \to X^\sigma$ es un isomorfismo birracional, podemos considerar $\phi^\sigma \circ f_\sigma \in L(X)$. De esta manera, obtenemos un automorfismo

$$\sigma^* : L(X) \to L(X) \in \mathrm{Aut}(L(X)/K),$$

definido por la regla

$$\sigma^*(\phi) = \phi^\sigma \circ f_\sigma = f_\sigma^*(\phi).$$

Ya que $f_e = I$, se tiene que $e^* : L(X) \to L(X)$ es la identidad.

Consideremos la función

$$\Phi : \mathrm{Aut}(L/K) \to \mathrm{Aut}(L(X)/K) : \sigma \mapsto \sigma^*.$$

Lema 3.3.1. — *La función* Φ *es un homomorfismo de grupos inyectivo.*

Demonstración. — Ya hemos notado que $\Phi(e) = I$. Ahora, supongamos que $\sigma, \tau \in \mathrm{Aut}(L/K)$ y $\phi \in L(X)$. Entonces tenemos que

$$\Phi(\tau)(\Phi(\sigma)(\phi)) = \tau^*(\sigma^*(\phi)) = \tau^*(\phi^\sigma \circ f_\sigma) = (\phi^\sigma \circ f_\sigma)^\tau \circ f_\tau = \phi^{\tau\sigma} \circ f_\sigma^\tau \circ f_\tau = \phi^{\tau\sigma} \circ f_{\tau\sigma},$$

con lo cual obtenemos que Φ es un homomorfismo de grupos. Para ver la inj=yectividad, supongamos que $\sigma \in \mathrm{Aut}(L/K)$ es diferente de la identidad, pero que σ^* es la identidad. Entonces, como σ no es la identidad (y la extensión $K < L$ es Galois), existe $r \in L - K$ tal que $\sigma(r) \neq r$. Tomemos $\phi = r$, la función constante igual a r. Entonces $\phi = \sigma^*(\phi) = \phi^\sigma \circ f_\sigma = \phi^\sigma = \sigma(r) \neq r = \phi$, una contradicción. □

Como consecuencia del Lema 3.3.1, tenemos el isomorfismo de grupos finitos

$$\Phi : \Gamma = \mathrm{Aut}(L/K) \to \Gamma^* = \Phi(\mathrm{Aut}(L/K)) < \mathrm{Aut}(L(X)/K).$$

Sea $\mathbb{F} < L(X)$ el cuerpo fijo por el grupo finito Γ^*. Luego,

(i) $K < \mathbb{F}$,

(ii) $\mathbb{F} < L(X)$ es una extensión de Galois de grado finito (de hecho del mismo grado que la extension $K < L$) y

(iii) $\mathbb{F}$ está finitamente generado sobre K [**34**].

Supongamos que $\mathbb{F}$ está generado, sobre K, por las funciones racionales ψ_1,..., ψ_s, es decir, $\mathbb{F} = K(\psi_1, ..., \psi_s)$. Consideremos el homomorfimo

$$\Theta : K[x_1, ..., x_s] \to \mathbb{F}$$

definido por la asignación $\Theta(x_j) = \psi_j$, para cada $j = 1, ..., s$. Entonces, $\ker(\Theta)$ define una variedad algebraica X_0, definida sobre K, con anillo de funciones $K[X_0] = K[x_1, ..., x_s]/\ker(\Theta)$. Es claro que por definición Θ induce un isomorfismo entre el cuerpo $K(X_0)$ de funciones racionales de X_0 y $\mathbb{F}$. Así, podemos asumir que la variedad X_0 tiene a $\mathbb{F}$ como cuerpo de funciones sobre K. En otras palabras, $L(X_0) = L(\psi_1, ..., \psi_s) < L(X)$.

Lema 3.3.2. — $L(X) = L(X_0)$.

Demonstración. — Es claro que tenemos la contensión $L(X_0) < L(X)$. Ahora, como

$$L(X_0) = \mathrm{Fix}(H^*)$$

donde

$$H^* = \{\sigma^* : \sigma \in \Gamma,\ \sigma(\alpha) = \alpha,\ \forall \alpha \in L,\ \text{y}\ \sigma^*(\psi_j) = \psi_j,\ j = 1, ..., s\},$$

observamos que, si $\sigma^* \in H^*$, entonces $\sigma = e$; con lo cual tenemos que $H^* = \{I\}$ y, en particular, $\mathrm{Fix}(H^*) = L(X)$. □

El Lema 3.3.2 nos dice que X y X_0 son birracionalmente equivalentes sobre L, es decir, existe un isomorfismo birracional, definido sobre L, digamos

$$R : X \to X_0$$

de manera que, para cada $\phi \in L(X)$, vale que

$$(*) \quad \phi = Q(\psi_1, ..., \psi_s) \circ R$$

donde Q es racional en s variables definida sobre L. Más aún, $\phi \in \mathbb{F}$ sí y sólo si Q tiene sus coeficientes en K.

Si $\phi \in \mathbb{F}$ y $\sigma \in \Gamma$, entonces podemos escribir $\phi = \psi \circ R$, donde $\psi^\sigma = \psi$. De esta manera, tenemos que

$$\psi \circ R = \phi = \sigma^*(\phi) = \sigma^*(\psi \circ R) = (\psi \circ R)^\sigma \circ f_\sigma = \psi^\sigma \circ R^\sigma \circ f_\sigma = \psi \circ R^\sigma \circ f_\sigma.$$

Luego, podemos deducir que $R = R^\sigma \circ f_\sigma$.

3.3.2. Existencia : caso biregular. — Los argumentos anteriores dan una demostración de la parte (1) del Teorema de Weil para el caso de isomorfismos birracionales, pero no para el caso biregular. A continución analizamos este caso. Sabemos de la existencia de una variedad algebraica Y, definida sobre K, y un isomorfismo birracional $R : X \to Y$, de manera que, para cada $\sigma \in \mathrm{Aut}(L/K)$, vale que $R = R^\sigma \circ f_\sigma$. Ahora estamos asumiendo que todos los isomorfismos $f_\sigma : X \to X^\sigma$ son biregulares.

Supongamos que $\mathrm{Aut}(L/K) = \{\sigma_1 = e, \sigma_2, ..., \sigma_r\}$, donde e es el automorfismo identidad, y consideremos una base de L sobre K, digamos $\{\alpha_1, ..., \alpha_r\}$.

Sean $f_j = f_{\sigma_j}$, para cada $j = 1, ..., r$. Previamente hemos notado que f_1 es la identidad $I : X \to X$. Consideremos la función regular

$$F : X \subset \mathbb{P}^n_L \to \mathbb{P}^n_L \times \overset{r}{\cdots} \times \mathbb{P}^n_L$$

$$x \in X \mapsto F(x) = (f_1(x) = x, f_2(x), ..., f_r(x)) = (y_1, ..., y_r).$$

Es claro que F es un isomorfismo biregular entre X y la variedad algebraica definida por $F(X)$.

Denotemos las coordenadas proyectivas x, y_1,..., y_r como sigue :

$$x = [x_0 : \cdots : x_n],$$

$$y_j = [y_{j0} : \cdots : y_{jn}], j = 1, ..., r.$$

Consideremos las siguientes $(n+1)^r$ coordenadas

$$z_{s_1,...,s_r} = y_{1s_1}y_{2s_2}\cdots y_{rs_r},\ s_1,...,s_r \in \{0,1,...,n\},$$

y la función regular

$$G : \mathbb{P}^n_L \times \overset{r}{\cdots} \times \mathbb{P}^n_L \to \mathbb{P}^{(n+1)^r-1}_L$$
$$(y_1,...,y_r) \mapsto G(y_1,...,y_r) = [z_{0,...,0} : \cdots : z_{n,...,n}].$$

Se tiene que G define un isomorfismo biregular entre $\mathbb{P}^n_L \times \overset{r}{\cdots} \times \mathbb{P}^n_L$ y $G(\mathbb{P}^n_L \times \overset{r}{\cdots} \times \mathbb{P}^n_L)$.

De esta manera,

$$H = G \circ F : X \subset \mathbb{P}^n_L \to H(X) \subset \mathbb{P}^{(n+1)^r-1}_L$$

define un isomorfismo biregular entre X y la variedad algebraica definida por $H(X)$.

Si

$$f_j(x) = [f_{j0}(x) : \cdots : f_{jn}(x)], j = 1,...,r,$$

entonces la coordenada $(s_1,...,s_r)$ de $H(x)$ es dada por

$$H_{s_1,...,s_r}(x) = f_{1s_1}(x)f_{2s_2}(x)\cdots f_{rs_r}(x)$$

y se tiene que

$$H(x) = [f_{10}(x)f_{20}(x)\cdots f_{r0}(x) : \cdots : f_{1n}(x)f_{2n}(x)\cdots f_{rn}(x)].$$

De la igualdad $f_{\sigma\tau} = f^\sigma_\tau \circ f_\sigma$, para cada $\sigma,\tau \in \mathrm{Aut}(L/K)$, se obtiene que para cada $\sigma \in \mathrm{Aut}(L/K)$ vale que

$$f^\sigma_{\sigma_j} = f_{\sigma\sigma_j} \circ f^{-1}_\sigma,$$

de donde

$$f^\sigma_{js_j} = (f_{\sigma\sigma_j})_{s_j} \circ f^{-1}_\sigma = f_{m(j)s_j} \circ f^{-1}_\sigma, \quad (\sigma \circ \sigma_j = \sigma_{m(j)}).$$

De esta manera,

$$H^\sigma_{s_1,...,s_r} = f^\sigma_{1s_1}f^\sigma_{2s_2}\cdots f^\sigma_{rs_r} = f_{m(1)s_1}f_{m(2)s_2}\cdots f_{m(r)s_r} \circ f^{-1}_\sigma.$$

Lo anterior nos dice que, para cada $\sigma \in \mathrm{Aut}(L/K)$, la función

$$H^\sigma : X^\sigma \to \mathbb{P}^{(n+1)^r-1}_L$$

satisface la relación

$$H^\sigma \circ f_\sigma = T_\sigma \circ H,$$

donde T_σ es una permutación de las coordenadas de $\mathbb{P}^{(n+1)^r-1}_L$. Luego, obtenemos un homomorfismo

$$\theta : \mathrm{Aut}(L/K) \to \theta(\mathrm{Aut}(L/K)) = \mathbb{G} < \mathrm{PGL}_{(n+1)^r}(L) : f_\sigma \mapsto \theta(f_\sigma) = T_\sigma,$$

donde $\mathbb{G}$ es un subgrupo de permutaciones de coordenadas, es decir, tenemos una acción de $\mathrm{Aut}(L/K)$ dada por permutación de coordenadas del espacio proyectivo $\mathbb{P}^{(n+1)^r-1}_L$.

Podemos ahora considerar la función

$$T = H \circ R^{-1} : Y \to T(Y) \subset \mathbb{P}^{(n+1)^r-1}$$

la cual es un isomorfismo birracional entre Y y $H(X)$ (la variedad algebraica que define $T(Y)$).

Si consideramos una coordenada $\rho = (s_1,...,s_r)$, entonces

$$T_\rho = H_\rho \circ R^{-1} = \sum_{j=1}^r \alpha_j h_{\rho j}$$

donde $h_{\rho j} : Y \to L$ son funciones racionales definidas sobre K.

De esta manera, para cada $\sigma \in \mathrm{Aut}(L/K)$, se tiene que

$$T^\sigma_\rho = \sum_{l=1}^r \sigma(\alpha_j)h_{\rho j}.$$

Consideremos el sistema lineal

$$\left\{\begin{array}{ccc} T_\rho^{\sigma_1} & = & \sum_{l=1}^r \sigma_1(\alpha_j)h_{\rho j} \\ \vdots & \vdots & \vdots \\ T_\rho^{\sigma_r} & = & \sum_{l=1}^r \sigma_r(\alpha_j)h_{\rho j} \end{array}\right\}$$

que dan representaciones lineales de las r funcions racionales $T_\rho^{\sigma_1}$,..., $T_\rho^{\sigma_r}$ en términos de las r funciones racionales $h_{\rho 1}$,..., $h_{\rho r}$.

Como la extensión $K < L$ es Galois, este sistema lineal es invertible. Luego, podemos obtener representaciones lineales de las r funcions racionales $h_{\rho 1}$,..., $h_{\rho r}$ en términos de las r funciones racionales $T_\rho^{\sigma_1}$,..., $T_\rho^{\sigma_r}$.

Esto nos da un automorfismo lineal de $\mathbb{P}_L^{(n+1)^r-1}$, digamos $J : \mathbb{P}_L^{(n+1)^r-1} \to \mathbb{P}_L^{(n+1)^r-1}$, de manera que, para cada $\sigma \in \mathrm{Aut}(L/K)$, la función racional

$$Q = J \circ T : Y \to \mathbb{P}_L^{(n+1)^r-1},$$

tiene como coordenadas las funciones $h_{\rho j}$, donde ρ recorre todas las coordenadas $(s_1, ..., s_r)$ módulo permutación por el grupo $\mathbb{G}$ y $j \in \{1, ..., r\}$, es un isomorfismo birracional entre Y y la variedad algebraica Z definida por $Q(Y)$. Como Y y Q están definidas sobre K, se tiene que la variedad algebraica Z está definida sobre K.

Ahora, consideramos la función

$$P = J \circ H : X \subset \mathbb{P}_L^n \to \mathbb{P}_L^{(n+1)^r-1},$$

que es un isomorfismo biregular entre X y $P(X)$. Como $P = Q \circ R$, notamos que $P(X) = Z$.

Ahora,

$$P^\sigma \circ f_\sigma = (Q \circ R)^\sigma \circ f_\sigma = Q^\sigma \circ (R^\sigma \circ f_\sigma) = Q^\sigma \circ R = Q \circ R = P.$$

3.4. Segunda demostración de la existencia : versión finita

Ya que la demostración de la parte biregular hecha anteriormente es explícita, lo único que necesitamos hacer es una demostración explícita de la parte existencial para el caso birracional. Ahora procedemos ha dar tal demostración de manera constructiva.

3.4.1. Sea V un espacio vectorial sobre K de dimensión finita, digamos $n \geq 1$. Sean x_1,..., x_n una base de V. El álgebra tensorial de V, digamos $K[V]$, puede ser identificado con el álgebra unitaria asociativa generada por x_1,..., x_n sobre K, es decir, con el álgebra de los polinomios en las variables x_1,..., x_n y coeficientes en K. Si Γ es un grupo que actúa de manera lineal sobre V, entonces tal acción se extiende de manera natural a una acción diagonal en $K[V]$.

***Teorema 3.4.1* (D. Hilbert - E. Noether [27, 28]).** — *Sea V un espacio vectorial de dimensión finita sobre un cuerpo K. Sea Γ un grupo finito actuando linealmente sobre V. Entonces, el álgebra Γ-invariante de polinomios $K[V]^\Gamma$ es finitamente generada.*

3.4.2. Sea $\mathcal{C}$ una clausura algebraica de L. Tenemos de manera natural un homomorfismo sobreyectivo $\rho : \mathrm{Gal}(\mathcal{C}/K) \to \Gamma$ definido por restricción.

