UNIVERSIDAD DE CHILE

FACULTAD DE CIENCIAS

MAGÍSTER EN CIENCIAS MATEMÁTICAS

SUBESPACIOS DE GALOIS PARA LA CURVA RACIONAL NORMAL

Sebastián Andrés Rahausen Rodríguez

Director de Tesis:
Dr. Robert Auffarth

Santiago, Chile
Enero, 2019

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN

TESIS MAGÍSTER

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magíster presentada por el candidato

Sebastián Andrés Rahausen Rodríguez

Ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito para optar al grado de Magíster en Ciencias Matemáticas, en el examen de Defensa de Tesis rendido el día 22 de Enero del 2019.

Director de Tesis

Dr. Robert Auffarth ______________________________

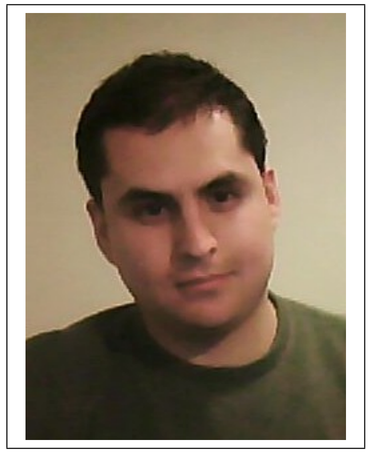
Comisión de Evaluación de la Tesis

Dra. Anita Rojas ______________________________

Dr. Giancarlo Lucchini ______________________________

Dedicado a Daniela
y a mi familia,
muy especialmente
a mi abuela Carmen

BIOGRAFÍA



Nací el 30 de Julio de 1989 en Santiago de Chile. Recibí mi educación básica en el colegio Trewhela's English School y luego seguí la enseñanza media en el Liceo José Victorino Lastarria.

Animado por un deseo de aprender sobre matemáticas y física, mi primera idea fue ingresar a estudiar Ingeniería Civil en alguna especialidad. Después de cursar los dos primeros años de Ingeniería Civil Química en USM San Joaquín, hubo un llamado a personas interesadas en cursos de matemáticas más abstractos/teóricos en comparación con los cursos de matemáticas generales para las ingenierías. Mi participación e interés en estos cursos hizo que decidiera cambiarme a estudiar Ingeniería Civil Matemática en USM Casa Central, Valparaíso, pero luego de un año me cambié a Licenciatura en Matemáticas, porque en realidad lo que me fue atrayendo fue la matemática en si misma más que el enfoque ingenieril.

Después de obtener el grado de Licenciado en Matemáticas, bajo la dirección del Dr. Víctor González y del Dr. Leonelo Iturriaga, pensé en ingresar a un programa de magíster en matemáticas para consolidar mis conocimientos y comenzar a especializarme en algún área. Durante el año 2016 trabajé como profesor jornada parcial para cursos de matemáticas en USM Vitacura y el año 2017 ingresé al programa de Magíster en Ciencias Matemáticas de la Universidad de Chile, bajo la dirección del Dr. Robert Auffarth.

AGRADECIMIENTOS

En el camino de este trabajo he contado con el apoyo de varias personas e instituciones que de distintas formas me han ayudado para que lo haya podido realizar, por lo que deseo expresar mi agradecimiento hacia ellos.

Primero a Robert Auffarth, mi profesor guía, por su generosidad al compartir sus conocimientos, no solo de matemáticas, por el tiempo que me ha dedicado, por su paciencia y por haberme acompañado en el desarrollo de esta tesis. Agradezco a las personas del Departamento de Matemáticas, por generar un ambiente adecuado y por el conocimiento que me han transmitido. En especial, quiero agradecer la presencia de los profesores Yves Martin, Anita Rojas, Giancarlo Lucchini y Luis Arenas por su disposición y atención para conversar o aclarar ideas. También a los profesores Víctor González y Leonelo Iturriaga, directores de mi tesis de Licenciatura en USM, por su apoyo y recomendaciones.

Por otro lado, quiero agradecer a mis compañeros de estudio y de viajes a congresos, en particular a Pablo Quezada, José Aburto, Claudio Bravo y Matías Alvarado.

Agradezco especialmente a Daniela, mi novia, por su apoyo constante. También a mis padres, mis hermanos, y mi abuela Carmen.

Finalmente, manifiesto mi agradecimiento a CONICYT por otorgarme la Beca de Magíster Nacional, la cual ha permitido dedicarme completamente a mis estudios; y al proyecto anillo CONICYT PIA ACT1415 por financiar parcialmente esta tesis y mi participación en diferentes congresos.

RESUMEN

Sea k un cuerpo y sea $\mathbb{P}^n = \mathbb{P}^n_k$ el *espacio proyectivo* de dimensión n sobre k. La única inmersión $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ asociada a un sistema lineal completo de divisores en $\mathbb{P}^1$ y cuya imagen no está contenida en un hiperplano, módulo cambio de coordenadas, es la *inmersión de Veronese* de grado n, denotada ν_n. Su imagen $\nu_n(\mathbb{P}^1)$ es llamada *curva racional normal* de grado n. Dado un subespacio lineal $W \in \mathbb{G}(n-2, n)$ consideremos la proyección $\pi_W : \mathbb{P}^n \dashrightarrow \mathbb{P}^1$ con centro W. La composición $\pi = \pi_W \circ \nu_n : \mathbb{P}^1 \to \mathbb{P}^1$ resulta ser un morfismo sobreyectivo. Diremos que W es un *subespacio de Galois* para ν_n si π es un cubrimiento de Galois. Lo que se hará en este trabajo es caracterizar a todos los subespacios de Galois para la inmersión de Veronese ν_n. Se dará una descripción de estos subespacios como una unión disjunta de subvariedades localmente cerradas en el Grassmanniano $\mathbb{G}(n-2, n)$.

Índice general

Capítulo 1

Nociones de geometría proyectiva

Este trabajo se desarrollará en el contexto de geometría algebraica clásica. Por esta razón, en este primer capítulo se repasarán las nociones de geometría proyectiva básica que se usarán a lo largo de este trabajo. Asumiremos que el lector ya está familiarizado con las nociones principales de geometría algebraica clásica, en particular, todo lo que se trata sobre variedades algebraicas afines [10, p. 3]. Por tanto, solo repasaremos los conceptos básicos sobre geometría proyectiva como modo de poner al lector en contexto, fijar notaciones y convenciones. Las principales referencias para este capítulo son [10], [12] y [17].

1.1. Variedades proyectivas, notaciones y convenciones

Sea k el cuerpo de base, de momento no necesariamente algebraicamente cerrado y de característica $p \geq 0$. Denotaremos por $\mathbb{P}^n_k$, o simplemente $\mathbb{P}^n$, al *espacio proyectivo* de dimensión n sobre k. Sea $A = k[x_0, \ldots, x_n]$ el anillo de polinomios en $n+1$ variables con coeficientes en el cuerpo k.

Un subconjunto X de $\mathbb{P}^n$ se dice que es un *conjunto algebraico* si existe un conjunto finito $T \subset A$ de polinomios homogeneos tal que $X = Z(T) := \{p \in \mathbb{P}^n : f(p) = 0 \text{ para todo } f \in T\}$. Se puede poner una topología en $\mathbb{P}^n$ definiendo los conjuntos cerrados como los conjuntos algebraicos. Esta topología es llamada *topología de Zariski*; y será la que se usará en este trabajo.

Recordemos que para un espacio topológico, se pueden definir las nociones de subconjunto irreducible y dimensión de un subconjunto [10, p. 10]. También es útil recordar que en la topología de Zariski todos los subconjuntos abiertos irreducibles son densos.

Definición 1.1.1. Una *variedad proyectiva* es un conjunto algebraico irreducible en $\mathbb{P}^n$, con la topología inducida. Un subconjunto abierto de una variedad proyectiva es una *variedad cuasi-proyectiva*. La *dimensión* de una variedad cuasi-proyectiva es su dimensión como espacio topológico y se denotará $\dim X$.

Recordamos que cada variedad algebraica afín es una variedad cuasi-proyectiva [17, p.

46]. En lo que sigue llamaremos simplemente *variedad* a las variedades cuasi-proyectivas. Las variedades de dimensión 1 son llamadas *curvas* y las de dimensión 2 *superficies*.

Definición 1.1.2. Sea X una variedad. Diremos que $Y \subset X$ es una *subvariedad* de X, si Y es en si misma una variedad.

Las siguientes son notaciones que usaremos a lo largo de este trabajo, por lo cual suponemos que el lector ya está familiarizado con las nociones correspondientes. Sea $X \subset \mathbb{P}^n$ una variedad

- I_X : ideal de $k[x_0, \ldots, x_n]$ que consiste de las formas que se anulan en X
- $k(X)$: cuerpo de funciones racionales de la variedad X
- $\mathrm{Aut}(X)$: grupo de automorfismos regulares de X
- $\mathrm{Div}(X)$: grupo abeliano de divisores en X
- $\mathrm{div}(f)$: divisor principal de una función $f \in k(X)$
- $\mathrm{PDiv}(X)$: subgrupo de divisores principales de $\mathrm{Div}(X)$
- $D \sim D' \Leftrightarrow D - D' \in \mathrm{PDiv}(X)$ (equivalencia lineal de divisores)
- $\mathrm{Cl}(X) := \mathrm{Div}(X)/\mathrm{PDiv}(X)$ (grupo de clases de divisores)
- $L(D) := \{f \in k(X)^\times : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$
- $|D| \leftrightarrow \mathbb{P}L(D)$: sistema lineal completo del divisor $D \in \mathrm{Div}(X)$
- $\mathrm{Pic}(X)$: grupo de fibrados en línea en X módulo isomorfismo
- $\mathcal{O}_X(D)$: fibrado en líneas asociado al divisor $D \in \mathrm{Div}(X)$
- $H^0(X, \mathcal{O}_X(D))$: k-espacio vectorial de secciones del fibrado en líneas $\mathcal{O}_X(D)$
- $\mathrm{Sym}^n(X) := (X \times \cdots \times X)/S_n$ (producto simétrico)

Es un hecho bien conocido que la dimensión de una variedad X coincide con el grado de trascendencia de su cuerpo de funciones sobre k, es decir, $\dim X = \mathrm{Tr}_k(k(X))$. Antes de pasar a la siguiente sección veremos algunos ejemplos de *variedades no singulares* y *variedades singulares* [10, p. 31].

Ejemplo 1.1.3.

- Sea $f(x,y,z) = x^3y + y^3z + z^3x$. Se verifica que $Z(f)$ es una variedad no singular (en toda característica) 1-dimensional llamada *curva de Klein*.
- Una variedad $Z(f) \subset \mathbb{P}^n$ definida por un solo polinomio homogéneo f es llamada *hipersuperficie*. El grado del polinomio f es el *grado* de la hipersuperficie.

- Sea m un entero positivo tal que $(m,p)=1$ y sea $f_m(x,y,z)=x^m+y^m+z^m$. Entonces se verifica que $F(m):=Z(f_m)$ es una variedad no singular 1-dimensional llamada *curva de Fermat* de grado m.

- Supongamos que $p\neq 2,3$ y que el polinomio $f(x)=x^3+ax+b\in k[x]$ no tiene raíces múltiples. Sea $X=\{[x:y:z]\in\mathbb{P}^2 : y^2z=x^3+axz^2+bz^3\}$, entonces $X\subset\mathbb{P}^2$ es una variedad no singular 1-dimensional llamada *curva elíptica*.

- Supongamos que $p=0$. Sea m un entero positivo y sea $f_m(x,y,z)=y(x^2+y^2)^m+x^{m+1}z^m+y^{m+1}z^m+yz^{2m}$. Entonces para cada m la variedad $Z(f_m)$ es una curva singular.

1.2. Subespacios lineales y Grassmannianos

Aquí serán de especial importancia las variedades lineales o *subespacios lineales* del espacio proyectivo, ya que en este trabajo caracterizaremos familias de subespacios lineales que cumplen ciertas propiedades, véase resumen del principio. Por esta razón, dedicaremos esta segunda sección a definir estos objetos. Aquí asumiremos que el cuerpo de base k es algebraicamente cerrado.

Los *subespacios lineales* de $\mathbb{P}^n$ son exactamente las subvariedades de $\mathbb{P}^n$ que son los ceros un conjunto finito de polinomios homogéneos, todos de grado uno. Otra manera de ver un subespacio lineal es considerando el espacio vectorial original k^{n+1}. Tomemos un subespacio vectorial (no nulo) $L\subset k^{n+1}$. Entonces el conjunto de los subespacios de dimensión 1 de L, denotado $\mathbb{P}L$, forman un subespacio lineal de $\mathbb{P}^n$, y cada subespacio lineal de $\mathbb{P}^n$ se obtiene de esta manera, para un único subespacio vectorial de k^{n+1}. La *dimensión* de un subespacio lineal $W=\mathbb{P}L$ de $\mathbb{P}^n$ se define como $\dim W:=\dim L-1$.

Ejemplo 1.2.1. Sean $x_0,\ldots,x_n$ las coordenadas homogéneas del espacio proyectivo $\mathbb{P}^n$ y sea $p(x_0,\ldots,x_n)=a_0x_0+\cdots+a_nx_n$ un polinomio homogéneo de grado 1. El conjunto $H=\{p=0\}$ es un subespacio lineal de codimensión 1, es decir, de dimensión $n-1$ en $\mathbb{P}^n$. Este subespacio lineal H de $\mathbb{P}^n$ es llamado un *hiperplano*.

El espacio proyectivo, por definición, parametriza los subespacios de dimensión 1 del espacio afín. Los *Grassmannianos* parametrizan subespacios de mayor dimensión.

Definición 1.2.2. Denotamos por $\mathrm{G}(l,m)$ al conjunto de todos los subespacios vectoriales de dimensión l de k^m y lo llamamos el *Grassmanniano*.

Se puede mostrar que el Grassmanniano $\mathrm{G}(l,m)$ es una variedad proyectiva de dimensión $l(m-l)$ [17, p. 42]. Notar que, por definición, $\mathrm{G}(1,n+1)=\mathbb{P}^n$.

Como a cada subespacio vectorial de dimensión $l+1$ de k^{m+1} se le asocia un único subespacio lineal de dimensión l de $\mathbb{P}^m$, usaremos la notación $\mathbb{G}(l,m):=\mathrm{G}(l+1,m+1)$ para considerar a los subespacios lineales de $\mathbb{P}^m$. Con esta notación, se tiene $\dim\mathbb{G}(l,m)=(l+1)(m-l)$.

Ejemplo 1.2.3. Por definición un hiperplano $H \subset \mathbb{P}^n$ es un elemento de $\mathbb{G}(n-1,n)$. Consideremos dos hiperplanos distintos $H_1, H_2 \in \mathbb{G}(n-1,n)$, entonces la intersección $H_1 \cap H_2$ es un subespacio lineal de codimensión 2 en $\mathbb{P}^n$, es decir, $H_1 \cap H_2 \in \mathbb{G}(n-2,n)$.

Sea $S \subset \mathbb{P}^n$ un subconjunto cualquiera y sea $p : k^{n+1} \setminus \{0\} \to \mathbb{P}^n$ la proyección natural. Definimos el *subespacio lineal generado por* S, denotado por $\langle S \rangle$, como el subespacio lineal $\mathbb{P}\langle p^{-1}(S)\rangle$.

El siguiente lema será útil para definir la noción de proyección lineal que veremos en la Sección 1.3.3.

Lema 1.2.4. *Si W y V son dos subespacios lineales de $\mathbb{P}^n$, entonces*

$$\dim\langle W \cup V\rangle = \dim W + \dim V - \dim(W \cap V).$$

Demostración. Se deduce fácilmente de la correspondiente formula para subespacios vectoriales de un espacio vectorial. $\square$

1.3. Morfismos entre variedades

Esta tercera sección esta dividida en tres subsecciones, en la primera definiremos los *morfismos regulares* y *morfismos racionales* entre variedades, para luego ver algunas de sus propiedades. En la segunda subsección definiremos las nociones de *grado* y *ramificación* de un morfismo; y en la tercera veremos *proyecciones y automorfismos lineales.* Debemos mencionar que en este trabajo apareceran frecuentemente las *inmersiones* al espacio proyectivo y las *proyecciones lineales* los cuales son casos particulares de morfismos entre variedades

1.3.1. Morfismos racionales y regulares

Sea $X \subset \mathbb{P}^n$ una variedad y sea $A = k[x_0, \dots, x_n]$.

Tomemos $m+1$ funciones racionales $f_0, \dots, f_m \in k(X)$, es decir, $f_i = F_i/G_i$ donde $F_i, G_i \in A$ son polinomios homogeneos del mismo grado y $G_i \notin I_X$. Supongamos que algún f_i no es identicamente cero en X y que los F_i son todos del mismo grado. Sea $f = (f_0, \dots, f_m) \in k(X)^{m+1}$ y consideremos el subconjunto de X

$$U_f := \left(\bigcup_{i=1}^{m} Z(F_i)^c\right) \cap \left(\bigcap_{i=1}^{m} Z(G_i)^c\right)$$

El conjunto U resulta ser un abierto en X y por tanto denso. Así, se puede definir un *morfismo racional* $\phi : X \dashrightarrow \mathbb{P}^m$ por $\phi(x) = [f_0(x) : \cdots : f_m(x)]$ para $x \in U_f$. Otra manera de denotar este morfismo es por $\phi = [f_0 : \cdots : f_m]$ y se debe notar que esta expresión no es única.

Se puede definir una noción de igualdad de morfismos de la siguiente manera [17, p. 51]:

Dos morfismos $[f_0 : \cdots : f_m]$ y $[g_0 : \cdots : g_m]$ son iguales si $f_i g_j = f_j g_i$ en X para todo i, j. Se puede verificar que esta condición es equivalente a que exista una función racional

$h \in k(X)$ tal que $g_i = hf_i$ para todo i. Por tanto, con esta noción de igualdad de morfismos se tiene lo siguiente:

Proposición 1.3.1. *Existe una correspondencia biyectiva entre el conjunto de morfismos racionales $X \dashrightarrow \mathbb{P}^m$ y el espacio proyectivo $\mathbb{P}^m_{k(X)}$ (el cual es el conjunto de subespacios de dimensión 1 del espacio vectorial $k(X)^{m+1}$ definido sobre el cuerpo $k(X)$).*

Si $f, g \in k(X)^{m+1}$ son distintos, entonces puede suceder que $U_f \neq U_g$ (incluso cuando ellos definen el mismo morfismo racional). La unión U_ϕ de todos los U_g, para $g \in [f] \in \mathbb{P}^m_{k(X)}$, se llama *dominio de definición* de $\phi = [f_0 : \cdots : f_m]$; el conjunto $\phi(U_\phi)$ es la *imagen* de X en $\mathbb{P}^m$, y anotaremos simplemente $\phi(X)$. Los puntos $x \in U_\phi$ se llaman *puntos regulares* de ϕ; si $U_\phi = X$ diremos que ϕ es un *morfismo regular*, y denotaremos $\phi : X \to \mathbb{P}^m$. Entonces también se puede definir un morfismo racional como uno que es regular en algún subconjunto abierto $U \subset X$.

