Curvas de Tipo Fermat

Tesis
Entregada A La
Universidad de Chile
En Cumplimiento Parcial De Los Requisitos
Para Optar Al Grado De

Doctor en Ciencias Mención Matemáticas

Facultad de Ciencias

Por

Jaime Eduardo Pinto Doveris

Septiembre, 2016

Director de Tesis: Ángel Denys Carocca Becerra

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACION

TESIS DE DOCTORADO

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Doctorado presentada por la candidata.

JAIME EDUARDO PINTO DOVERIS

Ha sido aprobada por la comisión de Evaluación de la tesis como requisito para optar al grado de Doctorado en Ciencias Mención Matemáticas, en el examen de Defensa Privada de Tesis rendido el día 30 de Agosto de 2016.

Director de Tesis:
Dr. Ángel Carocca

Co-Director de Tesis
Dra. Anita Rojas

Comisión de Evaluación de la Tesis

Dra. Rubí Rodriguez

Dr. Antonio Behn

Dra. Michela Artebani

Dr. Maximiliano Leyton

Biografía

Nací el 27 de Julio de 1985 en la comuna de Independencia, Santiago de Chile. Ese ha sido el lugar donde he residido hasta hoy en día y donde desarrollé mis estudios escolares, desde 1990 hasta 2003. En toda mi vida como escolar fui un estudiante destacado, especialmente en Matemáticas.

En 2003 Rendí la Prueba de Selección Universitaria, obteniendo buenos puntajes que me sirvieron para entrar a la Pontificia Universidad Católica de Chile al año siguiente. Estudié en esa casa de estudios Licenciatura en Matemática, egresando en 4 años con dos votos de distinción. En 2009 ingresé a la Universidad de Chile en la carrera de Magíster en Ciencias Matemáticas. Desarrollé mi tesis de grado bajo la dirección de la Profesora Anita Rojas, dentro de la especialidad de Geometría Compleja. Después de dos años de trabajo, conseguí egresar el día 5 de Enero de 2012 al defender exitosamente mi Tesis.

En Marzo de 2012 entré al Doctorado en Ciencias Mención Matemáticas de la Universidad de Chile. Ese año aprobé mis exámenes de Calificación y por ello, pude optar a tener un Director de Tesis, el cual fue el Profesor Ángel Carocca de la Universidad de la Frontera, también especialista en Geometría Compleja. El 2013 empezó mi trabajo de investigación, el cual ha tenido altos y bajos, pero que finalmente rindió frutos que se expresan en esta Tesis Doctoral.

Agradecimientos

Es mi deber como Alumno Tesista, agradecer a algunas personas e instituciones por ayudarme, ya sea moral, económica o intelectualmente, por permitirme desarrollar este trabajo de Tesis y mi vida como estudiante de Doctorado:

- A mi familia y compañeros cercanos de diferentes Universidades por apoyarme siempre cuando lo necesité en el desarrollo de mi vida como estudiante de Doctorado. En particular, a mi padre, Fernando Pinto, por su sabiduría tendiente al infinito a la hora de darme consejos en mi desarrollo como estudiante; y también a mis compañeros Alan Chávez y Daniel Sepúlveda por su grata amistad y buenas conversaciones.

- A la Universidad de Chile por darme la posibilidad de ser su estudiante, y en particular a la gente del Departamento de Matemáticas por su hospitalidad y apoyo para asistencia a Congresos durante estos años, incluso de antes cuando era estudiante de Magíster. Menciones especiales al Profesor Eduardo Friedman por su disposición como Coordinador del Doctorado y su gran calidad como docente; también a los Profesores Antonio Behn y Manuel Arenas por su amabilidad habiendo sido ayudante de ellos en cursos de Postgrado; y al auxiliar del Departamento, Santiago Andrews, por su disposición a ayudar en ciertas situaciones y por las entretenidas conversaciones que tuvimos.

- A la Comisión Nacional de Investigación Científica y Tecnológica, CONICYT, por brindarme la Beca de Estudios de Doctorado Nacional sin la cual no estaría desarrollando mi carrera de Doctorado.

- A mi Director de Tesis, el Profesor Ángel Carocca y a mi Co-Directora de Tesis, la Profesora Anita Rojas, por ser mi principal apoyo intelectual en mi trabajo de Tesis así como también estimularme a participar en actividades relacionadas con el área de la Geometría Compleja.

Resumen

Esta tesis trata sobre superficies de Riemann compactas con acción de ciertos grupos, con el propósito de generalizar las propiedades de las curvas de Fermat. En este trabajo se busca determinar los géneros de estas superficies, ecuaciones que las definan como curvas planas, grupos de automorfismos, realización de los generadores de los grupos de interés como automorfismos explícitos, géneros y ecuaciones para cocientes intermedios y descomposición isotípica de las Variedades Jacobianas de estas superficies.

Abstract

This thesis is about Compact Riemann Surfaces with action of some kind of groups, with the purpose of generalizing properties of Fermat Curves. We want to determine genera of these surfaces, defining equations for them as plane curves, automorphism groups, explicit formulas for the generatos of these groups as automorphisms, genera and equations for intermediate covers and the isotypical decomposition of the Jacobians of these surfaces.

Índice general

Capítulo 1

Introducción

Esta tesis trata sobre Superficies de Riemann con ciertas acciones de grupos. Los grupos que interesan son de la forma $G = \mathbb{Z}_n \rtimes \mathbb{Z}_n$ con n una potencia de un número primo. La acción la determinremos mediante una elección adecuada de los generadores de G, y a partir de eso, estudiaremos propiedades de estas superficies, como su género, grupo completo de automorfismos, ecuaciones que las definan como curvas algebraicas y realización de automorfismos en estas curvas algebraicas. También nos interesa estudiar los cocientes intermedios, obteniendo sus géneros, tipo de acción y ecuaciones como curvas algebraicas. También mencionaremos cosas sobre las Variedades Jacobianas de estas Superficies de Riemann, en particular su descomposición isógena como producto de subvariedades. El estudio divide casos para n de acuerdo si es una potencia de un primo impar, o si es potencia de 2, pues los grupos se comportan de diferentes formas dependiendo del tipo de primo.

La idea de este trabajo es generalizar la situación de las curvas de Fermat, que admiten acción de $\mathbb{Z}_n \times \mathbb{Z}_n$ y para las cuales se tienen resultados en cuanto a género y grupos de automorfismos mediante una acción determinada por una elección adecuada de los generadores del grupo. Este trabajo trata de usar las mismas ideas que para la curva de Fermat, pero usando una estructura de grupo diferente.

En el Capítulo 2 mencionaremos los preliminares necesarios de Superficies de Riemann para entender el trabajo que realizaremos en los siguientes capítulos, en particular ejemplos como las curvas planas afines y proyectivas. También mencionaremos sobre acción de grupos en superficies de Riemann, incluyendo acciones n-gonales. Finalmente hablaremos sobre Variedades Jacobianas y Abelianas.

En el Capítulo 3 estudiaremos el grupo $G = \mathbb{Z}_n \rtimes \mathbb{Z}_n$, de acuerdo si n es potencia de primo impar o de 2, centrándonos en determinar subgrupos relevantes, como los subgrupos generados por cada generador de G, y términos de las series centrales ascendente y descendente. También mostraremos la existencia de Superficies de Rie-

mann $\mathcal{X}$ con acción de G de acuerdo a una elección adecuada de sus generadores, calcularemos el género y firma de estas superficies y de los cocientes intermedios determinados por los subgrupos de G. Finalmente, determinaremos cuando G es el grupo de automorfismos completo de $\mathcal{X}$, o equivalentemente, determinar el índice de G en dicho grupo de automorfismos y la firma de la acción de este último.

En el Capítulo 4 estudiaremos a $\mathcal{X}$ como curva n-gonal, determinando una ecuación para ella, estudiar sus propiedades, realizar los generadores de G como automorfismos explícitos de $\mathcal{X}$ como curva plana, y verificar que se realiza la firma de la acción de G. También determinaremos ecuaciones para los cocientes intermedios asociados y si es posible, sus grupos de automorfismos. Finalmente, mencionaremos brevemente algunas hechos sobre el menor cuerpo de definición de $\mathcal{X}$.

En el Capítulo 5 estudiaremos las Jacobianas de las Superficies $\mathcal{X}$, mediante el estudio de las representaciones irreducibles complejas, encontrando su descomposición isógena, dimensiones de los factores de ésta, los núcleos de dichas representaciones, ecuaciones de cocientes intermedios determinados por dichos núcleos y Variedades de Prym asociadas a subgrupos de G.

Esta tesis incluye un Apéndice donde mostraremos algunas fórmulas que se usarán en algunos cálculos importantes que se realizarán en el desarrollo de este trabajo.

Capítulo 2

Superficies de Riemann

En esta sección presentaremos conceptos básicos sobre superficies de Riemann que son necesarios para desarrollar el problema de interés en esta tesis. Nos centraremos en el tema de acciones de grupos, curvas planas afines y proyectivas, particularmente curvas n-gonales y de Fermat. También mencionaremos algunos resultados sobre Variedades Jacobianas.