Podemos asumir que nuestra variedad algebraica $X \subset \mathcal{C}^n$ es afín, digamos definida como los ceros de los polinomios $P_1, ..., P_r \in L[x_1, ..., x_n]$.

Para cada $\eta \in \mathrm{Gal}(\mathcal{C}/K)$ podemos considerar la biyección $\widehat{\eta} : \mathcal{C}^n \to \mathcal{C}^n$, definida como $\widehat{\eta}(x_1, ..., x_n) = (\eta(x_1), ..., \eta(x_n))$.

Observemos en este caso que si $\sigma = \rho(\eta)$, then $\widehat{\eta}(X) = X^\sigma$ es la variedad algebraica definida por los polinomios P_1^σ,..., P_r^σ.

Consideremos la función

$$\Phi : X \to \prod_{\sigma \in \Gamma} \mathcal{C}^n : x \mapsto (f_\sigma(x))_{\sigma \in \Gamma}.$$

La imágen $\Phi(X)$ es la variedad algebraica afín definida como

$$\Phi(X) = \left\{(y_\sigma(x))_{\sigma\in\Gamma} : P_1(y_e) = 0, ..., P_r(y_e) = 0, y_\sigma = f_\sigma(y_e),\ \sigma \in \Gamma\right\}.$$

Ya que cada f_σ es un isomorfismo birracional, Φ induce de manera natural un isomorfismo birracional entre X y $\Phi(X)$. La función inversa es dada por la proyección en la primera coordenada.

Consideremos la acción de Γ por permutaciones en las coordenadas como sigue :

$$\Theta : \Gamma \times \prod_{\sigma\in\Gamma} \mathcal{C}^n \to \prod_{\sigma\in\Gamma} \mathcal{C}^n$$
$$\left(\tau, (y_\sigma(x))_{\sigma\in\Gamma}\right) \mapsto (y_{\tau\sigma}(x))_{\sigma\in\Gamma}$$

Sea $\tau \in \Gamma$ y $\eta \in \mathrm{Gal}(\mathcal{C}/K)$ tal que $\rho(\eta) = \tau$. Como

$$\Phi^\tau(f_\tau(x)) = (f_\sigma^\tau(f_\tau(x)))_{\sigma\in\Gamma} = (f_{\tau\sigma}(x))_{\sigma\in\Gamma} = \Theta(\tau)(\Phi(x))$$

y

$$\Phi(\widehat{\eta}^{\,-1}(f_\tau(x))) = \left(f_\sigma(\widehat{\eta}^{\,-1}(f_\tau(x)))\right)_{\sigma\in\Gamma} = \left(\widehat{\eta}^{\,-1}(f_\sigma^\tau(f_\tau(x)))\right)_{\sigma\in\Gamma} = \left(\widehat{\eta}^{\,-1}(f_{\tau\sigma}(x))\right)_{\sigma\in\Gamma} = \widehat{\eta}^{\,-1}(\Theta(\tau)(\Phi(x))),$$

obtenemos el siguiente diagrama conmutativo :

$$\begin{array}{ccc} X & \stackrel{\Phi}{\to} & \Phi(X) \\ \downarrow f_\tau & & \downarrow \Theta(\tau) \\ X^\tau & \stackrel{\Phi^\tau}{\to} & \Theta(\tau)(\Phi(X)) = \Phi^\tau(X^\tau) \\ \downarrow \widehat{\eta}^{\,-1} & & \downarrow \widehat{\eta}^{\,-1} \\ X & \stackrel{\Phi}{\to} & \Phi(X) \end{array} \tag{1}$$

De manera similar, no es dificil ver que, para cada $\tau \in \Gamma$ y cada $\eta \in \mathrm{Gal}(\mathcal{C}/K)$, se tiene que

$$(*) \quad \Theta(\tau) \circ \widehat{\eta} = \widehat{\eta} \circ \Theta(\tau).$$

Consideremos el siguiente subgrupo de Γ :

$$G = \{\tau \in \Gamma : \Theta(\tau)(\Phi(X)) = \Phi(X)\}.$$

De la definición, los elementos $\tau \in G$ son exáctamente aquellos para los cuales $\Theta(\tau) \in \mathrm{Aut}(\Phi(X))$.

3.4.3. Primer caso. — Supongamos que $G = \{e\}$, es decir, no hay ningún subgrupo no-trivial H de Γ tal que $\Phi(X)$ sea $\Theta(H)$-invariante (por ejemplo, esto ocurre si $\mathrm{Aut}_{\mathcal{C}}(X)$ es trivial).

Ya que $\Theta(\Gamma) \cong \Gamma$ es un grupo finito de permutaciones, se tiene del Teorema de Hilbert-Noether que el álgebra $L[\prod_{\sigma\in\Gamma} \mathcal{C}^n]^\Gamma = \mathcal{C}[(y_\sigma)_{\sigma\in\Gamma}]^\Gamma$, de los polinomios $\Theta(\Gamma)$-invariantes con coeficientes en $\mathcal{C}$, es finitamente generado.

Consideremos un conjunto finito de generadores de $\mathcal{C}[(y_\sigma)_{\sigma\in\Gamma}]^\Gamma$, digamos

$$E_1((y_\sigma)_{\sigma\in\Gamma}), ..., E_N((y_\sigma)_{\sigma\in\Gamma}) \in \mathcal{C}[(y_\sigma)_{\sigma\in\Gamma}]^\Gamma.$$

Ahora consideramos la función

$$\Psi : \prod_{\sigma\in\Gamma} \mathcal{C}^n \to \mathcal{C}^N$$
$$(y_\sigma)_{\sigma\in\Gamma} \mapsto (E_1((y_\sigma)_{\sigma\in\Gamma}), ..., E_N((y_\sigma)_{\sigma\in\Gamma}))$$

Notemos que la acción por permutaciones en las coordenadas (producida por $\Theta(\Gamma)$) no depende del cuerpo $\mathcal{C}$, es decir, podemos considerar tal acción por permutaciones sobre el espacio producto $\prod_{\sigma\in\Gamma} \mathcal{B}$, donde $\mathcal{B}$ es el cuerpo básico de $\mathcal{C}$. De esta manera observamos que

$$E_1((y_\sigma)_{\sigma\in\Gamma}), ..., E_N((y_\sigma)_{\sigma\in\Gamma}) \in K[(y_\sigma)_{\sigma\in\Gamma}].$$

Como consecuencia de los resultados en [**13**] sobre grupos reductibles (ver el libro de Mumford-Fogarty-Kirwan [**26**]) y el hecho que los grupos finitos son reductibles, uno tiene que la función Ψ satisface las siguientes tres propiedades :

1. $\Psi^\sigma = \Psi$, para cada $\sigma \in \Gamma$;
2. para cada $\sigma \in \Gamma$ vale que $\Psi \circ \Theta(\sigma) = \Psi$; y
3. si $\Psi(w) = \Psi(z)$, entonces existe algún $\gamma \in \Gamma$ de manera que $w = \Theta(\gamma)(z)$.

Sea $Z = \pi(\Phi(X))$.
Sea $\tau \in \Gamma$ y $\eta \in \mathrm{Gal}(\mathcal{C}/K)$ tal que $\rho(\eta) = \tau$. Entonces por $(*)$ arriba y (2) vale que

$$\Psi \circ \widehat{\eta}^{\,-1} \circ \Theta(\tau) = \Psi \circ \Theta(\tau) \circ \widehat{\eta}^{\,-1} = \Psi \circ \widehat{\eta}^{\,-1}.$$

Así podemos ver que $\widehat{\eta}^{\,-1}$ desciende en una biyección $\widehat{\eta}^{\,-1} : \mathcal{C}^N \to \mathcal{C}^N$. Ahora, se sigue del diagrama (1) que $\widehat{\eta}(Z) = Z$, es decir, $Z^\tau = Z$ para cada $\tau \in \Gamma$. El Teorema 2.1.10 ahora asegura que Z está definida sobre K.

Como hemos asumido que $\Phi(X)$ no es $\Theta(H)$-invariante para cualquier subgrupo no-trivial H de Γ, obtenemos que existe un abierto no-vací de Zariski Ω de$\Phi(X)$ sobre el cual Ψ es inyectivo. De hecho, esta condición nos asegura que la subvariedad algebraica $W_\eta = \Theta(\eta)(\Phi(X)) \cap \Phi(X)$ tiene co-dimensión positiva en $\Phi(X)$. Si $W = \cup_{\eta \in \Gamma} W_\eta$, entonces $\Omega = \Phi(X) - W$.

Como Ψ es un cubriente regular (ramificado) con grupo finito algebraico $\Theta(\Gamma)$ como grupo de transformaciones de cubrimiento, se sigue que $\Psi : \Omega \to \pi(\Omega)$ es un isomorfismo biregular, en particular, que $R = \Psi \circ \Phi : X \to Z$ es un isomorfismo birracional.

Observación 3.4.2. — Los polinomios $E_1, ..., E_N$ proveen de un número finito $\mathcal{F}_1$ de polinomios (definidos sobre K) describiendo la variedad algebraica $\Psi\left(\prod_{\sigma\in\Gamma} L^n\right)$. La variedad algebraica $\Phi^\tau(X^\tau)$ es definida como

$$\Phi^\tau(X^\tau) = \left\{(y_\sigma(x))_{\sigma\in\Gamma} : P_1^\tau(y_e) = 0, ..., P_r^\tau(y_e) = 0, y_\sigma = f_\sigma^\tau(y_e),\ \sigma \in \Gamma\right\}.$$

Como los polinomios $\mathrm{Tr}(P_1)$,..., $\mathrm{Tr}(P_r)$ pertenecen al álgebra $L[\prod_{\sigma\in\Gamma} L^n]^\Gamma$, tenemos que los polinomios $\mathrm{Tr}(P_j)$ serán de la forma $T_j(E_1, ..., E_N)$ (donde T_j es un polinomio con coeficientes en L). Podemos asumir que cada $\mathrm{Tr}(f_\sigma)$ puede ser expresada como una función racional $R_\sigma(E_1, ..., E_N)$, con coeficientes en L. Pueden también ser asumidos como polinomios ya que estamos mirando a los ceros. De esta manera, Z se define como los ceros de los polinomios en $\mathcal{F}_1$ junto con los polinomios $T_1(E_1, ..., E_N)$,..., $T_r(E_1, ..., E_N)$ y $R_\sigma(E_1, ..., E_N)$, for $\sigma \in \Gamma$. Ahora, cada uno de esos polinomios, digamos F, que no esté definido sobre K, puede ser reemplazado por los polinomios (los cuales están ahora definidos sobre K) $\mathrm{Tr}(e_1F)$, $\mathrm{Tr}(e_2F)$,..., $\mathrm{Tr}(e_mF) \in K[x_1, ..., x_n]$, donde $\{e_1, ..., e_m\}$ es una base de L como K-espacio vectorial.

3.4.4. Segundo caso. — Supongamos que $G = \Gamma$.

Si $\tau \in G$ y $\eta \in \mathrm{Gal}(\mathcal{C}/K)$ es tal que $\rho(\eta) = \tau$, entonces tenemos el siguiente diagrama conmutativo (donde $h_\tau = \Phi^{-1} \circ \Theta(\tau) \circ \Phi \in \mathrm{Aut}_{\mathcal{C}}(X)$)

$$\begin{array}{ccc} X & \stackrel{\Phi}{\to} & \Phi(X) \\ \downarrow{\scriptstyle h_\tau} & & \downarrow{\scriptstyle \Theta(\tau)} \\ X & \stackrel{\Phi}{\to} & \Phi(X) \end{array} \tag{2}$$

Ahora, diagrama (2), junto con el diagrama (1), aseguran que $f_{\tau\sigma}(x) = f_\sigma(y)$, para todo $\sigma \in \Gamma$, y que $y = h_\tau(x)$. Tomando $\sigma = e$, vemos que $y = f_\tau(x)$ y, en particular, que $X^\tau = X$. Como es to es válido para todo $\tau \in \Gamma$, vemos que X está definida sobre K por el Teorema 2.1.10. De hecho, X está definida por los polinomios $\mathrm{Tr}(e_1P_j)$, $\mathrm{Tr}(e_2P_j)$,..., $\mathrm{Tr}(e_mP_j) \in \mathcal{K}[x_1, ..., x_n]$, para $j = 1, ..., r$, y donde $\{e_1, ..., e_m\}$ es una bases de $\mathcal{L}$ como $\mathcal{K}$-espacio vectorial.

3.4.5. Tercer caso. — Supongamos ahora que $\{e\} \neq G \neq \Gamma$ y escribamos $G = \{e, \tau_1, ..., \tau_m\}$. Para cada τ_j podemos encontrar $a_j \in \mathcal{L}$ tal que $\tau_j(a_j) \neq a_j$. Podemos considerar la variedad algebraica $Y \subset \mathcal{L}^{n+m}$ definida por los polinomios

$$P_1(x_1, ..., x_n) = 0, ...P_r(x_1, ..., x_n) = 0,$$
$$x_{n+1} = a_1, ..., x_{n+m} = a_m.$$

La función

$$Q : X \to Y : (x_1, ..., x_n) \mapsto (x_1, ..., x_n, a_1, ..., a_m)$$

define un isomorfismo biracional cuya inversa es dada por la proyección

$$Q^{-1}i : Y \to X : (x_1, ..., x_n, a_1, ..., a_m) \to (x_1, ..., x_n).$$

De la construcción podemos ver que $Y^\sigma \neq Y$ para todo $\sigma \in \Gamma - \{e\}$. Consideremos la familia de isomorfismos biracionales

$$\{g_\sigma = Q^\sigma \circ f_\sigma \circ Q^{-1} : Y \to Y^\sigma\}_{\sigma \in \Gamma}.$$

Ahora podemos trabajar con Y (y la familia anterior de isomorfismos) en vez de X para asumir que $G = \{e\}$ y estamos en el caso discutido antes.

CAPÍTULO 4

APLICACIONES DEL TEOREMA DE WEIL

En este capítulo veremos algunos resultados que se obtienen como consecuencia del Teorema de Weil.

4.1. Cubrientes de Galois y modelo canónico

En toda esta sección estaremos trabajando con una extensión de cuerpos $K < L$. Cada vez que hablemos de una variedad algebraica definida sobre L estaremos pensando que tenemos una variedad algebraica sobre una clausura algebraica definida por polinomios con coeficientes en L.

Si X es una variedad algebraica proyectiva, entonces denotamos por $\mathrm{Aut}(X)$ al grupo de sus automorfismos birracionales.

En [**4**] se obtuvo la siguiente aplicación del Teorema de Weil.

Teorema 4.1.1 **([4])**. — *Sea $K < L$ una extensión de Galois de grado finito y X una curva algebraica proyectiva no-singular definida sobre L, donde $K = M_{L/K}(X)$. Supongamos que los automorfismos birracionales de X están definidos sobre L. Si $P : X \to \mathbb{P}^1_L$ un cubriente de Galois (regular), es decir dado por la acción de un grupo finito $G < \mathrm{Aut}(X)$, entonces $P : X \to \mathbb{P}^1_L$ se puede definir sobre $M_{L/K}(P : X \to \mathbb{P}^1_L, G)$.*

Observación 4.1.2. — Notar, en el teorema anterior, que X está entonces definida sobre $M_{L/K}(P : X \to \mathbb{P}^1_L, G)$, pero como ya hemos notado, $M_{L/K}(P : X \to \mathbb{P}^1_L, G)$ puede ser una extensión no trivial de $M_{L/K}(X)$.