Ejemplo 1.3.2. Los morfismos regulares $[\frac{z-y}{x} : \frac{z+y}{x}]$ y $[\frac{x}{z+y} : \frac{x}{z-y}]$ de $\{x^2 + y^2 = z^2\} \subset \mathbb{P}^2$ a $\mathbb{P}^1$ son iguales.

Sea $\phi : X \dashrightarrow \mathbb{P}^m$ un morfismo racional. Si $Y \subset \mathbb{P}^m$ es una variedad cuasi-proyectiva, decimos que ϕ *envía* X a Y si existe un abierto $U \subset X$ tal que $\phi(X) \subset Y$ y denotaremos $\phi : X \dashrightarrow Y$. Si $\phi : X \to Y$ es un morfismo regular que tiene un morfismo regular inverso, entonces diremos que ϕ es un *isomorfismo*. En este caso diremos que X e Y son *isomorfos*, y denotaremos $X \simeq Y$.

Ejemplo 1.3.3. Las variedades afines $X = \{y = x^k\}$ y $\mathbb{A}^1$ son isomorfas. Un isomorfismo es $\phi : \mathbb{A}^1 \to X$, $t \mapsto (t, t^k)$ y su inversa es $\psi : X \to \mathbb{A}^1$, $(x, y) \mapsto x$.

Ahora daremos una defininción que será importante en nuestro trabajo.

Definición 1.3.4. Si $\phi : X \to Y$ es un morfismo regular tal que $X \simeq \phi(X)$, entonces diremos que ϕ es una *inmersión* y denotaremos $\phi : X \hookrightarrow Y$.

La definción anterior será importante para introducir la noción de *inmersión de Galois* (Definición 2.1.1) que veremos en el siguiente capítulo.

Ejemplo 1.3.5. El morfismo $\phi : \mathbb{P}^1 \hookrightarrow \mathbb{P}^3$, $[x : y] \mapsto [x^4 : xy^3 : x^3y : y^4]$ es una inmersión.

Ahora daremos otra definición.

Definición 1.3.6. Sea $\phi : X \dashrightarrow Y$ un morfismo racional. Diremos que ϕ es *dominante* si la imagen de ϕ es densa en Y, es decir, si $\overline{\phi(X)} = Y$.

Sea $\phi : X \dashrightarrow Y$ un morfismo racional. Si ϕ es dominante, entonces ϕ define una incrustación de cuerpos $\phi^* : k(Y) \hookrightarrow k(X)$; $r \mapsto r \circ \phi$ (véase [17, p. 51]). Si ϕ tiene un morfismo racional inverso entonces diremos que ϕ es *birracional* o *equivalencia birracional*, y diremos que X e Y son *birracionales*. En este caso la incrustación $\phi^* : k(Y) \hookrightarrow k(X)$ resulta ser un isomorfismo de cuerpos.

La siguiente proposición clarifica la relación entre las nociones de isomorfismo y equivalencia birracional.

Proposición 1.3.7. *Dos variedades X e Y son biracionales si y sólo si ellas contienen subconjuntos abiertos $U \subset X$ y $V \subset Y$ que son isomorfos.*

Demostración. Véase [17, Proposición 1.1, p. 51] $\square$

Ejemplo 1.3.8. La hipérbola $X = \{xy = 1\}$ no es isomorfa a $\mathbb{A}^1$, pero sí son birracionales. La proyección $X \to \mathbb{A}^1$, $(x, y) \mapsto x$ es una equivalencia birracional y es un isomorfismo cuando se restringe su codominio a $\mathbb{A}^1 \setminus \{0\}$ cuya inversa regular es $t \mapsto (t, 1/t)$.

Ejemplo 1.3.9. Las variedades afines $X = \{y^2 = x^2 + x^3\}$ y $\mathbb{A}^1$ no son isomorfas, pero si son birracionales. Una equivalencia birracional es $\phi : \mathbb{A}^1 \to X$, $t \mapsto (t^2 - 1, t(t^2 - 1))$ y la restricción $\phi : \mathbb{A}^1 \setminus \{\pm 1\} \to X \setminus \{(0, 0)\}$ es un isomorfismo cuya inversa regular es $\psi : X \setminus \{(0, 0)\} \to \mathbb{A}^1 \setminus \{\pm 1\}$, $(x, y) \mapsto y/x$.

El siguiente es un ejercicio que aparece en [17, Ejercicio 5, p. 53].

Ejemplo 1.3.10. Cada morfismo racional $\mathbb{P}^1 \to \mathbb{P}^n$ es regular.

Finalizamos esta subsección enunciando un resultado que será útil para la demostración de la Proposición 3.5.2 (parte final de nuestro trabajo), el cual es llamado "Teorema de Dimensión de las Fibras".

Teorema 1.3.11. *Sea $\phi : X \to Y$ un morfismo regular entre variedades. Supongamos que ϕ es sobreyectiva: $\phi(X) = Y$, y que $\dim X = n$, $\dim Y = m$. Entonces $m \leq n$, y*

1. *Para cada $y \in Y$ y para cada componente F de la fibra $\phi^{-1}(y)$ se tiene $\dim F \geq n - m$.*
2. *Existe un subconjunto abierto no vacío $U \subset Y$ tal que dim $(\phi^{-1}(y)) = n - m$ para $y \in U$.*

Demostración. Véase [17, Teorema 1.25, p.75] $\square$

1.3.2. Grado de un morfismo y ramificación

Llamaremos *cubrimiento* a un morfismo sobreyectivo con fibras finitas. Por el teorema 1.3.11 se tiene que si $\phi : X \to Y$ es un cubrimiento, entonces $\dim X = \dim Y$.

Definición 1.3.12. Sean X e Y variedades de la misma dimensión y $\phi : X \to Y$ un morfismo regular dominante. El grado de la extensión de cuerpos $\phi^* (k(Y)) \subset k(X)$, la cual es finita bajo estas hipótesis, es llamado el *grado* de ϕ

$$\deg \phi = [k(X) : \phi^* (k(Y))]$$

Ilustraremos la definición anterior a través de un sencillo ejemplo.

Ejemplo 1.3.13. El cubrimiento $\phi : \mathbb{A}^1 \to \mathbb{A}^1$, $t \mapsto t^n$ induce la extensión de cuerpos $k(t^n) \subset k(t)$ la cual es de grado n y por tanto $\deg \phi = n$.

Para entender adecuadamente el concepto de *ramificación* de un cubrimiento necesitaremos introducir el concepto de *variedad normal*. Para introducir este concepto el lector debe recordar la noción de *anillo integralmente cerrado* de álgebra.

Definición 1.3.14. Una variedad afín X es *normal* si $k[X]$ es integralmente cerrado. Una variedad cualquiera X es *normal* si cada punto tiene una vecindad afín normal.

El siguiente resultado nos dará intuición geométrica sobre las variedades normales.

Teorema 1.3.15. *El conjunto de puntos singulares de una variedad normal tiene codimensión* ≥ 2.

El siguiente resultado clarifica la relación entre el grado de un morfismo y la cardinalidad de sus fibras en el caso que el codominio sea una variedad normal. Como para toda variedad existe su *normalización* [17, p. 128], esta hipótesis siempre es posible.

Teorema 1.3.16. *Si* $\phi : X \to Y$ *es un cubrimiento e* Y *es normal, entonces para cada* $y \in Y$ *la cardinalidad del conjunto* $\phi^{-1}(y)$ *es* $\leq \deg \phi$.

Demostración. Véase [17, Teorema 2.28, p. 141] □

En lo que sigue de esta subsección asumiremos que Y es una variedad normal.

Definición 1.3.17. Sea $\phi : X \to Y$ un cubrimiento. Diremos que ϕ es *no ramificada* sobre $y \in Y$ si la cardinalidad de $\phi^{-1}(y)$ es igual a $\deg \phi$. En caso contrario, diremos que ϕ es *ramificada* en y, o que y es un *punto rama* de ϕ.

Teorema 1.3.18. *El conjunto de puntos en los cuales un cubrimiento* $\phi : X \to Y$ *es no ramificado es abierto (por tanto denso), y es no vacío si* $\phi^*(k(Y)) \subset k(X)$ *es una extensión de cuerpos separable.*

Demostración. Véase [17, Teorema 2.29, p. 142] □

Notar que el morfismo regular ϕ del Ejemplo 1.3.13 anterior induce una extensión de cuerpos separable (de hecho es Galois). En este caso el único punto rama de ϕ es el $0 \in \mathbb{A}^1$ y por tanto el conjunto donde ϕ es no ramificado es $\mathbb{A}^1 \setminus \{0\}$ el cual es claramente es denso.

Sea X una variedad y sea G un subgrupo finito de $\mathrm{Aut}(X)$ tal que la característica de k no divide el orden de G, y sea $Y = X/G$ la *variedad cociente* [17, Ejemplo 1.21, p. 31]. Entonces la proyección natural $\phi : X \to Y$ resulta ser un cubrimiento. En este caso las fibras de ϕ son orbitas del grupo G. Además, se verifica que la extensión de cuerpos $\phi^*(k(Y)) \subset k(X)$ es Galois y su grupo de Galois es isomorfo a G. Se debe notar que $\deg \phi = |G|$.

Definición 1.3.19. Un cubrimiento $\phi : X \to Y$ es llamado *cubrimiento de Galois*, si existe un subgrupo finito G de $\mathrm{Aut}(X)$ tal que $Y \simeq X/G$ y las fibras de ϕ son orbitas del grupo G. El grupo G es llamado *grupo de Galois* del cubrimiento ϕ.

Notar que el cubrimiento ϕ del Ejemplo 1.3.13 anterior es un cubrimiento de Galois, cuyo grupo de Galois es $G = \langle t \mapsto \zeta_n t \rangle$ donde ζ_n es una raíz primitiva n-ésima de la unidad. En este caso la fibra $\phi^{-1}(0) = \{0\}$ tiene cardinalidad 1, ya que $0 \in \mathbb{A}^1$ es fijado por los elementos de G. En general para todo cubrimiento de Galois sus puntos ramas son imagenes de elementos que tienen estabilizador no trivial por la acción del grupo de Galois.

Terminaremos esta subsección introduciendo un concepto que esta muy relacionado con la definición anterior.

Definición 1.3.20. Sea $\phi : X \to Y$ un morfismo dominante finito y supongamos que la extensión $\phi^* (k(Y)) \subset k(X)$ es separable. Sea L la clausura de Galois de esta extensión y sea $G = \mathrm{Gal}\,(L/\phi^* (k(Y)))$. Este grupo G es llamado *grupo de monodromía* de ϕ.

1.3.3. Proyecciones y automorfismos lineales

Un concepto que aparecerá frecuentemente en este trabajo es el de proyección lineal desde un subespacio lineal del espacio proyectivo, por lo que ahora repasaremos este concepto.

Sea $L \subset k^{n+1}$ un subespacio vectorial de dimensión $n-d$ y sea $L_0 \subset k^{n+1}$ algún subespacio vectorial complementario de L (y por tanto $\dim L_0 = d+1$). Consideremos los correspondientes subespacios lineales $W = \mathbb{P}L \in \mathbb{G}(n-d-1, n)$ y $W_0 = \mathbb{P}L_0 \in \mathbb{G}(d, n)$. Notar que W y W_0 son disjuntos, ya que $L \cap L_0 = \{0\}$. Además, usando la fórmula del Lema 1.2.4 se puede verificar fácilmente que $\langle W \cup W_0 \rangle = \mathbb{P}^n$. Dos subespacios lineales W y W_0 que satisfacen las dos condiciones anteriores son llamados subespacios lineales *complementarios*. Como existe una correspondencia 1-1 entre subespacios lineales de $\mathbb{P}^n$ y subespacios vectoriales de k^{n+1}, para cada subespacio lineal W siempre se puede encontrar otro subespacio lineal W_0 de manera que W y W_0 sean complementarios.

Sean $W \in \mathbb{G}(n-d-1, n)$ y $W_0 \in \mathbb{G}(d, n)$ subespacios lineales complementarios. Supongamos que $p \in \mathbb{P}^n$ es un punto tal que $p \notin W$. Entonces $W_1 = \langle W \cup \{p\} \rangle$ es un subespacio lineal de $\mathbb{P}^n$ que tiene dimensión $1 + \dim W$. Usando la formula del Lema 1.2.4, vemos que

$$\begin{aligned} \dim(W_1 \cap W_0) &= \dim W_1 + \dim W_0 - \dim\langle W \cup W_0 \rangle \\ &= (n-d) + d - n = 0, \end{aligned}$$

por tanto $W_1 \cap W_0$ es un punto único en W_0.

Definición 1.3.21. La *proyección lineal* desde W a W_0 es el morfismo regular

$$\pi_W : \mathbb{P}^n \setminus W \to W_0$$

definido por $\pi_W(p) \in \langle W \cup \{p\} \rangle \cap W_0$. El subespacio lineal W es llamado el *centro* de la proyección.

Como la codimensión de W en $\mathbb{P}^n$ es positiva, la mayoría de los puntos de $\mathbb{P}^n$ no están en W. De hecho, $\mathbb{P}^n \setminus W$ es un abierto de $\mathbb{P}^n$ en la topología de Zariski y por tanto es denso. Entonces $\pi_W : \mathbb{P}^n \dashrightarrow W_0$ resulta ser un morfismo racional. Esto se puede escribir explícitamente de la siguiente manera: supongamos que $W = \{L_0 = \cdots = L_d = 0\}$, donde L_i son formas lineales. Entonces para un W_0 adecuado, $\pi_W(x) = [L_0(x) : \cdots : L_d(x) : 0 \cdots : 0]$, donde $x = [x_0 : \cdots : x_n]$.

Ejemplo 1.3.22. Sean $W = \{x_0 = x_n = 0\} \in \mathbb{G}(n-2, n)$ y $W_0 = \{x_1 = \cdots = x_{n-1} = 0\} \in \mathbb{G}(1, n)$. Notar que W y W_0 son subespacios lineales complementarios. La proyección lineal $\pi_W : \mathbb{P}^n \dashrightarrow W_0$ con centro W es dada por $\pi_W[x_0 : \cdots : x_n] = [x_0 : 0 : \cdots : 0 : x_n]$. En este caso se puede anotar simplemente $\pi_W[x_0 : \cdots : x_n] = [x_0 : x_n]$.

Se debe notar que si $X \subset \mathbb{P}^n$ es una variedad disjunta de W, entonces la restricción $\pi := \pi_W|_X$ define un morfismo regular $\pi : X \to W_0 \simeq \mathbb{P}^d$. Por otro lado, si $X \cap W \neq \varnothing$ pero X no está contenida en W, entonces $\pi : X \dashrightarrow \mathbb{P}^d$ es un morfismo racional. Debemos observar que para esta tesis será relevante el caso cuando X no está contenida en un hiperplano y $\dim(X) = d$. Es un hecho que en este caso el morfismo $\pi : X \dashrightarrow \mathbb{P}^d$ inducido por la proyección π_W es un morfismo finito y si $X \cap W = \varnothing$, es de grado D^d el cual es el *número de auto-intersección* de D (véase [17, p. 234]). En particular, si $d = 1$, se tiene que $\deg(\pi) = \deg(D)$.

Para varios conceptos y resultados que aparecerán en este trabajo será irrelevante el sistema de coordenadas homogéneas particular que se escoga, es decir, serán módulo cambio de coordenadas lineales. Ahora repasaremos cómo se obtienen estos cambios de coordenadas. Lo que veremos ahora es básicamente lo mismo que aparece en [12, p. 97] generalizado a un cuerpo arbitrario k.

Sea $T : k^{n+1} \to k^{n+1}$ un isomorfismo k-lineal. Entonces T manda subespacios en subespacios, preservando la dimensión; en particular envía cada subespacio 1-dimensional en otro. Por tanto T induce un morfismo regular $T : \mathbb{P}^n \to \mathbb{P}^n$; este morfismo regular es llamado un *automorfismo lineal* de $\mathbb{P}^n$.

En términos de coordenadas homogeneas, pensemos en k^{n+1} como vectores columnas de la manera usual, de modo que aplicar el morfismo T es igual a la multiplicación por una matriz cuadrada invertible $A_T = (a_{ij})$ de tamaño $n+1$:

$$T \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = A_T \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=0}^n a_{0j} x_j \\ \vdots \\ \sum_{j=0}^n a_{nj} x_j \end{pmatrix}.$$

Por tanto, podemos usar las mismas formulas para transformar las coordenadas homogeneas de puntos en $\mathbb{P}^n$ bajo T:

$$T[x_0 : \cdots : x_n] = \left[\sum_{j=0}^n a_{0j} x_j : \cdots : \sum_{j=0}^n a_{nj} x_j \right].$$

Se llama *cambio de coordenadas* a esta aplicación del automorfismo lineal T en $\mathbb{P}^n$.

Denotaremos por $\mathrm{Aut}(\mathbb{P}^n)$ al conjunto de todos los automorfismos lineales de $\mathbb{P}^n$. Se puede notar que $\mathrm{Aut}(\mathbb{P}^n) \simeq \mathrm{PGL}(n+1, k)$ es un *grupo algebraico* [17, p. 184] de dimensión $(n+1)^2 - 1$.

1.4. Divisores y morfismos racionales

Esta cuarta sección se divide en dos subsecciones, en la primera estudiaremos una notable correspondencia entre *sistemas lineales de divisores* y morfismos al espacio proyectivo. La idea es aplicar este estudio al caso particular de la línea proyectiva $\mathbb{P}^1$. Para esto será necesirio obtener una caracterización del grupo de clases de divisores en $\mathbb{P}^1$, lo cual se hará en la segunda subsección.

1.4.1. Sistemas lineales y construcción de morfismos

Sea X una variedad no singular y sean $D_1, \ldots, D_n \in \mathrm{Div}(X)$. Supongamos que

$$D_i = \sum k_{ij} C_j$$

con los C_j *divisores primos*, es decir, irreducibles y de multiplicidad 1. Se define el mayor común divisor de los divisores $D_1, \ldots, D_n$ como el divisor

$$\mathrm{mcd}\{D_1, \ldots, D_n\} := \sum l_j C_j \ , \quad \text{donde } l_j := \min_{1 \leq i \leq n} k_{ij}.$$

Escribiendo $D'_i = D_i - \mathrm{mcd}\{D_1, \ldots, D_n\}$, es claro que $D'_i \geq 0$ y que los D'_i no tienen componente común.