2.1. Definición y Ejemplos

Comenzamos con la definición de Superficie de Riemann:

Definición 2.1.1 *Sea X un espacio topológico. Diremos que el siguiente conjunto de homeomorfismos*

$$A = \{\phi_i : U_i \to V_i, i \in I\},$$

*con $\{U_i\}_{i\in I}$ una familia de abiertos en X y $\{V_i\}_{i\in I}$ una familia de abiertos en $\mathbb{C}$, es un **atlas complejo** si cumple que*

$$\bigcup_{i\in I} U_i = X,$$

y para $i, j \in I$, o bién $U_i \cap U_j$ es vacío, ó bien

$$\phi_j \circ \phi_i^{-1} : \phi_i(U_i \cap U_j) \to \phi_j(U_i \cap U_j)$$

*es una aplicación bi-holomorfa. X se dice **superficie de Riemann** si es conexo, Hausdorff, admite una base numerable, y está provisto de un atlas complejo $\mathcal{A}$*

Ejemplo 2.1.1 *Sea $X = \mathbb{C}$ con su topología usual. Como espacio topológico, es conexo, Hausdorff y tiene una base numerable. Consideremos $A = \{Id\}$ donde Id es la función identidad en $\mathbb{C}$. Es evidente que A es un atlas complejo que dota a X de una estructura de superficie de Riemann. Si ahora consideramos $A = \{\varrho\}$ donde ϱ es la conjugación compleja en $\mathbb{C}$, tambien es un atlas complejo que dota a X de una estructura de superficie de Riemann.*

El siguiente ejemplo es importante en la teoría de superficies de Riemann. Lo introduciremos como una proposición:

Proposición 2.1.1 *Sea $\hat{\mathbb{C}} = \{(x,y,z) \in \mathbb{R}^3 | x^2 + y^2 + z^2 = 1\}$ la esfera real de dimensión 2, con la topología heredada de la usual en $\mathbb{R}^3$. Sean:*

$$U_1 = \hat{\mathbb{C}} - \{(0,0,1)\}$$
$$U_2 = \hat{\mathbb{C}} - \{(0,0,-1)\}$$

Sean $\phi_1 : U_1 \to \mathbb{C}$ y $\phi_2 : U_2 \to \mathbb{C}$ definidas por:

$$\phi_1(x,y,z) = \frac{x+yi}{1-w}, \quad \phi_2(x,y,z) = \frac{x-yi}{1+w}$$

*Entonces $A = \{\phi_1, \phi_2\}$ es un atlas complejo para $\hat{\mathbb{C}}$ que la define como superficie de Riemann, llamada la **esfera de Riemann**.*

Demostración: Ver en [18], pág. 3.

Otro ejemplo importante de superficies de Riemann son las curvas planas afines suaves, las cuales se definen a continuación:

Definición 2.1.2 *Sea $f(x,y)$ un polinomio en 2 variables con coeficientes en $\mathbb{C}$. Sea*

$$X = \{(a,b) \in \mathbb{C}^2 | f(a,b) = 0\}$$

*Diremos que X es una **curva plana afín** definida por f.*

Interesa dotar de una estructura de superficie de Riemann a una curva plana afín. Para ello, exigimos algunas condiciones sobre la curva:

Definición 2.1.3 *Sea X una curva plana afín en $\mathbb{C}^2$ definida por un polinomio $f(x,y)$. Sea $p \in X$. Si las derivadas parciales $\partial f/\partial x$ y $\partial f/\partial y$ se anulan simultáneamente en p decimos que X es **singular** en p. En caso contrario decimos que X es **no singular** en p. Si X es no singular en todos sus puntos, decimos que X es una **curva plana afín suave**.*

El nombre de *curva plana afín suave* se debe a que si X es el lugar de ceros de un polinomio no singular en todos los puntos de X, entonces por el Teorema de la Función Implícita, X es localmente el gráfico de una función holomorfa $h : A \to \mathbb{C}$ con $A \subseteq \mathbb{C}$. Se puede dotar de un atlas complejo a una curva plana afín suave X, usando el Teorema de la Función Implícita. Para ver la demostracion de eso, consultar en [18] (pág 11). Sin embargo, dependiendo del polinomio que defina a X, tal curva puede ser conexa o no. Existe una condición que asegura dicha conexidad:

Proposición 2.1.2 *Sea X una curva plana afín suave en $\mathbb{C}^2$ definida por un polinomio $f(x, y)$. Si f es irreducible, entonces X es conexa.*

Demostración: ver [24], pág. 321.

Una propiedad importante de una superficie de Riemann es que se puede ver de forma natural como una variedad topológica real 2-dimensional, C^∞ y orientable. Por ello, si es compacta, o bien, es homeomorfa a la esfera 2-dimensional en $\mathbb{R}^3$, o bien, es homeomorfa a una suma conexa de toros topológicos. En el primer caso, diremos que el **género** de la superficie es cero, y en el segundo caso, diremos que su género es la cantidad de sumandos en la suma conexa respectiva.

2.2. Espacios proyectivos

Un tipo de espacios topológicos que se relacionan con las superficies de Riemann son los espacios proyectivos complejos. En estos espacios viven naturalmente todas las superficies de Riemann compactas, que de hecho se pueden ver como ceros de polinomios en dichos espacios.

Definición 2.2.1 *Sea n un entero positivvo. Sea $\Theta_n = \mathbb{C}^{n+1} \backslash \{(0, ..., 0)\}$. Sean u, v elementos de Θ_n. Diremos que $u \sim v$ si existe $\lambda \in \mathbb{C}^*$ tal que $x = \lambda y$.*

Se puede verificar que $\sim$ es una relación de equivalencia. De esta forma, procedemos a definir el espacio proyectivo como un cociente determinado por dicha relación de equivalencia:

Definición 2.2.2 *Considerando la notación de la definición anterior. Definimos el **espacio proyectivo complejo de dimensión** n como el siguiente espacio cociente:*

$$\mathbb{P}^n = \Theta_n / \sim$$

Dotaremos a $\mathbb{P}^n$ de la topología cociente heredada de la usual de Θ_n bajo la proyección canónica π_n. Si $w = (x_0, ..., x_n)$ es un elemento de Θ_n, denotaremos a $\pi_n(w)$ como $[x_0 : ... : x_n]$. Llamaremos a los x_j las **coordenadas homogéneas** de un punto en $\mathbb{P}^n$. Es claro que para todo $\lambda \in \mathbb{C}^*$:

$$[x_0 : ... : x_n] = [\lambda x_0 : ... : \lambda x_n]$$

La siguiente proposición nos da una importante propiedad de un espacio proyectivo complejo:

Proposición 2.2.1 *$\mathbb{P}^n$ es compacto para todo n.*

Demostración: se puede ver en [18], página 16.

En el caso particular de $n = 1$, tenemos lo siguiente:

Proposición 2.2.2 *$\mathbb{P}^1$ es homeomorfo a $\hat{\mathbb{C}}$.*

Demostración: se puede ver en [18], pág.12.

Esto nos dice que $\mathbb{P}^1$ es una superficie de Riemann compacta de género cero.

Veamos ahora algunas superficies de Riemann que viven naturalmente como subconjuntos de los espacios proyectivos. Estas se definen de la misma forma que las curvas planas afines, sólamente que por la naturaleza de los puntos de estos espacios, se definen mediante polinomios homogéneos. Por simplicidad trabajaremos en el caso de $\mathbb{P}^2$:

Definición 2.2.3 *Sea $H(x, y, z)$ un polinomio homogéneo en tres variables con coeficientes complejos. Sea $X = \{[a : b : c] \in \mathbb{P}^2 | H(a, b, c) = 0\}$. Diremos que X es una **curva plana proyectiva** definida por H.*

Ejemplo 2.2.1 *Sea $H(x, y, z) = xy^3 + yz^3 + zx^3$. La curva plana proyectiva definida por H se llama la **curva de Klein**.*

Es evidente que una curva plana proyectiva es cerrada, y por ende, compacta. Al igual que en las curvas afines, podemos definir cuando una curva proyectiva es una superficie de Riemann, usando esencialmente la misma idea que resumimos en la siguiente proposición:

Proposición 2.2.3 *Sea $X \subset P^2$ una curva plana proyectiva definida por un polinomio homogeneo $H(x, y, z)$. Si en ningún punto de X las derivadas parciales de primer orden de H se anulan simultáneamente, entonces X es una superficie de Riemann compacta que llamamos **curva plana proyectiva suave**.*

Demostración: se puede ver en [18], págs. 14-16.

En el ejemplo anterior, es un ejercicio estándar verificar que el polinomio que define la curva de Klein no tiene singularidades en $\mathbb{P}^2$. Por lo tanto, es una superficie de Riemann compacta.