Una generalización del Teorema 4.1.1 fué obtenida por Dèbes-Emsalem [**6**], también utilizando el Teorema de Weil.

Teorema 4.1.3. — [**6**] *Sea $K < L$ una extensión de Galois de grado finito y X una variedad algebraica proyectiva definida sobre L con $M_{L/K}(X) = K$ y $\mathrm{Aut}(X)$ un grupo finito. Sean E una variedad algebraica proyectiva definida sobre L y $P : X \to L$ un cubriente de Galois con grupo cobertor $\mathrm{Aut}(X)$ también definido sobre L.*

Entonces existe una variedad algebraica proyectiva $B \cong E$, definida sobre K (llamado un modelo canónico), y un isomorfismo $R : E \to B$ definido sobre L, de manera que, si $Q = R \circ P$, entonces $M_{L/K}(Q : X \to B) = K$.

Más aún, si podemos encontrar un punto en $B - B_Q$, donde B_Q denota el conjunto de valores críticos de Q, que sea K-racional, entonces K es un cuerpo de definición de X.

Demonstración. —
(1) Como K es el cuerpo de móduli de X, para cada $\sigma \in \mathrm{Aut}(L/K)$ existe un isomorfismo birracional $f_\sigma : X \to X^\sigma$ definido sobre L. Por otro lado, existe necesariamente un isomorfismo birracional (únicamente determinado por σ) $g_\sigma : E \to E^\sigma$ tal que $g_\sigma \circ P = P^\sigma \circ f_\sigma$. Tales isomorfismos g_σ están definidos sobre L.

Notemos que, para cada $\tau, \sigma \in \mathrm{Aut}(L/K)$, vale que $f_\tau^\sigma \circ f_\sigma \circ f_{\sigma\tau}^{-1} \in \mathrm{Aut}(X^{\sigma\tau})$. En particular, $P^{\sigma\tau} = P^{\sigma\tau} \circ f_\tau^\sigma \circ f_\sigma \circ f_{\sigma\tau}^{-1}$, o equivalentemente, $P^{\sigma\tau} \circ f_{\sigma\tau} = P^{\sigma\tau} \circ f_\tau^\sigma \circ f_\sigma$. Como $P^{\sigma\tau} \circ f_\tau^\sigma = (P^\tau \circ f_\tau)^\sigma = (g_\tau \circ P)^\sigma = g_\tau^\sigma \circ P^\sigma$, lo anterior es equivalente a tener la igualdad $g_{\sigma\tau} \circ P = P^{\sigma\tau} \circ f_{\sigma\tau} = g_\tau^\sigma \circ P^\sigma \circ f_\sigma = g_\tau^\sigma \circ g_\sigma \circ P$. Como las transformaciones g_η están únicamente determinadas, esta última igualdad es equivalente a tener $g_{\sigma\tau} = g_\tau^\sigma \circ g_\sigma$.

Ahora, tenemos las condiciones del Teorema de Weil para asegurar la existencia de una variedad algebraica proyectiva $B \cong E$, definida sobre K, y un isomorfismo birracional $R : E \to B$ definido sobre L, de manera que $R = R^\sigma \circ g_\sigma$, para cada $\sigma \in \mathrm{Aut}(L/K)$.

Consideremos $Q = R \circ P : X \to B$. Para cada $\sigma \in \mathrm{Aut}(L/K)$, tenemos que $Q = Q^\sigma \circ f_\sigma$. En efecto, $Q^\sigma \circ f_\sigma = R^\sigma \circ P^\sigma \circ f_\sigma = R^\sigma \circ g_\sigma \circ P = R \circ P = Q$. Luego, $M(Q : X \to B) = K$.

(2) Supongamos ahora que existe un punto $r \in B - B_Q$ que es K-racional. Sea $p \in X$ tal que $Q(p) = r$. Si $\sigma \in \mathrm{Aut}(L/K)$, entonces el punto $\sigma(p) \in X^\sigma$ satisface que $Q^\sigma(\sigma(p)) = r$ (ya que $Q^\sigma(\sigma(p)) = \sigma(Q(p)) = \sigma(r) = r$). Luego, existe $h_\sigma \in \mathrm{Aut}(X)$ de manera que $f_\sigma \circ h_\sigma(p) = \sigma(p)$. Sea $t_\sigma = f_\sigma \circ h_\sigma$. Tenemos que $t_\sigma : X \to X^\sigma$ es un isomorfismo birracional, definido sobre L, tal que $t_\sigma(p) = \sigma(p)$. Notemos que t_σ está únicamente determinado por σ. En efecto, si $t : X \to X^\sigma$ es otro isomorfismo tal que $t(p) = \sigma(p)$, entonces $h = t^{-1} \circ t_\sigma \in \mathrm{Aut}(X)$ es tal que $h(p) = p$. Como r no es un valor crítico de Q, se debe tener que $h = I$, es decir $t = t_\sigma$. Ahora, la unicidad en la elección de t_σ asegura que la familia $\{t_\sigma : \sigma \in \mathrm{Aut}(L/K)\}$ satisface las condiciones de Weil. Se sigue que X está definida sobre K.

□

Observación 4.1.4. — En la demostración del Teorema 4.1.3, tenemos un isomorfismo $R : E \to B$ satisfaciendo la propiedad que, para cada $\sigma \in \mathrm{Aut}(L/K)$, vale la igualdad $R = R^\sigma \circ g_\sigma$. El buscar un punto $r \in B - B_Q$ que sea K-racional es equivalente a buscar un punto $s \in E - B_P$ tal que $\sigma(R(s)) = R(s)$, para cada $\sigma \in \mathrm{Aut}(L/K)$. Como $\sigma(R(s)) = R^\sigma(\sigma(s))$, esto es equivalente a buscar un punto $s \in E - B_P$ tal que $g_\sigma(s) = \sigma(s)$, para cada $\sigma \in \mathrm{Aut}(L/K)$. Es decir, para la busqueda de puntos K-racionales en B no es necesario saber quien es B.

Tarea 18. — *Supongamos que X es una curva, $X/\mathrm{Aut}(X) = E = \mathbb{P}^1_L$ y que tenemos que para cada $\sigma \in \mathrm{Aut}(L/K)$ vale que $g_\sigma(z) = (a_\sigma z + b_\sigma)/(c_\sigma z + d_\sigma)$, donde $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in K$ y $a_\sigma d_\sigma - b_\sigma c_\sigma = 1$.*

1. *La función $\Psi : \mathrm{Aut}(L/K) \to \mathrm{Aut}(\mathbb{P}^1_L) \cong \mathrm{PSL}_2(L)$, definida por $\Psi(\sigma) = g_\sigma^{-1}$, resulta ser un homomorfsimo de grupos.*
2. *Sean $\sigma_1, ..., \sigma_n \in \mathrm{Aut}(L/K)$ tales que g_{σ_1},..., g_{σ_n} generan el grupo $\Psi(\mathrm{Aut}(L/K))$. Supongamos que tenemos un punto $s \in \ker(\Psi)$ tal que $\sigma_j(s) = g_{\sigma_j}(s)$, para cada $j \in \{1, ..., n\}$. Entonces se tiene que $g_\sigma(s) = \sigma(s)$, para cada $\sigma \in \mathrm{Aut}(L/K)$.*

Notemos que si X es una curva algebraica proyectiva no-singular de género $g \geq 2$ definida sobre un cuerpo L, entonces $\mathrm{Aut}(X)$ (grupo de automorfismos de X definidos sobre L) es un grupo finito. Podemos entonces considerar el cubriente de Galois $P : X \to X/\mathrm{Aut}(X)$. En este caso, tenemos la siguiente consecuencia.

Corolario 4.1.5. — [**6**] *Sea $K < L$ una extensión de Galois de grado finito, X una curva algebraica proyectiva no-singular de género $g \geq 2$ definida sobre L y $M_{L/K}(X) = K$. Supongamos que E es una curva algebraica proyectiva definida sobre L y que $P : X \to E$ es un cubriente de Galois, con grupo cobertor $\mathrm{Aut}(X)$, definido sobre L. Entonces existe una curva algebraica proyectiva no-singular $B \cong E$, definida sobre K (llamado un modelo canónico)), y un isomorfismo $R : E \to B$ definido sobre L, de manera que, si $Q = R \circ P$, entonces $M_{L/K}(Q : X \to B) = K$.*

Más aún, si podemos encontrar un punto en $B - B_Q$, donde B_Q denota el conjunto de valores críticos de Q, que sea K-racional, entonces K es un cuerpo de definición de X.

En el Corolario 4.1.5, la condición de que X sea una curva no-singular de género al menos 2 puede ser eliminada, pero debemos asegurarnos que su grupo de automorfismos birracionales sea finito.

El Teorema 4.1.3 puede ser generalizado a ciertos subgrupos de automorfismos, siguiendo una demostración similar, como se puede ver en el siguiente.

Teorema 4.1.6. — *Sea $K < L$ una extensión de Galois de grado finito, X una variedad algebraica proyectiva definida sobre L y $M_{L/K}(X) = K$. Sea $G < \mathrm{Aut}(X)$ un grupo finito, E variedad algebraica definida sobre L y $P : X \to E$ un cubriente de Galois, definido sobre L, con grupo cobertor G. Supongamos que las siguientes propiedades valen :*

1. *G es su propio normalizador en $\mathrm{Aut}(X)$, y*
2. *para cada $\sigma \in \mathrm{Aut}(L/K)$ existe un isomorfismo birracional $f_\sigma : X \to X^\sigma$, definido sobre L, de manera que $G^\sigma = f_\sigma G f_\sigma^{-1}$.*

Entonces

1. *Existe una variedad algebraica proyectiva $B \cong E$, definida sobre K, y un isomorfismo $T : E \to B$ definido sobre L, de manera que, si $Q = T \circ P$, entonces $M_{L/K}(Q : X \to B, G) = K$. Más aún, si podemos encontrar un punto en $B - B_Q$, donde B_Q denota el conjunto de valores críticos de Q, que sea K-racional, entonces K es un cuerpo de definición de X.*
2. *Si además los isomorfismos f_σ son biregulares, entonces podemos escoger T biregular.*

Demonstración. — Demostremos la parte 1. Por cada $\sigma \in \mathrm{Aut}(L/K)$ tenemos un isomorfismo $f_\sigma : X \to X^\sigma$ que satisface la igualdad $G^\sigma = f_\sigma G f_\sigma^{-1}$. El hecho que el normalizador de G es G, cualquier otro isomorfimo $\widehat{f}_\sigma : X \to X^\sigma$ tal que $G^\sigma = \widehat{f}_\sigma G \widehat{f}_\sigma^{-1}$ es de la forma $\widehat{f}_\sigma = f_\sigma \circ h$, para $h \in G$. Lo anterior nos dice que existe isomorfismo $g_\sigma : E \to E^\sigma$, de manera que

$$g_\sigma \circ P = P^\sigma \circ f_\sigma$$

que está únicamente determinado por σ. Tales isomorfismos g_σ están definidos sobre L.

Como $f_{\sigma\tau}^{-1} \circ f_\tau^\sigma \circ f_\tau \in \mathrm{Aut}(X)$ normaliza G, se tiene que $f_{\sigma\tau}^{-1} \circ f_\tau^\sigma \circ f_\tau \in G$. De esta manera,

$$P \circ f_{\sigma\tau}^{-1} \circ f_\tau^\sigma \circ f_\tau = P,$$

de donde se concluye que

$$g_{\sigma\tau} = g_\tau^\sigma \circ g_\tau.$$

Tenemos así que la familia $\{g_\sigma : \sigma \in \mathrm{Aut}(L/K)\}$ satisface las condiciones de Weil y entonces existe una curva algebraica proyectiva no-singular $B \cong E$, definida sobre K, y un isomorfismo $T : E \to B$ definido sobre L, de manera que, para cada $\sigma \in \mathrm{Aut}(L/K)$ vale la igualdad

$$T = T^\sigma \circ g_\sigma.$$

Si $Q = T \circ P$, entonces la última igualdad nos asegura que, para cada $\sigma \in \mathrm{Aut}(L/K)$ valen las igualdades

$$Q = Q^\sigma \circ f_\sigma, \quad G^\sigma = f_\sigma G f_\sigma^{-1},$$

es decir, $M_{L/K}(Q : X \to B, G) = K$.

La demostración de la última parte se demuestra igual que en el caso de la demostración hecha del Teorema 4.1.3.

La demostración de la parte 2.- sigue de lo anterior y de la última parte del Teorema sigue del Teorema de Weil.

□

Observación 4.1.7. — Un subgrupo G como en las hipótesis del Teorema 4.1.6 es, por ejemplo, un subgrupo característico de $\mathrm{Aut}(X)$ de manera que X/G no tenga automorfimos no-triviales.

Teorema 4.1.8 **([5])**. — *Sean $K < L$ extensión de Galois, donde K es un cuerpo finito, X una curva algebraica proyectiva no-singular definida sobre L y $M_{L/K}(X) = K$. Supongamos que $\mathrm{Aut}(X)$ es finito, que E es una variedad algebraica proyectiva definida sobre L y que $P : X \to E$ es un cubriente de Galois, definido sobre L, con G como grupo cobertor. Entonces, X se puede definir sobre K.*

Demonstración. — Como consecuencia del Teorema 4.1.3, podemos asumir que tenemos un cubriente de Galois $P : X \to B$, con grupo cobertor $\mathrm{Aut}(X)$, donde B es un modelo canónico. Como K es finito, $\mathrm{Aut}(L/K)$ es un grupo proyectivo profinito (es decir, el limite inverso de grupos finitos proyectivos). Como consecuencia del Corolario 3.3., en [**5**], el cubriente $P : X \to B$ se puede definir sobre K, en particular X se puede definir sobre K.

□

4.1.1. Construcción del modelo canónico B en el caso que $\mathbf{X/Aut(X) = E = \mathbb{P}^1_L}$. — Si en el Teorema 4.1.3 tenemos $X/\mathrm{Aut}(X) = E = \mathbb{P}^1_L$, entonces la construcción del modelo canónico B es hecha como sigue. Consideremos el cubriente $P : X \to \mathbb{P}^1_L$, cuyo grupo cobertor es $\mathrm{Aut}(X)$. Denotemos por $t = P(x)$, $x \in X$. El cuerpo de funciones meromorfas (sobre L) de $\mathbb{P}^1$ se puede identificar con $L(t)$, el cuerpo de funciones racionales en la variable t y coeficientes en L.