Sea $\phi : X \dashrightarrow \mathbb{P}^m$ un morfismo racional, entonces $\phi = [f_0 : \cdots : f_m]$, para ciertos $f_i \in k(X)$. Ahora consideremos los *divisores principales* [17, p. 149]

$$\mathrm{div}(f_i) = \sum_{j=1}^{n} k_{ij} C_j \in \mathrm{Div}(X).$$

Sea

$$D = -\mathrm{mcd}\{\mathrm{div}(f_0), \ldots, \mathrm{div}(f_m)\}.$$

Entonces $\mathrm{div}(f_i) + D \geq 0$ y por tanto $f_i \in L(D)$ para todo i.

Sin perdida de generalidad podemos suponer que ϕ tiene *imagen no degenerada*, es decir, que $\phi(X)$ no está contenido en un hiperplano, ahora explicaremos por qué. Notar que ϕ tiene imagen no degenerada si y sólo si las funciones f_i son linealmente independientes. Entonces si ϕ tiene imagen degenerada, basta eliminar algunos f_i para obtener un conjunto linealmente independiente de f_i que definen esencialmente el mismo morfismo.

Ahora veremos que se puede asociar un único *sistema lineal de divisores* al morfismo ϕ. Lo que veremos ahora es básicamente lo mismo que aparece en una parte de [17, p. 157-158].

Manteniendo las notaciones anteriores, notar que se le puede asociar al morfismo ϕ el único k-subespacio vectorial $M_\phi \subset L(D)$ generado por las funciones f_i. Así se puede ver que la elección de las funciones f_i corresponde a una elección de una base particular de M_ϕ. Por tanto, módulo cambio de coordenadas, ϕ corresponde al subespacio vectorial M_ϕ. Manteniendo estas notaciones, introducimos la siguiente definición

Definición 1.4.1. El conjunto de divisores efectivos $\{\text{div}(g) + D : g \in M_\phi\}$, es llamado un *sistema lineal* de divisores, y si $M_\phi = L(D)$ se llama un *sistema lineal completo*, que denotaremos $|D|$. Si los divisores del sistema lineal $\{\text{div}(g) + D : g \in M_\phi\}$ no tienen componente común diremos que este es *libre de componentes base*.

Se puede notar fácilmente lo siguiente

Proposición 1.4.2. *Se tiene una biyección natural*

$$|D| \leftrightarrow \mathbb{P}L(D), \text{ dada por: } \text{div}(f) + D \leftrightarrow [f] = \{\lambda f : \lambda \in k^\times\}.$$

Demostración. La sobreyectividad es clara. Para ver la inyectividad supongamos que $\text{div}(f)+D = \text{div}(g) + D$. Entonces $\text{div}(g/f) = 0$ y por tanto $g/f = \lambda \in k$, es decir, $g = \lambda f$. □

Notar que se tiene una simple interpretación geométrica de los divisores $\text{div}(f) + D$ para $f \in M_\phi$: ellos son pullbacks de los divisores de hiperplano de $\mathbb{P}^m$ bajo ϕ.

De manera inversa, se pueden construir todos los morfismos racionales de una variedad no singular X a diferentes espacios proyectivos. Para esto, se necesita tomar un divisor arbitrario D, y un subespacio de dimensión finita $M \subset L(D)$. Luego tomando una base $f_0, \dots, f_m$ de M se obtiene el morfismo racional $\phi = [f_0 : \cdots : f_m]$ y $-\text{mcd}\{\text{div}(f_0), \dots, \text{div}(f_m)\} \leq D$.

Sea $\phi = [f_0 : \cdots : f_m]$ un morfismo racional. Como multiplicar todos los f_i por un factor común $g \in k(X)$ no cambia al morfismo ϕ, y reemplaza al divisor

$$D = -\text{mcd}\{\text{div}(f_0), \dots, \text{div}(f_m)\}$$

por el divisor linealmente equivalente $D - \text{div}(g)$, vemos que la clase del divisor D es un invariante del morfismo racional ϕ. Por tanto tenemos el siguiente método para construir todos los morfismos racionales $\phi : X \dashrightarrow \mathbb{P}^m$ con imagen no degenerada: tomamos una clase de divisores en X y tomamos cualquier divisor D en esta clase, luego tomamos un subespacio vectorial de dimensión finita $M \subset L(D)$ tal que su sistema lineal asociado es libre de componentes base. Si $f_0, \dots, f_m$ es una base de M entonces se obtiene el morfismo racional $\phi = [f_0 : \cdots : f_m]$. Por supuesto, puede suceder que $L(D) = 0$, o que todos los divisores $\text{div}(f) + D$ para $f \in L(D)$ tengan componentes en común, y entonces no se obtiene ningún morfismo racional de esta clase de divisores.

Se puede observar una interesante característica de la imagen que obtuvimos. Entre todos los morfismos racionales que corresponden a una clase de divisores C, hay uno que es maximal: el que se obtiene tomando M como todo el espacio $M = L(D)$ (el cual es de dimensión finita, véase [10, Teorema 5.19, p. 122]) con $D \in C$, es decir, el que corresponde al sistema lineal completo $|D|$. Todos los demás morfismos que corresponden a esta clase se obtienen componiendo este morfismo $\phi_{|D|} : X \dashrightarrow \mathbb{P}^N$ con los varios morfismos de proyección $\mathbb{P}^N \dashrightarrow \mathbb{P}^m$. De hecho, si $\phi = [f_0 : \cdots : f_N]$, y, digamos, $\psi = [f_0 : \cdots : f_m]$ con $m < N$ entonces $\psi = \pi\phi$, donde $\pi[x_0 : \cdots : x_N] = [x_0 : \cdots : x_m]$ es la proyección, visto como un morfismo racional. Ahora introduciremos una definición

Definición 1.4.3. Sea X una variedad no singular y sea $D \in \mathrm{Div}(X)$. Diremos que D es un divisor *muy amplio* si el sistema lineal completo $|D|$ es libre de componentes base y el morfismo racional $\phi_{|D|}$ inducido es una inmersión al espacio proyectivo.

Por lo visto antes, para cada clase de divisores $C \in \mathrm{Cl}(X)$ tal que existe $D \in C$ muy amplio, existe (módulo cambio de coordenadas) una única inmersión al espacio proyectivo $\phi_{|D|} : X \hookrightarrow \mathbb{P}^{\dim(L(D))-1}$ inducida por el sistema lineal completo $|D|$. Terminaremos esta subsección enunciando dos resultados que permiten ver la situación estudiada recién en términos de secciones de fibrados en línea.

Proposición 1.4.4. *Existe un isomorfismo de grupos abelianos* $\mathrm{Cl}(X) \simeq \mathrm{Pic}(X)$.

Demostración. Para cualquier divisor $D \in \mathrm{Div}(X)$, se puede asociar el fibrado en líneas $\mathcal{O}_X(D)$ de la siguiente manera. Supongamos que D es descrito por la familia (U_α, h_α), entonces el fibrado en líneas $\mathcal{O}_X(D)$ es definido por las funciones de transición $g_{\alpha\beta} = h_\alpha/h_\beta$. De esta manera se define un homomorfismo de grupos $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ cuyo núcleo es exactamente el subgrupo de divisores principales. Para ver la sobreyectividad tomemos un fibrado en líneas L en X con una sección racional $s = (s_\alpha)$ que no es identicamente cero. Entonces las $g_{\alpha\beta} = s_\alpha/s_\beta$ son funciones racionales que definen un divisor $D = \mathrm{div}(s)$, tal que $L \simeq \mathcal{O}_X(D)$. □

Proposición 1.4.5. *Sea* $D \in \mathrm{Div}(X)$*, entonces existe un isomorfismo natural de* k*-espacios vectoriales* $L(D) \simeq H^0(X, \mathcal{O}(D))$.

Demostración. Supongamos que $D \in \mathrm{Div}(X)$ es descrito por la familia (U_α, h_α) y sea $f \in L(D)$, es decir, $f \in k(X)$ es una función tal que $\mathrm{div}(f) + D \geq 0$. La función fh_α es regular en U_α y estas funciones definen una sección de $\mathcal{O}_X(D)$. Conversamente, para cada sección de $\mathcal{O}_X(D)$ descrita por una familia (s_α) de funciones regulares, se puede asociar la función racional f definida por s_α/h_α en U_α. □

1.4.2. Divisores en la línea proyectiva

En esta subsección determinaremos el grupo de clases de divisores $\mathrm{Cl}(\mathbb{P}^1)$ y encontraremos k-bases explicitas para los k-espacios vectoriales $L(D)$ donde $D \in \mathrm{Div}(\mathbb{P}^1)$. Este análisis será útil para estudiar inmersiones $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ lo cual se hará en la siguiente sección.

El siguiente resultado será útil para caracterizar al grupo de clases de divisores $\mathrm{Cl}(\mathbb{P}^1)$.

Proposición 1.4.6. *Si* $D_1, D_2 \in \mathrm{Div}(\mathbb{P}^1)$*, entonces* $D_1 \sim D_2$ *si y sólo si* $\deg(D_1) = \deg(D_2)$.

Demostración. La demostración de [12, p. 140] se generaliza a un cuerpo arbitrario k. □

Por la proposición anterior se obtiene el isomorfismo de grupos $\mathrm{Cl}(\mathbb{P}^1) \simeq \mathbb{Z}$; $D \leftrightarrow \deg(D)$.

El siguiente resultado caracteriza a los divisores muy amplios en $\mathbb{P}^1$.

Proposición 1.4.7. *Si* $D \in \mathrm{Div}(\mathbb{P}^1)$*, entonces* D *es muy amplio si y sólo si* $\deg(D) > 0$.

Demostración. El resultado de [12, p. 168] se generaliza a un cuerpo arbitrario k. □

Ahora veremos un resultado que caracteriza a los k-espacios vectoriales $L(D)$ para divisores $D \in \mathrm{Div}(\mathbb{P}^1)$.

Proposición 1.4.8. *Si $D \in \mathrm{Div}(\mathbb{P}^1)$, entonces*

$$\dim L(D) = \begin{cases} 0 & si \ \deg(D) < 0 \\ 1 + \deg(D) & si \ \deg(D) \geq 0 \end{cases}$$

Más aún, si $D = \sum_{i=1}^{r} m_i[p_i : q_i]$, entonces una base para el espacio $L(D)$ es dada por los elementos

$$f_D(x,y)x^n, f_D(x,y)x^{n-1}y, \ldots, f_D(x,y)xy^{n-1}, f_D(x,y)y^n$$

donde

$$f_D(x,y) = \prod_{i=1}^{r}(q_i x - p_i y)^{-m_i} \in k(x,y)$$

Demostración. La demostración de [12, p. 149-150] se generaliza a un cuerpo arbitrario k. □

Ahora veremos como los resultados anteriores se pueden usar para obtener explícitamente el isomorfismo de la Proposición 1.4.5 para el caso de $X = \mathbb{P}^1$. Recordemos que las secciones del fibrado en líneas $\mathcal{O}_{\mathbb{P}^1}(n)$ forman un k-espacio vectorial que corresponde al espacio de formas de grado n en las coordenadas homogéneas x e y de $\mathbb{P}^1$, es decir, $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n)) = \langle x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n\rangle$. Entonces si $D \in \mathrm{Div}(\mathbb{P}^1)$ es de grado positivo (por tanto muy amplio), por el resultado anterior se tiene que

$$\begin{aligned} L(D) &= \langle f_D x^n, f_D x^{n-1}y, \ldots, f_D xy^{n-1}, f_D y^n\rangle \\ &= f_D\langle x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n\rangle \\ &= f_D H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n)). \end{aligned}$$

Por tanto, se tiene el isomorfismo de k-espacios vectoriales $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n)) \simeq L(D)$; $s \leftrightarrow f_D s$.

1.5. Inmersión de Veronese y la curva racional normal

En esta quinta sección, usaremos los resultados vistos en la sección anterior para caracterizar a todas las inmersiones $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ que corresponden a sistemas lineales completos de divisores en $\mathbb{P}^1$ y por tanto con imagen no-degenerada. Veremos que para cada sistema lineal completo existe una única inmersión módulo cambio de coordenadas, la cual es llamada *inmersión de Veronese*.

Por lo visto en la Subsección 1.4.1 se sabe que para cada clase de divisores $C \in \mathrm{Cl}(\mathbb{P}^1)$ tal que contiene un divisor muy amplio D, existe una única inmersión $\phi_{|D|} : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n$, módulo cambio de coordenadas, donde $n = \dim(L(D)) - 1$. Por la Proposición 1.4.7 se tiene que el grupo de clases $\mathrm{Cl}(\mathbb{P}^1)$ es isomorfo al grupo aditivo $\mathbb{Z}$, y que los divisores muy amplios en $\mathbb{P}^1$ son los de grado positivo. Esto da una correspondencia biyectiva entre el conjunto $\{[D] \in \mathrm{Cl}(\mathbb{P}^1) : D \text{ es muy amplio}\}$ y el conjunto de los enteros positivos $\mathbb{Z}_{>0}$. Por tanto, para cada entero positivo $n \in \mathbb{Z}_{>0}$ existe una única inmersión $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ que viene de un único sistema lineal completo $|D|$, donde $D \in \mathrm{Div}(\mathbb{P}^1)$ y $n = \deg(D)$. Ahora queremos construir explícitamente esta única inmersión. Para esto usaremos los resultados obtenidos en las subsecciones 1.4.1 y 1.4.2 de la sección anterior.

Sea D un divisor en $\mathbb{P}^1$ de grado $n > 0$. Por la Proposición 1.4.7 sabemos que D es un divisor muy amplio. Para construir la inmersión de $\mathbb{P}^1$ al espacio proyectivo asociada al sistema lineal completo $|D|$ necesitamos encontrar una base del k-espacio vectorial $L(D)$. Si $D = \sum_{i=1}^{r} m_i[p_i : q_i]$, entonces tomando la base para el espacio $L(D)$ dada por la Proposición 1.4.8, la inmersión es

$$\phi_D : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n \ ;$$

$$[x : y] \mapsto [f_D(x,y)x^n : f_D(x,y)x^{n-1}y : \cdots : f_D(x,y)xy^{n-1} : f_D(x,y)y^n]$$

Se puede notar que $-\mathrm{mcd}\{f_D(x,y)x^n y^{n-i}\} = D$. Por la noción de igualdad de morfismos introducida en la Subsección 1.3.1, se sabe que un morfismo no cambia al multiplicar sus funciones componentes por un factor común y por tanto

$$\phi_D[x : y] = [x^n : x^{n-1}y : \cdots : xy^{n-1} : y^n]$$

para todo divisor D en $\mathbb{P}^1$ de grado $n > 0$.

Definición 1.5.1. La *inmersión de Veronese* de grado n es

$$\nu_n : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n; \ [x : y] \mapsto [x^n : x^{n-1}y : \cdots : xy^{n-1} : y^n].$$

Su imagen $\nu_n(\mathbb{P}^1)$ es llamada *curva racional normal* de grado n.

Por el análisis anterior, hemos obtenido lo siguiente

Proposición 1.5.2. *Para cada entero positivo n existe (módulo cambio de coordenadas) una única inmersión $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ que viene de un único sistema lineal completo $|D|$, donde $D \in \mathrm{Div}(\mathbb{P}^1)$ y $n = \deg(D)$, la cual es ν_n.*

Se debe notar que existen inmersiones $\phi : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ que no corresponden a un sistema lineal completo, como por ejemplo, $\phi[x : y] = [x^4 : x^3y : xy^3 : y^4] \in \mathbb{P}^3$.

Capítulo 2

Inmersiones de Galois de variedades proyectivas

Lo que se hará en este trabajo es caracterizar a los subespacios lineales de $\mathbb{P}^n$ tales que la proyección lineal inducida, cuando se restringe a la curva racional normal, da un morfismo de Galois. Estos subespacios lineales serán llamados *subespacios de Galois* para la inmersión de Veronese. El concepto de subespacio de Galois proviene de la noción introducida en [21] por el matemático japonés Hisao Yoshihara, llamada *inmersión de Galois*. Este será el punto de vista que adoptaremos para este trabajo. Por esta razón, en este segundo capítulo introduciremos las principales nociones y resultados sobre las inmersiones de Galois. Las principales referencias para este capítulo son [21] y [23].

2.1. Definiciones básicas y problemas

Sea X una variedad proyectiva no singular de dimensión d con un divisor muy amplio D. Sea $\phi = \phi_D : X \hookrightarrow \mathbb{P}^n$ la inmersión asociada al sistema lineal completo $|D|$, donde $n+1 = \dim H^0(X, \mathcal{O}(D))$. Sean $W \in \mathbb{G}(n-d-1, n)$ y $W_0 \in \mathbb{G}(d, n)$ subespacios lineales complementarios. Consideremos la proyección $\pi_W : \mathbb{P}^n \dashrightarrow W_0 \simeq \mathbb{P}^d$ con centro W. La composición $\pi = \pi_W \circ \phi : X \dashrightarrow \mathbb{P}^d$ resulta ser un morfismo racional dominante y finito.

El morfismo π induce una extensión finita de cuerpos $\pi^* : k(W_0) \hookrightarrow k(X)$. Es fácil ver que la estructura de esta extensión no depende de W_0 sino solo de W. Por tanto denotamos $K_W = k(W_0)$ y $K = k(X)$. Si la extensión K/K_W es separable, tomamos la clausura de Galois L_W de esta extensión y denotamos $G_W := \mathrm{Gal}(L_W/K_W)$ al cual lo llamaremos el *grupo de Galois* de W. Notar que G_W es isomorfo al grupo de monodromía de π.

Debemos observar que en el caso $W \cap \phi(X) = \varnothing$ se verifica que $\pi : X \to \mathbb{P}^d$ es un morfismo sobreyectivo y $\deg \pi = [K : K_W] = D^d$ el cual es el *número de auto-intersección* de D, véase [17, p. 234]. En particular, si $d = 1$, se tiene que $\deg \pi = [K : K_W] = \deg(D)$.

Definición 2.1.1. Diremos que ϕ es una *inmersión de Galois* si existe $W \in \mathbb{G}(n-d-1, n)$ tal que K/K_W es Galois. En este caso diremos que W es un *subespacio de Galois* para ϕ.

Definición 2.1.2. Diremos que X *tiene una inmersión de Galois* si existe un divisor muy amplio $D \in \mathrm{Div}(X)$ tal que la inmersión asociada a $|D|$ es de Galois. En este caso diremos que el par (X, D) *define una inmersión de Galois*.