Consideremos un polinomio $f(x,y)$ en $\mathbb{C}[x,y]$, y denotamos por n su grado, la **homogeneización** de f se define como:

$$H_f(x,y,z) = z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$$

La homogeneización de f es un polinomio homogéneo que define una curva plana proyectiva en $\mathbb{P}^2$. De esta forma, introducimos lo siguiente:

Definición 2.2.4 *Sea $Y \subset \mathbb{C}^2$ uan curva plana afín definida por $f(x,y)$. La curva plana proyectiva en $\mathbb{P}^2$ definida por $H_f(x,y,z)$ se llama la* ***clausura proyectiva*** *de Y, y la denotamos por $\mathbb{P}_Y$*

Ahora, veamos el proceso inverso: si $X \subset \mathbb{P}^2$ es una curva plana proyectiva definida por un polinomio homogéneo $H(x,y,z)$, podemos crear una curva plana afín en base a este polinomio "deshomogeneizando" H en una de las variables. Sean

$$A_{H,x} = H(1,y,z)$$
$$A_{H,y} = H(x,1,z)$$
$$A_{H,z} = H(x,y,1)$$

Estas son las deshomogeneizaciones de H en x, y y z respectivamente. Estos polinomios definen curvas planas afines que las llamaremos las **versiones afines** de X en x, y, z respectivamente. Estas curvas las denotamos $\mathcal{A}_{X,x}$, $\mathcal{A}_{X,y}$ y $\mathcal{A}_{X,z}$ respectivamente.

2.3. Aplicaciones Holomorfas entre Superficies de Riemann

Una vez definido el concepto de superficies de Riemann, interesa estudiar funciones entre ellas que preserven su estructura determindada por sus respectivos átlas complejos. Como las superficies de Riemann tienen coordenadas locales en $\mathbb{C}$, se puede definir el concepto de *ser holomorfa* de una aplicación entre dos superficies de la siguiente manera:

Definición 2.3.1 *Sean X e Y dos superficies de Riemann y $F : X \to Y$ una aplicación continua entre X e Y. Diremos que F es* ***holomorfa*** *en $x \in X$ si existen cartas $\phi_1 : U_1 \to V_1$ con $x \in U_1$ y $\phi_2 : U_2 \to V_2$ con $F(x) \in U_2$ tales que $\phi_2 \circ F \circ \phi_1^{-1}$ es holomorfa en $\phi_1(x)$. Si $W \subseteq X$ es abierto, entonces llamaremos a F una* ***aplicación holomorfa*** *en W si es holomorfa en todo punto de W.*

Se puede demostrar que componer dos aplicaciones holomorfas da como resultado una aplicación holomorfa. Recordemos que en Topología, dos espacios topológicos son *el mismo* si existe un homeomorfismo entre ellos; en estructuras algebraicas, dos espacios vectoriales, grupos o anillos son *el mismo* si existe un isomorfismo entre ellos. Aquí vamos a definir un concepto análogo para superficies de Riemann:

Definición 2.3.2 *Sean X, Y superficies de Riemann y F una aplicación de X en Y. Diremos que F es un* ***isomorfismo*** *de superficies de Riemann si F es aplicación holomorfa, biyectiva y con inversa F^{-1} holomorfa. Si existe un isomorfismo entre dos superficies de Riemann X e Y, diremos que X e Y son isomorfas. En el caso que $X = Y$, F se denomina como automorfismo de X.*

Se puede demostrar que si X es una superficie de Riemann, entonces el conjunto de todos los automorfismos de X, es un grupo con la composición. A tal grupo lo denotamos $\mathbf{Aut}(X)$.

Ejemplo 2.3.1 *Toda superficie de Riemann de género cero es isomorfa a $\hat{\mathbb{C}}$. La demostración de este hecho se puede ver en [18], página 197.*

En adelante usaremos $\hat{\mathbb{C}}$ como superficie de Riemann compacta de género cero para efectos del desarrollo de la tesis.

La siguiente proposición determina que si una aplicación holomorfa no constante tiene como dominio una superficie de Riemann compacta, su recorrido tiene que ser compacto:

Proposición 2.3.1 *Sean X e Y superficies de Riemann, con X compacta y F una aplicación holomorfa no constante entre X e Y. Entonces F es epiyectiva e Y es compacta.*

Demostración: Se puede ver en [18], página 41.

La siguiente proposición nos da una forma de como representar localmente una aplicación holomorfa no constante entre superficies de Riemann:

Proposición 2.3.2 *Sea $F : X \to Y$ una aplicación holomorfa entre superficies de Riemann y sea $x \in X$. Entonces existe un único entero positivo $m_{F,x}$ que satisface la siguiente propiedad: para toda carta $\phi_2 : U_2 \to V_2$ en Y que contiene a $F(x)$, existe una carta $\phi_1 : U_1 \to V_1$ en X que contiene a x tal que $\phi_2(F(\phi_1^{-1}(z))) = z^{m_{F,x}}$. Entonces definimos la* ***multiplicidad*** *de F en x como el número $m_{F,x}$.*

Demostración: se puede ver en [18], pág. 44-45.

Interesa discriminar la naturaleza de los puntos de una superficie de Riemann bajo un aplicación holomorfa de acuerdo a su multiplicidad. Esto se expresa en la siguiente definición:

Definición 2.3.3 *Sea $F : X \to Y$ una aplicación holomorfa no constante entre superficies de Riemann y sean $x \in X$, $y \in Y$. Si $m_{F,x} \geq 2$ entonces diremos que x es un* ***punto de ramificación*** *de F. Si y es imagen de un punto de ramificación de F entonces llamaremos a y un* ***punto rama.***

Se puede demostrar que en una aplicación holomorfa $F : X \to Y$ entre superficies de Riemann tal que Y es compacta, los puntos de ramificación F forman un subconjunto discreto de X. Para ello, veanse los detalles en [18], pág. 45. Como consecuencia de esto, los puntos rama de una aplicación holomorfa forman un subconjunto discreto del espacio de llegada, y cuando X es compacta, hay sólo un número finito de éstos.

La siguiente proposición sólo tiene sentido en aplicaciones holomorfas entre superficies de Riemann compactas:

Proposición 2.3.3 *Sea $F : X \to Y$ un aplicación holomorfa entre superficies de Riemann compactas. Para cada $y \in Y$ sea*

$$deg(F) = \sum_{x \in F^{-1}(y)} m_{f,x}.$$

Entonces $deg(F)$ es constante, independiente de y, y se denomina el ***grado*** *de F.*

Existe una fórmula que relaciona los géneros de dos superficies de Riemann compactas dada una aplicación holomorfa no constante entre ambas, la cual se conoce como la *fórmula de Riemann-Hurwitz*:

Teorema 2.3.1 *Sea $F : X \to Y$ una aplicación holomorfa no constante entre superficies de Riemann compactas. Sean $g(X)$ y $g(Y)$ los géneros de X e Y respectivamente. Entonces*

$$2g(X) - 2 = deg(F)(2g(Y) - 2) + \sum_{x \in X}(m_{F,x} - 1).$$

Demostración: ver [18], pág. 52-53.

2.4. Resolución de Singularidades

Veremos ahora como se puede construir una superficie de Riemann a partir de una curva plana afín con puntos singulares (que llamaremos también **singularidades**). El principio general se basa en la siguiente idea.

Sea X una curva plana afín en $\mathbb{C}^2$ definida por un polinomio $f(x,y)$ libre de cuadrados. Supongamos que el punto $z \in X$ es una singularidad de X. Consideremos $Y = X \backslash \{x\}$. Es un hecho que las singularidades de una curva plana afín definida por un polinomio de esa forma forman un conjunto finito (ver [13], págs. 236-237), por lo que existen abiertos U en Y que son homeomorfos a discos pinchados $D = \{x \in C | 0 < |x| < r\}$. Llamemos ϕ al homeomorfismo en cuestión. Pegamos tantos discos como sea necesario, lo que se explicará en la siguiente proposición. Así, llamamos Z al pegado topológico de X con los discos $\bar{D}$ por ϕ. Entonces repetimos el proceso con las demás singularidades y el resultado final es una superficie de Riemann que denominamos **Resolución de X**. El proceso lo denominamos **resolución de singularidades.**

Definición 2.4.1 *Sea X una curva plana afín en $\mathbb{C}^2$ definida por el polinomio $f(x,y)$. Supongamos que $z \in X$ es una singularidad. Diremos que z es de tipo **(n,m)-monomial** si existen dos series de potencias g y h centradas en z, ambas sin término constante y con factores lineales linealmente inependientes, tales que $f(x,y) = g^n - h^m$*

La siguiente proposición nos ilustra el proceso de cómo resolver una singularidad (n,m)-monomial.

Proposición 2.4.1 *Una singularidad (n,m)-monomial de una curva plana afín en $\mathbb{C}^2$ definida por un polinomio $F(x,y)$ se resuelve removiendo dicha singularidad. Esa singularidad deja exactamente (n,m) hoyos los cuales se tapan de acuerdo al proceso antes descrito.*

Demostración: se puede ver ver [18], págs. 71-72. Ahí también se describe cómo dar cartas a usa superficie de Riemann obtenida al resolver singularidades.