En este caso, como $K = M_{L/K}(X)$, tenemos que para cada $\sigma \in \mathrm{Aut}(L/K)$ existen isomorfismos (definidos sobre L) $f_\sigma : X \to X^\sigma$ y $\widehat{f_\sigma} : \mathbb{P}^1 \to \mathbb{P}^1$ tal que $P^\sigma \circ f_\sigma = \widehat{f_\sigma} \circ P$. Además sabemos que $\widehat{f_\sigma}$ está únicamente determinado por σ. Por otro lado, existen $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in L$, tal que $a_\sigma d_\sigma - b_\sigma c_\sigma \neq 0$ y

$$\widehat{f_\sigma}(t) = \frac{a_\sigma t + b_\sigma}{c_\sigma t + d_\sigma}.$$

Tarea 19. —

1. *Verifique que, para cada $\sigma, \tau \in \mathrm{Aut}(L/K)$ vale que*
$$\widehat{f_{\sigma\tau}} = \widehat{f_\sigma}^{\tau} \circ \widehat{f_\tau}.$$
2. *Concluir que*
$$\Psi : \mathrm{Aut}(L/K) \to \mathrm{Aut}_L(\mathbb{P}^1_L) : \sigma \mapsto \widehat{f_\sigma}^{-1}$$
satisface la propiedad que
$$\Psi(\sigma\tau) = \Psi(\sigma)\Psi(\tau)^\sigma.$$
3. *Supongamos que para cada $\sigma, \tau \in \mathrm{Aut}(L/K)$ vale que $\widehat{f_\tau}^{\sigma} = \widehat{f_\tau}$ (por ejemplo, si tenemos que $a_\tau, b_\tau, c_\tau, d_\tau \in K$, para cada $\tau \in \mathrm{Aut}(L/K)$).*
   (a) Ψ resulta ser un homomorfismo de grupos (ver Tarea 18).
   (b) Concluir que (como $g \geq 2$) $\Psi(\mathrm{Aut}(L/K))$ es un grupo finito.
   (c) Verifique que el subcuerpo fijo en L por $\ker(\Psi)$ es $M(P : X \to \mathbb{P}^1_L)$.
   (d) Concluir que $M(P : X \to \mathbb{P}^1_L)$ es una extensión finita de $M(X)$.

Para cada $\sigma \in \mathrm{Aut}(L/K)$ podemos definir $\widehat{\sigma} \in \mathrm{Aut}(L(t)/K)$ por la regla siguiente :

$$\begin{cases} \widehat{\sigma}(t) = \dfrac{a_\sigma t + b_\sigma}{c_\sigma t + d_\sigma} \\ \\ \widehat{\sigma}(l) = \sigma(l),\ l \in L. \end{cases}$$

Tarea 20. — *Verificar que la función*

$$\Phi : \mathrm{Aut}(L/K) \to \mathrm{Aut}(L(t)/K) : \sigma \mapsto \widehat{\sigma}$$

es un homomorfismo de grupos.

Teorema 4.1.9. — *El modelo canónico B es dado por la variedad algebraica proyectiva no-singular definida sobre K cuyo cuerpo de funciones es el cuerpo fijo $N < L(t)$ por el grupo $\Phi(\mathrm{Aut}(L/K))$.*

Tarea 21. —

1. *Si para cada $\sigma \in \mathrm{Aut}(L/K)$ vale que $\widehat{\sigma}(t) = t$, entonces $N = K(t)$.*
2. *Considere el homomorfismo de grupos*

$$\widehat{\Phi} : \mathrm{Aut}(L/K) \to \mathrm{Aut}(K(t)/K) : \sigma \mapsto \widehat{\sigma}|_{K(t)}.$$

   (a) *Verificar que* $\ker(\widehat{\Phi}) = \ker(\Psi) = M(P : X \to \mathbb{P}^1_L)$.

   (b) *Supongamos que para cada $\sigma, \tau \in \mathrm{Aut}(L/K)$ vale que $\widehat{f_\tau}^{\,\sigma} = \widehat{f_\tau}$ (por ejemplo, si tenemos que $a_\tau, b_\tau, c_\tau, d_\tau \in K$, para cada $\tau \in \mathrm{Aut}(L/K)$). Concluir que $\widehat{\Phi}(\mathrm{Aut}(L/K)) \cong \Psi(\mathrm{Aut}(L/K))$ es grupo finito.*

4.2. Cubrientes regulares

Teorema 4.2.1 **([6])**. — *Sea K un cuerpo perfecto y $\overline{K}$ una clausura algebraica de K. Sea $X \subset \mathbb{P}^n_{\overline{K}}$ una curva algebraica proyectiva no-singular. Si*

1. *$\mathrm{Aut}(X)$ no tienen centro y el grupo de automorfimos internos de $Aut(X)$ tiene un complemento en el grupo de automorfismos de $\mathrm{Aut}(X)$; o*
2. *$M_{\overline{K}/K}(X)$ tiene dimensión cohomológica menor o igual a 1 ; o*
3. *$X/\mathrm{Aut}(X)$ tiene su modelo canónico B con al menos un punto $M_{\overline{K}/K}(X)$-racional,*

entonces $M_{\overline{K}/K}(X)$ es un cuerpo de definición de X.

CAPÍTULO 5

EJEMPLOS

En este capítulo consideraemos el caso de curvas de género 0 y 1 y las curvas hiperelípticas. En el caso de curvas de género 0 y 1 (curvas elípticas) se sabe que el cuerpo de móduli es un cuerpo de definición. Para el caso de curvas hiperel'ıticas también es sabido cuando el cuerpo de móduli es cuerpo de definición en términos de su grupo de automorfismos.

5.1. Curvas de género 0

Sea $K < L$ una extensión de Galois general, $\mathcal{C}$ una clausura algebraica de L y $X \subset \mathbb{P}^n_{\mathcal{C}}$ una curva de género 0 definida sobre L. Entonces, como $X \cong \mathbb{P}^1_L$, el cual puede verse como la variedad algebraica de $\mathbb{P}^2_L$ definida por el polinomio $P(x_0, x_1, x_2) = x_2 \in K[x_0, x_1, x_2]$, se tiene que K es un cuerpo de definición. Como todo cuerpo de definición contiene al cuerpo de móduli $M_{L/K}(X)$, se tiene la igualdad $M_{L/K}(X) = K$.

5.2. Curvas de género 1

Sea K un cuerpo perfecto y $\overline{K}$ una clausura algebraica de K. Sea $X \subset \mathbb{P}^n_{\overline{K}}$ una curva de género 1. Se sabe que X tiene un modelo biracional $C_\lambda \subset \mathbb{P}^2_{\overline{K}}$ definido por el polinomio

$$P_\lambda(x_0, x_1, x_2) = x_1^2 x_2 - x_0(x_0 - x_2)(x_0 - \lambda x_2) \in \overline{K}[x_0, x_1, x_2],$$

donde $\lambda \in \overline{K} - \{0, 1\}$. Más aún, dos tales modelos C_λ y C_μ,son biracionalmente equivalentes sí y sólo si $j(\lambda) = j(\mu)$, donde $j(x)$ es el j-invariante

$$j(x) = 256\frac{(1 - x + x^2)^3}{x^2(1 - x)^2}$$

Si $\sigma \in \mathrm{Aut}(\overline{K}/K)$, entonces $C_\lambda^\sigma = C_{\sigma(\lambda)}$. Luego,

$$\overline{K}_K(C_\lambda) = \{\sigma \in \mathrm{Aut}(\overline{K}/K) : j(\lambda) = j(\sigma(\lambda)) = \sigma(j(\lambda))\}$$

de donde se obtiene que

$$M_{\overline{K}/K}(C_\lambda) = K(j(\lambda))$$

Por otro lado, la curva C_λ tiene un modelo plano biracional $E_\lambda \subset \mathbb{P}^2_{\overline{K}}$ definido por :

1. en el caso que $j(\lambda) \notin \{0, 1728\}$, por el polinomio

$$Q_\lambda(x_0, x_1, x_2) = x_1^2 x_2 + x_0 x_1 x_2 - x_0^3 + \frac{36}{j(\lambda) - 1728} x_0 x_2^2 + \frac{1}{j(\lambda) - 1728} x_2^3 \in K(j(\lambda))[x_0, x_1, x_2],$$

2. en el caso que $j(\lambda) = 0$, por el polinomio
$$Q_\lambda(x_0, x_1, x_2) = x_1^2 x_2 + x_1 x_2^2 - x_0^3 \in K[x_0, x_1, x_2],$$
3. en el caso que $j(\lambda) = 1728$, por el polinomio
$$Q_\lambda(x_0, x_1, x_2) = x_1^2 x_2 - x_0^3 - x_0 x_2^2 \in K[x_0, x_1, x_2]$$

Todo lo anterior nos dice que $M_{\overline{K}/K}(C_\lambda) = K(j(\lambda))$ es cuerpo de definición.

5.3. Curvas de género 2

Teorema 5.3.1. — **[2]** *Sea K un cuerpo perfecto de característica $p = 2$ y $\overline{K}$ una clausura algebraica de K. Si $X \subset \mathbb{P}^n_{\overline{K}}$ es una curva algebraica de género 2, entonces su cuerpo de móduli es un cuerpo de definición.*

Teorema 5.3.2. — **[29]** *Sea K un cuerpo perfecto de característica $p \neq 2$ y $\overline{K}$ una clausura algebraica de K. Sea $X \subset \mathbb{P}^n_{\overline{K}}$ una curva algebraica de género 2, con involución hiperelítica $j : X \to X$. Si $Aut(X)/\langle j\rangle$ no es trivial, entonces su cuerpo de móduli es un cuerpo de definición.*

5.4. Curvas hiperelípticas

Teorema 5.4.1. — **[15, 16]** *Sea K un cuerpo perfecto de característica $p \neq 2$ y $\overline{K}$ una clausura algebraica de K. Sea $X \subset \mathbb{P}^n_{\overline{K}}$ una curva hiperelíptica de género $g \geq 2$, con involución hiperelítica $j : X \to X$, y grupo de automorfismos $Aut(X)$. Si*

1. *$Aut(X)/\langle j\rangle$ no es cíclico ; o*
2. *$Aut(X)/\langle j\rangle$ es cíclico de orden divisible por p,*

entonces $M_{\overline{K}/K}(X)$ es un cuerpo de definición de X.

Observación 5.4.2. — En el caso $K = \mathbb{R}$, en la Thesis de B. Huggins **[15]** está hecha la lista de aquellas curvas hiperelípticas cuyo cuerpo de definición es $\mathbb{R}$ pero que este no es un cuerpo de definición. Del resultado anterior, estas curvas tienen $Aut(X)/\langle j\rangle$ un grupo cíclico no trivial.

Observación 5.4.3. — Recientemente, D. Kohel (2007) ha construido un algoritmo que permite determinar cuando una curva de género 3 está o no definida sobre su cuerpo de móduli. En particular, construye ejemplos con una obstrucción genérica a este problema.

CAPÍTULO 6

CASO COMPLEJO : $K = \mathbb{R}$, $\overline{K} = \mathbb{C}$

Aquí consideraremos el caso de variedades algebraicas proyectivas definidas sobre el cuerpo de los números complejos $\mathbb{C}$ y la extensión de Galois $\mathbb{R} < \mathbb{C}$.

6.1. Notaciones preliminares

$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \langle \sigma(x) = \overline{x} \rangle \cong \mathbb{Z}_2$. Denotemos por $e \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$ el elemento identidad.

Si $X \subset \mathbb{P}^n_{\mathbb{C}}$ es una variedad algebraica proyectiva compleja, entonces el cuerpo de móduli $M_{\mathbb{C}/\mathbb{R}}(C)$ siempre contiene a $\mathbb{R}$ por la definición.

Consideremos la conjugación

$$J_n : \mathbb{P}^n_{\mathbb{C}} \to \mathbb{P}^n_{\mathbb{C}}$$
$$J_n([x_0 : \cdots : x_n]) = [\overline{x_0} : \cdots : \overline{x_n}].$$

Si tenemos dos variedades algebraicas complejas, digamos $X \subset \mathbb{P}^n_{\mathbb{C}}$ e $Y \subset \mathbb{P}^m_{\mathbb{C}}$, y también un morfismo $f : X \to Y$, entonces

$$f^\sigma = J_m \circ f \circ J_n$$

Definición 6.1.1. — Un **isomorfismo anti-birracional** entre dos variedades algebraicas complejas $X \subset \mathbb{P}^n_{\mathbb{C}}$ e $Y \subset \mathbb{P}^m_{\mathbb{C}}$ es una función $f : X \to Y$ de manera que $f \circ J_n : X \to Y$ es un isomorfismo birracional. Si además $Y = X$, entonces decimos que f es un **automorfismo anti-birracional**.

Observación 6.1.2. — Notemos que $J_n : X \to \overline{X}$ induce un automorfismo anti-birracional, donde $\overline{X}$ es la variedad algebraica definida por los polynomios de la forma P_j^σ, donde X está definida por los polinomios P_j y donde $\sigma(z) = \overline{z}$.

6.2. ¿Cuándo es $\mathbb{R}$ cuerpo de móduli ?

Teorema 6.2.1. — *Sea $X \subset \mathbb{P}^n_{\mathbb{C}}$ una variedad algebraica proyectiva compleja. Entonces $M_{\mathbb{C}/\mathbb{R}}(X) = \mathbb{R}$ sí y sólo si X admite un automorfismo anti-birracional.*

Demonstración. — Supongamos que tenemos una variedad algebraica proyectiva compleja $X \subset \mathbb{P}^n_{\mathbb{C}}$. De la definición, $M_{\mathbb{C}/\mathbb{R}}(X) = \mathbb{R}$ sí y sólo si X y $X^\sigma = \overline{X}$ son birracionalmente equivalentes. Como X y $\overline{X}$ son anti-birracionalemente equivalentes bajo la transformación J_n, entonces obtenemos el resultado.

□

6.3. ¿Cuándo es $\mathbb{R}$ cuerpo de definición ?

Teorema 6.3.1. — *Sea $X \subset \mathbb{P}^n_{\mathbb{C}}$ una variedad algebraica proyectiva compleja. Entonces X se puede definir sobre $\mathbb{R}$ sí y sólo si X admite un automorfismo anti-birracional de orden 2 (involucion anti-birracional).*

Demonstración. — Si la variedad algebraica X se puede definir sobre $\mathbb{R}$, entonces $J_n : X \to X$ induce un automorfismo anti-birracional de orden 2 en X.

Supongamos ahora que tenemos una involución anti-birracional $\tau : X \to X$. De esta manera, podemos tomar el isomorfismo birracional $f_\sigma = J_n \circ \tau : X \to X^\sigma = \overline{X}$. Sea $f_e = I$, el isomorfismo identidad de X. Notemos que $f_\sigma = f_\sigma^e \circ f_e$, $f_\sigma = f_e^\sigma \circ f_\sigma$ y $f_e = f_e^e \circ f_e$. Por otro lado, $f_\sigma^\sigma \circ f_\sigma = J_n^\sigma \circ \tau^\sigma \circ J_n \circ \tau = J_n \circ \tau^\sigma \circ J_n \circ \tau = \tau \circ \tau = f_e$. De esta manera, el par $\{f_e, f_\sigma\}$ satisface las condiciones del teorema de Weil para obtener que X se puede definir sobre $\mathbb{R}$.

□

6.4. ¿Cuándo es $\mathbb{R}$ cuerpo de móduli y no es cuerpo de definición ?

Los dos teoremas anteriores nos dicen que para tener ejemplos donde $M_{\mathbb{C}/\mathbb{R}}(X) = \mathbb{R}$ no es un cuerpo de definición, debemos buscar tales variedades X que admiten automorfismos anti-birracionales pero que no admiten automorfismos anti-birracionales de orden 2.

Los primeros ejemplos de este tipo fueron dados, para el caso de curvas algebraicas, por G. Shimura [**31**] y C.J. Earle [**7**]. Ambos ejemplos corresponden a curvas hiperelípticas.