Si W es un subespacio de Galois para ϕ y T un automorfismo lineal de $\mathbb{P}^n$, entonces $T(W)$ es un subespacio de Galois para la inmersión $T \circ \phi$. Por tanto la existencia de un subespacio de Galois no depende de la elección de la base que da la inmersión.

En el caso que W no es un subespacio de Galois, existe una variedad X_W tal que $k(X_W) = L_W$ que llamaremos *variedad de clausura de Galois*. Esta resulta ser única módulo equivalencia birracional.

Considerando el marco de referencia que hemos introducido, se han obtenido numerosos resultados, de los cuales veremos algunos en las siguientes secciones de este capítulo. No obstante, hay muchos problemas abiertos (véase [23]). En particular, el problema principal que abordaremos en este trabajo ha sido planteado en [23] (ver Sección 3.1). Ahora enunciaremos algunos problemas que surgen naturalmente:

- ¿X tiene inmersión de Galois? Si tiene ¿cuál es la estructura de X?
- Estudiar el conjunto $\{[D] \in \mathrm{Cl}(X) : (X, D)$ define una inmersión de Galois$\}$
- Para una inmersión fija ϕ estudiar los conjuntos

  $$\{G_W : W \text{ es subespacio de Galois para } \phi\} \text{ (módulo isomorfismo)}$$

  $$\{G_W : W \text{ no es subespacio de Galois para } \phi\} \text{ (módulo isomorfismo)}$$

- Para un grupo fijo G y una inmersión fija ϕ estudiar el conjunto

  $$\{W \in \mathbb{G}(n-d-1, n) : G_W \simeq G\}$$

  ¿Es finito? ¿Es una subvariedad del Grassmanniano? ¿Cuál es su dimensión?

- Encontrar todos los subespacios de Galois para una inmersión fija ϕ

  $$\{W \in \mathbb{G}(n-d-1, n) : W \text{ es un subespacio de Galois para } \phi\}$$

  ¿Cómo es la configuración geométrica de este conjunto?

- Estudiar el conjunto de *centros extraños* $\{W \in \mathbb{G}(n-d-1, n) : K/K_W$ es inseparable$\}$
- Estudiar las variedades de clausura de Galois

  $$\{X_W : W \text{ no es un subespacio de Galois}\} \text{ (salvo equivalencia biracional/isomorfismo)}$$

- ¿Es X caracterizada por alguno de estos conjuntos?

2.2. Representaciones del grupo de Galois

En esta sección suponemos que $\phi(X) \cap W = \varnothing$. Por definición, si W es un subespacio de Galois, entonces cada elemento $\sigma \in G_W$ es un automorfismo de K sobre K_W. Por tanto induce un morfismo birracional de X sobre W_0. Esto implica que G_W se puede ver como un subgrupo de $\mathrm{Bir}(X/W_0)$, el grupo de aplicaciones birracionales de X sobre W_0. Más aún podemos decir lo siguiente:

Proposición 2.2.1. *Los elementos de G_W resultan ser regulares en X, por tanto se tiene una representación $G_W \hookrightarrow \mathrm{Aut}(X)$*

Demostración. Ver [21, Representation 1, p. 3 y p. 10]. □

Corolario 2.2.2. *Si $\mathrm{Aut}(X)$ es trivial, entonces X no tiene inmersiones de Galois.*

Por la misma razón, si el orden de $\mathrm{Aut}(X)$ es suficientemente pequeño, entonces X no puede tener una inmersión de Galois. Por otro lado, hay ejemplos tales que existen infinitas inmersiones de Galois distintas. Por ejemplo, veremos en la Sección 2.5 que la inmersión de Veronese ν_n es una inmersión de Galois para cada $n \in \mathbb{N}$. Otro que veremos más adelante es el Ejemplo 2.4.12.

Supongamos que (X, D) define una inmersión de Galois. Sea $H \subset \mathbb{P}^n$ un hiperplano que contiene a W y sea D' el divisor de intersección de $\phi(X)$ y H. Como $D' \sim D$ y $\sigma^*(D') = D'$ para cada $\sigma \in G_W$, vemos que σ induce un automorfismo de $H^0(X, \mathcal{O}(D)) \simeq k^{n+1}$. Por tanto

Proposición 2.2.3. *Se tiene una representación $G_W \hookrightarrow \mathrm{GL}(n+1, k)$.*

Como vimos en Subsección 1.3.3, cada automorfismo de k^{n+1} induce un automorfismo lineal de $\mathbb{P}^n$. Entonces, por resultado anterior, se tiene una representación $G_W \hookrightarrow \mathrm{PGL}(n, k)$. Por tanto G_W es un subgrupo de $\mathrm{Lin}(X) = \{\sigma \in \mathrm{Aut}(X) : \exists \tilde{\sigma} \in \mathrm{Aut}(\mathbb{P}^n) \text{ tal que } \tilde{\sigma}|_X = \sigma\}$.

2.3. Algunos resultados

Durante esta sección también asumiremos que $\phi(X) \cap W = \varnothing$. Como G_W es un subgrupo finito de $\mathrm{Aut}(X)$, podemos considerar la variedad cociente X/G_W. Sea p_W la proyección natural $p_W : X \to X/G_W$.

Proposición 2.3.1. *Si (X, D) define una inmersión de Galois con un subespacio de Galois W, entonces existe un isomorfismo $h : X/G_W \to W_0$ que satisface $h \circ p_W = \pi$. Por tanto la proyección π es un morfismo finito y el lugar con estabilizador no trivial por la acción de G_W consiste solo de divisores.*

Demostración. Ver [21, Theorem 2.1, p. 3 y p. 10]. □

Por tanto $\pi : X \to W_0$ resulta ser un morfismo de Galois con grupo G_W. Las fibras de π son órbitas de G_W. Ahora presentamos un criterio para determinar cuándo el par (X, D) define una inmersión de Galois.

Teorema 2.3.2. *El par (X, D) define una inmersión de Galois ϕ (con subespacio de Galois disjunto de $\phi(X)$) si y sólo si se satisfacen las siguientes condiciones:*

1. *Existe un subgrupo G de $\operatorname{Aut}(X)$ tal que $|G| = D^d$ y preserva la clase lineal de D.*

2. *Existe un subespacio vectorial G-invariante $\mathcal{L}$ de $H^0(X, \mathcal{O}(D))$ de dimensión $d+1$ tal que, para cada $\sigma \in G$, la restricción $\sigma^*|_{\mathcal{L}}$ es un múltiplo de la identidad.*

3. *El sistema lineal $\mathcal{L}$ no tiene puntos base.*

Demostración. Ver [21, Theorem 2.2, p. 3 y p. 10]. □

Esencialmente, el Teorema 2.3.2 muestra que se quiere encontrar un subgrupo finito $G \leq \operatorname{Aut}(X)$ tal que $X/G \simeq \mathbb{P}^d$ y $\pi^*\mathcal{O}_{\mathbb{P}^d}(1)$ es muy amplio, donde $\pi : X \to \mathbb{P}^d$ es la proyección, ya que si esto se cumple, entonces existirá un subespacio lineal $\mathcal{L}$ que satisfaga las condiciones 2 y 3 del Teorema 2.3.2. Para construir el correspondiente subespacio de Galois, se toma una base $\{f_0, \ldots, f_n\}$ de $H^0(X, \mathcal{O}(D))$, donde $f_0, \ldots, f_d$ son dadas por la Condición 2. del Teorema 2.3.2. Entonces $\phi = [f_0 : \cdots : f_n]$ define una inmersión $X \hookrightarrow \mathbb{P}^n$ y si $x_0, \ldots, x_n$ son las coordenadas homogeneas correspondientes en $\mathbb{P}^n$, entonces $W = \{x_0 = \cdots = x_d = 0\}$ es un subespacio de Galois para ϕ tal que $G = G_W$. La Condición 3. del Teorema 2.3.2 implica que $W \cap \phi(X) = \varnothing$.

Si W es un subespacio de Galois para ϕ es fácil ver que cada $\sigma \in G_W$ induce un automorfismo de W. Se debe notar que pueden existir varios subespacios de Galois y grupos de Galois para una inmersión fija. En general se tiene lo siguiente.

Proposición 2.3.3. *Supongamos que (X, D) define una inmersión de Galois ϕ. Sean W, W' subespacios de Galois para ϕ disjuntos de $\phi(X)$ tales que $W \neq W'$. Entonces $G_W \neq G_{W'}$ en* $\operatorname{Aut}(X)$.

Demostración. Ver [21, Proposition 2.5, p. 5 y p. 11]. □

Es un hecho bien conocido que si X es una variedad de tipo general, entonces $\operatorname{Aut}(X)$ es un grupo finito, por tanto se tiene lo siguiente

Corolario 2.3.4. *Si X es de tipo general, entonces hay finitos subespacios de Galois disjuntos de $\phi(X)$ para una inmersión fija ϕ.*

Puede suceder que exista una cantidad infinita de subespacios de Galois para una inmersión fija si la dimensión de Kodaira de X es pequeña. En un resultado principal de esta tesis veremos que esto sucede para $\mathbb{P}^1$, el cual tiene dimensión de Kodaira $-\infty$. Debemos observar que el resultado de la Proposición 2.3.3 no se cumple si los subespacios de Galois no son disjuntos de $\phi(X)$, lo cual será ilustrado para el caso de $\mathbb{P}^1$ en la sección final de este trabajo.

2.4. Aplicaciones

En esta sección ilustraremos mediante ejemplos concretos algunas aplicaciones de las nociones introducidas en las secciones anteriores y mencionaremos resultados interesantes que se han publicado en artículos. Pero debemos observar que lo que se verá aquí no es esencial para el problema principal de esta tesis y por tanto si el lector desea puede pasar directamente a la siguiente sección.

2.4.1. Puntos de Galois

En 1996 Yoshihara introdujo la noción de punto de Galois, la cual después fue generalizada al concepto de inmersión de Galois y subespacio de Galois en [21]. En esta subsección mostraremos algunos resultados obtenidos por Miura y Yoshihara para el caso de puntos de Galois (véase [19] y [13]). Aquí suponemos que $k = \mathbb{C}$.

Consideremos el caso de una curva plana no singular $X \subset \mathbb{P}^2$. Es decir, $d = 1$, $n = 2$ y $W = \{p\} \in \mathbb{G}(0, 2) = \mathbb{P}^2$. Antes de enunciar los resultados, veremos algunas definiciones.

Definición 2.4.1. Si $p \in X$ entonces llamamos a p *punto interior* y si $p \notin X$ entonces llamamos a p *punto exterior*. Denotamos por $\delta(X)$ al número de puntos interiores de Galois y por $\delta'(X)$ al número de puntos exteriores de Galois.

Lo que se quiere hacer es determinar la distribución de puntos de Galois para X y ver cómo esto caracteriza a la curva X. Aquí la inmersión de X en el espacio proyectivo es simplemente el morfismo identidad $X \hookrightarrow X \subset \mathbb{P}^2$. Debemos notar que en este caso el grado del morfismo $\pi = \pi_p \circ \mathrm{Id}_X$ es igual a m si p es un punto exterior y $m - \mathrm{mult}_p X$ si $p \in X$, donde m es el grado de X. Debemos notar que $m \neq 1$, ya que estamos asumiendo que X no está contenido en un subespacio lineal (una línea) de $\mathbb{P}^2$.

Sea m el grado de X. Si $m = 2$ el problema es trivial, ya que cada punto exterior (resp. interior) induce una extensión de cuerpos de funciones de grado 2 (resp. 1) y por tanto Galois con grupo de Galois isomorfo a $\mathbb{Z}/2\mathbb{Z}$ (resp. trivial). Si $m = 3$, todos los puntos interiores son de Galois, ya que inducen extensiones de cuerpos de funciones de grado ≤ 2 y por tanto Galois. Si $m = 3$, para los puntos exteriores se tiene el siguiente resultado que aparece en [13]. Denotaremos $g(p)$ para el género de la curva de clausura de Galois X_p.

Proposición 2.4.2. *Para cada curva plana cúbica no singular X y cada punto $p \in \mathbb{P}^2 \setminus X$, se tiene que $g(p) \in \{1, 2, 3, 4\}$. Si p es un punto general de $\mathbb{P}^2$, entonces $G_p \simeq S_3$, y $g(p) = 4$. Por el contrario, $g(p) = 1$ si y sólo si p es un punto de Galois.*

Demostración. Véase [13, Note 2.2, p. 285 y p. 290] □

Necesitaremos algunas definiciones antes de ver los resultados para el caso general $m \geq 4$. Denotaremos por $i(X_1, X_2; p)$ al *número de intersección* de X_1 y X_2 en p.

Definición 2.4.3. Una línea $l \subset \mathbb{P}^2$ es llamada *multitangente* a X si se satisface alguna de las siguientes condiciones

1. Existe $p \in X \cap l$ tal que $i(X, l; p) \geq 3$. En este caso p se llama *punto de inflexión*.
2. Existen al menos dos puntos $p_i \in X \cap l$ tales que $i(X, l; p_i) \geq 2$ para $i = 1, 2$.

Denotamos por $X^{\#}$ a la unión de todas las multitangentes a X.

Los siguientes resultados aparecen en el artículo [19]:

Teorema 2.4.4. *Sea X una curva plana no singular de grado $m \geq 4$.*

- *Si $p \in \mathbb{P}^2 \setminus (X \cup X^{\#})$, entonces $G_p \simeq S_m$ y $g(p) = (m-1)!(m^2 - m - 4)/4 + 1$.*
- *Si $p \in X \setminus X^{\#}$, entonces $G_p \simeq S_{m-1}$ y $g(p) = (m-1)!(m+2)(m-3)/4 + 1$.*

Ahora, supongamos que p es un punto de Galois. Entonces

- *Si p es un punto exterior se tiene que $G_p \simeq \mathbb{Z}/m\mathbb{Z}$.*
- *Por el contrario, si $p \in X$ se tiene que $G_p \simeq \mathbb{Z}/(m-1)\mathbb{Z}$.*

Por tanto, los puntos de Galois están en $X^{\#}$. Más aún, se tiene que $\delta'(X) \in \{0, 1, 3\}$ y $\delta(X) \in \{0, 1, 4\}$, por tanto hay finitos puntos de Galois.

Es notable el hecho que se pueda caracterizar a X en términos de su ecuación cuando existen puntos de Galois. Los siguientes resultados son también de [19].

Teorema 2.4.5. *Sea X una curva plana no singular de grado $m \geq 4$. Entonces*

- *$\delta(X) > 0$ si y sólo si X es proyectivamente equivalente a $\{x^{m-1}z + h(y, z) = 0\}$, donde h es una forma de grado m con distintos factores. Más aún, $\delta(X) = 4$ si y sólo si $m = 4$ y $h(y, z) = y^4 + z^4$.*
- *$\delta'(X) > 0$ si y sólo si X es proyectivamente equivalente a $\{x^m + h(y, z) = 0\}$, donde h es una forma de grado m con distintos factores. Más aún, $\delta'(X) = 3$ si y sólo si $h(y, z) = y^m + z^m$ (curva de Fermat $F(m)$).*

Por tanto se tiene una caracterización de la curva de Fermat en términos de puntos de Galois: una curva plana no singular X de grado $m \geq 4$ es proyectivamente equivalente a la curva de Fermat $F(m)$ si y sólo si X tiene un número máximo de puntos de Galois exteriores.

Ahora mostraremos un ejemplo de [13, p. 285 y p. 292] donde se tiene una caracterización completa de la distribución de puntos Galois y no Galois, y los grupos que aparecen.

Ejemplo 2.4.6. Sea $X = F(m)$ la curva de Fermat de grado $m \geq 4$. Entonces se tiene que $\delta(X) = 0$ y $\delta'(X) = 3$. Los puntos de Galois exteriores son exactamente $[1:0:0], [0:1:0]$ y $[0:0:1]$. Ahora supongamos que $m = 4$. Para los puntos exteriores en $X^{\#}$ se tiene que existen 12 puntos tales que $G_p \simeq D_4$, el grupo dihedral de orden 8; no existe punto tal que $G_p \simeq A_4$, el grupo alternante de orden 12; se puede verificar que no aparecen mas grupos de Galois (véase [13, p. 292]), es decir, se tiene que $G_p \simeq S_4$ excepto en 15 puntos. Para los puntos interiores en $X^{\#}$ se tiene que hay 12 puntos de inflexión; si p es un punto de inflexión entonces $G_p \simeq S_3$ y $g(p) = 9$; si p no es un punto de inflexión, entonces $G_p \simeq S_3$ y $g(p) = 10$.

El siguiente es un ejemplo donde aparece un punto exterior (no Galois) con grupo A_4.

Ejemplo 2.4.7. Si X es la curva definida por $x^3y + y^4 + x^3z + y^3z + 4yz^3 + z^4 = 0$ y $p = [0 : 0 : 1]$, entonces se tiene que $G_p \simeq A_4$. Véase [13, Example 4.9, p. 293].

El siguiente ejemplo muestra que existen curvas sin puntos de Galois.

Ejemplo 2.4.8. La curva de Klein $x^3y + yz^3 + xz^3 = 0$ tiene solo un punto de inflexión y se puede demostrar que $\delta(X) = \delta'(X) = 0$ (ver [13, Example 4.8, p. 293]). Observar que esto es interesante dado que la curva de Klein tiene muchos automorfismos, de hecho alcanza la cota de Hurwitz.

En el caso de curvas singulares pueden aparecer grupos de Galois no cíclicos.

Ejemplo 2.4.9. Para cada m la curva plana definida por $y(x^2+y^2)^m + x^{m+1}z^m + y^{m+1}z^m + yz^{2m} = 0$ es singular. El punto $p = [0 : 0 : 1]$ es un punto interior de Galois tal que $G_p \simeq D_m$. Véase [19, Remark 1, p. 343].

Antes de terminar esta subsección, mencionaremos que uno de los resultados más importantes que se han obtenido usando puntos de Galois aparece en el artículo [7]. En este artículo se ha logrado caracterizar a varias hipersuperficies normales a través de cotas superiores para la cantidad de puntos de Galois.

2.4.2. Curvas elípticas

Para esta subsección asumiremos que el lector ya está familiarizado con las nociones principales de geometría compleja. Aquí suponemos que $k = \mathbb{C}$.

Un *curva elíptica* es un grupo cociente $X = \mathbb{C}/\Gamma$, donde Γ es un *reticulado* en $\mathbb{C}$. Se demuestra que E tiene estructura de *variedad analítica compleja* de dimensión 1. Ahora veremos cómo construir una *inmersión holomorfa* de una curva elíptica en el espacio proyectivo.