2.5. Acción de Grupos en Superfices de Riemann

En esta sección mencionaremoss algunos resultados sobre acciones de grupos en superficies de Riemann. Nos enfocaremos en acciones de grupos finitos, pues como veremos, las superfices de Riemann compactas sólo tienen una cantidad finita de automorfismos, además que en esos casos es fácil introducir una estructura de superficie de Riemann para superfices cocientes generadas por dichas acciones. Empezamos con la siguiente definición:

Definición 2.5.1 *Sea X una superficie de Riemann y G un grupo finito. Una* ***acción holomorfa*** *de G en X se define como un homomorfismo $\mathcal{A} : G \to \boldsymbol{Aut}(X)$. En caso de que el núcleo de la acción es trivial, la acción $\mathcal{A}$ se dice* ***efectiva.***

En la acción de un grupo en una superficie de Riemann interesa conocer cómo son los estabilizadores de cada uno de sus puntos:

Proposición 2.5.1 *Sea G un grupo finito actuando holomorfa y efectivamente en una superficie de Riemann X. Sea $x \in X$. Entonces el estabiizador de x en G, que denotamos $Stab_G(x)$, es un grupo cíclico.*

Demostración: se puede ver en [18], pág. 76.

Ahora, dada una superficie de Riemann X con acción holomorfa y efectiva de un grupo finito G, se puede dar naturalmente una estructura de superficie de Riemann al espacio cociente X_G. Para ver la construcción de ello, véase [18], págs. 77-78. Ésto se resume en el siguiente teorema:

Teorema 2.5.1 *Sea G un grupo finito actuando de forma holomorfa y efectiva en una superficie de Riemann X. Entonces X_G se puede dotar de una estructura de superficie de Riemann. Además, la aplicación cociente $\pi : X \to X_G$ es holomorfa de grado $|G|$ y $m_{\pi,x} = |Stab_G(x)|$ para todo $x \in X$.*

Como consecuencia de esto, uno puede combinar este teorema con la fórmula de Riemann-Hurwitz para producir el siguiente corolario:

Corolario 2.5.1 *Considerando la notación del teorema anterior. Sea g el género de X y g_G el género de X_G. Suponga que X es compacta y que el número de puntos rama de π es k y que los índices de ramificación son $r_1, ..., r_k$ respectivamente. Entonces X/G es compacta y:*

$$g = |G|(g_G - 1) + 1 + \frac{|G|}{2} \sum_{l=1}^{k} \left(1 - \frac{1}{r_l}\right)$$

Denotamos por $(g_G; r_1, .., r_k)$ la ***firma*** *de la acción de G en X.*

Observación 2.5.1 *Para simplificar escritura, firmas largas, como por ejemplo*

$$(3; 2,2,2,2,2,2,2,2,2,2,2,2,3,3,3,3,3,3,3,3,3,3,3,5,5,5,5,5,5)$$

se escribirán de forma reducida como $(3; 2^{(12)}, 3^{(10)}, 5^{(6)})$. *El superíndice en paréntesis indicará la cantidad de veces que se repite el número en cuestión dentro de la firma de la acción de un grupo en una superficie de Riemann compacta.*

Es un hecho importante que todo grupo finito actúa en alguna superficie de Riemann de acuerdo a una elección de generadores de dicho grupo. Para entender este resultado, introducimos la siguiente definición:

Definición 2.5.2 *Sea G un grupo finito. Sea*

$$\{a_1, ..., a_{g_G}, b_1, ..., b_{g_G}, c_1, ..., c_t\}$$

un subconjunto de G. Diremos que la tupla

$$V = (a_1, ..., a_{g_G}, b_1, ..., b_{g_G}, c_1, ..., c_t)$$

es un ***vector generador*** *de G, con firma $(g_G; m_1, ..., m_t)$ si*

- $G = \langle a_1, ..., a_{g_G}, b_1, ..., b_{g_G}, c_1, ..., c_t \rangle$
- *Para todo* $1 \leq k \leq t$, $|c_k| = m_k$
- $$\prod_{k=1}^{g_G} [a_k, b_k] \prod_{k=1}^{t} c_k = 1$$

Ahora, presentaremos el **Teorema de existencia de Superficies de Riemann** que determina que eligiendo un vector generador para un grupo, existe una superficie de Riemann compacta bajo la acción de G, y dicha acción estará determinada por el vector generador.

Teorema 2.5.2 *Sea G un grupo finito, y sea $V = (a_1, ..., a_\gamma, b_1, ..., b_\gamma, c_1, ..., c_t)$ un vector generador de G con firma $(\gamma; m_1, ..., m_t)$. Entonces existe una superficie de Riemann compacta X con acción de G y firma de la acción $(\gamma; m_1, ..., m_t)$ de modo que X/G tiene género γ y el género de X que llamamos g es:*

$$g = |G|(\gamma - 1) + 1 + \frac{|G|}{2} \sum_{j=1}^{r} \left(1 - \frac{1}{m_j}\right)$$

Demostración: una demostración de este teorema se puede encontrar en [2], pág. 239.

2.6. Curvas n-gonales

Es esta sección presentaremos un tipo especial de curvas planas o más bién de superficies de Riemann que se pueden representar vía isomorfismo como una curva plana. Se destacan por el hecho que el polinomio que la define es *simple*. Introduzcamos la definición:

Definición 2.6.1 *Sea X una superficie de Riemann compacta de género mayor o igual a 2. Diremos que X es una* ***curva n-gonal*** *si admite acción de un grupo cíclico C_n con $n > 1$ de modo que*

$$X_{C_n} \cong \hat{\mathbb{C}}$$

En ese caso, llamaremos a C_n un ***grupo n-gonal*** *para X*

La expresión algebraica para una curva n-gonal se expresa en el siguiente teorema:

Teorema 2.6.1 *Sea X una curva n-gonal con grupo n-gonal C_n. Suponga que la proyección cociente $X \to \hat{\mathbb{C}}$ tiene exactamente t puntos rama $a_1, ..., a_t$.*

1. Si ninguno de los a_l es igual a ∞ entonces X es isomorfa a la resolución de singularidades de una curva plana afín definida por la ecuación

$$y^n = \prod_{l=1}^{t} (x - a_l)^{m_l}$$

donde los m_l son números enteros positivos, determinados bajo la acción de C_n, tales que:

$$mcd(n, m_1, ..., m_t) = 1, \quad \sum_{l=1}^{t} m_l \equiv_n 0$$

donde $\equiv_n$ denota equivalencia módulo n y mcd denota el máximo común divisor de una colección finita de números..

2. si uno de los a_l, digamos a_1, es igual a ∞, entonces X es isomorfa a la resolución de singularidades de una curva plana afín definida por el polinomio

$$y^n - \prod_{l=2}^{t} (x - a_l)^{m_l}$$

donde los m_l son números enteros positivos menores a n tales que

$$mcd(n, m_2, ..., m_t) = 1, \quad n \nmid \sum_{l=2}^{t} m_l$$

Demostración:ver [9].

Esto indica que una curva n-gonal se puede definir por un polinomio de la forma $y^n - f(x)$, donde $f \in \mathbb{C}[x]$ es no constante. El polinomio f no es único, ya que trasladando los a_i por una transformación de Möbius ϕ, podemos obtener números $b_l = \phi(a_l)$ tales que $y^n - \prod_{l=1}^{t}(x - b_l)^{m_l}$ es otro polinomio que define a X como curva plana afín. La condiciones sobre f implican que éste no es una potencia d-ésima de otro polinomio para cualquier divisor d de n. Esto hace que $y^n - f(x)$ sea irreducible, y por ello, la curva plana es conexa.

En esta sección presentaremos un resultado de [29] en el cual se desarrolla un método para construir ecuaciones que definan a una curva n-gonal como una curva plana afín. Este método se concentra en el caso en que n es primo, pero se puede extender a otros casos. Previamente fijaremos cierta notación. En lo que sigue en esta sección, X es una curva n-gonal con n primo, $N = N_{Aut(X)}(C_n)$ y sea $K = N/C_n$. El grupo N lo denominamos **supergrupo normal** de C_n. El grupo K se denomina el **grupo de esfera**, pues ese grupo actúa naturalmente en X/C_n que es isomorfo a la esfera de Riemann. Consecuentemente, K es (isomorfo a) uno de los grupos finitos que actúan en $\hat{\mathbb{C}}$, los cuales se indican en la siguiente tabla con su respectivo dato de ramificación:

Grupo	Dato de Ramificación
C_k	$(k, k), k \geq 2$
D_k	$(2, 2, k), k \geq 2$
A_4	(2,3,3)
S_4	(2,3,4)
A_5	(2,3,5)

Tabla 1: Grupos finitos que actúan en la esfera de Riemann.