6.5. Ejemplo de Shimura

Sean $a_0 \in \mathbb{R}$, $a_m = 1$, $a_2, ..., a_{m-1} \in \mathbb{C}$ y m entero impar. Supongamos que además

$$\{a_0, a_1, ..., a_{m-1}, \overline{a}_1, ..., \overline{a}_{m-1}\}$$

son algebraicamente independientes sobre $\mathbb{Q}$. Denotemos por $[x : y : z]$ los puntos de $\mathbb{P}^2_{\mathbb{C}}$.

Sea $X \subset \mathbb{P}^2_{\mathbb{C}}$ la curva plana hiperelíptica definida por el polinomio

$$P(x, y, z) = y^2 z^{2m-2} - a_0 x^m z^m - \sum_{r=1}^{m} \left(a_r x^{m+r} z^{m-r} + (-1)^r \overline{a}_r x^{m-r} z^{m+r} \right)$$

La involución hiperelíptica es dada por

$$j([x : y : z]) = [x : -y : z]$$

y un automorfismo anti-analítico de X es dado por

$$\nu([x : y : z]) = \left[\frac{-\overline{z}}{\overline{x}} : \frac{-i\overline{y}\ \overline{z}^{m-1}}{\overline{x}^m} : 1 \right]$$

donde $\nu^2 = j$, es decir, ν es de orden 4. De esta manera, $M_{\mathbb{C}/\mathbb{R}}(X) = \mathbb{R}$.

Si X tuviese además un automorfismo anti-analítico de orden 2, digamos τ, entonces $\nu\tau$ sería una automorfismo analítico de X. Ahora, como la involución hiperelíptica j es única, se tiene que $j \neq \nu\tau$. En efecto, si $j = \nu\tau$, entonces, $\nu = j\tau$ (pues $\tau^2 = I$) y luego, $\nu^2 = j\tau j\tau = j^2\tau^2 = I$ (pues j conmuta con τ por la unicidad de j).

Ahora, las condiciones impuestas a los coeficientes a_j son tales que los únicos automorfismos analíticos de X sean I y j. Así, X no puede ser definida sobre $\mathbb{R}$.

6.6. Ejemplo de Earle

Sean $a \in (-\infty, -3-2\sqrt{2})$ y $b \in \mathbb{C}$ tal que $Im(b) > 0$, $Re(b) < 0$ y $|b|^2 = -a$. Denotemos por $[x : y : z]$ los puntos de $\mathbb{P}^2_{\mathbb{C}}$. Sea $X \subset \mathbb{P}^2_{\mathbb{C}}$ la curva plana hiperelíptica definida por el polinomio

$$P(x, y, z) = y^2z^3 - x(x - z)(x - az)(x^2 - b^2z^2)$$

La involución hiperelíptica es dada por

$$j([x : y : z]) = [x : -y : z]$$

y un automorfismo anti-analítico de X es dado por

$$\nu([x : y : z]) = \left[\frac{a\overline{z}}{\overline{x}} : \frac{ia^2\overline{y}\,\overline{z}^2}{\overline{b}\,\overline{x}^3} : 1\right]$$

donde $\nu^2 = j$. De esta manera, $M_{\mathbb{C}/\mathbb{R}}(X) = \mathbb{R}$.

Supongamos que existe una automorfismo anti-analítico τ de orden 2 en X. Al igual que antes, se tiene que $\tau\nu \neq j$. Luego, el automorfismo $\rho = \tau\nu$ induce una transformación de Möbius $A \neq I$, que preserva el conjunto de valores críticos de $\pi([x : y : z :]) = x/z$ (es decir, el conjunto de puntos dado por las projecciones bajo π de los puntos fijos de j) :

$$\{\infty, 0, 1, a, b, -b\}.$$

Los únicos subconjuntos de 4 puntos de tal conjunto que pertenecen a un mismo círculo en $\widehat{\mathbb{C}}$ son

$$\{\infty, 0, 1, a\} \quad \{\infty, 0, b, -b\}.$$

Las transformaciones de Möbius preservan los círculos de $\widehat{\mathbb{C}}$ y también las razones cruzadas de cuatro puntos. Como las razones cruzadas de esos dos subconjuntos son diferentes, módulo permutación, se tiene que cada uno de tales subconjuntos debe ser invariante por A. En particular, A deja invariante los subconjuntos

$$\{\infty, 0\} \quad \{1, a\} \quad \{b, -b\}.$$

1. Si $A(\infty) = \infty$ y $A(0) = 0$, entonces $A(z) = Rz$, en particular, $A(1) = R$. Como $A \neq I$, se tiene que $R = a$. En tal caso, $A(b) = ab \in \{b, -b\}$, de donde se obtiene que $a \in \{-1, 1\}$, una contradicción.
2. Si $A(\infty) = 0$, entonces $A(z) = R/z$, y $A(1) = R$. Si $A(1) = 1$, entonces $R = 1$ y $a = A(a) = 1/a$, obteniendo $a \in \{-1, 1\}$, una contradicción. Luego, $A(1) = a$, es decir $R = a$. En tal caso, $a/b = A(b) \in \{-b, b\}$, de donde $a \in \{-b^2, b^2\}$, una contradicción.

Así, X no puede ser definida sobre $\mathbb{R}$.

6.7. Ejemplo no-hiperelíptico

El ejemplo de Earle puede ser modificado adecuadamente para obtener un ejemplo de una curva no-hiperelíptica con cuerpo de móduli $\mathbb{R}$ pero que no se puede definir sobre $\mathbb{R}$ [**12**].

Consideremos $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{C} - \{0, 1\}$ tales que $\lambda_j \neq \lambda_k$ si $j \neq k$. Con este data, podemos construir las siguientes curvas algebraicas proyectivas no-singulares :

$$C_{(\lambda_1,\lambda_2,\lambda_3)} := \left\{ \begin{array}{rcl} x_1^2 + x_2^2 + x_3^2 & = & 0 \\ \lambda_1 x_1^2 + x_2^2 + x_4^2 & = & 0 \\ \lambda_2 x_1^2 + x_2^2 + x_5^2 & = & 0 \\ \lambda_3 x_1^2 + x_2^2 + x_6^2 & = & 0 \end{array} \right\} \subset \mathbb{P}^5_{\mathbb{C}}.$$

Estas curvas definen superficies de Riemann no-hiperelípticas de género $g = 17$. Las transformaciones

$$a_1([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [-x_1 : x_2 : x_3 : x_4 : x_5 : x_6]$$

$$a_2([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [x_1 : -x_2 : x_3 : x_4 : x_5 : x_6]$$
$$a_3([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [x_1 : x_2 : -x_3 : x_4 : x_5 : x_6]$$
$$a_4([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [x_1 : x_2 : x_3 : -x_4 : x_5 : x_6]$$
$$a_5([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [x_1 : x_2 : x_3 : x_4 : -x_5 : x_6]$$

generan un grupo Abeliano $H \cong \mathbb{Z}_2^5$ que actúa como grupo de automorfismos analíticos de $C_{(\lambda_1,\lambda_2,\lambda_3)}$. El cociente $C_{(\lambda_1,\lambda_2,\lambda_3)}/H$ es dada por la esfera de Riemann con puntos cónicos siendo ∞, 0, 1, λ_1, λ_2 y λ_3, todos ellos de orden 2. Un cubriente ramificado, con H como grupo de transformaciones de cubrimiento, es dado por

$$\pi([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = -\left(\frac{x_2}{x_1}\right)^2.$$

En [**3**] se verificó que H es un subgrupo normal de $\mathrm{Aut}(C_{(\lambda_1,\lambda_2,\lambda_3)})$. En particular, todo automorfismo analítico (anti-analítico) desciende por π a un automorfismo analítico (anti-analítico) de la esfera de Riemann que deja invariante el conjunto

$$\{\infty, 0, 1, \lambda_1, \lambda_2, \lambda_3\}.$$

Si consideramos los valores $\lambda_1 = a$, $\lambda_2 = -\lambda_3 = b$, donde a y b satisfacen las mismas condiciones del ejemplo de Earle, entonces $C_{(a,b,-b)}$ admite el automorfismo anti-analítico de orden 4 dado por

$$\nu([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [\overline{x_2} : \sqrt{a}\,\overline{x_1} : \overline{x_4} : \sqrt{a}\,\overline{x_3} : \sqrt{b}\,\overline{x_6} : i\sqrt{b}\,\overline{x_5}]$$

donde escogemos $Im(\sqrt{a}) > 0$. Ahora, se puede seguir el mismo argumento hecho en el ejemplo de Earle para verificar que esta curva no admite un automorfismo anti-analítico de orden 2.

CAPÍTULO 7

CURVAS DE BELYI

En este capítulo nos restrictiremos al caso de curvas algebraicas complejas proyectivas no singulares, es decir, superficies de Riemann compactas, que son un cubriente ramificado (no necesariamente Galois) sobre $\mathbb{P}^1_{\mathbb{C}} = \widehat{\mathbb{C}}$ con a lo más 3 valores de ramificación. Estas curvas (o superficies de Riemann) fueron consideradas por Grothendieck en su **Esquisse d'un programme**, una propuesta para obtener una posición en el "Centre National de la Recherche Scientifique" que han sido una fuente de inspiración en el estudio de **dessins d'enfants** (diseños de niños).

7.1. Curvas de Belyi

Definición 7.1.1. — Una curva algebraica proyectiva no-singular C, definida sobre $\mathbb{C}$, (es decir una superficie de Riemann de algún género g) es llamada una curva de Belyi si existe una función meromorfa $P : C \to \mathbb{P}^1$ con a lo más 3 valores de ramificación. La función P es llamada una función de Belyi para C.

Notemos que si tenemos una función de Belyi $P : C \to \mathbb{P}^1$ con a lo más dos valores de ramificación, entonces es posible contruir una función racional $Q : \mathbb{P}^1 \to \mathbb{P}^1$ de manera que $Q \circ P : C \to \mathbb{P}^1$ tiene exáctamente 3 valores de ramificación.

7.2. Teorema de Belyi

El siguiente resultado describe quienes son las curvas de Belyi de manera algebraica.

Teorema 7.2.1 **(Teorema de Belyi [35])**. — *Una curva algebraica proyectiva no-singular es de Belyi sí y sólo si se puede definir sobre* $\overline{\mathbb{Q}}$.

Demonstración. — Sea C una curva algebraica proyectiva no-singular de género g.

7.2.1. Caso $g = 0$**.** — Por el teorema de uniformización de Koebe, si $g = 0$, entonces C es isomorfa a $\mathbb{P}^1$, luego está definida sobre $\mathbb{Q}$. También es claro que $P(z) = z$ es una función de Belyi para C.

7.2.2. Caso $g \geq 1$**.** — Ahora en adelante, supondremos que $g \geq 1$.

7.2.3. Demostración de la parte "sólo si". — Supongamos que C es una curva de Belyi y sea $P : C \to \mathbb{P}^1$ una función de Belyi, la cual podemos suponer que está ramificada sobre los puntos ∞, 0 y 1. Supongamos que los ordenes de ramificación de P sobre ∞, 0 y 1 son, respectivamente, a, b y c.

Sea $X \in \{\mathbb{C}, \mathbb{H}^2\}$ el cubriente universal de C, d el grado de P y Γ un grupo de transformaciones de Möbius con presentación

$$\Gamma = \langle x, y, z : x^a = y^b = z^c = xyz = 1\rangle.$$

Podemos asumir que existe un cubriente universal (ramificado) $\pi : X \to \mathbb{P}^1$; donde miramos $\mathbb{P}^1$ como un orbifold con puntos cónicos ∞, 0 y 1 con ordenes, respectivamente, a, b y c. Con esta elección, el teorema de uniformización nos asegura que existe un subgrupo $K < \Gamma$ de índice d, un cubriente ramificado $Q : X \to C$ con grupo cobertor K de manera que $\pi = P \circ Q$.

Si $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, entonces C^σ sigue siendo una curva de Belyi y $P^\sigma : C^\sigma \to \mathbb{P}^1$ una función de Belyi, también ramificada sobre ∞, 0 y 1. Más aún, los valores de ramificación de P y P^σ son los mismos en $p \in \{\infty, 0, 1\}$. De esta manera, podemos ver que $C^\sigma = X/K_\sigma$, donde K_σ es subgrupo de Γ de índice d y un cubriente ramificado $Q_\sigma : X \to C^\sigma$ tal que $\pi = P_\sigma \circ Q_\sigma$.

Como sólo existen un número finito de subgrupos de índice d en Γ, esto nos asegura que el subgrupo

$$J = \{\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q}) : C^\sigma \cong C\}$$

es un subgrupo de índice finito de $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Esto nos dice que el cuerpo de móduli $M(C)$ es una extensión de grado finito sobre $\mathbb{Q}$. Como consecuencia del teorema 2.4.4, C se puede definir sobre una extensión finita de $M(C)$, luego sobre una extensión finita de $\mathbb{Q}$; es decir, C se puede definir sobre $\overline{\mathbb{Q}}$.

7.2.4. Demostración de la parte "sí". — Ahora, para ver la otra dirección, seguiremos la demostración hecha en [**36**].

Lema 7.2.2. — *Sean $A : S \to \mathbb{P}^1$ y $B : \mathbb{P}^1 \to \mathbb{P}^1$ funciones holomorfas ambas no-constante, donde S es una superficie de Riemann. Supongamos que los valores críticos de A es $VC(A) \subset \mathbb{P}^1$ y $VC(B) \subset \mathbb{P}^1$ es el conjunto de los valores críticos de B. Entonces el conjunto de los valores críticos de $B \circ A$ es $B(VC(A)) \cup VC(B)$.*

Demonstración. — Si $p \in S$, entonces, usando cartas locales, vemos por la regla de la cadena que $B'(A(p))A'(p) = (B \circ A)'(p)$. Así. p es un punto crítico de $B \circ A$ sí y sólo si p es punto crítico de A o bien $A(p)$ es punto crítico de B. Como $B \circ A$ no es constante, esta es una función sobreyectiva, estamos listos. □

Supongamos que C se puede definir sobre $\overline{\mathbb{Q}}$. Luego, esta se puede definir sobre un cuerpo K que es extensión de grado finita sobre $\mathbb{Q}$. Supongamos que $C \subset \mathbb{P}^r$ es dada como los ceros comunes de ciertos polinomios homogéneos con coeficientes en K. Consideremos la función

$$T([x_0 : \cdots : x_r]) = x_0/x_r.$$

Los valores críticos de T es una colección finita de puntos que viven en algún cuerpo que es una extensión de grado finita sobre $\mathbb{Q}$ y quizás el punto ∞. Sea F el polinomio mínimo, definido sobre $\mathbb{Q}$, de esos números algebraicos, digamos de grado $m > 0$. Luego, por el Lema 7.2.2, los valores críticos de $F \circ T : C \to \mathbb{P}^1$ son ahora ∞, 0 y una cantidad de a lo más $m - 1$ de números algebraicos (diferentes de 0) de grados a lo más $m - 1$. Así, si iteramos un número finito de veces este procedimiento, entonces podemos obtener una función $Q : C \to \mathbb{P}^1$ cuyos valores críticos son números racionales y posiblemente el punto ∞. Sean tales puntos racionales dados por

$$r_1, ..., r_n \in \mathbb{Q}.$$

Si $n \leq 2$, entonces, por el Lema 7.2.2, podemos encontrar una transformación de Möbius de la forma $M(z) = az+b$ de manera que los valores críticos de $M \circ Q : C \to \mathbb{P}^1$ estén contenidos en $\{\infty, 0, 1\}$ y estaremos listos.