Sea $\Gamma = \langle 1, \tau \rangle \subset \mathbb{C}$, aquí $\tau \in \mathbb{C}$ es tal que $\mathrm{Im}\tau > 0$. Entonces $E = \mathbb{C}/\Gamma$ una curva elíptica. Se define la función $\wp$ de Weiestrass (que dependerá de Γ) como la función

$$\wp(s) := \frac{1}{s^2} + \sum_{w \in \Gamma \setminus \{0\}} \left(\frac{1}{(s-w)^2} - \frac{1}{w^2} \right).$$

Se tiene que $\wp$ es una función meromorfa par en $\mathbb{C}$ con polos dobles en cada punto de Γ. Esta función y su primera derivada están relacionadas por la ecuación

$$\wp'(s)^2 = 4\wp(s)^3 + a\wp(s) + b,$$

donde $a, b \in \mathbb{C}$ son constantes que dependen de Γ. Las funciones $\wp$ de Weierstrass y su derivada $\wp'$ son ambas Γ-periódicas, y por tanto ellas son funciones meromorfas en la curva elíptica $E = \mathbb{C}/\Gamma$. Usando estas funciones se obtiene una inmersión de E al espacio proyectivo

$$\phi : E \hookrightarrow \mathbb{P}^2 \ ; \quad s + \Gamma \mapsto [\wp(s) : \wp'(s) : 1].$$

Debemos notar que $D := -\mathrm{mcd}\{\wp, \wp', 1\} = 3[\Gamma]$ y $L(D) = \langle \wp, \wp', 1\rangle$. Así $\phi_D = \phi$.

Si x, y, z son las coordenadas homogéneas en $\mathbb{P}^2$, entonces se tiene que E es una curva plana no singular definida por la ecuación homogénea $y^2z = 4x^3 + axz^2 + bz^3$. Por tanto, cada curva elíptica es una variedad proyectiva no singular. Poniendo $z = 1$ se obtiene $y^2 = 4x^3 + ax + b$, la cual es llamada *forma normal de Weierstrass* de E.

¿Es ϕ es una inmersión de Galois? Para responder esta pregunta consideremos el punto $p = [0 : 1 : 0] = \{x = z = 0\} \in \mathbb{G}(0, 2) = \mathbb{P}^2$. Notar que $p \in E$ es un punto interior. En este caso la proyección $\pi = \pi_p\mathrm{Id} : E \dashrightarrow \mathbb{P}^1$ es $\pi[x : y : z] = [x : z]$. Si consideramos el abierto estandar $U_2 = \{z \neq 0\}$, podemos poner $z = 1$. Entonces la proyección $\pi[x : y : 1] = [x : 1]$ induce la extensión algebraica de cuerpos $\mathbb{C}(x, y)/\mathbb{C}(x)$ de grado 2, la cual es Galois con grupo de Galois $G_p = \langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, donde

$$\sigma : \mathbb{C}(x, y) \to \mathbb{C}(x, y)\ ;\quad x \mapsto x,\ y \mapsto -y.$$

Por tanto p es un punto de Galois para ϕ. Esto ya lo sabíamos desde la Subsección 2.4.1, porque E es de grado 3 y p es un punto interior, pero aquí se ve explícitamente. Entonces efectivamente ϕ es una inmersión de Galois.

Otra pregunta que se puede hacer es: ¿Tiene E un punto exterior de Galois? Supongamos que E tiene un punto exterior de Galois p. Veremos cómo esto determina a E. Por lo visto en la Subsección 2.4.1, se tiene que el grupo de Galois G_p es de orden 3 y por tanto cíclico. Como $G_p \hookrightarrow \mathrm{Aut}(E)$, entonces E debe tener un automorfismo de orden 3 y $E/G_p \simeq \mathbb{P}^1$. Asumamos que $\tau = e^{2\pi i/3}$. En este caso $\sigma : z + \Gamma \mapsto \tau z + \Gamma$ es un automorfismo de orden 3 de E tal que $E/\langle\sigma\rangle \simeq \mathbb{P}^1$ y fija el divisor D. Entonces se tiene una acción del grupo $\langle\sigma\rangle$ en $L(D)$ por pullback

$$\sigma^* : L(D) \to L(D)\ ;\quad f \mapsto f \circ \sigma.$$

Por el Teorema 2.3.2, para encontrar el punto de Galois asociado al grupo $\langle\sigma\rangle$, se necesita encontrar un subespacio vectorial 2-dimensional $\langle\sigma\rangle$-invariante $\mathcal{L}$ de $L(D)$ tal que $\sigma^*|_{\mathcal{L}}$ es un múltiplo de la identidad. Notar que la función constante 1 es trivialmente invariante bajo σ^*. Por otro lado, un cálculo directo muestra que $\wp(\tau s) = \tau\wp(s)$, lo que implica

$$\sigma^*(\wp')(s) = \wp'(\tau s) = \wp'(s).$$

Por tanto $\wp'$ también es invariante bajo σ^*. Entonces $\mathcal{L} = \langle\wp', 1\rangle$ es el subespacio buscado. Considerando las coordenadas homogéneas x, y, z en $\mathbb{P}^2$, se tiene que el punto exterior

$$p = \{y = z = 0\} = [1 : 0 : 0]$$

es el punto de Galois asociado al grupo $\langle\sigma\rangle$. En este caso, la proyección $\pi = \pi_p\mathrm{Id} : E \to \mathbb{P}^2$ es $\pi[x : y : z] = [y : z]$. Como antes, poniendo $z = 1$, se tiene que $\pi[x : y : 1] = [y : 1]$ induce la extensión algebraica de cuerpos $\mathbb{C}(x, y)/\mathbb{C}(y)$ la cual es Galois con grupo de Galois $G_p = \langle\sigma\rangle \simeq \mathbb{Z}/3\mathbb{Z}$, donde

$$\sigma : \mathbb{C}(x, y) \to \mathbb{C}(x, y)\ ;\quad x \mapsto \tau x,\ y \to y.$$

Ahora veremos un ejemplo de una línea de Galois l con grupo de Galois $G_l \simeq \mathbb{Z}/4\mathbb{Z}$.

Ejemplo 2.4.10. Consideremos otra inmersión

$$\phi : E \hookrightarrow \mathbb{P}^3 \; ; \quad s + \Gamma \mapsto [\wp(s) : \wp(s)^2 : \wp'(s) : 1].$$

Sean x_0, x_1, x_2, x_3 las coordenadas homogéneas en $\mathbb{P}^3$. De forma similar, se puede demostrar que $l = \{x_1 = x_3 = 0\} \in \mathbb{G}(1,3)$ es una línea de Galois disjunta de $\phi(E)$, si $\tau = i$. En este caso la proyección $\pi = \pi_l \phi : E \to \mathbb{P}^1$ es $\pi(s) \mapsto [\wp(s)^2 : 1]$, la cual induce la extensión Galois de cuerpos $\mathbb{C}(x,y)/\mathbb{C}(x^2)$ cuyo grupo de Galois es $G_l = \langle \sigma \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, donde

$$\sigma : E \to E \; ; s + \Gamma \mapsto is + \Gamma$$

$$\sigma : \mathbb{C}(x,y) \to \mathbb{C}(x,y) \; ; \quad x \mapsto -x, \; y \mapsto iy.$$

Ahora veremos un ejemplo de un subespacio de Galois W con grupo de Galois $G_W \simeq \mathbb{Z}/6\mathbb{Z}$.

Ejemplo 2.4.11. Consideremos ahora la inmersión

$$\phi : E \hookrightarrow \mathbb{P}^5 \; ; \quad s + \Gamma \mapsto [\wp(s) : \wp(s)^2 : \wp(s)^3 : \wp'(s) : \wp(s)\wp'(s) : 1].$$

Si $x_0, \ldots, x_5$ son las coordenadas homogéneas en $\mathbb{P}^5$, entonces se puede demostrar que el subespacio lineal $W = \{x_2 = x_5 = 0\} \in \mathbb{G}(3,5)$ es un subespacio de Galois disjunto de $\phi(E)$, cuando $\tau = e^{2\pi i/3}$. En este caso la proyección $\pi = \pi_W \phi : E \to \mathbb{P}^1$ es $\pi(s) \mapsto [\wp(s)^3 : 1]$, la cual induce la extensión Galois de cuerpos $\mathbb{C}(x,y)/\mathbb{C}(x^3)$ cuyo grupo de Galois es $G_W = \langle \sigma \rangle \simeq \mathbb{Z}/6\mathbb{Z}$, donde

$$\sigma : E \to E \; ; s + \Gamma \mapsto -\tau s + \Gamma$$

$$\sigma : \mathbb{C}(x,y) \to \mathbb{C}(x,y) \; ; \quad x \mapsto \tau x, \; y \mapsto -y.$$

Sea $\mathrm{Aut}^0(E) = \{\sigma \in \mathrm{Aut}(E) : \sigma(0) = 0\}$. Se sabe que para cada curva elíptica E se tiene que $\mathrm{Aut}^0(E) \simeq \mathbb{Z}/n\mathbb{Z}$, para algún $n \in \{2,4,6\}$. Por tanto para cada subgrupo G de $\mathrm{Aut}^0(E)$, se tiene que $G \simeq \mathbb{Z}/n\mathbb{Z}$ para algún $n \in \{2,3,4,6\}$. En los ejemplos anteriores hemos visto que para cada uno de estos G se tiene un subespacio de Galois asociado.

El siguiente ejemplo de [21] muestra que para una variedad fija pueden existir infinitas inmersiones de Galois.

Ejemplo 2.4.12. Sea $E = \mathbb{C}/\langle 1, \tau \rangle$ una curva elíptica, aquí $\tau \in \mathbb{C}$ es tal que $\mathrm{Im}\tau > 0$. Sean A y B los automorfismos de E definidos por $A(s) = s + (1/m)$ y $B(s) = -s$ respectivamente, donde $s \in \mathbb{C}$ y $m \in \mathbb{N}$ es mayor que 2. Sea G el subgrupo de $\mathrm{Aut}(E)$ generado por A y B. Entonces se tiene que $G \simeq D_m$, el grupo dihedral de orden $2m$ y $E/G \simeq \mathbb{P}^1$. Sea $y^2 = 4x^3 + ax + b$ la forma normal de Weierstrass de E y sea $K = \mathbb{C}(x,y)$. Entonces el subcuerpo de K fijo por G es racional $\mathbb{C}(f(x))$, donde $f(x) \in \mathbb{C}(x)$. Si $D := \mathrm{div}(f)_\infty$ es el divisor de polos de f, se tiene que $\deg(D) = 2m \geq 4$ y por tanto D es muy amplio. Por tanto (E, D) define una inmersión de Galois para todo $m \in \mathbb{N}$ mayor que 2.

Terminamos esta sección comentando un resultado interesante que se ha obtenido para curvas elípticas inmersas en $\mathbb{P}^3$. En [22] Yoshihara demuestra que cada curva elíptica E inmersa en $\mathbb{P}^3$ tiene sólo 6 líneas de Galois l con grupo de Galois $G_l \simeq K_4$, el grupo de Klein de orden 4. Estas líneas forman las aristas de un tetraedro. En el caso $j(E) = 1$, por cada vértice del tetrahedro pasan dos líneas de Galois l con grupo de Galois $G_l \simeq \mathbb{Z}/4\mathbb{Z}$.

2.4.3. Variedades abelianas

Un *toro complejo* $X = \mathbb{C}^n/\Gamma$, donde Γ es un *reticulado* en $\mathbb{C}^n$, tiene estructura de *variedad analítica compleja* de dimensión n y estructura algebraica de grupo. Una *variedad abeliana* es un toro complejo que tiene una *inmersión holomorfa* en un espacio proyectivo. Por tanto, identificando con su imagen bajo la inmersión holomorfa, cada variedad abeliana es una *subvariedad analítica compleja* de un espacio proyectivo. Un teorema de Chow establece que cada subvariedad analítica compleja de un espacio proyectivo es una variedad proyectiva no singular, es decir, está definida por ceros de polinomios homogéneos. Por tanto, las variedades abelianas son variedades proyectivas. Entonces es natural preguntar cuándo estas inmersiones son de Galois. Veremos que estas inmersiones no siempre son de Galois cuando $\dim X \geq 2$. Notar que una variedad abeliana de dimensión 1 es una curva elíptica.

Sea X una variedad abeliana y sea D un divisor muy amplio en X. Primero veremos una condición necesaria para que (X, D) defina una inmersión de Galois. Aquí suponemos que $\dim X \geq 2$.

Proposición 2.4.13. *Supongamos que (X, D) define una inmersión de Galois con grupo de Galois G. Sea R_π el divisor de ramificación de la proyección $\pi : X \to \mathbb{P}^n$. Entonces cada componente de R_π es una traslación de una subvariedad abeliana de dimensión $n-1$ y $R_\pi \sim (n+1)D$. En particular, R_π es muy amplio y $R_\pi^n = (n+1)^n|G|$.*

Demostración. Ver [21, Proposition 3.1, p. 5 y p. 11]. □

Recordamos que una variedad abeliana es *simple* si sus únicas subvariedades abelianas son $\{0\}$ y ella misma. De la proposición anterior se obtiene directamente el siguiente corolario.

Corolario 2.4.14. *Variedades abelianas simples no tienen inmersión de Galois.*

Por tanto, las variedades abelianas simples son ejemplos de variedades que tienen inmersión en el espacio proyectivo, pero que no son Galois.

Recordamos que una *isogenia* entre dos variedades abelianas es una función holomorfa sobreyectiva que además es un homomorfismo de grupos con núcleo finito. Si existe una isogenia entre dos variedades abelianas X e Y, anotaremos $X \sim Y$. Terminamos esta sección mostrando el resultado principal de [2].

Teorema 2.4.15. *Sea X una variedad abeliana de dimensión n.*

- *Si X tiene una inmersión de Galois en algún espacio proyectivo, entonces existe una curva elíptica E tal que $X \sim E^n$.*
- *Si $X = E^n$, entonces X tiene infinitas inmersiones de Galois con grupos de Galois de orden arbitrariamente grande.*

Demostración. Ver [2, Theorem 1.2]. □

2.5. Inmersión de Veronese

Sea k el cuerpo de base y asumamos que la característica de k no divide a n y que k contiene una raíz primitiva n-ésima de la unidad ζ_n.

En esta subsección estudiaremos el caso $X = \mathbb{P}^1$. Primero queremos saber si acaso $\mathbb{P}^1$ tiene una inmersión de Galois. Para abordar este problema, tomemos un divisor D de grado n en $\mathbb{P}^1$. Supongamos que D es muy amplio, lo cual es equivalente, por lo visto en la Subsección 1.4.2, a que $n = \deg(D) > 0$. Por lo visto en la Sección 1.5 se sabe que la clase del divisor D le corresponde una única inmersión en $\mathbb{P}^n$, la cual es la inmersión de Veronese

$$\nu_n : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n;\ [x : y] \mapsto [x^n : x^{n-1}y : \cdots : xy^{n-1} : y^n].$$

Entonces ahora nuestra pregunta es la siguiente: ¿Es ν_n una inmersión de Galois?

Para responder la pregunta anterior sean las coordenadas homogéneas x, y en $\mathbb{P}^1$, y $x_0, x_1, \ldots, x_n$ en $\mathbb{P}^n$. Tomemos el subespacio lineal $W = \{x_0 = x_n = 0\} \in \mathbb{G}(n-2, n)$. Notar que W y $\nu_n(\mathbb{P}^1)$ con disjuntos. En este caso la proyección $\pi = \pi_W \circ \nu_n : \mathbb{P}^1 \to \mathbb{P}^1$ es $\pi[x : y] = [x^n : y^n]$. Consideremos el abierto estandar $U_1 = \{y \neq 0\} \subset \mathbb{P}^1$ y pongamos $t = x/y$. Entonces la proyección $\pi[t : 1] = [t^n : 1]$ induce la extensión de cuerpos K/K_W donde $K = k(t)$ y $K_W = k(t^n)$. La extensión de cuerpos anterior resulta ser Galois con grupo de Galois $G_W = \langle t \mapsto \zeta_n t\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Por tanto W es un subespacio de Galois para ν_n. Esto demuestra que ν_n es una inmersión de Galois. Hemos obtenido lo siguiente

Proposición 2.5.1. *La inmersión de Veronese ν_n es una inmersión de Galois para cada $n \in \mathbb{N}$. Más aún, se tiene que el conjunto*

$$\{[D] \in \mathrm{Cl}(\mathbb{P}^1) : (\mathbb{P}^1, D) \textit{ define una inmersión de Galois}\}$$

está en correspondencia biyectiva con el conjunto de números naturales $\mathbb{N}$, la cual es dada por $[D] \leftrightarrow \deg(D)$; y la inmersión asociada a la clase $[D]$ es ν_n, donde $n = \deg(D)$.

De la misma manera se puede demostrar que $W = \{x_0 = x_2 = 0\} \in \mathbb{G}(n-2, n)$ es un subespacio de Galois para ν_n con grupo de Galois $G_W \simeq \mathbb{Z}/2\mathbb{Z}$. Pero este subespacio, a diferencia del caso anterior, es no disjunto de $\nu_n(\mathbb{P}^1)$ cuando $n \geq 3$. Por ejemplo $\nu_n[0 : 1] \in W$. Por tanto también existen subespacios de Galois para ν_n que no son disjuntos de $\nu_n(\mathbb{P}^1)$.

Ahora nos podemos preguntar si acaso existe un grupo de Galois para ν_n que no sea cíclico. Para responder esta pregunta supongamos que $n = 2m \geq 4$ es par y consideremos el subespacio lineal $W = \{x_0 + x_n = x_m = 0\} \in \mathbb{G}(n-2, n)$. Entonces la proyección $\pi = \pi_W \circ \nu_n : \mathbb{P}^1 \to \mathbb{P}^1$ es $\pi[x : y] = [x^n + y^n : (xy)^m]$, y poniendo $t = x/y$ con $y \neq 0$, la proyección queda $\pi[t : 1] = [1/t^m + t^m : 1]$. El pullback π^* induce la extensión de cuerpos $k\left(1/t^m + t^m\right) \subset k(t)$, la cual es Galois y G_W es generado por $t \mapsto \zeta_m t$ y $t \mapsto 1/t$, donde $\zeta_m = \zeta_n^2$. Por tanto $G_W \simeq D_m$ el grupo dihedral de orden $2m$.

Capítulo 3

Subespacios de Galois para la curva racional normal

3.1. Introducción al problema principal

Teniendo en cuenta que ν_n es una inmersión de Galois para cada $n \in \mathbb{N}$ (ver Proposición 2.5.1), se puede proponer el siguiente problema:

Problema principal : Para cada $n \in \mathbb{N}$ fijo, encontrar todos los grupos de Galois y todos los subespacios de Galois para ν_n, disjuntos y no disjuntos de $\nu_n(\mathbb{P}^1)$.