Supongamos que $n = p$ es primo. En [29] se establece el siguiente resultado que dice cómo encontrar una ecuación para una curva p-gonal:

Teorema 2.6.2 *Sea X una superficie cíclica p-gonal, C_p su grupo p-gonal, G el respectivo supergrupo normal, y K el grupo de esfera. Entonces X es isomorfa a la superficie definida por la ecuación:*

$$y^p = \prod_{i=1}^{r'} \prod_{j=0}^{r_i} \prod_{g \in k_0^j Ker(\mathcal{A}) \cap S_{\widehat{a}_i}} (x - g(\widehat{a}_i))^{N^j \widehat{n}_i},$$

donde los $\widehat{a}_i$ son representantes de las K-órbitas de puntos rama de π_K, b es un generador de C_p tal que como automorfismo de la curva plana,

$$b(x, y) = (x, e^{2\pi i/p} y),$$

$r_i = [K : Stab_K(\widehat{a}_i)]$, los $\widehat{n}_i$ son números entre 1 y $p-1$ tales que $\varrho(c_i) = b^{\widehat{n}_i}$, $\mathcal{A}$ es la acción por conjugación de K en $\mathbf{Aut}(C_p)$, k_0 es tal que $\mathcal{A}(k_0)$ genera $\mathcal{A}(K)$ en C_p, N es tal que $\mathcal{A}(k_0)(b) = b^N$ y para cada i se considera $\widehat{n}_i N^j$ módulo p para todo j.

Esto en principio es válido si $n = p$ es primo, dado que $\mathbf{Aut}(C_n)$ es cíclico como se usó en el Lema 2.7.3. Esto se puede extender al caso en que n es potencia de primo y la firma de la acción del grupo n-gonal es de la forma $(0; n^{(r)})$. Veremos que los grupos que nos interesan en esta tesis cumplen exactamente estas 2 condiciones.

Algunos ejemplos de curvas n-gonales se describen a continuación:

Ejemplo 2.6.1 *Una **curva hiperelíptica** es una superficie de Riemann X compacta de género g mayor o igual a 2 que admite una aplicación holomorfa $h : X \to \hat{\mathbb{C}}$ de grado 2. En [18], pág. 92, se demuestra que si X es hiperelíptica, es isomorfa a una curva algebraica de la forma*

$$y^2 = f(x)$$

*donde f es un polinomio de grado $2g+1$ ó $2g+2$ sin raices múltiples. Por lo tanto, X es una curva 2-gonal. El automorfismo 2-gonal se llama la **involución hiperelíptica**, la cual se define por*

$$\sigma(x, y) = (x, -y)$$

y es un elemento del centro de $\mathbf{Aut}(X)$ (ver [8], pág. 437).

Ejemplo 2.6.2 *Sea X la superficie de Riemann definida en $\mathbb{P}^3$ por la intersección de los lugares de ceros de los polinomios homogéneos*

$$P(x, y, z, t) = x^2 + y^2 + z^2, \;\; Q(x, y, z, t) = t^3 - xyz.$$

En [17], se establece que X es una superficie de Riemann de género 4. En [20], usando el teorema anterior, se establece que X es isomorfa a la curva plana definida por la ecuación:

$$y^3 = x^5 - x$$

Un automorfismo 3-gonal está dado por:

$$\alpha([x : y : z : t]) = [x : y : z : e^{2\pi i/3}t]$$

2.7. Curvas de Fermat

Introducimos a continuación la curva de Fermat, la cual es la base de nuestro trabajo. Esta curva tiene algunas propiedades interesantes en cuanto a su expresión algebraica y sus automorfismos.

Definición 2.7.1 *Sea $n > 2$ un entero positivo. Sea $\mathcal{F}_n$ el lugar de ceros del siguiente polinomio en $\mathbb{P}^2$:*

$$f_n(x, y, z) = x^n + y^n + z^n$$

*$\mathcal{F}_n$ se denomina la **curva de Fermat** de grado n.*

Es evidente que una expresión afin para $\mathcal{F}_n$ es $y^n = x^n + 1$ y también se puede verificar que $\mathcal{F}_n$ no es singular. Es un ejercicio estándar demostrar que el género de $\mathcal{F}_n$ es

$$g = \frac{(n-1)(n-2)}{2}$$

Además, el grupo $(\mathbb{Z}_n)^2 = \mathbb{Z}_n \times \mathbb{Z}_n$ actúa de forma natural en $\mathcal{F}_n$ mediante:

$$(r, s) \to a_{r,s}, \quad a_{r,s}([x : y : z]) = [\lambda^r x : \lambda^s y : z]$$

donde $\lambda = e^{2\pi i/n}$. Esta acción es efectiva en $\mathcal{F}_n$ (ver [28]). Sean $a = a_{1,0}$, $b = a_{0,1}$ y $c = a^{-1}b^{-1} = a_{n-1,n-1}$. Se verifica que

$$a([x : y : z]) = [x : y : z] \Leftrightarrow [\lambda x : y : z] = [x : y : z] \Leftrightarrow x = 0$$

De esta forma, se tiene que $y^n = -z^n$. Eligiendo $z = 1$, se ve que y es una raiz n-ésima de -1. En total, tenemos n puntos fijos bajo a. Para b y c también hay n puntos fijos, usando el mismo procedimiento y observando en el caso de c que

$$c([x : y : z]) = [\lambda^{n-1}x : \lambda^{n-1}y : z] = [x : y : \lambda z]$$

De esta forma vemos que la proyección cociente $\mathcal{F}_n \to (\mathcal{F}_n)_{(\mathbb{Z}_n)^2}$ tiene al menos $3n$ puntos de ramificación con multiplicidad n. Llamando g el género de dicho cociente y aplicando la fórmula de Riemann-Hurwitz se obtiene:

$$\frac{(n-1)(n-2)}{2} = n^2(g-1) + 1 + \frac{3n(n-1)}{2} + R$$

Donde R es un entero no negativo. Pero:

$$n^2(g-1) + 1 + \frac{3n(n-1)}{2} + R = n^2g - n^2 + 1 + \frac{3n^2-3)}{2} + R$$
$$= n^2g + \frac{n^2 - 3n + 2}{2} + R = n^2g + R + \frac{(n-1)(n-2)}{2}$$

De esto, tenemos que $n^2g + R = 0$, lo que obliga a que $g = R = 0$. Por lo tanto $(\mathcal{F}_n)_{(\mathbb{Z}_n)^2}$ es de género cero. Como la proyección cociente tiene $3n$ puntos de ramificación, necesariamente tiene 3 puntos rama, dado que esos forman 3 órbitas bajo la acción de $(\mathbb{Z}_n)^2$. Así, la firma de la acción de $(\mathbb{Z}_n)^2$ es $(0; n, n, n)$.

Sobre $\mathbf{Aut}(\mathcal{F}_n)$, se puede decir lo siguiente:

Teorema 2.7.1 ***Aut***$(\mathcal{F}_n)$ *es isomorfo a un producto semidirecto* $(\mathbb{Z}_n)^2 \rtimes \boldsymbol{S}_3$, *donde* $\boldsymbol{S}_3$ *es el grupo de permutaciones de tres elementos.*

Demostración: se puede consultar en [28].

De hecho, los generadores de $\mathbf{S}_3$ como automorfismos de $\mathcal{F}_n$ son:

$$\gamma([x : y : z]) = [z : x : y]$$
$$\delta([x : y : z]) = [x : z : y]$$

2.8. Jacobianas de Superficies de Riemann

En esta sección mencionaremos los conceptos básicos de las variedades Jacobianas asociadas a superficies de Riemann compactas. Más adelante haremos una descrip-

ción de la descomposición isógena de las Jacobianas de las superficies de Riemann que nos interesan, aprovechándonos de la acción de los grupos en cuestión.

Definición 2.8.1 *Sea X una superficie de Riemann compacta de género $g > 0$. La* ***variedad Jacobiana*** *de X, denotada por JX se define como el cociente $\Omega^1(X)^*/\Upsilon$ donde $\Omega^1(X)$ es el espacio de 1-formas holomorfas de X y Υ es el reticulado de su dual $\Omega^1(X)^*$ generado por los funcionales del tipo $\int_{[c]}$ que son integrales sobre algun representante de los generadores de $H_1(X)$.*

Para ver en detalle la teoría básica de variedades Jacobianas se recomienda leer el capítulo VIII de [18]. Las variedades Jacobianas son un caso particular de las llamadas variedades Abelianas:

Definición 2.8.2 *Una* ***variedad Abeliana*** *de dimensión $d > 0$ se define como un cociente $A = V/T$ donde V es un $\mathbb{C}$-espacio vectorial de dimensión d y T un subgrupo discreto de V de rango $2d$, que admite una forma Hermitiana Θ positiva definida tal que su parte imaginaria toma valores en T. A Θ se le denomina* ***Polarización*** *de A. Denotamos la dimensión de A por* $\dim(A)$.

Se puede ver que toda Jacobiana de una superficie de Riemann compacta de género mayor a cero es una variedad Abeliana. Para más información sobre variedades Abelianas, se recomienda leer [12]. Además, de una forma parecida a superficies de Riemann, a toda variedad Abeliana (en particular Jacobianas) se le puede dotar de una estructura compleja de modo que es una variedad compleja cuya dimensión topológica es la misma que su dimensión como variedad Abeliana, y en el caso de Jacobianas, igual al género de la superficie de Riemann respectiva. También las variedades Abelianas heredan la estructura de grupo del espacio vectorial que las originan, convirtiéndolas en un grupo topológico abeliano.