Supongamos ahora que $n \geq 3$. Definamos los números

$$y_i = \left(\prod_{j \neq i} (r_i - r_j) \right)^{-1} \in \mathbb{Q}.$$

Lema 7.2.3. — *Valen las siguientes igualdades.*

$$(1) \quad y_1 + \cdots + y_n = 0.$$

$$(2) \quad \sum_{i=1}^{n} \frac{y_i}{x - r_i} = \frac{1}{\prod_{i=1}^{n}(x - r_i)}.$$

Demonstración. — Consideremos el polinomio de interpolación de Lagrange asociado al conjunto de los n pares $(r_1, 1)$,..., $(r_n, 1)$, el cual tiene la forma $P(x) = \sum_{j=1}^{n} L_j(x)$, donde $L_j(x) = \prod_{i \neq j} \frac{x - r_i}{r_j - r_i}$. Este es el único polinomio de grado a lo más $(n-1)$ que satisface $P(r_j) = 1$. Luego, $P(x) \equiv 1$.

En particular, el coeficiente que acompaña al término x^{n-1} deber ser igual a cero. Como tal coeficiente es $y_1 + \cdots + y_k = \sum_{j=1}^{n} \prod_{i \neq j} \frac{1}{r_j - r_i}$, obtenemos (1).

Ya que

$$1 = P(x) = \sum_{i=1}^{n} \prod_{i \neq j} \left(\frac{x - r_j}{r_i - r_j} \right) = \sum_{i=1}^{n} \frac{\prod_{i \neq j}(x - r_j)}{\prod_{i \neq j}(r_i - r_j)} = \sum_{i=1}^{n} y_i \prod_{i \neq j}(x - r_j) = \sum_{i=1}^{n} \frac{y_i}{x - r_i} \prod_{j=1}^{n}(x - r_j),$$

obtenemos (2).

□

Sea N el mínimo comun denominador de los números racionales y_1,..., y_n. Entonces, $a_i = N y_i \in \mathbb{Z}$ (pueden ser enteros negativos o positivos) y se tiene, por (1) en Lema 7.2.3, que

$$(3) \quad a_1 + \cdots + a_n = 0.$$

Consideremos la función racional

$$G(x) = \prod_{i=1}^{n} (x - r_i)^{a_i} \in \mathbb{Q}(x).$$

Si $a_j < 0$ (respectivamente, $a_j > 0$), entonces $G(r_j) = \infty$ (respectivamente, $G(r_j) = 0$). Más aún, por (3) se tiene que $G(\infty) = 1$.

Por (2) del Lema 7.2.3 se puede ver que

$$\frac{G'(x)}{G(x)} = \sum_{i=1}^{n} \frac{a_i}{x - r_i} = \sum_{i=1}^{n} \frac{N y_i}{x - r_i} = \frac{N}{\prod_{i=1}^{n}(x - r_i)}.$$

De esta manera, la función G sólo tiene sus puntos críticos contenidos en el conjunto $\{r_1, ..., r_n, \infty\}$. Ahora, por el lema 7.2.2, se obtiene que los valores críticos de

$$P = G \circ Q : C \to \mathbb{P}^1$$

están contenidos en el conjunto $\{\infty, 0, 1\}$.

□

Observación 7.2.4. — Otra manera de ver (1) en el Lema 7.2.3 es como sigue (esta idea es de Gabino González). Podemos suponer que $r_1 < r_2 < \cdots < r_n$.

Dados números reales $\lambda_1 < \lambda_2 < \cdots < \lambda_k$, tenemos el determinante de Vandermonde

$$V(\lambda_1, \lambda_2, \cdots \lambda_n) = \mathrm{Det} \begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{k-2} & \lambda_1^{k-1} \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{k-2} & \lambda_2^{k-1} \\ 1 & \lambda_3 & \lambda_3^2 & \cdots & \lambda_3^{k-2} & \lambda_3^{k-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \lambda_{k-1} & \lambda_{k-1}^2 & \cdots & \lambda_{k-1}^{k-2} & \lambda_{k-1}^{k-1} \\ 1 & \lambda_k & \lambda_k^2 & \cdots & \lambda_k^{k-2} & \lambda_k^{k-1} \end{bmatrix} = \prod_{j>i} (\lambda_j - \lambda_i) > 0.$$

Notamos que $N = V(r_1, r_2, \cdots, r_n)$ y si $V_i := V(r_1, \cdots, r_{i-1}, r_{i+1} \cdots, r_n)$, entonces

$$V \sum y_i = \sum V y_i = V_n - V_{n-1} + \cdots + (-1)^n V_1.$$

La expresión a la derecha no es nada más que el determinate de la matriz

$$\begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{k-2} & 1 \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{k-2} & 1 \\ 1 & \lambda_3 & \lambda_3^2 & \cdots & \lambda_3^{k-2} & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \lambda_{k-1} & \lambda_{k-1}^2 & \cdots & \lambda_{k-1}^{k-2} & 1 \\ 1 & \lambda_k & \lambda_k^2 & \cdots & \lambda_k^{k-2} & 1 \end{bmatrix}$$

de donde obtenemos que $\sum y_i = 0$.

Observación 7.2.5 **(Primera demostración de Belyi)**. — La demostración de la parte "sí" que hemos hecho no es la que primero produjo Belyi (esta la formuló más tarde). La primera demostración es como sigue. Supongamos que hemos logrado encontrar una función holomorfa $F : C \to \mathbb{P}^1$ cuyos valores críticos son los úmeros racionales r_1,..., r_n y probablemente el punto ∞. Si $n \geq 3$, podemos componer F a la izquierda por una transformación de Móbius, de la forma $M(z) = (z - r_1)/(r_2 - r_1)$, para suponer que $r_1 = 0$, $r_2 = 1$ y todos los demás aún contenidos en $\mathbb{Q} \cup \{\infty\}$. Ahora, coponiendo a la izquierda con la transformación de Móbius $T(z) = 1/z$ si es necesario, también podemos asumir que $r_j \in (0, 1)$, para algún $j \geq 3$. Reindexando, si es necesario, podemos asumir que $r_3 \in (0, 1)$. Podemos escribir $r_3 = a/(a + b)$ para ciertos $a, b \in \mathbb{N}$. Ahora consideramos el polinomio de Belyi

$$Q(x) = \frac{(a+b)^{a+b}}{a^a b^b} x^a (1 - x)^b \in \mathbb{Q}[x].$$

Notamos que $Q(\infty) = \infty$, $Q(0) = Q(1) = 0$ y $Q(r_3) = 1$ y $Q(r_j) \in \mathbb{Q}$ para cada $j = 4, ..., n$. Más aún, como

$$Q'(x) = -\frac{(a+b)^{a+b}}{a^a b^b} x^{a-1} (1 - x)^{b-1} ((a + b)x - a),$$

de donde vemos que los puntos críticos de Q están contenidos en el conjunto $\{\infty, 0, 1, r_3\}$, luego sus valores críticos están contenidos en el conjunto $\{\infty, 0, 1\}$. De esta manera, por el Lema 7.2.2, obtenemos una nueva función holomorfa $Q \circ F : C \to \mathbb{P}^1$ cuyos valores críticos están contenidos en el conjunto $\{s_1 = 0, s_2 = 1, s_3, ..., s_m\} \cup \{\infty\}$, donde $s_j \in \mathbb{Q}$ y $m < n$. Si $m \geq 3$, entonces procedemos de la misma manera hasta lograr una función holomorfa no-constante $P : C \to \mathbb{P}^1$ con a lo más 3 valores críticos contenidos en el conjunto $\{\infty, 0, 1\}$.

Corolario 7.2.6. — *Toda curva de Belyi se puede definir sobre una extensión finita de $\mathbb{Q}$. En particular, como consecuencia del teorema del elemento primitivo, toda curva de Belyi se puede definir sobre un cuerpo $\mathbb{Q}(\alpha)$, donde $\alpha \in \overline{\mathbb{Q}}$.*

7.3. Curvas casi-platónicas

Ejemplos de curvas de Belyi son aquellas que tienen muchos automorfimos.

Definición 7.3.1. — Sea $C \subset \mathbb{P}^n_{\mathbb{C}}$ una curva algebraica no-singular y $\mathrm{Aut}(C)$ su grupo de automorfismos birracionales (luego, biregulares) definidos sobre el cuerpo $\mathbb{C}$. Diremos que C es casi-platónica si $C/\mathrm{Aut}(C) \cong \mathbb{P}^1_{\mathbb{C}}$ y tiene a lo más 3 valores de ramificación.

El siguiente resultado fué probado por Wolfart [**35**]. Nosotros daremos una demostración basada en la demostración hecha del Teorema 4.1.3.

Teorema 7.3.2 **([35])**. — *Toda curva casi-platónica se puede definir sobre su cuerpo de móduli.*

Demonstración. — Denotemos por K el cuerpo de móduli de C.

Por el Corolario 7.2.6, C se puede definir sobre una extensión finita L de $\mathbb{Q}$. Por otro lado, sabemos que el cuerpo de móduli K es un subcuerpo de L, es decir, tenemos $\mathbb{Q} < K < L$. Más aún, podemos suponer que la extensión $K < L$ es Galois de grado finito.

Consideremos el cubriente de Galois $P : C \to C/\mathrm{Aut}(C) = \mathbb{P}^1_{\mathbb{C}}$, y supongamos que los tres valores críticos son ∞, 0 y 1.

Para cada $\sigma \in \mathrm{Aut}(L/K)$ tenemos un isomorfismo birracional (de hecho es biregular) $f_\sigma : C \to C^\sigma$. Tenemos un único automorfismo birracional $g_\sigma : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ (es decir una transformación de Möbius) tal que

$$P^\sigma \circ f_\sigma = g_\sigma \circ P.$$

Notar que, como estamos cocientando por todo el grupo $\mathrm{Aut}(C)$, el automorfsimo g_σ está únicamente determinado por σ y no la elección de f_σ. Más aún, como g_σ debe permutar los puntos en $\{\infty, 0, 1\}$, se ve que $g_\sigma \in \mathfrak{S}_3 = \langle A(z) = 1/z, B(z) = 1/(1-z)\rangle$. En particular, para cada $\tau, \sigma \in \mathrm{Aut}(L/K)$, vale que $g_\sigma^\tau = g_\sigma$ y que $g_e = I$, donde $e \in \mathrm{Aut}(L/K)$ es la identidad.

Notemos que existe un homomorfimo natural de grupos definido por

$$\Psi : \mathrm{Aut}(L/K) \to \mathfrak{S}_3 : \sigma \mapsto g_\sigma^{-1}.$$

La familia $\{g_\sigma : \sigma \in \mathrm{Aut}(L/K)\}$ satisface las condiciones del Teorema de Weil, luego, existe un isomorfismo birracional $R : \mathbb{P}^1_{\mathbb{C}} \to B$, donde R está definida sobre L y B está definida sobre K, de manera que, para cada $\sigma \in \mathrm{Aut}(L/K)$, vale que $R = R^\sigma \circ g_\sigma$.

Si tomamos $Q = R \circ P : C \to B$, cubrimiento de Galois asociado a la acción de $\mathrm{Aut}(C)$, entonces, para cada $\sigma \in \mathrm{Aut}(L/K)$, vale que $Q = Q^\sigma \circ f_\sigma$.

Ahora, para poder terminar la demostración, usando el Teorema 4.1.3, sólo necesitamos encontrar un punto K-racional en B, fuera de los valores críticos de Q. Al igual que antes, esto es equivalente a encontrar un punto $r \in \mathbb{P}^1_{\mathbb{C}} - \{\infty, 0, 1\}$ tal que, para cada $\sigma \in \mathrm{Aut}(L/K)$, vale la igualdad $\sigma(r) = g_\sigma(r)$.

Denotemos por $G = \Psi(\mathrm{Aut}(L/K)) < \mathfrak{S}_3$.

1. Si $G = \{I\}$, entonces basta tomar $r = -1$.
2. Si $G \cong \mathbb{Z}_2$, entonces tenemos las siguientes posibilidades para el generador T de G :
   (a) $T(z) = 1/z$, en cuyo caso basta tomar $r = -1$.
   (b) $T(z) = z/(z-1)$, en cuyo caso basta tomar $r = 2$.
   (c) $T(z) = 1 - z$, en cuyo caso basta tomar $r = 1/2$.

3. Si $G \cong \mathbb{Z}_3$, entonces $\ker(\Psi) = \{\sigma \in \mathrm{Aut}(L/K) : g_\sigma = I\}$ es subgrupo de índice 3 en $\mathrm{Aut}(L/K)$. Sea $K < J < L$ el cuerpo fijo de $\ker(\Psi)$, luego $[J : K] = 3$. Notemos que en este caso, $\forall r \in K - \{0, 1\}$ satisface la igualdad $\sigma(r) = g_\sigma(r)$, para cada $\sigma \in \ker(\Psi)$. Esto nos dice que, para tales r, $R(r) \in B$ es un punto J-racional de B fuera de los valores de ramificación. Usando el Corolario 2.1.9, obtenemos la existencia de un punto K-racional fuera de la ramificación de B.
4. Si $G = \mathfrak{S}_3$, entonces podemos considerar $H = \langle A(z) = 1/z\rangle \cong \mathbb{Z}_2$ y $\Psi(H)^{-1} < \mathrm{Aut}(L/K)$. Luego, el cuerpo fijo N del grupo $\Psi(H)^{-1}$ es una extensión de grado 3 de K. Por 2, sabemos de la existencia de puntos N-racionales, y por el Corolario 2.1.9, de la existencia de puntos K-racionales.

□

Observación 7.3.3. — En 3. y 4., al final de la demostración anterior, tenemos que los tres valores de ramificación de $C/\mathrm{Aut}(C)$ tienen el mismo orden, digamos $k \geq 2$. Podemos considerar un cubriente regular $J : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, cuyo grupo de transformaciones de cubrimiento es $\mathfrak{S}_3$. La función J se puede definir sobre $\mathbb{Q}$ y el cubriente $U = J \circ P : C \to \mathbb{P}^1_{\mathbb{C}}$ es ramificada sobre los puntos ∞ (con order 2), 0 (con orden 3) y 1 con orden $2k$. Como por cada $\sigma \in \mathrm{Aut}(L/K)$ se tiene que $g_\sigma \in \mathfrak{S}_3$, tenemos la relación $U = U^\sigma \circ f_\sigma$. Esto nos dice que el cubriente $U : C \to \mathbb{P}^1_{\mathbb{C}}$ tiene a K como su cuerpo de móduli.

7.4. Cocientes de curvas de Belyi son curvas de Belyi

En esta sección recordaremos dos resultados obtenidos en [**10**] por Gabino González-Diez .