Este problema ha sido planteado por Yoshihara en su lista de problemas abiertos [23]. De hecho, este problema ya fue abordado por el propio Yoshihara en el caso disjunto, para $n = 3$, y cuando el cuerpo de base es de característica 0 y algebraicamente cerrado (véase [20, Prop. 4.1]). En este caso particular Yoshihara obtuvo el siguiente resultado:

Teorema 3.1.1. *El conjunto de grupos de Galois*

$$\{G_W : W \text{ es un subespacio de Galois para } \nu_n \text{ tal que } W \cap \nu_3(\mathbb{P}^1) = \varnothing\}$$

módulo isomorfismo, es exactamente $\{\mathbb{Z}/3\mathbb{Z}\}$; y la familia de líneas de Galois

$$\{W \in \mathbb{G}(1,3) : G_W \simeq \mathbb{Z}/3\mathbb{Z}\}$$

es una subvariedad 2-dimensional localmente cerrada del Grassmanniano $\mathbb{G}(1,3)$.

Por tanto, lo que se hará en este trabajo puede ser visto como una generalización del resultado obtenido por Yoshihara para dimensión n arbitraria, donde además se considera el caso no disjunto y la característica del cuerpo de base es arbitraria. No siempre asumiremos que el cuerpo de base es algebraicamente cerrado.

Hasta ahora, por lo visto en la Subsección 2.5, sabemos que para cada $n \geq 3$ existen subespacios de Galois disjuntos y no disjuntos, y el conjunto de grupos de Galois debe contener a $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\}$, y si $n = 2m$ es par tambien debe estar el grupo dihedral D_m. Con esta información es natural también preguntar si acaso estos grupos corresponden a familias de subespacios de Galois o subvariedades del Grassmanniano, y cuáles son sus dimensiones.

3.2. Resultados preliminares

En esta sección veremos algunos resultados generales que serán útiles para resolver el problema principal que fue enunciado en la sección anterior. Sea $\mathrm{End}_n(\mathbb{P}^1)$ el conjunto de los endomorfismos de $\mathbb{P}^1$ de grado n. Vemos que $\mathrm{Aut}(\mathbb{P}^1)$ actúa en $\mathrm{End}_n(\mathbb{P}^1)$ vía composición por la izquierda. Usando esta notación se tiene el siguiente lema.

Lema 3.2.1. *Existe una correspondencia biyectiva entre* $\mathrm{End}_n(\mathbb{P}^1)/\mathrm{Aut}(\mathbb{P}^1)$ *y todos los subespacios lineales* $W \in \mathbb{G}(n-2,n)$ *que son disjuntos de* $\nu_n(\mathbb{P}^1)$.

Demostración. Sean x, y las coordenadas de $\mathbb{P}^1$. Entonces un endomorfismo de grado n de $\mathbb{P}^1$ es dado por $[p(x,y) : q(x,y)]$ donde p y q son polinomios homogéneos de grado n sin factores en común. Anotemos

$$p(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n$$

$$q(x,y) = b_0x^n + b_1x^{n-1}y + \cdots + b_{n-1}xy^{n-1} + b_ny^n.$$

Entonces enviamos f al subespacio lineal

$$W_f := \{a_0x_0 + \cdots + a_nx_n = b_0x_0 + \cdots + b_nx_n = 0\} \in \mathbb{G}(n-2,n).$$

Si $W_f \cap \nu_n(\mathbb{P}^1) \neq \varnothing$, entonces existe $[\alpha : \beta] \in \mathbb{P}^1$ tal que

$$a_0\alpha^n + a_1\alpha^{n-1}\beta + \cdots + a_n\beta^n = b_0\alpha^n + b_1\alpha^{n-1}\beta + \cdots + b_n\beta^n = 0.$$

Esto, sin embargo, implica que los polinomios $p(x,y)$ y $q(x,y)$ tienen un factor común, y por tanto f no es de grado n. Por tanto $W_f \cap \nu_n(\mathbb{P}^1) = \varnothing$.

Ahora tomemos $W \in \mathbb{G}(n-2,n)$ tal que $W \cap \nu_n(\mathbb{P}^1) = \varnothing$. Sean $L_0, L_1 \in k[x_0,\ldots,x_n]_1$ los dos polinomios que definen a W, y consideremos el morfismo $\pi = [L_0 : L_1] \circ \nu_n : \mathbb{P}^1 \to \mathbb{P}^1$. Primero notemos que las secciones $\nu_n^*L_0, \nu_n^*L_1$ no tienen raíces comunes, ya que esto contradiría el hecho que $W \cap \nu_n(\mathbb{P}^1) = \varnothing$. En segundo lugar, estas formas tienen grado n ya que $\nu_n(\mathbb{P}^1)$ es de grado n en $\mathbb{P}^n$. Por último, se debe notar que ecuaciones distintas que definen a W difieren por una acción de $\mathrm{GL}(2,k)$, y esto se traduce en componer el morfismo π con un automorfismo lineal de $\mathbb{P}^1$. $\square$

Llamaremos *endomorfismo de Galois* de $\mathbb{P}^1$ a un morfismo $\mathbb{P}^1 \to \mathbb{P}^1$ que es de Galois. El siguiente corolario es claro a partir de la demostración anterior:

Corolario 3.2.2. *La correspondencia anterior da una biyección entre endomorfismos de Galois de grado n de $\mathbb{P}^1$ módulo la acción de* $\mathrm{Aut}(\mathbb{P}^1)$*, y subespacios de Galois de $\mathbb{P}^n$ para ν_n disjuntos de $\nu_n(\mathbb{P}^1)$.*

Esto muestra que caracterizar subespacios de Galois de $\mathbb{P}^n$ para ν_n (disjuntos de $\nu_n(\mathbb{P}^1)$) es esencialmente lo mismo que caracterizar endomorfismos de Galois de grado n de $\mathbb{P}^1$, y por tanto lo mismo que caracterizar subcuerpos racionales $k(f(t)) \subset k(t)$ que dan extensiones de Galois de grado n.

Por el Teorema 2.3.2, para encontrar todos los grupos de Galois para ν_n, necesitamos conocer los posibles grupos finitos que actúan en la línea proyectiva $\mathbb{P}^1$. Supongamos que G es un subgrupo finito de $\mathrm{Aut}(\mathbb{P}^1)$ tal que su orden $|G| = n$ no es divisible por la característica del cuerpo base k. Por la fórmula de Riemann-Hurwtiz se tiene que $\mathbb{P}^1/G \simeq \mathbb{P}^1$. Entonces el morfismo cociente $\pi : \mathbb{P}^1 \to \mathbb{P}^1/G \simeq \mathbb{P}^1$ es un endomorfismo de Galois de grado n de $\mathbb{P}^1$. Aplicando el Corolario 3.2.2 se obtiene lo siguiente

Proposición 3.2.3. *Un grupo G tal que p no divide a $|G| = n$ es un grupo de Galois para ν_n con un subespacio de Galois disjunto de $\nu_n(\mathbb{P}^1)$ si y sólo si G es un subgrupo de* $\mathrm{Aut}(\mathbb{P}^1)$.

Supongamos que G es un grupo de orden n actuando (fielmente) en la línea proyectiva $\mathbb{P}^1$. Entonces por la Proposición 3.2.3 se sabe que G es un grupo de Galois para ν_n. Por el Teorema 2.3.2, para encontrar el subespacio de Galois (disjunto de $\nu_n(\mathbb{P}^1)$) asociado al grupo G debemos estudiar la acción de G en el k-espacio vectorial $L(D)$ por pullback, donde D es un divisor invariante por G. De hecho, basta encontrar un subespacio vectorial 2-dimensional $\mathcal{L}$ de $L(D)$ tal que cada elemento de G actúa como un múltiplo de la identidad en $\mathcal{L}$.

3.3. Subgrupos finitos de PGL$(2, k)$

Por la Proposición 3.2.3, vemos que para encontrar todos los subespacios de Galois para ν_n, es esencial conocer los posibles grupos finitos que actuán (fielmente) en la línea proyectiva $\mathbb{P}^1$. Esto es, encontrar todos los subgrupos finitos de $\mathrm{Aut}(\mathbb{P}^1)$. Pero esto es equivalente a caracterizar todos los subgrupos finitos de $\mathrm{PGL}(2, k)$, ya que se tiene un isomorfismo $\mathrm{Aut}(\mathbb{P}^1) \simeq \mathrm{PGL}(2, k)$.

Sea G un grupo actuando (fielmente) en $\mathbb{P}^1$ tal que su orden no es divisible por $\mathrm{car} k = p \geq 0$. Por un estudio detallado de la fórmula de Riemann-Hurwitz para morfismos cociente y los puntos de ramificación que pueden aparecer, se concluye que G puede ser $\mathbb{Z}/n\mathbb{Z}$ para cualquier $n \in \mathbb{N}$, el grupo dihedral D_m de orden $2m$ para cualquier $m \in \mathbb{N}$, A_4, S_4 o A_5. Sobre el cuerpo de números complejos $k = \mathbb{C}$, estos tres últimos grupos aparecen como grupos de automorfismos holomorfos de la esfera de Riemann que dejan invariante a los vértices de los sólidos platónicos inscritos en ella (A_4 deja invariante al tetrahedro, S_4 al cubo y al octahedro, y A_5 al dodecahedro y al icosahedro). En un cuerpo arbitrario, sin embargo, no siempre aparecen todos estos grupos. De hecho, se tiene el siguiente resultado [4, Prop 1.1] que muestra las condiciones necesarias para que aparezca cada grupo.

Proposición 3.3.1.

1. *$PGL(2, k)$ contiene a $\mathbb{Z}/n\mathbb{Z}$ y el grupo dihedral D_n si y sólo si k contiene $\zeta + \zeta^{-1}$ para alguna raíz primitiva n-ésima de la unidad ζ.*

2. *$PGL(2, k)$ contiene a A_4 y a S_4 si y sólo si -1 es la suma de dos cuadrados en k.*

3. *$PGL(2, k)$ contiene a A_5 si y sólo si -1 es la suma de dos cuadrados y 5 es un cuadrado en k.*

En particular, cuando k es algebraicamente cerrado, se satisfacen todas las condiciones de la Proposición 3.3.1 y por tanto aparecen todos los grupos anteriores como subgrupos finitos de $\mathrm{PGL}(2,k)$. Debemos observar que juntando los resultados de la Proposición 3.2.3 y la Proposición 3.3.1 hemos obtenido una respuesta parcial del problema principal. Estos resultados nos muestran cuáles son todos los grupos de Galois que pueden aparecer para ν_n que corresponden a subespacios de Galois disjuntos. Para encontrar explícitamente estas familias de subespacios de Galois disjuntos o conocer sus estructuras geométricas, sería útil tener información sobre cómo se configuran dentro de $\mathrm{PGL}(2,k)$ sus subgrupos finitos. En relación a esto, en [4, Teorema 4.2] se ha obtenido un resultado que clasifica todas las clases de conjugación en $\mathrm{PGL}(2,k)$. Ahora mostraremos algunos hechos que se obtienen de este teorema que serán útiles para nuestro trabajo:

Denotaremos $\mu_l(k)$ al conjunto de raíces l-ésimas de la unidad en k. Supongamos que existe una raíz primitiva n-ésima de la unidad $\zeta_n \in k$, entonces:

1. *$PGL(2,k)$ contiene sólo una clase de conjugación de subgrupos isomorfos a $\mathbb{Z}/n\mathbb{Z}$ ($n > 2$), A_4, S_4 o A_5.*

2. *Asumamos que $n = 2m > 4$ es par y sea $\zeta_m = \zeta_n^2$. Las clases de conjugación de subgrupos D_m de $PGL(2,k)$ son parametrizadas por $k^\times/(k^\times)^2\mu_m(k)$. El subgrupo que corresponde a $\alpha \in k^\times$ es el generado por $t \mapsto \zeta_m t$ y $t \mapsto \alpha/t$ donde $\langle\zeta_m\rangle = \mu_m(k)$.*

3. *Las clases de conjugación de subgrupos de $PGL(2,k)$ isomorfos a $(\mathbb{Z}/2\mathbb{Z})^2$ son parametrizadas por $k^\times/(k^\times)^2$. El subgrupo que corresponde a $\beta \in k^\times/(k^\times)^2$ es el generado por $t \mapsto (\lambda t - \beta)/(t-\lambda)$ y $t \mapsto \beta/t$ donde $\lambda \in k$ es un elemento que satisface la ecuación de una cónica [4, p. 27].*

Ahora veremos algunos ejemplos concretos de subgrupos de orden n de $\mathrm{PGL}(2,k)$. En todos ellos asumiremos que la característica de k no divide al orden del grupo y que k contiene una raíz primitiva n-ésima de la unidad ζ_n.

Ejemplo 3.3.2. El elemento

$$C_n := \begin{pmatrix} \zeta_n & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}(2,k)$$

genera un subgrupo de $\mathrm{PGL}(2,k)$ que es cíclico $\langle C_n\rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Ejemplo 3.3.3. Supongamos que $n = 2m$ es par y sea $\alpha \in k^\times$. Los elementos

$$C_m = \begin{pmatrix} \zeta_n^2 & 0 \\ 0 & 1 \end{pmatrix}, \ I_\alpha = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}(2,k)$$

satisfacen las relaciones

$$C_m^m = I_\alpha^2 = (C_m I_\alpha)^2 = I_2,$$

donde $I_2 = \mathrm{diag}(1,1)$ es la matriz identidad. Por tanto, ellos generan un subgrupo dihedral $\langle C_m, I_\alpha\rangle \simeq D_m$ de orden $2m$ de $\mathrm{PGL}(2,k)$.

Ejemplo 3.3.4. Supongamos que $k = \mathbb{Q}(\sqrt{3}, i)$. Notar que $\zeta_{12} = (\sqrt{3}/2) + (i/2) \in k$. Los elementos

$$A = \begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix}, \ B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}(2, k)$$

satisfacen las relaciones

$$A^3 = B^2 = (AB)^3 = I_2.$$

Por tanto, ellos generan un subgrupo alternante $\langle A, B \rangle \simeq A_4$ de orden 12. Notar que $-1 = i^2 + 0^2$ y por tanto se satisface la hipótesis de la Proposición 3.3.1 parte 2.

3.4. Teorema principal para el caso disjunto

Ahora es momento de enunciar el Teorema 3.4.1 principal que caracteriza a todos los subespacios de Galois para ν_n que son disjuntos de $\nu_n(\mathbb{P}^1)$, el cual será demostrado en las Subsecciones 3.4.1 y 3.4.2. También veremos un resultado para casos excepcionales en la Proposición 3.4.2, y será demostrado en la Subsección 3.4.3.

Antes de enunciar el teorema principal para el caso disjunto, definiremos los subespacios lineales con los cuales trabajaremos. Para $a, b, c, d \in k$ definimos los polinomios homogéneos en las variables $x_0, x_1, \ldots, x_n$

$$L_{a,c} := \sum_{i=0}^{n} \binom{n}{i} (-1)^i a^i c^{n-i} x_i.$$

Si $\alpha \in k$ y $n = 2m$ es par, definimos los polinomios

$$A_{a,b,c,d} := \sum_{i+j+l=m} \binom{m}{i, j, l} (-1)^i (ad + bc)^i (ab)^j (cd)^l x_{i+2l}$$

$$B^{\alpha}_{a,b,c,d} := \sum_{i=0}^{n} \binom{n}{i} (-1)^i (\alpha^m a^{n-i} c^i + b^{n-i} d^i) x_i$$

Notar que el hiperplano definido por $L_{a,c}$ sólo depende de la clase de (a, c) en $\mathbb{P}^1$ cuando (a, c) no es cero, y por tanto lo denotaremos $H_{[a:c]}$. El subespacio lineal de codimensión 2 definido por $A_{a,b,c,d} = B^{\alpha}_{a,b,c,d} = 0$ sólo depende de la clase de $(a, b, c, d) \in \mathbb{P}^3$ y de α, y por tanto será denotado $V^{\alpha}_{[a:b:c:d]}$.

Teorema 3.4.1. *Sea k un cuerpo, sea $\nu_n : \mathbb{P}^1 \to \mathbb{P}^n$ la inmersión de Veronese de grado $n \geq 3$ sobre k, y asumamos que la característica de k no divide n y que k contiene una raíz primitiva n-ésima de la unidad ζ_n. Entonces tenemos lo siguiente:*

1. *Para cada $([a : c], [b : d]) \in (\mathbb{P}^1 \times \mathbb{P}^1) \setminus \Delta$,*

$$W_{[a:c][b:d]} := H_{[a:c]} \cap H_{[b:d]}$$

es un subespacio de Galois de $\mathbb{P}^n$ para ν_n con grupo de Galois cíclico que es conjugado al grupo generado por $[x : y] \mapsto [\zeta_n x : y]$. Esto da una subvariedad 2-dimensional localmente cerrada $\mathcal{C}_n$ de $\mathbb{G}(n-2, n)$.