En general interesa ver cuándo una variedad Abeliana admite subconjuntos que también son variedades Abelianas:

Definición 2.8.3 *Sea $A = V/T$ una variedad Abeliana y Θ su polarización. Decimos que $B \subset A$ no vacío es una* ***subvariedad*** *de A si existe un subespacio W de V y un reticulado U tal que $U = W \cap T$ y $B = W/U$.*

Considerando la notación de esta definición, se puede ver que $\Theta|_B$ es una polarización para B, lo que la hace una variedad Abeliana contenida en A.

En cuanto a aplicaciones entre variedades Abelianas, se puede decir lo siguiente:

Definición 2.8.4 *Una aplicación $f : A_1 \to A_2$ entre variedades Abelianas se dice un* ***homomorfismo*** *de variedades Abelianas si es un homomorfismo de grupos y además es holomorfa como aplicación entre variedades complejas. Si además f es epiyectiva y su núcleo es finito, se dice que f es una* ***isogenia*** *entre A_1 y A_2. Si el núcleo de una isogenia f es trivial, se dice que es un* ***isomorfismo*** *y si $A_1 = A_2$, f se denomina un* ***automorfismo.***

En general no es fácil encontrar isomorfismos entre variedades abelianas pero si es más asequible obtener isogenias. Además, isogenias definen una relación de equivalencia y si dos variedades Abelianas son isógenas, deben tener la misma dimensión. Esto nos dice que una isogenia es una forma más general de isomorfismo. Se puede ver también que para toda variedad Abeliana A, el conjunto de sus automorfismos, que denotamos $\mathbf{Aut}(A)$, es un grupo. En ese sentido, podemos adaptar la definición de acción holomorfa de superficies de Riemann para variedades Abelianas. En particular, la acción de un grupo finito en una superficie de Riemann compacta se puede extender naturalmente a su variedad Jacobiana respectiva.

Relacionando el concepto de isogenia con el concepto de subvariedad y el de acción de grupo, existe un resultado que establece una descomposición salvo isogenia de una variedad Jacobiana en términos de subvariedades determinadas por las representaciones complejas irreducibles de algún grupo actuando en ella. Para ello, previamente introducimos algunas definiciones:

Definición 2.8.5 *Sea G un grupo finito. Para cada $1 \leq j \leq r$, se definen:*

1. *W_j como las representaciones racionales irreducibles de G.*

2. *V_j una representación compleja irreducible de G asociada a W_j.*

3. *$K(W_j)$ como el cuerpo obtenido al adjuntar a $\mathbb{Q}$ todos los valores del caracter de V_j en G.*

4. *m_j como el* ***índice de Schur*** *de W_j, definido como el menor entero positivo tal que existe una extensión L_j de $K(W_j)$ en que la representación se define sobre L_j.*

5. *$\boldsymbol{Fix}_{c_j}(V_j)$ como el subespacio de V_j fijo bajo $\langle c_j \rangle$.*

Con estas definiciones introducimos a continuación el **Teorema de Descomposición Isotípica** para Variedades Jacobianas.

Teorema 2.8.1 *Sea $A = JX$ para alguna superficie de Riemann X de género $g > 1$, y G un grupo finito actuando de forma holomorfa y efectiva en X. Sea $(g_G; m_1, ..., m_t)$ la firma de la acción de G y $(a_1, ..., a_{g_G}, b_1, ..., b_{g_G}, c_1, ..., c_t)$ un vector generador de*

G con dicha firma. Considerando la notación de la definición anterior. Existen subvariedades $D_1, ..., D_n$ cada una asociadas 1 a 1 a las representaciones irreducibles racionales W_j de G tales que

$$A \sim D_1^{r_1} \times ... \times D_n^{r_n}$$

Además si W_j no es trivial, la dimensión de D_j es:

$$\dim(D_j) = K(W_j) \cdot m_j \cdot \left(\dim(V_j)(g_G - 1) + \frac{1}{2} \sum_{k=1}^{t} (\dim(V_j) - \dim(\boldsymbol{Fix}_{c_j}(V_j))) \right)$$

y si W_j es trivial, la dimensión de D_j es g_G.

Demostración: se puede consultar en [21], páginas 401 y 416.

Para cualquier subgrupo H de G, la descomposición isotípica de JX_H se puede determinar conociendo la descomposición de JX. Ésto se expresa en el siguiente teorema:

Teorema 2.8.2 *Considerando la notación del teorema anterior y sea H un subgrupo. Entonces $JX \sim J(X_H) \times D_1^{t_1} \times ... \times D_n^{t_n}$ donde*

$$t_j = r_j - \frac{Dim(\boldsymbol{Fix}_H(V_j))}{sch(V_j)}$$

De esta forma, $J(X_H) \sim D_1^{r_1 - t_1} \times ... \times D_n^{r_n - t_n}$. En particular $t_j = 0$ si y sólo si H está contenido en el núcleo de V_j.

Demostración: Se puede ver en [5].

Relacionado al teorema anterior, se puede demostrar que una subvariedad de una Variedad Jacobiana A admite un complemento en el sentido que se indica en el siguiente teorema demostrado en [5]:

Teorema 2.8.3 *Considerando la notación de la proposición anterior. Para todo subgrupo H de G, existe una variedad Abeliana $P(X|X_H)$ tal que $JX \sim JX_H \times P(X|X_H)$, denominada la **variedad de Prym** de X asociada a H. Además*

$$P(X|X_H) = D_1^{t_1} \times ... \times D_n^{t_n}$$

Capítulo 3

Los grupos $G = \mathbb{Z}_{p^m} \rtimes \mathbb{Z}_{p^m}$ actuando en superficies de Riemann

En este capítulo estudiaremos el grupo de interés, $G = \mathbb{Z}_n \rtimes \mathbb{Z}_n$. Describiremos sus propiedades como grupo, en particular estudiaremos algunos subgrupos que nos interesan. Dividiremos este estudio de acuerdo a si $n = p^m$ es una potencia de primo impar o una potencia de 2, en ambos casos con $m \geq 3$. Esto es porque en cada caso se presentan diferencias estructurales en $\mathbb{Z}_n \rtimes \mathbb{Z}_n$ que deben tratarse por separado.

3.1. Propiedades de $G = \mathbb{Z}_n \rtimes \mathbb{Z}_n$

3.1.1. Caso p impar

Para definir el producto semidirecto en cuestión, notamos que para cada $1 \leq j \leq m-1$ hay una sola acción de $\mathbb{Z}_n$ en $\mathbb{Z}_n$, cuyo núcleo tiene orden p^j, y determinada por $a \to a^{r_j}$ donde $r_j = 1 + p^j$. De esta forma el grupo G tiene la siguiente presentación:

$$G = G_{n,j} = \langle a, b | a^n = b^n = 1, b^{-1}ab = a^{r_j} \rangle$$

En general omitiremos los subíndices de $G_{n,j}$ a menos de que se necesite enfatizar la dependencia de j. Es claro que si $j \neq j'$, $G_{n,j}$ no es isomorfo con $G_{n,j'}$. También es evidente que en cualquier caso, G no es abeliano.

Una primera observacion, es que el subgrupo $A = A_{n,j} = \langle a \rangle$ es normal en G para cualquier n y j. Sin embargo, el subgrupo $B = B_{n,j} = \langle b \rangle$ no es normal pues

$$aba^{-1} = ba^{r_j}a^{-1} = ba^{r_j - 1} = ba^{p^j} \notin B$$

Por simplicidad, denotaremos r_j por r a menos de que se necesite enfatizar la dependencia de j.

El siguiente lema será de utilidad en cálculos posteriores y su demostración es directa:

Lema 3.1.1 $b^{-t}ab^t = a^{r^t}$

De este lema, y el lema A.0.2 (Apéndice A) podemos obtener lo siguiente:

Corolario 3.1.1 $b^{p^{m-j}}$ *conmuta con* a

Observación 3.1.1 $(ab)^{-1}a(ab) = b^{-1}a^{-1}aab = b^{-1}ab = a^r$

Sea $C = C_{n,j} = \langle ab \rangle$. Es claro que a y b tienen orden n. Es de interés determinar el orden de ab. Para ello, demostraremos lo siguiente:

Lema 3.1.2 *Sea* $z_t = \sum_{l=1}^{t} r^l$. *Entonces,* $(ab)^t = b^t a^{z_t}$.

Demostración: Por inducción sobre t. Si $t = 1$, queda demostrado, pues por definición de G, $ab = ba^r$. Supongamos que la afirmación es válida para $t \geq 1$. La demostraremos para $t+1$

$$(ab)^{t+1} = (ab)^t(ab) = b^t a^{z_t} ba^r = b^t ba^{rz_t} a^r$$
$$b^{t+1} a^{rz_t + r}$$

Notando que $rz_t + r = z_{t+1}$, se demuestra la afirmación para $t+1$. □

De esto podemos deducir el siguiente corolario:

Corolario 3.1.2 *El elemento* ab *tiene orden* n.