Teorema 7.4.1. — *Sea $f : C_1 \to C_2$ un morfismo sobreyectivo entre curvas algebraicas complejas proyecticas irreducibles no-singulares (luego superficies de Riemann). Si C_2 y los valores críticos de f están definidos sobre $\overline{\mathbb{Q}}$, entonces C_1 se puede definir sobre $\overline{\mathbb{Q}}$.*

Demonstración. — La idea es considerar la extensión de Galois general $\overline{\mathbb{Q}} < \mathbb{C}$. Sea $\Gamma = \mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$. Si $\sigma \in \Gamma$, entonces tenemos un morfismo sobreyectivo $f^\sigma : C_1^\sigma \to C_2$. Más aún, como los valores críticos de f está definidos sobre $\overline{\mathbb{Q}}$, entonces los valores críticos de f^σ son los mismos que para f. Por el teorema de monodromía [**25**], sólo hay un número finito de tales cubrientes (módulo isomorfía). Esto asegura que el grupo

$$K = \{\sigma \in \Gamma : C_1^\sigma \cong C_1\}$$

tiene índice finito en Γ. De esta manera, el cuerpo de móduli $M_{\mathbb{C}/\overline{\mathbb{Q}}}(C_1)$ es una extensión de grado finito sobre $\overline{\mathbb{Q}}$; es decir, $M_{\mathbb{C}/\overline{\mathbb{Q}}}(C_1) = \overline{\mathbb{Q}}$. Esto nos asegura que $M_{\mathbb{C}/\mathbb{Q}}(C_1) < \overline{\mathbb{Q}}$. Como C_1 se puede definir sobre una extensión finita de su cuerpo de móduli [**11**], tenemos que C_1 se puede definir sobre $\overline{\mathbb{Q}}$. □

Teorema 7.4.2. — *Sea $f : C_1 \to C_2$ un morfismo sobreyectivo entre curvas algebraicas complejas proyecticas irreducibles no-singulares (luego superficies de Riemann). Si C_1 es una curva de Belyi, entonces también lo es C_2.*

Demonstración. — Podemos asumir que C_1 está definida sobre $\overline{\mathbb{Q}}$. La idea es otra véz considerar la extensión de Galois general $\overline{\mathbb{Q}} < \mathbb{C}$. Sea $\Gamma = \mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$. Si $\sigma \in \Gamma$, entonces tenemos un morfismo sobreyectivo $f^\sigma : C_1 \to C_2^\sigma$.

Por el teorema de Franchis-Severi [**9, 14, 19, 23**], sólo hay un número finito de tales cocientes (módulo isomorfía). Esto asegura que el grupo

$$K = \{\sigma \in \Gamma : C_2^\sigma \cong C_2\}$$

tiene índice finito en Γ. De esta manera, el cuerpo de móduli $M_{\mathbb{C}/\overline{\mathbb{Q}}}(C_2)$ es una extensión de grado finito sobre $\overline{\mathbb{Q}}$; es decir, $M_{\mathbb{C}/\overline{\mathbb{Q}}}(C_2) = \overline{\mathbb{Q}}$. Esto nos asegura que $M_{\mathbb{C}/\mathbb{Q}}(C_2) < \overline{\mathbb{Q}}$. Como C_2 se puede definir sobre una extensión finita de su cuerpo de móduli [**11**], tenemos que C_2 se puede definir sobre $\overline{\mathbb{Q}}$. □

7.5. Curvas de Belyi reales

Sea S una superficie de Riemann cerrada. Como ya hemos observado anteriormente, debido al teorema de Riemann-Roch, S puede ser definida por curvas algebraicas proyectivas complejas , no-singulares e irreducibles.

El teorema de Belyi nos asegura que S se puede describir por una tal curva definida sobre $\overline{\mathbb{Q}}$ sí y sólo si S admite una función de Belyi, es decir, una función meromorfa no-constante $\beta : S \to \widehat{\mathbb{C}}$ ramificada sólo en tres valores; decimos que S es una curva de Belyi y que la función β es una función de Belyi.

Por otro lado, S se puede describir por una curva definida sobre $\mathbb{R}$ sí y sólo si S admite una involución anticonformal; se dice que S es simétrica y que la involución es una simetría de S.

En [**21**] Koeck-Singerman vieron que si S es una curva de Belyi simétrica, con una simetría con puntos fijos, entonces S se puede describir por una curva definida sobre $\mathbb{R} \cap \overline{\mathbb{Q}}$. Luego, en [**20**] Koeck-Lau se dieron cuenta que tal resultado seguía válido aún si la simetría no tenía puntos fijos. En ese mismo trabajo, los autores observaron que sus argumentos se podían generalizar a variedades algebraicas que admiten un número finito de automorfsimos.

Un isomorfismo entre variedades algebraicas proyectivas complejas irreducibles y no-singulares es asumido ser biregular; en particular, automorfismos son bireguares.

Teorema 7.5.1. — *Sea V una variedad algebraica proyectiva compleja, irreducible y no-singular, la cual puede ser definida sobre $\overline{\mathbb{Q}}$ y que también se puede definir sobre $\mathbb{R}$. Si V tiene un grupo finito de automorfismos, entonces, V se puede definir sobre $\mathbb{R} \cap \overline{\mathbb{Q}}$.*

Demonstración. — Sea $\Gamma = \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\sigma_1, \sigma_2\} = \langle \sigma_2 \rangle \cong \mathbb{Z}_2$, donde $\sigma_1(z) = z$ y $\sigma_2(z) = \overline{z}$.

Tenemos que V puede ser descrita por una variedad algebraica proyectiva compleja, irreducible y no-singular $X \subset \mathbb{P}^n_{\mathbb{C}}$ definida sobre $\overline{\mathbb{Q}}$, es decir, X es dada como los ceros comunes de polinomios

$$P_1, ..., P_r \in \overline{\mathbb{Q}}[x_0, ..., x_n].$$

Como X también puede ser definida sobre $\mathbb{R}$, entonces existe un isomorfismo $T : X \to \widehat{X}$, definido sobre $\mathbb{C}$, donde $\widehat{X}$ está definida sobre $\mathbb{R}$. Definimos el isomorfismo $f_{\sigma_2} = (T^{\sigma_2})^{-1} \circ T : X \to X^{\sigma_2} = \overline{X}$, definido a priori sobre $\mathbb{C}$.

Sean $X^{\sigma_1} = X$, $f_1 = f_{\sigma_1} = I$, el automorfismo identidad de X, y $f_2 = f_{\sigma_2}$. No es dificil verificar que $f_{\sigma_i \sigma_j} = f_{\sigma_j}^{\sigma_i} \circ f_{\sigma_i}$ (recordar el Teorema de Weil).

Es claro que, Si $\rho \in \mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$, entonces podemos considerar el isomorfismo $f_2^\rho : X^\rho \to \overline{X}^\rho$. Como X y $\overline{X}$ están definidas sobre $\overline{\mathbb{Q}}$, tenemos el isomorfismo $f_2^\rho : X \to \overline{X}$. Como X tiene un grupo finito de automorfismos, se sigue que $K = \{\rho \in \mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}}) : f_2 = f_2^\rho\}$ es un subgrupo de índice finito de $\mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$. Como $\mathrm{Fix}(K)$ es una extensión finita de $\overline{\mathbb{Q}}$, tenemos que$\mathrm{Fix}(K) = \overline{\mathbb{Q}}$; luego $K = \mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$ y, en particular, que f_2 está definido sobre $\overline{\mathbb{Q}}$.

Cada $\sigma \in \Gamma$ produce una permutación $\theta(\sigma) \in \mathfrak{S}_2$ tal que $\sigma\sigma_j = \sigma_{\theta(\sigma)(j)}$, para cada $j = 1, 2$. De hecho, $\theta(\sigma_1) = (1)(2)$ y $\theta(\sigma_2) = (1, 2)$. Así, tenemos un isomorfismo

$$\theta : \Gamma \to \mathfrak{S}_2 : \sigma \mapsto \theta(\sigma).$$

Ahora consideramos la acción de $\mathfrak{S}_2$ en $(\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}) \times (\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}})$ dada por la permutación de los dos factores $(\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}})$. De manera más precisa, $\theta(\sigma_1)(w_1, w_2) = (w_1, w_2)$ and $\theta(\sigma_2)(w_1, w_2) = (w_2, w_1)$, donde $w_1, w_2 \in \mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}$.

Sea

$$\Phi : X \subset \mathbb{P}^n_{\mathbb{C}} \to (\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}) \times (\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}})$$

dada por

$$\Phi(x) = \left(\underbrace{f_1(x), f_2(x)}_{\Phi_1(x)}, \underbrace{f_2(x), f_1(x)}_{\Phi_2(x)} \right)$$

Se tiene que $\Phi_j : X \to \mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}$ es un isomorfismo entre X y $\Phi_j(X)$. En particular, Φ es también un isomorfismo entre X y $\Phi(X)$.

Notemos que $\Phi(X)$ está definida por las siguientes ecuaciones (todas definidas sobre $\overline{\mathbb{Q}}$)

$$\left\{ \begin{array}{c} y_1 - y_4 = 0 \\ y_2 - y_3 = 0 \\ y_2 = f_2(y_1) \\ P_1(y_1) = \cdots = P_r(y_1) = 0 \end{array} \right\}$$

donde $(y_1, y_2, y_3, y_4) \in \mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}$.

Si $\sigma \in \Gamma$, entonces

$$\sigma(f_j(x)) = f_j^{\sigma}(\sigma(x)) = f^{\sigma}_{\sigma_j}(\sigma(x)) = f_{\sigma\sigma_j}(f_{\sigma}^{-1}(\sigma(x))) =$$
$$= f_{\sigma_{\theta(\sigma)(j)}}(f_{\sigma}^{-1}(\sigma(x))) = f_{\theta(\sigma)(j)}(f_{\sigma}^{-1}(\sigma(x))).$$

De lo anterior y el hecho que θ es un homomorfismo se obtiene que

$$\sigma(\Phi_j(x)) = \Phi_{\theta(\sigma)(j)} \circ f_{\sigma}^{-1}(\sigma(x)),$$

en particular, se obtienen las siguientes dos observaciones :

(*) $\sigma(\Phi(x)) = \theta(\sigma) \circ \Phi \circ f_{\sigma}^{-1}(\sigma(x))$;

(**) si $y \in \Phi(X)$ y $\sigma \in \Gamma$, entonces $\sigma(y) \in \theta(\sigma)(\Phi(X))$.

Si $w = (y_1, y_2) \in \mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}$, donde

$$y_j = [y_{j0} : \cdots : y_{jn}],\ j = 1, 2,$$

entonces definimos

$$z_{s_1,s_2} = y_{1s_1} y_{2s_2},\ s_1, s_2 \in \{0, 1, ..., n\},$$

y consideramos la función

$$G : \mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}} \to \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}}$$
$$w \mapsto G(w) = [z_{0,0} : \cdots : z_{n,n}].$$

La función G define un isomorfismo, definido sobre $\mathbb{Q}$, entre $\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}$ y su imágen.

Ahora consideremos la función

$$\Psi_1 : (\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}) \times (\mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}) \to \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}} \times \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}}$$

dada por

$$\Psi_1(w_1, w_2) = (G(w_1), G(w_2))$$

donde $w_j \in \mathbb{P}^n_{\mathbb{C}} \times \mathbb{P}^n_{\mathbb{C}}$, para cada $j = 1, 2$.

La función $\Psi_1 \circ \Phi : X \to (\mathbb{P}^{(n+1)^2-1}_{\mathbb{C}})^2$ define un isomorfismo entre X y su imágen.

El grupo Γ induce una acción por permutaciones, say $\eta : \Gamma \to \mathfrak{S}_2$, de los dos factores $\mathbb{P}^{(n+1)^2-1}_{\mathbb{C}}$ del producto $\mathbb{P}^{(n+1)^2-1}_{\mathbb{C}} \times \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}}$. De manera precisa, $\eta(\sigma_1)(w_1, w_2) = (w_1, w_2)$ y $\eta(\sigma_2)(w_1, w_2) = (w_2, w_1)$, donde $w_1, w_2 \in \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}}$.

Lema 7.5.2. — *Existe una función regular*

$$\Psi_2 : \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}} \times \mathbb{P}^{(n+1)^2-1}_{\mathbb{C}} \to \mathbb{P}^N_{\mathbb{C}} : (w_1, w_2) \mapsto \Psi_2(w_1, w_2)$$

donde $N = 3(n+1)^2 - 6$*, la cual satisface las siguientes tres propiedades.*

1. $\Psi_2^\sigma = \Psi_2$, *para cada* $\sigma \in \Gamma$.
2. *Para cada* $\sigma \in \Gamma$ *vale que* $\Psi_2 \circ \eta(\sigma) = \Psi_2$.
3. *Si* $\Psi_2(w) = \Psi_2(z)$, *entonces existe* $\gamma \in \Gamma$ *tal quet* $w = \eta(\gamma)(z)$.

Demonstración. — Sea $m = (n+1)^2 - 1$ y consideremos

$$H : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^{3m-1}$$

definida por

$$H(z_1, ..., z_m, w_1, ..., w_m)$$
$$||$$
$$(z_1 + w_1, z_2 + w_2, ..., z_m + w_m, z_1w_1, z_2w_2, ..., z_mw_m, z_1z_2 + w_1w_2, z_1z_3 + w_1w_3, ..., z_1z_m + w_1w_m).$$

Se puede ver que $H(z, w) = H(\widehat{z}, \widehat{w})$ sí y sólo si $(\widehat{z}, \widehat{w}) \in \{(z, w), (w, z)\}$.

Si homogenizamos H obtenemos una función

$$\Psi_2 : \mathbb{P}_{\mathbb{C}}^{(n+1)^2-1} \times \mathbb{P}_{\mathbb{C}}^{(n+1)^2-1} \to \mathbb{P}_{\mathbb{C}}^N$$

que satisface las propiedades (1), (2) y (3) como se quería. □

Si $\Psi = \Psi_2 \circ \Psi_1$, donde Ψ_2 es dada por el lema anterior, entonces

$$\Psi : (\mathbb{P}_{\mathbb{C}}^n \times \mathbb{P}_{\mathbb{C}}^n) \times (\mathbb{P}_{\mathbb{C}}^n \times \mathbb{P}_{\mathbb{C}}^n) \to \mathbb{P}_{\mathbb{C}}^N : (w_1, w_2) \mapsto \Psi(w_1, w_2)$$

satisface las siguinetes propiedades.

4. $\Psi \circ \Phi$ es un isomorfismo sobre su imágen.
5. $\Psi^\sigma = \Psi$, para cada $\sigma \in \Gamma$;
6. Para cada $\sigma \in \Gamma$ vale que $\Psi \circ \theta(\sigma) = \Psi$.

Si $Z = \Psi(\Phi(X))$, entonces podemos notar que Z está definida sobre $\overline{\mathbb{Q}}$ (ya que todas las funciones involucradas anteriormente están definidas sobre $\overline{\mathbb{Q}}$). Así, podemos mirar

$$Z_{\overline{\mathbb{Q}}} \subset \mathbb{P}_{\overline{\mathbb{Q}}}^N,$$

dada por los mismos polinomios sobre $\overline{\mathbb{Q}}$ que definen Z. Basta con verificar que $Z_{\overline{\mathbb{Q}}}$ está definida sobre $\mathbb{R} \cap \overline{\mathbb{Q}}$.