2. *Si $n = 2m \geq 6$ es par, además del item anterior, para cada $\alpha \in k^\times/(k^\times)^2\mu_m(k)$ tenemos los subespacios de Galois $V^\alpha_{[a:b:c:d]}$ para $[a : b : c : d] \in \mathbb{P}^3$ y $ad - bc \neq 0$. Aquí el grupo de Galois es el grupo dihedral de orden $2m$ y es conjugado al grupo generado por $[x : y] \mapsto [\zeta_n^2 x : y]$ y $[x : y] \mapsto [\alpha y : x]$. Por tanto obtenemos familias $\mathcal{D}^\alpha_m$ que sobre $\overline{k}$ dan una subvariedad 3-dimensional localmente cerrada $\mathcal{D}_m$ de $\mathbb{G}(n-2, n)$.*

Los subespacios de Galois anteriores son todos disjuntos de la curva racional normal $\nu_n(\mathbb{P}^1)$. Más aún, si $n \notin \{2, 4, 12, 24, 60\}$, estos son los únicos subespacios de $\mathbb{P}^n$ para ν_n disjuntos de $\nu_n(\mathbb{P}^1)$

Los casos excepcionales $n \in \{2, 4, 12, 24, 60\}$ se abordan en la siguiente proposición:

Proposición 3.4.2. *Tenemos las siguientes familias de subespacios de Galois disjuntas de la curva racional normal $\nu_n(\mathbb{P}^1)$*

1. *Para $n = 2$, cada elemento de $\mathbb{P}^2 \setminus \nu_2(\mathbb{P}^1)$ da un subespacio de Galois para $\nu_2(\mathbb{P}^1)$.*

2. *Para $n = 4$, aparte de $\mathcal{C}_4$, para cada $\beta \in k^\times/(k^\times)^2$ hay una familia $\mathcal{K}^\beta \subset \mathbb{G}(2, 4)$ que corresponde a subespacios de Galois cuyo grupo de Galois es el grupo de Klein K_4 de orden cuatro. Sobre $\overline{k}$ estas dan una subvariedad 3-dimensional localmente cerrada $\mathcal{K}$ de $\mathbb{G}(2, 4)$.*

Si, más aún, -1 es la suma de dos cuadrados en k, entonces:

3. *Para $n = 12$, aparte de $\mathcal{C}_{12}$ y los espacios $\mathcal{D}^\alpha_{12}$, existe una subvariedad 3-dimensional localmente cerrada $\mathcal{A}_4 \subset \mathbb{G}(10, 12)$ que corresponde a subespacios de Galois con grupo de Galois A_4.*

4. *Para $n = 24$, aparte de $\mathcal{C}_{24}$ y los espacios $\mathcal{D}^\alpha_{24}$, existe una subvariedad 3-dimensional localmente cerrada $\mathcal{S}_4 \subset \mathbb{G}(22, 24)$ que corresponde a subespacios de Galois con grupo de Galois A_4.*

1. *Para $n = 60$, si 5 es un cuadrado en k, entonces aparte de $\mathcal{C}_{60}$ y los espacios $\mathcal{D}^\alpha_{60}$, existe una subvariedad 3-dimensional localmente cerrada $\mathcal{A}_5 \subset \mathbb{G}(58, 60)$ que corresponde a subespacios de Galois con grupo de Galois A_5.*

Los dos resultados anteriores dan la lista completa de posibles subespacios de Galois para ν_n en el caso que sean disjuntos de $\nu_n(\mathbb{P}^1)$ y nos dan información sobre su configuración geométrica en el Grassmanniano $\mathbb{G}(n-2, n)$. Para cada posible subgrupo finito de $\mathrm{Aut}(\mathbb{P}^1)$ se tiene una subvariedad localmente cerrada de $\mathbb{G}(n-2, n)$ de dimensión positiva y son todas disjuntas entre ellas. En el caso que el cuerpo de base sea algebraicamente cerrado, los resultados para el caso disjunto están resumidos en el Cuadro 3.1. Estos resultados serán

n	Familia	Dimensión	Grupo
$n \geq 2$	$\mathcal{C}_n$	2	$\mathbb{Z}/n\mathbb{Z}$
4	$\mathcal{K}$	3	K_4
$2m \geq 6$	$\mathcal{D}_m$	3	D_m
12	$\mathcal{A}_4$	3	A_4
24	$\mathcal{S}_4$	3	S_4
60	$\mathcal{A}_5$	3	A_5

Cuadro 3.1: Familias de subespacios de Galois disjuntos de $\nu_n(\mathbb{P}^1)$

demostrados en las siguientes subsecciones y así habremos solucionado el problema principal para el caso disjunto. El caso no disjunto será analizado en la Sección 3.5 donde se dará una clasificación completa de todos los subespacios de Galois para la inmersión de Veronese de grado n arbitrario en el caso que el cuerpo de base sea algebraicamente cerrado. En particular, demostraremos que para cada $n \geq 60$ hay $n + \lfloor n/2 \rfloor + 2$ familias disjuntas de subespacios de Galois en el Grassmanniano $\mathbb{G}(n-2, n)$, y la familia más grande es de dimensión n. Ver Cuadro 3.2 para la clasificación completa.

3.4.1. Grupo cíclico de orden n

En esta subsección demostraremos la primera parte del Teorema 3.4 dando una parametrización explícita de la familia de subespacios de Galois para ν_n disjuntos de $\nu_n(\mathbb{P}^1)$ con grupo cíclico de orden $n \geq 3$.

Sea $n \geq 3$ y asumamos que k contiene una raíz primitiva n-ésima de la unidad ζ_n. Consideremos el automorfismo de orden n

$$C_n : \mathbb{P}^1 \to \mathbb{P}^1 \ ; \quad [x : y] \mapsto [\zeta_n x : y],$$

que visto como un elemento de $\mathrm{PGL}(2, k)$ corresponde a la matriz

$$C_n = \begin{pmatrix} \zeta_n & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}(2, k),$$

la cual genera un subgrupo cíclico $\langle C_n \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ de $\mathrm{PGL}(2, k)$. Por [4, Teorema 4.2] se sabe que cada subgrupo cíclico de orden n es conjugado a $\langle C_n \rangle$. Entonces, tomando un elemento arbitrario

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}(2, k)$$

el elemento conjugado

$$T_n := M C_n M^{-1} = \begin{pmatrix} ad\zeta_n - bc & ab(1-\zeta_n) \\ cd(\zeta_n - 1) & ad - bc\zeta_n \end{pmatrix}$$

genera un subgrupo cíclico de orden n de $\mathrm{PGL}(2,k)$ arbitrario. Por tanto, el correspondiente automorfismo de orden n

$$T_n : \mathbb{P}^1 \to \mathbb{P}^1;\ [x:y] \mapsto [(ad\zeta_n - bc)x + (ab(1-\zeta_n))y : (cd(\zeta_n - 1))x + (ad - bc\zeta_n)y]$$

genera un subgrupo cíclico de orden n de $\mathrm{Aut}(\mathbb{P}^1)$ arbitrario. Por la Proposición 3.2.3, para cada uno de estos grupos cíclicos se tiene un único subespacio de Galois disjunto de $\nu_n(\mathbb{P}^1)$. Para encontrar explícitamente estos subespacios de Galois, consideremos el divisor $D := n[a : c] = nM[1:0]$ que es invariante bajo T_n. Entonces se tiene una acción de $\langle T_n \rangle$ en $L(D)$ por pullback

$$T_n^* : L(D) \to L(D)\ ;\quad f \mapsto f \circ T_n.$$

Queremos encontrar un subespacio vectorial $\langle T_n \rangle$-invariante de $\mathcal{L}$ de $L(D)$ de dimensión 2 tal que $T_n^*|_{\mathcal{L}}$ sea un múltiplo de la identidad. Para esto consideremos la base de $L(D)$ dada por la Proposición 1.4.8

$$L(D) = \langle f_D(x,y)x^n, f_D(x,y)x^{n-1}y, \ldots, f_D(x,y)xy^{n-1}, f_D(x,y)y^n \rangle,$$

donde

$$f_D(x,y) = (cx - ay)^{-n} \in k(x,y).$$

Usando esta base, encontraremos dos elementos en $L(D)$ invariantes bajo T_n^*. Se tiene que

$$1 = (cx - ay)^n f_D(x,y) \in L(D)$$

es trivialmente invariante bajo T_n^*. Por lado, un cálculo directo muestra que

$$T_n^*(g) = g \circ T_n = \zeta_n g,$$

con $g(x,y) = \left(\frac{dx-by}{cx-ay}\right)$. Por tanto, el elemento

$$g(x,y)^n = (dx - by)^n f_D(x,y) \in L(D)$$

también es invariante bajo T_n^*. Esto significa que el subespacio vectorial $\mathcal{L}$ de $L(D)$ generado por

$$1 = f_D(x,y) \sum_{i=0}^{n} (-1)^i a^i c^{n-i} x^{n-i} y^i$$

$$(dx - cy)^n f_D(x,y) = f_D(x,y) \sum_{i=0}^{n} (-1)^i b^i d^{n-i} x^{n-i} y^i$$

es un subespacio de dimensión 2 tal que $T_n^*|_{\mathcal{L}} = \mathrm{Id}$. Por tanto, considerando el sistema de coordenadas homogeneas en $\mathbb{P}^n$ que corresponde a la base de $L(D)$ que obtuvimos antes, y usando la notación introducida antes del Teorema 3.4.1, se obtienen los siguientes subespacios de Galois para ν_n

$$W_{[a:c],[b:d]} := \{L_{a,c} = L_{b,d} = 0\} \in \mathbb{G}(n-2, n).$$

Estos son todos los subespacios de Galois (disjuntos de $\nu_n(\mathbb{P}^1)$) con grupo de Galois cíclico y dan una familia $\mathcal{C}_n \subset \mathbb{G}(n-2,n)$. Para cada elemento $W_{[a:c],[b:d]}$ de $\mathcal{C}_n$ se tiene una proyección con centro en este subespacio lineal, la cual induce el morfismo de Galois

$$\pi : \mathbb{P}^1 \to \mathbb{P}^1; [t:1] \mapsto \left[\left(\frac{dt-b}{ct-a}\right)^n : 1\right].$$

El morfismo π induce la extensión de Galois de cuerpos de funciones $k(t)/k(t')$ con

$$t' = \left(\frac{dt-b}{ct-a}\right)^n,$$

cuyo grupo de Galois es

$$G_{[a:c],[b:d]} = \langle T_n \rangle \simeq \mathbb{Z}/n\mathbb{Z}.$$

Verificaremos en la Subsección 3.4.3 que la familia $\mathcal{C}_n$ es una subvariedad 2-dimensional localmente cerrada del Grassmanniano $\mathbb{G}(n-2,n)$.

3.4.2. Grupo dihedral de orden $2m$

En esta subsección demostraremos la segunda parte del Teorema 3.4. De manera similar a como en la subsección anterior, daremos una parametrización explícita de la familia de subespacios de Galois para ν_n (disjuntos de $\nu_n(\mathbb{P}^1)$) con grupo de Galois isomorfo al grupo dihedral de orden $n = 2m \geq 6$.

Sea $n = 2m \geq 6$ par, asumamos que k contiene una raíz primitiva n-ésima de la unidad ζ_n y sea $\zeta_m := \zeta_n^2$. Para $\alpha \in k^\times/(k^\times)^2\mu_m(k)$ consideremos los automorfismos de $\mathbb{P}^1$

$$C_m : \mathbb{P}^1 \to \mathbb{P}^1;\ [x:y] \mapsto [\zeta_m x : y]$$

$$I_\alpha : \mathbb{P}^1 \to \mathbb{P}^1;\ [x:y] \mapsto [\alpha y : x],$$

que corresponden a las matrices en $\mathrm{PGL}(2,k)$

$$C_m = \begin{pmatrix} \zeta_m & 0 \\ 0 & 1 \end{pmatrix},\ I_\alpha = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$$

las cuales generan un subgrupo $\langle C_m, I_\alpha \rangle$ de $\mathrm{PGL}(2,k)$ isomorfo al grupo dihedral de orden $2m$. Por [4, Teorema 4.2] se sabe que cada subgrupo dihedral de orden $2m$ es conjugado a $\langle C_m, I_\alpha \rangle$ para algún $\alpha \in k^\times/(k^\times)^2\mu_m(k)$. Entonces, tomando un elemento arbitrario

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}(2,k).$$

Los elementos conjugados

$$T_m = MC_mM^{-1} = \begin{pmatrix} ad\zeta_m - bc & ab(1-\zeta_m) \\ cd(\zeta_m - 1) & ad - bc\zeta_m \end{pmatrix}$$

$$J_\alpha := MI_\alpha M^{-1} = \begin{pmatrix} bd-\alpha ac & \alpha a^2 - b^2 \\ d^2-\alpha c^2 & \alpha ac - bd \end{pmatrix},$$

generan un subgrupo de $\mathrm{PGL}(2,k)$ que es isomorfo al grupo dihedral de orden $2m$, y todo subgrupo dihedral de orden $2m$ de $\mathrm{PGL}(2,k)$ se obtiene de esta manera para algún M. Los automorfismos de $\mathbb{P}^1$ que corresponden a las matrices anteriores son

$$T_m : \mathbb{P}^1 \to \mathbb{P}^1;\ [x:y] \mapsto [(ad\zeta_m - bc)x + (ab(1-\zeta_m))y : (cd(\zeta_m - 1))x + (ad - bc\zeta_m)y]$$
$$J_\alpha : \mathbb{P}^1 \to \mathbb{P}^1;\ [x:y] \mapsto \left[(bd-\alpha ac)x + (\alpha a^2 - b^2)y : (d^2 - \alpha c^2)x + (\alpha ac - bd)y\right].$$

Estos automorfismos generan a los subgrupos de $\mathrm{Aut}(\mathbb{P}^1)$ que son isomorfos al grupo dihedral de orden $2m$ y para cada uno de estos subgrupos se tiene un único subespacio de Galois para ν_n (disjunto de $\nu_n(\mathbb{P}^1)$). Queremos encontrar explícitamente estos subespacios de Galois. Para ello consideremos el divisor $D := m[a:c] + m[b:d] = mM[1:0] + mMI_\alpha[1:0]$ que es invariante bajo ambos automorfismos T_m y J_α. Por tanto el grupo $\langle T_m, J_\alpha\rangle$ actúa en $L(D)$ vía pullback

$$T_m^* : L(D) \to L(D)\ ;\quad f \mapsto f \circ T_m$$
$$J_\alpha^* : L(D) \to L(D)\ ;\quad f \mapsto f \circ J_\alpha.$$

Queremos hallar dos elementos de $L(D)$ que sean invariantes bajo T_m^* y J_α^*. Para esto usaremos la siguiente base del espacio $L(D)$

$$L(D) = \langle f_D(x,y)x^n, f_D(x,y)x^{n-1}y, \ldots, f_D(x,y)xy^{n-1}, f_D(x,y)y^n\rangle,$$

donde

$$f_D(x,y) = (cx-ay)^{-m}(dx-by)^{-m} \in k(x,y).$$

De la misma manera que en la sección anterior, vemos que

$$1 = (cx-ay)^m(dx-by)^m f_D(x,y) \in L(D)$$

es trivialmente invariante bajo T_m^* y J_α^*. Para encontrar otro elemento invariante, notemos que mediante cálculos directos se obtienen las siguientes relaciones

$$T_m^*(g) = g \circ T_m = \zeta_m g$$

$$J_\alpha^*(g) = g \circ J_\alpha = \alpha\,(1/g)$$

con $g(x,y) = \left(\frac{dx-by}{cx-ay}\right)$ como en la subsección anterior. Usando estas relaciones, se obtiene que el elemento

$$\alpha^m g^m + (1/g^m) = (\alpha^m(cx-ay)^n + (dx-by)^n)f_D(x,y) \in L(D)$$

también es invariante bajo T_m^* y J_α^*. Entonces, luego de expandir las expresiones de los elementos invariantes, se obtiene que el subespacio vectorial $\mathcal{L}$ de $L(D)$ generado por

$$f_D(x,y) \sum_{i+j+l=m} \binom{m}{i,j,l} (-1)^i (ad+bc)^i (ab)^j (cd)^l x^{i+2l} y^{i+2j}$$

$$f_D(x,y)\sum_{i=0}^{n}\binom{n}{i}(-1)^i(\alpha^m a^{n-i}c^i+b^{n-i}d^i)x^iy^{n-i}.$$

es un subespacio 2-dimensional tal que $\sigma^*|_{\mathcal{L}} = \mathrm{Id}$ para cada $\sigma \in \langle T_m, J_\alpha\rangle$. Ahora, ponemos las coordenadas homogéneas en $\mathbb{P}^n$ que corresponden a la base de $L(D)$ obtenida antes y consideremos la notación introducida antes del Teorema 3.4. Con esto se obtiene que los subespacios lineales

$$V^{\alpha}_{[a:b:c:d]} := \{A_{a,b,c,d} = B^{\alpha}_{a,b,c,d} = 0\} \in \mathbb{G}(n-2,n)$$

son todos los subespacios de Galois (disjuntos de $\nu_n(\mathbb{P}^1)$) para ν_n con grupo de Galois isomorfo al grupo dihedral de orden $2m$. Estos dan, para cada $\alpha \in k^\times/(k^\times)^2\mu_m(k)$, una familia $\mathcal{D}^{\alpha}_m \subset \mathbb{G}(n-2,n)$. Si $V^{\alpha}_{[a:b:c:d]}$ es un elemento arbitrario de $\mathcal{D}^{\alpha}_m$, entonces la proyección con centro en este subespacio lineal induce el siguiente morfismo de Galois

$$\pi : \mathbb{P}^1 \to \mathbb{P}^1;\ [t:1] \mapsto \left[\alpha^m\left(\frac{ct-a}{dt-b}\right)^m + \left(\frac{dt-b}{ct-a}\right)^m : 1\right].$$

El pullback π^* induce la extensión Galois de cuerpos de funciones $k(t)/k(t')$ con

$$t' = \alpha^m\left(\frac{ct-a}{dt-b}\right)^m + \left(\frac{dt-b}{ct-a}\right)^m,$$

la cual tiene grupo de Galois

$$G_{[a:b:c:d]} = \langle T_m, J_\alpha\rangle \simeq D_m.$$

En la subsección siguiente demostraremos que, sobre la clausura algebraica $\overline{k}$, las familias $\mathcal{D}^{\alpha}_m$ dan una subvariedad 3-dimensional localmente cerrada $\mathcal{D}_m$ de $\mathbb{G}(n-2,n)$.

3.4.3. Casos excepcionales

En esta subsección demostraremos la Proposición 3.4.2, es decir, estudiaremos los casos excepcionales $n \in \{2,4,12,24,60\}$. Aquí asumiremos que k es algebraicamente cerrado.

Primero analizaremos el caso $n = 2$, que corresponde a puntos de Galois (véase Subsección 2.4.1). Para $n = 2$, cada proyección lineal compuesta con la inmersión de Veronese ν_2 es de grado 2 o 1, dependiendo si el centro de la proyección es disjunto de $\nu_2(\mathbb{P}^1)$ o no. En cualquier caso, la extensión de cuerpos inducida es del mismo grado, y por tanto es Galois. Por tanto, cada elemento de $\mathbb{G}(0,2) = \mathbb{P}^2$ induce un morfismo de Galois. Esto demuestra que cada punto de $\mathbb{P}^2$ es un punto de Galois para ν_2. Si $p \in \mathbb{P}^2 \setminus \nu_2(\mathbb{P}^1)$, entonces el grupo de Galois es $G_p \simeq \mathbb{Z}/2\mathbb{Z}$. Si $p \in \nu_2(\mathbb{P}^1)$ el grupo de Galois es el grupo trivial.

Para los casos $n \in \{4,12,24,60\}$ no vamos a calcular explícitamente los subespacios de Galois como lo hicimos para el caso cíclico y el caso dihedral, ya que estos cálculos, aunque son elementales, son bastante tediosos. Ahora demostraremos que en cada uno de estos casos, para el grupo de Klein K_4 de orden 4, A_4, S_4 y A_5 hay una subvariedad 3-dimensional localmente cerrada de subespacios de Galois en el respectivo Grassmanniano.