Demostración: Usando el lema anterior para $t = p^{m-j}$ y el Lema A.0.3 (Apéndice A), se ve que

$$(ab)^t = b^t a^t$$

Como $b^{p^{m-j}}$ conmuta con a, al elevar ab a n, se tendrá que

$$(ab)^n = ((ab)^{p^{m-j}})^{p^j} = (b^{p^{m-j}} a^{p^{m-j}})^{p^j}$$

$$= (b^{p^{m-j}})^{p^j}(a^{p^{m-j}})^{p^j} = b^n a^n = 1 \cdot 1 = 1$$

Lo que demuestra lo pedido. □

Es de interés ver cómo se comportan los conjugados de b por potencias de a:

Lema 3.1.3 $a^t b a^{-t} = b a^{tp^i}$

Demostración: Observamos que $b^{-1}a^t b = (b^{-1}ab)^t = a^{rt}$, de lo que obtenemos que $a^t b = b a^{rt}$, y por ello:

$$a^t b a^{-t} = b a^{rt} a^{-t} = b a^{rt-t} = b a^{t(r-1)} = b a^{tp^i}. \square$$

Con consecuencia de lo anterior podemos obtener el siguiente corolario:

Corolario 3.1.3 $a^{p^{m-j}}$ *conmuta con* b.

Demostración: En el lema anterior con $t = p^{m-i}$, se tiene que:

$$a^{p^{m-j}} b a^{-p^{m-j}} = b a^{p^{m-j}p^j} = b a^n = b. \square$$

De los Corolarios 3.1.1 y 3.1.3, podemos establecer la siguiente proposición:

Proposición 3.1.1 *El centro de* G *es* $Z(G) = \langle a^{p^{m-j}}, b^{p^{m-j}} \rangle$ *y el normalizador en* G *de* B *es* $N_G(B) = \langle b, a^{p^{m-j}} \rangle$.

De la misma forma que con B, vemos que C no es normal en G, pues:

$$b^{-1}(ab)b = (b^{-1}ab)b = a^r b = b a^{r^2} \notin C$$

Ya vimos que $a^{p^{m-i}}$ conmuta con b, y por ello, conmuta con ab. De forma similar a $N_G(B)$, se puede establecer lo siguiente:

Proposición 3.1.2 $N_G(C) = \langle b, a^{p^{m-j}} \rangle$

Ahora, por definición de G, vemos que $A \cap B = \{1\}$. A continuación determinaremos las intersecciones $A \cap C$ y $B \cap C$:

Proposición 3.1.3 $A \cap C = B \cap C = \{1\}$

Demostración: Sea $x \in A \cap C$. Entonces existen t, u números naturales tales que $x = a^t = (ab)^u$, de lo que obtenemos que $a^t = b^u a^{z_t}$. Comparando ambas igualdades, vemos que $u \equiv_n 0$ y por ello, $t =_n z_t \equiv_n 0$. Por lo tanto, $x = 1$. Un argumento similar demuestra que $B \cap C = \{1\}$. □

Lema 3.1.4 *Los subgrupos B y C no son conjugados.*

Demostración: Si B y C son conjugados, existe un $a^t b^{-u} \in G$ que conjuga (ab) con alguna potencia de b, digamos b^v. Entonces si $a^t b^{-u} abb^u a^{-t} = b^v$, tenemos que $a^t b^{-u} ab^u ba^{-t} = b^v$, luego, $a^t a^{r^u} ba^{-t} = b^v$, de lo cual obtenemos que $a^{r^u} ba^{tp^j} = b^v$, y con ello, $ba^{r^{u+1}+tp^j} = b^v$. Esto nos dice que $v \equiv_n 1$ y que $r^{u+1} + tp^j \equiv_n 0$. La última igualdad implica que r es múltiplo de p, lo cual no es cierto. Por lo tanto, B no es conjugado con C. □

Sobre la serie central ascendente de G, se puede decir lo siguiente:

Proposición 3.1.4 *1. Si $j \geq m - j$, entonces la serie central de G es*

$$1 \to Z(G) \to G.$$

2. Si $j < m \quad j$ y $s = \left[\frac{m}{j}\right] \quad 1$, donde [] es la función parte entera. Entonces la serie central de G tiene $s+2$ términos. Para $2 \leq l \leq s+1$, los términos de la serie central ascendente son de la forma:

$$Z_l =< a^{p^{m-lj}}, b^{p^{m-lj}} >$$

Demostración: Sea $Z_1 = Z(G)$ y consideremos G/Z_1. Sea $\hat{x}$ la clase de un elemento $x \in G$ módulo Z_1. Observamos que $\hat{b}^{-1}\hat{a}\hat{b} = \hat{b^{-1}ab} = \hat{a}^r$. Además el orden de $\hat{a}$ y $\hat{b}$ es p^{m-i}, pues al elevar a y b a dicho número, quedan dentro de Z_1. Por lo tanto, G/Z_1 es un producto semidirecto de $< \hat{a} >$ y $< \hat{b} >$. Dependiendo de j, este grupo cociente puede ser abeliano o no:

1. Si $j \geq m - j$, entonces $p^{m-j} | p^j$ y por ello, $r = 1 + p^j \equiv_{p^{m-j}} 1$. Luego, G/Z_1 es abeliano, y así, $Z_2 = G$, completando la serie central ascendente.

2. Si $j < m - j$, Entonces $r \not\equiv_{p^{m-j}} 1$, por lo que G/Z_1 no es abeliano. Más aún, G/Z_1 es un grupo de la misma familia de G, por lo que su centro se calcula como se hizo antes, quedando como $Z(G/Z_1) = \langle \hat{a}^{p^{m-2j}}, \hat{b}^{p^{m-2j}} \rangle$. Este grupo cociente es de la forma Z_2/Z_1 con Z_2 el segundo término de la serie cental ascendente. Es claro que

$\langle a^{p^{m-2j}}, b^{p^{m-2j}} \rangle \leq Z_2$. Ahora, si $a^t b^{-u}$ está en Z_2, entonces $\hat{a}^t \hat{b}^{-u} \in Z(G/Z_1)$. Esto implica que t y u son múltiplos de p^{m-2j}, lo que demuestra que $\langle a^{p^{m-2j}}, b^{p^{m-2j}} \rangle = Z_2$.

De forma inductiva, podemos ver que los siguientes términos de la serie central tienen la forma deseada, notando que si

$$Z_l =< a^{p^{m-lj}}, b^{p^{m-lj}} >$$

es el l-ésimo término, con $l \leq s+1$, entonces $j < m-lj$, y por ello. r no es congruente a 1 módulo p^{m-lj}. Por lo tanto, G/Z_l no es abeliano y su centro es

$$Z(G/Z_l) =< \hat{a}^{p^{m-lj-j}}, \hat{b}^{p^{m-lj-j}} >= Z_{l+1}/Z_l$$

Donde Z_{l+1} es subgrupo propio y normal en G. Aplicando el mismo argumento que en el caso $l = 2$, se puede ver que Z_{l+1} tiene la forma deseada. Para verificar que el $(s+2)$-ésimo término es igual a G observamos que el orden de las clases de a y b en ese grupo cociente es $p^{m-(s+1)j}$. Por definición de s, $(s+1)j \geq m-j$, o equivalentemente $j \geq m-(s+1)j$, luego $r \equiv_{p^{m-(s+1)j}} 1$, y así, G/Z_{s+1} es abeliano. De esta forma, $Z_{s+2} = G$ concluye la serie central ascendente. □

A continuación determinaremos el conmutador de G y los términos de la serie central descendente:

Proposición 3.1.5 $[G,G] = \langle a^{p^j} \rangle$. *Sea* $\bar{s} = \bar{s}_{m,j}$ *el menor entero tal que* $\bar{s}j \geq m$. *Para todo* $1 \leq k\bar{s}$ *el término* k*-ésimo de la serie central descendente es* $G_k = \langle a^{p^{kj}} \rangle$.

Demostración: Primero calculamos $[G,G]$. Sean $x = a^s b^{-t}$ y $z = a^u b^{-v}$. Vemos que:

$$xzx^{-1}z^{-1} = a^s b^{-t} a^u b^{-v} b^t a^{-s} b^v a^{-u} = a^s b^{-t} a^u b^t b^{-v} a^{-s} b^v a^{-u}$$
$$= a^s a^{r^t u} a^{-sr^v} a^{-u} = a^{s(1-r^v)+u(r^t-1)}$$

El número $s(1-r^v) + t(r^t - 1)$ es un múltiplo de p^j, por lo que $xzx^{-1}z^{-1}$ está contenido en $< a^{p^t} >$. En particular eligiendo $s = 0$ y $u = t = 1$, se ve que $xzx^{-1}z^{-1} = a^{r-1} = a^{p^j}$. Por lo tanto, $[G,G] =< a^{p^j} >$ es cíclico. A continuación, determinamos la serie central descendiente. Sea $G_0 = G$ y recursivamente, $G_{k+1} = [G_k, G]$. Haremos el proceso por inducción sobre k. Es claro que ya está demostrado para $k = 1$. Supongamos que la proposición es válida para $1 \leq j < s$. La demostraremos para $j+1$. Sea $x = a^t b^{-u} \in G$ y $z = a^{vp^{kj}} \in G_j$. Se observa que:

$$xzx^{-1}z^{-1} = a^t b^{-u} a^{vp^{kj}} b^u a^{-t} a^{-vp^{kj}} = a^t a^{r^u vp^{kj}} a^{-t-vp^{kj}} = a^{vp^{kj}(r^u-1)}$$

El número $vp^{kj}(r^u - 1)$ es un múltiplo de $p^{(k+1)j}$, por ende, $G_{k+1} \subseteq \langle a^{p^{(k+1)j}} \rangle$. En particular, si $v = u = 1$, $vp^{kj}(r^u - 1) = p^{jk}(r-1) = p^{kj}p^j = p^{(k+1)j}$. De esta forma, $G_{j+1} =< a^{p^{(k+1)j}} >$, lo que demuestra la afirmación. □

Cuando $k = s$, $p^{sj} =_n 0$, por lo tanto $G_s = \{1\}$, y de esa manera se completa la serie central descendiente.