Consideremos el grupo $\Gamma_0 = \langle \sigma(z) = \overline{z} \rangle < \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) = \Gamma_1$. Notemos que $\mathrm{Fix}(\Gamma_0) = \mathbb{R} \cap \overline{\mathbb{Q}}$, es decir, $\mathbb{R} \cap \overline{\mathbb{Q}} < \overline{\mathbb{Q}}$ es una extensión de Galois de grado dos.

Si consideramos la biyección $\widehat{\sigma} : \mathbb{P}_{\overline{\mathbb{Q}}}^N \to \mathbb{P}_{\overline{\mathbb{Q}}}^N$, dada por $\widehat{\sigma}([x_0 : \cdots : x_N]) = (\overline{x_0} : \cdots : \overline{x_N}]$, entonces las propiedades $(**)$ y (6.) nos aseguran que $\widehat{\sigma}(Z_{\overline{\mathbb{Q}}}) = Z_{\overline{\mathbb{Q}}}$. Sigue del Teorema 2.1.10 que $Z_{\overline{\mathbb{Q}}}$ se define sobre $\mathbb{R} \cap \overline{\mathbb{Q}}$. □

CAPÍTULO 8

JACOBIANAS

8.1. Jacobianas y Matrices de Riemann

Consideremos una superficie de Riemann S de género $g \geq 1$. Denotemos por $\mathrm{H}_1(S,\mathbb{Z}) \cong \oplus^{2g}\mathbb{Z}$ al primer grupo de homología de S. Este grupo codifica (en parte) la parte topológica de la superficie S. Una base de homología de S es una *base simpléctica* si está representada por $2g$ curvas cerradas orientadas, α_1,..., α_g, β_1,..., β_g, tal que

$$\alpha_j \cdot \alpha_k = \beta_j \cdot \beta_k = 0$$

$$\alpha_j \cdot \beta_k = \delta_{kj}$$

También asociado a S es el espacio vectorial complejo de dimensión g de las 1-formas holomorfas [**8**], denotado por $\mathrm{H}^{1,0}(S)$. Existe una base de este espacio, digamos w_1,..., w_g, satisfaciendo que

$$\int_{\alpha_j} w_k = \delta_{jk}$$

llamada una base dual a la base simpléctica anterior. En este espacio tenemos una forma Hermitiana positiva definida dada por :

$$(\theta_1,\theta_2) = \frac{i}{2}\int\int_S \theta_1 \wedge \overline{\theta_2} = \frac{i}{2}\sum_{j=1}^{g}\left[\int_{\alpha_j}\theta_1\overline{\int_{\beta_j}\theta_2} - \int_{\beta_j}\theta_1\overline{\int_{\alpha_j}\theta_2}\right]$$

para $\theta_1, \theta_2 \in \mathrm{H}^{1,0}(S)$. Por ejemplo, para la base dual w_1,..., w_g anterior tenemos que

$$(w_j, w_k) = Im\left(\int_{\beta_j} w_k\right)$$

Luego, esta forma Hermitiana queda representada en esta base dual como

$$((x_1,...,x_g),(y_1,...,y_g)) = \sum_{j=1}^{g}\sum_{k=1}^{g} x_j\overline{y_k}Im\left(\int_{\beta_j} w_k\right)$$

Si denotamos por $\mathrm{H}^{1,0}(S)^*$ el espacio dual de $\mathrm{H}^{1,0}(S)$, entonces la forma Hermitiana anterior nos da un anti-isomorfismo

$$\Psi : \mathrm{H}^{1,0}(S) \to \mathrm{H}^{1,0}(S)^*$$

definido por

$$\Psi(\theta) = (\cdot, \theta)$$

De esta manera, tenemos inducida la forma Hermitiana

$$(\Psi(\theta_1), \Psi(\theta_2)) = \overline{(\theta_1,\theta_2)}$$

Integración de 1-formas sobre curvas (orientadas) en S da la función

$$\Phi_S : \mathrm{H}_1(S,\mathbb{Z}) \to \left(\mathrm{H}^{1,0}(S)\right)^*$$

definida por

$$\phi([\gamma]) = \int_\gamma$$

Ejercicio. Verificar que esta función es un homomorfismo inyectivo entre $\mathbb{Z}$-módulos. La base dual en $\mathrm{H}^{1,0}(S)^*$ respecto a la base w_1,..., w_g es exactamente la dada por $w_1^* = \int_{\alpha_1}$,..., $w_g^* = \int_{\alpha_g}$

De esta manera, la forma Hermitiana inducida en $\mathrm{H}^{1,0}(S)^*$ en la base dual queda dada por

$$((x_1,...,x_g),(y_1,...,y_g)) = \sum_{j=1}^{g}\sum_{k=1}^{g} \overline{x_j} y_k Im\left(\int_{\beta_j} w_k\right)$$

Se puede ver $\mathrm{H}_1(S,\mathbb{Z})$ como un reticulado en el espacio $\left(\mathrm{H}^{1,0}(S)\right)^*$. El cociente

$$J(S) = (\mathrm{H}^{1,0}(S))^*/\mathrm{H}_1(S,\mathbb{Z})$$

es la *Jacobiana* de S, la cual resulta ser una variedad Abeliana principalmente polarizada (ver la primera parte de este libro).

Usando la base simpléctica α_1,..., α_g, β_1,..., β_g y su base dual w_1,..., w_g de 1-formas holomorfas en S, uno puede escribir lo anterior en coordenadas. Esto es, si usamos la base dual w_1^*,..., w_g^* para el espacio $\left(\mathrm{H}^{1,0}(S)\right)^*$, entonces podemos identificar $\left(\mathrm{H}^{1,0}(S)\right)^*$ con $\widehat{\mathbb{C}}^g$ y el reticulado $\mathrm{H}_1(S,\mathbb{Z})$ se identifica con un reticulado L en $\widehat{\mathbb{C}}^g$ generado por los vectores $e_1 = (1,0,...,0)$, $e_2 = (0,1,0,...,0)$,..., $e_g = (0,...,0,1)$, $z_1 = (z_{1,1},...,z_{g,1})$,..., $z_g = (z_{1,g},...,z_{g,g})$, donde

$$z_{kj} = \int_{\beta_j} w_k = \int_{\beta_k} w_j$$

La matriz $Z = (z_1 z_2 \cdots z_g)$ es llamada una *matriz de Riemann* para S. Luego $J(S)$ es analíticamente equivalente a la variedad abeliana principalmente polarizada obtenida como $\widehat{\mathbb{C}}^g/L$ con la polarización dada por

$$((x_1,...,x_g),(y_1,...,y_g)) = \sum_{j=1}^{g}\sum_{k=1}^{g} \overline{x_j} y_k Im(z_{jk})$$

***Teorema 8.1.1* (Teorema de Torelli [8]).** — *San S y R dos superficies de Riemann cerradas. Entonces S es conformalmente equivelante a R sí y sólo si sus variedaes jacobianas $J(S)$ y $J(R)$ son isomorfas como variedades abelinas principalmente polarizadas.*

Observación 8.1.2. — Denotemos por $\mathrm{Pic}^0(S)$ el espacio de las clases de divisores de grado cero en S (un divisor de grado cero es trivial si es el divisor de una función meromorfa en S). Tomemos un punto $p_0 \in S$. El teorema de Abel [8] dice que la función

$$H : \mathrm{Pic}^0(S) \to J(S)$$

definida por

$$H(p_1 + \cdots + p_g - q_1 - \cdots - q_g) = \left[\int_{p_0}^{p_1} + \cdots + \int_{p_0}^{p_g} - \int_{p_0}^{q_1} - \cdots - \int_{p_0}^{q_g}\right]$$

resulta ser un isomorfismo.

8.2. Cuerpo de definicion de Jacobianas

Consideremos una superficie de Riemann S de género $g \geq 2$. Supongamos que S se puede definir por una curva irreducible no-singular algebraica proyectiva C.

Sea $D = p_1 + \cdots + p_g - q_1 - \cdots - q_g$ es un divisor de grado cero de C y $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Podemos considerar el divisor de grado cero de C^σ dado por

$$D^\sigma = \sigma(p_1) + \cdots + \sigma(p_g) - \sigma(q_1) - \cdots - \sigma(q_g).$$

Si D es el divisor de una función meromorfa $f : C \to \widehat{\mathbb{C}}$, entonces D^σ es el divisor de la función meromorfa $f^\sigma : C^\sigma \to \widehat{\mathbb{C}}$.

De esta manera, tenemos de manera natural una acción del grupo $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ sobre el grupo $\mathrm{Pic}^0(C)$: Si $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, entonces

$$\sigma : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C^\sigma) : [D] \mapsto [D^\sigma].$$

Más aún, tenemos que $\mathrm{Pic}^0(C^\sigma) = \mathrm{Pic}^0(C)^\sigma$.

Lo anterior nos dice que para cada $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ tenemos una acción natural

$$\sigma : J(C) \to J(C^\sigma)$$

de manera que $J(C^\sigma) = J(C)^\sigma$.

Supongamos ahora que C está definida sobre el cuerpo $\mathbb{K} < \mathbb{C}$ Notemos que para cada $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{K})$ vale que $C^\sigma = C$, en particular, $J(C) = \mathrm{Pic}^0(C) = \mathrm{Pic}^0(C^\sigma) = \mathrm{Pic}^0(C)^\sigma = J(C)^\sigma$. Esta igualdad nos asegura que $J(C)$ también se puede definir sobre el cuerpo $\mathbb{K}$.

El recíproco a lo anterior es dado por el Teorema de Torelli.

Teorema 8.2.1. — *Sea S una superficie de Riemann cerrada. Entonces S se puede definir sobre un cuerpo $\mathbb{K} < \mathbb{C}$ sí y sólo si su variedad Jacobiana $J(S)$ se puede definir sobre $\mathbb{K}$.*

REFERENCIAS

[1] E. Artin. *Galois Theory.* Dover Publications (1998). ISBN 0-486-62342-4. (Reprinting of second revised edition of 1944, The University of Notre Dame Press).

[2] G. Cardona, E. Nart and J. Pujolàs. Curves of genus two over fields of even characteristic. *Math. Z.* **250** No. 1 (2005), 177-201.

[3] A. Carocca, V. Gonzalez, R.A. Hidalgo and R. Rodriguez. Generalized Humbert Curves.] *Israel Journal of Mathematics* **64**, No. 1 (2008), 165-192.

[4] K. Coombes and D. Harbater. Hurwitz families and arithmetic Galois theory. *Duke Math. J.* **52** (1985), 821-839.

[5] P. Dèbes and J.-C. Douai. Algebraic covers : field of moduli versus field of definition. *Ann. Sci. École Norm. Sup.* (4) **30** (1997), no. 3, 303-338.

[6] P. Dèbes and M. Emsalem. On fields of moduli of curves. *J. Algebra* **211** No. 1 (1999), 42-56.

[7] C.L. Earle. On the moduli of closed Riemann surfaces with symmetries. *Advances in the Theory of Riemann Surfaces*. Ann. of Math. Studies **66** (1971), 119-130.

[8] H. Farkas and I. Kra. *Riemann Surfaces*. Springer-Verlag, New York, 1980.

[9] M. de Franchis. Un teorema sulle involutioni irrazionalli. *Rend. Circ. Palermo* **36** (1913), 386.

[10] G. Gonzáez-Diez. Varietaions on Belyi's theorem. *The Quaterly Journal of Mathematics.* **57** (2006), 339-354.

[11] H. Hammer and F Herrlich. A Remark on the Moduli Field of a Curve. *Arch. Math.* **81** (2003), 5-10.

[12] R.A. Hidalgo. Non-hyperelliptic Riemann surfaces which cannot be defined over the reals. *Archiv der Math.* **93** (2009), 219-222.

[13] D. Hilbert. Über die Theorie der algebraischen Formen. *Math. Ann.* **36** (1890), 473-534.

[14] A. Howard and A.J. Sommese. On the theorem of de Franchis. *Ann. Scuola Norm. Pisa Cl. Sci.* **10** (1983), 429-436.

[15] B. Huggins. Fields of Moduli and Fields of Definition of Curves. Ph.D. Thesis, UCLA, 2005.

[16] B. Huggins. Fields of moduli of hyperelliptic curves. *Math. Research Letters* **12** No. 2 (2007), 249-262.

[17] T.W. Hungerford. *Algebra*. Reprint. (English) Graduate Texts in Mathematics, Vol. **73**. New York, Heidelberg, Berlin : Springer-Verlag.

[18] N. Jacobson. *Basic Algebra I* (2nd ed). W.H. Freeman and Company, (1985).

[19] E. Kani. Bounds on the number of non-rational subfields of a function field. *Invent. Math.* **85** (1986), 185-198.

[20] B. Koeck and E. Lau. A note on Belyi's theorem for Klein surfaces. *The Quaterly J. of Math.* Access published on December 12, 2008 ; doi : doi :10.1093/qmath/han034.

[21] B. Koeck and D. Singerman. Real Belyi theory. *Q. J. Math.* **58** (2007), 463-478.

[22] S. Koizumi. Fields of moduli for polarized Abelian varieties and for curves. *Nagoya Math. J.* **48** (1972), 37-55.

[23] H.H. Martens. Observations on morphisms of closed Riemann surfaces. II. *Bull. London Math. Soc.* **20** (1988), 253-254.

[24] T. Matsusaka. Polarized varieties, fields of moduli and generalized Kummer varieties of polarized abelian varieties. *Amer. J. Math.* **80** (1958), 45-82.

[25] R. Miranda. *Algebraic curves and Riemann surfaces*. Graduate Studies in Mathematics **5**, American Mathematical Society, Providence, 1995.

[26] D. Mumford, J. Fogarty and F. Kirwan. *Geometric Invariant Theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], **34** (3rd ed.), Berlin, New York : Springer-Verlag, 1994.

[27] E. Noether. Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachr. Ges. Wiss. Göttingen* (1926), 28-35.

[28] E. Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* **77** (1916), 89-92.

[29] J. Quer and G. Cardona. Fields of moduli and field of definition for curves of genus 2. Computational aspects of algebraic curves. *Lecture Notes Series Comput.* **13** (2005), 71-83.

[30] G. Shimura. On the theory of automorphic functions. *Ann. of Math.* **70** No. 2 (1959), 101-144.

[31] G. Shimura. On the fields of rationality of an Abelian variety. *Nagoya Math. J.* **45** (1972), 167-178.

[32] I. Stewart. *Galois Theory.* Chapman and Hall. (1989).

[33] A. Weil. The field of definition of a variety. *Amer. J. Math.* **78** (1956), 509-524.

[34] A. Weil. On algebraic groups of transformations. *Amer. J. of Math.* **77** (1955), 355-391.

[35] J. Wolfart. The Obvious Part of Belyi's Theorem and Riemann Surfaces with many Automorphisms. In : Geometric Galois Actions 1. Leila Schneps and Pierre Lochak eds. *London Math. Soc. Lect. Notes Ser.* **242**, Cambridge 1995.

[36] J. Wolfart. ABC for polynomials, dessins d'enfants, and uniformization - a survey. Proceedings der ELAZ-Konferenz 2004, Hrsg. W. Schwarz, J. Steuding, Steiner Verlag Stuttgart 2006, pp. 313-345.

INDICE