Primero observamos que $\mathrm{PGL}(2,k)$ es 3-dimensional, y la clase de conjugación de un subgrupo dado $G \leq \mathrm{PGL}(2,k)$ es parametrizada por $\mathrm{PGL}(2,k)/N_G$, donde N_G es el normalizador de G en $\mathrm{PGL}(2,k)$. Si C_G es el centralizador de G en $\mathrm{PGL}(2,k)$, tenemos el homomorfismo de grupos natural $\varphi : N_G \to \mathrm{Aut}(G)$ cuyo núcleo es C_G. En particular, si G es finito, entonces C_G es de índice finito en N_G. Por la tabla en la página 27 de [4] se sabe que los centralizadores de K_4, D_m, A_4, S_4 y A_5 son todos finitos y por tanto sus normalizadores son también finitos. En el caso de $\mathbb{Z}/n\mathbb{Z}$, el centralizador es 1-dimensional y por tanto el normalizador también. Por [4, Teorema 4.2], como estamos asumiendo que k es algebraicamente cerrado, solo hay una clase de conjugación para cada subgrupo finito de $\mathrm{PGL}(2,k)$. Por tanto hemos obtenido el siguiente resultado.

Proposición 3.4.3. *Las familias $\mathcal{C}_n$ son 2-dimensionales y las familias $\mathcal{D}_m$ son 3-dimensionales para todo $n, m \geq 3$. Para K_4, A_4, S_4 y A_5 obtenemos familias de subespacios de Galois $\mathcal{K} \subset \mathbb{G}(2,4)$, $\mathcal{A}_4 \subset \mathbb{G}(10,12)$, $\mathcal{S}_4 \subset \mathbb{G}(22,24)$ y $\mathcal{A}_5 \subset \mathbb{G}(58,60)$, respectivamente, que son todas 3-dimensionales.*

Esto completa la demostración del Teorema 3.4.1 y de la Proposición 3.4.2. Hasta ahora se ha obtenido una respuesta para el problema principal en el caso que los subespacios de Galois para ν_n son disjuntos de $\nu_n(\mathbb{P}^1)$. En la siguiente sección consideraremos el caso general, es decir, cuando los subespacios de Galois para ν_n no son necesariamente disjuntos de $\nu_n(\mathbb{P}^1)$, y así lograremos responder la pregunta principal de esta tesis.

3.5. Subespacios de Galois no disjuntos

En esta última sección estudiaremos los subespacios de Galois para ν_n que no son necesariamente disjuntos de $\nu_n(\mathbb{P}^1)$. Aquí asumiremos que k es algebraicamente cerrado.

Sea $W \in \mathbb{G}(n-2,n)$ un subespacio de Galois que no es disjunto de $\nu_n(\mathbb{P}^1)$. La proyección con centro W compuesta con ν_n puede dar un morfismo de Galois como, por ejemplo, en el caso de $W = \{x_0 = x_2 = 0\}$, si $n \geq 3$. En este caso la correspondencia que se obtuvo en el Corolario 3.2.2 no es biyectiva. Ilustraremos esta situación en el siguiente ejemplo.

Ejemplo 3.5.1. Sea $n = 3$. Consideremos la familia 1-dimensional de subespacios lineales $W_{[\alpha:\beta]} \in \mathbb{G}(1,3)$ definidos por $W_{[\alpha:\beta]} = \{\alpha x_0 + \beta x_1 = \alpha x_2 + \beta x_3 = 0\}$. Estos subespacios no son disjuntos de $\nu_3(\mathbb{P}^1)$ ya que $\nu_3[\beta : -\alpha] \in W_{[\alpha:\beta]}$. Sea $\pi_{[\alpha:\beta]}$ la composición de la proyección lineal con centro $W_{[\alpha:\beta]}$ y la inmersión de Veronese ν_3. Entonces $\pi_{[\alpha:\beta]}[x : y] = [\alpha x^3 + \beta x^2 y : \alpha x y^2 + \beta y^3] = [(\alpha x + \beta y)x^2 : (\alpha x + \beta y)y^2] = [x^2 : y^2]$. Por tanto, para cada $[\alpha : \beta] \in \mathbb{P}^1$, $W_{[\alpha:\beta]}$ es un subespacio de Galois para ν_3 con grupo de Galois $G_{[\alpha:\beta]} = \langle [x : y] \mapsto [-x : y] \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Pero es importante observar lo siguiente $\pi_{[\alpha:\beta]}[x : y] = [x^2 : y^2] = \pi_{\widetilde{W}} \circ \nu_2[x : y]$, donde $\widetilde{W} = \{x_0 = x_2 = 0\} \in \mathbb{G}(0,2)$.

El ejemplo anterior muestra que la correspondencia obtenida en el Corolario 3.2.2 no es 1-1 en el caso no disjunto. De hecho, tampoco es finito a 1.

Por el Lema 3.2.1 y su demostración vemos que si $W \in \mathbb{G}(n-2,n)$ y $W \cap \nu_n(\mathbb{P}^1) \neq \varnothing$, entonces $\pi = \pi_W \circ \nu_n : \mathbb{P}^1 \to \mathbb{P}^1$ es un morfismo de grado $m < n$, donde $\pi_W : \mathbb{P}^n \dashrightarrow \mathbb{P}^1$ es la proyección con centro W. De hecho, por el mismo lema, existe un único $\widetilde{W} \in \mathbb{G}(m-2,m)$ tal que $\pi_{\widetilde{W}} \circ \nu_m = \pi$ (módulo automorfismos de $\mathbb{P}^1$). Por tanto obtenemos un morfismo

$$\Phi_{n,m} : \mathfrak{X}_{n,m} := \{W \in \mathbb{G}(n-2,n) : \deg(\pi_W \circ \nu_n) = m\} \to \mathbb{G}(m-2,m)$$

que envía W a $\widetilde{W}$.

Proposición 3.5.2. *Las fibras de $\Phi_{n,m}$ son irreducibles y de dimensión $n-m$. En particular $\Phi_{n,m}$ es inyectiva si y sólo si $n = m$.*

Demostración. Primero calcularemos la dimensión de las fibras. Notar que la imagen de $\Phi_{n,m}$ consiste de subespacios lineales que son disjuntos de $\nu_m(\mathbb{P}^1)$ y por lo tanto $\Phi_{n,m}$ es dominante. De hecho, tenemos el morfismo $i_{m,n} : \mathbb{G}(m-2,m) \hookrightarrow \mathbb{G}(n-2,n)$ que toma un subespacio lineal definido por dos ecuaciones y lo envía al subespacio lineal de dimensión $n-2$ definido por las mismas dos ecuaciones. Si $\widetilde{W} \in \mathbb{G}(m-2,m)$ es disjunto de $\nu_m(\mathbb{P}^1)$, entonces por el Lema 3.2.1 se tiene que $\deg(\pi_{\widetilde{W}} \circ \nu_m) = m$. Luego, escribiendo $W = i_{m,n}(\widetilde{W})$, es claro que $\pi_W \circ \nu_n = \pi_{\widetilde{W}} \circ \nu_m$ y por tanto $\deg(\pi_W \circ \nu_n) = m$. Esto implica que $W \in \mathfrak{X}_{n,m}$ y $\Phi_{n,m}(W) = \widetilde{W}$. Por tanto $\Phi_{n,m} \circ i_{m,n}$ es la identidad en aquellos subespacios de $\mathbb{G}(m-2,m)$ que son disjuntos de $\nu_m(\mathbb{P}^1)$.

En particular, si F es una fibra general de $\Phi_{n,m}$, entonces (ver Teorema 1.3.11)

$$\dim F = \dim \mathfrak{X}_{n,m} - 2(m-1).$$

Tomemos $W \in \mathfrak{X}_{n,m}$ como la intersección de dos hiperplanos $H_1, H_2 \in \mathbb{G}(n-1,n)$. Anotemos

$$\nu_n^* H_1 = p_1 + \cdots + p_n$$

$$\nu_n^* H_2 = q_1 + \cdots + q_n$$

donde los puntos $p_1, \ldots, p_n, q_1, \ldots, q_n$ no son necesariamente diferentes. Luego como $W \in \mathfrak{X}_{n,m}$, tenemos que exactamente $n-m$ de los p_i (contados con multiplicidad) son iguales a $n-m$ de los q_i (contados con multiplicidad). Tenemos un morfismo racional

$$\mathrm{Sym}^{n-m}(\mathbb{P}^1) \times \mathrm{Sym}^m(\mathbb{P}^1) \times \mathrm{Sym}^m(\mathbb{P}^1) \dashrightarrow \mathbb{G}(n-2,n)$$

donde

$$(D_1, D_2, D_3) \mapsto \mathrm{span}\{\nu_n(D_1 + D_2)\} \cap \mathrm{span}\{\nu_n(D_1 + D_3)\}.$$

Sea $\mathfrak{Y}_{m,n}$ el conjunto de todos los $(D_1, D_2, D_3) \in \mathrm{Sym}^{n-m}(\mathbb{P}^1) \times \mathrm{Sym}^m(\mathbb{P}^1) \times \mathrm{Sym}^m(\mathbb{P}^1)$ tales que $\mathrm{supp}(D_i) \cap \mathrm{supp}(D_j) = \varnothing$ para todo $i \neq j$ y D_i es reducido para todo $i = 1,2,3$. Entonces el morfismo racional anterior corresponde al morfismo

$$\theta_{m,n} : \mathfrak{Y}_{m,n} \to \mathbb{G}(n-2,n)$$

cuya imagen contiene un abierto de $\mathfrak{X}_{n,m}$. Como el morfismo natural de intersección

$$(\mathbb{G}(n-1,n) \times \mathbb{G}(n-1,n)) \setminus \Delta \to \mathbb{G}(n-2,n)$$

tiene fibras de dimensión 2, obtenemos que las fibras del morfismo θ son de dimensión 2. Esto implica que

$$\dim \mathfrak{X}_{n,m} = n + m - 2.$$

Por tanto concluimos que una fibra general de $\Phi_{n,m}$ tiene dimensión

$$n + m - 2 - 2(m-1) = n - m.$$

Un analisis más cuidadoso muestra que si $V \in \mathbb{G}(m-2,m)$ es disjunto de $\nu_m(\mathbb{P}^1)$, y $(D_1, D_2, D_3) \in \theta^{-1}\Phi_{n,m}^{-1}(V)$ es una preimagen arbitraria, entonces

$$\Phi_{n,m}^{-1}(V) = \theta_{m,n}\left(\mathrm{Sym}^{n-m}(\mathbb{P}^1) \times \{D_2\} \times \{D_3\}\right)$$

y por tanto es irreducible. $\square$

Con respecto a determinar cuándo un elemento $W \in \mathbb{G}(n-2,n)$ que no es disjunto de $\nu_n(\mathbb{P}^1)$ da un subespacio de Galois, es claro que se tiene el siguiente resultado:

Proposición 3.5.3. *Si $W \in \mathbb{G}(n-2,n)$ es tal que $\deg(\pi_W \circ \nu_n) = m$, entonces W es un subespacio de Galois para ν_n si y sólo si $\Phi_{n,m}(W)$ pertenece a una de las familias presentadas en el Teorema 3.4.1 y la Proposición 3.4.2.*

Definimos $\Phi_{n,1}(\mathcal{C}_1)$ como el conjunto de todos los $W \in \mathbb{G}(n-2,n)$ tales que $\pi_W \nu_n$ es un automorfismo de $\mathbb{P}^1$. Por el análisis previo es fácil ver que esta familia es de dimensión $n-1$. Con esta notación y con la Proposición 3.5.3 se obtiene una caracterización de todos los grupos de Galois y todos los subespacios de Galois para ν_n, disjuntos y no disjuntos de $\nu_n(\mathbb{P}^1)$. Así hemos obtenido una respuesta para el problema principal de esta tesis. Terminaremos mostrando todos los subespacios de Galois para ν_n.

Teorema 3.5.4. *El Cuadro 3.2 da la lista de todos los subespacios de Galois para ν_n.*

En particular, vemos que la familia más grande es $\Phi_{n,2}^{-1}(\mathcal{C}_2)$ la cual es de dimensión n.

	Families of Galois subspaces	Dimension of families	Number of families
$n = 2, 3$	$\Phi_{n,1}^{-1}(\mathcal{C}_1)$ $\Phi_{n,k}^{-1}(\mathcal{C}_k)$, $k = 2, \ldots, n$	$n-1$ $n-k+2$	n
$4 \leq n \leq 11$	$\Phi_{n,1}^{-1}(\mathcal{C}_1)$ $\Phi_{n,k}^{-1}(\mathcal{C}_k)$, $k = 2, \ldots, n$ $\Phi_{n,2k}^{-1}(\mathcal{D}_k)$, $k = 3, \ldots, \lfloor \frac{n}{2} \rfloor$ $\Phi_{n,4}^{-1}(\mathcal{K})$	$n-1$ $n-k+2$ $n-2k+3$ $n-1$	$n + \lfloor \frac{n}{2} \rfloor - 1$
$12 \leq n \leq 23$	$\Phi_{n,1}^{-1}(\mathcal{C}_1)$ $\Phi_{n,k}^{-1}(\mathcal{C}_k)$, $k = 2, \ldots, n$ $\Phi_{n,2k}^{-1}(\mathcal{D}_k)$, $k = 3, \ldots, \lfloor \frac{n}{2} \rfloor$ $\Phi_{n,4}^{-1}(\mathcal{K})$ $\Phi_{n,12}^{-1}(\mathcal{A}_4)$	$n-1$ $n-k+2$ $n-2k+3$ $n-1$ $n-9$	$n + \lfloor \frac{n}{2} \rfloor$
$24 \leq n \leq 59$	$\Phi_{n,1}^{-1}(\mathcal{C}_1)$ $\Phi_{n,k}^{-1}(\mathcal{C}_k)$, $k = 2, \ldots, n$ $\Phi_{n,2k}^{-1}(\mathcal{D}_k)$, $k = 3, \ldots, \lfloor \frac{n}{2} \rfloor$ $\Phi_{n,4}^{-1}(\mathcal{K})$ $\Phi_{n,12}^{-1}(\mathcal{A}_4)$ $\Phi^{-1}(\mathcal{S}_4)$	$n-1$ $n-k+2$ $n-2k+3$ $n-1$ $n-9$ $n-21$	$n + \lfloor \frac{n}{2} \rfloor + 1$
$n \geq 60$	$\Phi_{n,1}^{-1}(\mathcal{C}_1)$ $\Phi_{n,k}^{-1}(\mathcal{C}_k)$, $k = 2, \ldots, n$ $\Phi_{n,2k}^{-1}(\mathcal{D}_k)$, $k = 3, \ldots, \lfloor \frac{n}{2} \rfloor$ $\Phi_{n,4}^{-1}(\mathcal{K})$ $\Phi_{n,12}^{-1}(\mathcal{A}_4)$ $\Phi_{n,24}^{-1}(\mathcal{S}_4)$ $\Phi_{n,60}^{-1}(\mathcal{A}_5)$	$n-1$ $n-k+2$ $n-2k+3$ $n-1$ $n-9$ $n-21$ $n-57$	$n + \lfloor \frac{n}{2} \rfloor + 2$

Cuadro 3.2: Lista de todas las familias de subespacios de Galois para ν_n

Bibliografía

[1] N. Adrianov. *Primitive monodromy grops of rational functions with one multiple pole.* J. Math. Sci. (N.Y.) 226 (2017), no. 5, 548-560.

[2] R. Auffarth. *A note on Galois embeddings of abelian varieties.* Manuscripta Math. 154, 279-284 (2017).

[3] R. Auffarth, S. Rahausen. *Galois subspaces for the rational normal curve.* Preprint, 2018. https://arxiv.org/abs/1809.02635.

[4] A. Beauville. *Finite subgroups of $PGL_2(K)$.* Vector bundles and complex geometry, 23-29, Contemp. Math., 522, Amer. Math. Soc., Providence, RI, 2010.

[5] F. Cukierman. *Monodromy of projections.* Mat. Contemp. 16. 15th School of Algebra (Portuguese), 9-30.

[6] O. Debarre. *Complex tori and abelian varieties.* American Mathematical Society, Providence, RI; Société Mathématique de France, Paris, 2005

[7] S. Fukasawa, T. Takahashi. *Galois points for a normal hypersurface.* Trans. Amer. Math. Soc., 366 (2014), 1639-1658.

[8] P. Griffiths, J. Harris. *Principles of Algebraic Geometry.* Pure and Applied Mathematics, A Wiley-Interscience Publication, New York, 1978.

[9] R.M. Guralnick, J. Saxl. *Monodromy groups of polynomials.* Groups of Lie type and their geometries. 125-160. Cambridge Univ. Press, Cambridge, 1995.

[10] R. Hartshorne. *Algebraic Geometry*, volume 52 of Graduate Texts in Mathemat- ics. Springer, 1977.

[11] J. König. *On rational functions with monodromy group M_{11}.* J. Symbolic Comput. 79 (2017), part 2, 372-383.

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

[13] K. Miura, H. Yoshihara. *Field theory for function fields of plane quartics*. J. Algebra 226 (2000), 283-294.

[14] P. Müller. *Primitive monodromy groups of polynomials.* Recent developments in the inverse Galois problem (Seattle, WA, 1993), 385-401, Contemp. Math., 186, Amer. Math. Soc., Providence, RI, 1995.

[15] P. Müller. (A_n, S_n) *realizations by polynomials - on a question of Fried.* Finite Fields Appl. 4 (1998), 465-468.

[16] G.P. Pirola, E. Schlesinger. *Monodromy of projective curves.* J. Algebraic Geom. 14, 623-642 (2005).

[17] I. Shafarevich. *Basic algebraic geometry. 1. Varieties in projective space*. Third edition. Translated from the 2007 third Russian edition. *Springer, Heidelberg*, 2013.

[18] T. Takahashi. *Projection of a nonsingular plane quintic curve and the dihedral group of order eight.* Rend. Semin. Mat. Univ. Padova 135, 39-61 (2016)

[19] H. Yoshihara. *Function field theory of plane curves by dual curves*. J. Algebra 239 (2001), no. 1, 340-355.

[20] H. Yoshihara. *Galois lines for space curves*. Algebra Collow. 13 (2006), no. 3, 455-469.

[21] H. Yoshihara. *Galois embedding of algebraic variety and its application to abelian surface.* Rend. Semin. Mat. Univ. Padova 117 (2007), 69-85.

[22] H. Yoshihara. *Galois lines for normal elliptic space curves, II.* Algebra Colloquium, 19 (2012), No. spec01, 867-876.

[23] H. Yoshihara. *List of problems.* url: http://hyoshihara.web.fc2.com/20170925.pdf.