Por el lema 4.1.3, se puede deducir la siguiente proposición:

Proposición 3.1.6 *El subgrupo $\langle a^{p^j}, b \rangle$ es normal en G.*

Denotamos $H_l = \langle a^{p^l}, b \rangle$, $K_l = \langle a^{p^l}, ab \rangle$. Es claro que $H_{m-j} = N_G(B)$ y $K_{m-j} = N_G(C)$.

Ejemplo 3.1.1 *Consideremos G en un caso particular, con $n = 243$, es decir, $p = 3$, $m = 5$. Elegimos $r = 1 + 3^2 = 10$ $(j = 2)$. El orden multiplicativo de 10 módulo 243 es 27. Así, se tienen los generadores de los siguientes subgrupos calculados de acuerdo a la regla anterior:*

Subgrupo	*Generadores*	*Subgrupo*	*Generadores*	*Subgrupo*	*Generadores*
$N_G(B)$	b, a^{27}	Z_2	a^3, b^3	H_4	b, a^{81}
$N_G(C)$	ab, a^{27}	G_2	a^{81}	K_1	ab, a^3
$Z(G)$	a^{27}, b^{27}	H_1	b, a^3	K_2	ab, a^9
$[G, G]$	a^9	H_2	b, a^9	K_4	ab, a^{81}

Tabla 2: Subgrupos de $G_{243,2}$.

3.1.2. Caso $p = 2$

En el caso de $p = 2$, el grupo G tiene una presentación parecida a la del caso primo impar, pero nos centraremos en las acciones definidas por los números ν_j con $j \in \{1, 2, 3\}$, definidos en el Apéndice A, y listados a continuación:

$$\nu_1 = \frac{n}{2} - 1, \quad \nu_2 = \frac{n}{2} + 1, \quad \nu_3 = n - 1$$

En este caso, fijando $n = 2^m$ con $m \geq 3$, la presentación de G es de la forma

$$G = G_{n,j} = \langle a, b | a^n = b^n = 1, b^{-1}ab = a^{\nu_j} \rangle$$

Proposición 3.1.7 *Si $1 \leq j < j' \leq 3$, entonces $G_{n,j}$ y $G_{n,j'}$ no son isomorfos.*

Demostración: Demostraremos el teorema con $j = 1$ y $j' = 3$. Usamos las siguientes presentaciones para $G_{n,1}$ y $G_{n,3}$:

$$G_{n,1} = \langle a, b | a^n = b^n = 1, b^{-1}ab = a^{\nu_1} \rangle$$
$$G_{n,2} = \langle x, y | x^n = y^n = 1, y^{-1}xy = x^{\nu_3} \rangle$$

Si ambos grupos son isomorfos, entonces existe un isomorfismo que envía x e y en $a^t b^u$ y $a^k b^l$ respectivamente. Entonces, por las relaciones de los grupos, se debe verificar queda

$$(a^k b^l)^{-1}(a^t b^u)(a^k b^l) = (a^t b^u)^{\nu_3} \Rightarrow b^{-l}a^{-k}a^t b^u a^k b^l = (a^t b^u)^{n-1}$$
$$\Rightarrow b^{-l}b^u a^{(t-k)(\nu_1)^u} a^k b^l = b^{-u}a^{-t} \Rightarrow b^u a^{((t-k)(\nu_1)^u + k)(\nu_1)^l} = b^{-u}a^{-t}$$

De esto se obtiene que $2u =_n 0$, o equivalentemente, u es múltiplo de $\frac{n}{2}$. Esto implica que $((t-k)(\nu_1)^u + k)(\nu_1)^l = ((t-k)+k)(\nu_1)^l = t\nu_1^k \equiv_n -t$. Si k es par, entonces $t \equiv_n -t$, por lo que t es múltiplo de $\frac{n}{2}$. Si k es impar, entonces $t\nu_1^k = t\nu_1$, lo que implica que $t(\nu_1 + 1) \equiv_n 0$. Como $\nu_1 = \frac{n}{2} - 1$, tenemos que t debe ser par. En cualquier caso, se puede ver que $a^t b^u$ tiene orden menor a n, contradiciendo que es imagen de x. Por lo tanto, $G_{n,1}$ y $G_{n,3}$ no son isomorfos.

Para ver las restantes situaciones, las deduciremos a partir del cálculo del centro de cada uno de estos grupos, viendo que el centro de $G_{n,2}$ es de índice 4 y el de $G_{n,1}$ y $G_{n,3}$ es de índice n. □

Para estudiar este caso conviene separar los diferentes sub-casos determinados por los ν_j. De todas formas hay algunas situaciones que son comunes a los tres casos y que se demuestran de forma análoga al caso de p impar:

Lema 3.1.5 *Se tienen las siguientes identidades:*

1. $b^{-t}ab^t = a^{\nu_j^t}$
2. $a^t b a^{-t} = b a^{t(\nu_j - 1)}$
3. $(ab)^t = b^t a^{\sum_{l=1}^{t} r^l}$
4. $(ab)^{-t}a(ab)^t = a^{\nu_j^t}$

Como primera observacion, vemos que independiente de j, el subgrupo $A = \langle a \rangle$ es normal en G, y los subgrupos $B = \langle b \rangle$ y $C = \langle ab \rangle$ no son normlaes. De la misma forma que en el caso de primo impar, podemos establecer los siguientes lemas:

Lema 3.1.6 *El elemento ab tiene orden n y b^2 conmuta con a.*

Lema 3.1.7 *Los subgrupos B y C no son conjugados.*

Caso $j = 1$

Recordamos que $\nu_1 = \frac{n}{2} - 1$. Primero, calculemos $Z(G)$ y $N_G(B)$:

Proposición 3.1.8 *$Z(G) = \langle a^{\frac{n}{2}}, b^2 \rangle$ y $N_G(B) = \langle a^{\frac{n}{2}}, b \rangle$.*

Demostración: Sólo basta ver que potencias de a, digamos a^t conmuta con b o dejan fijo a B por conjugación. Del lema anterior, parte a), tenemos que $t(\nu_1 - 1) \equiv_n 0$. Como $\nu_1 - 1 = \frac{n}{2} - 2$ es un número par no divisible por 4, tenemos que t es múltiplo de $n/2$. □

El normalizador de C se calcula de la misma forma que el normalizador de B y esto se resume en lo siguiente:

Proposición 3.1.9 *$N_G(C) = \langle a^{\frac{n}{2}}, ab \rangle$*

De la misma forma que en el caso de primo impar, tenemos que $A \cap B = \{1\}$. Ademas

Proposición 3.1.10 *$A \cap C = \{1\}$, y $B \cap C = \langle b^4 \rangle$.*

Demostración: Si $x \in A \cap C$ entonces existen t, u enteros positivos pares tales que

$$x = a^t = (ab)^u = b^u a^{\frac{u(r+1)}{2}}$$

t y u deben ser pares pues $a \notin A \cap C$. Notamos que

$$\frac{r+1}{2} = \frac{2^{m-1}}{2} = 2^{m-2}$$

Volviendo a la igualdad anterior, notamos que $u \equiv_n 0$, y por ello:

$$t \equiv_n \frac{u(r+1)}{2} \equiv_n \frac{0(r+1)}{2} = 0$$

De esta forma $A \cap C = \{1\}$. Si $y \in B \cap C$, entonces, por el mismo argumento anterior, existen t, u enteros positivos pares tales que:

$$x = b^t = (ab)^u = b^u a^{\frac{u(r+1)}{2}}$$

En este caso vemos que:

$$0 =_n \frac{u(r+1)}{2} = 2^{m-2}u$$

De esta forma, u y t deben ser múltiplos de 4, lo que demuestra que $B \cap C = \langle b^4 \rangle = \langle (ab)^4 \rangle$. □

Ahora, calcularemos la serie central ascendente de G:

Proposición 3.1.11 *Para todo $2 \leq j \leq m-1$, los términos de la serie central ascendente son:*

$$Z_k = \langle a^{2^{m-k}}, b^2 \rangle$$

.

Demostración: Fijamos $Z_1 = Z(G)$ que sabemos que es $< a^{\frac{n}{2}}, b^2 >$. Consideremos G/Z_1. Sea $\hat{x}$ la clase de un elemento x de G en G/Z_1. Entonces $|\hat{a}| = \frac{n}{2}$ y $|\hat{b}| = 2$. Observamos que

$$\hat{b}^{-1}\hat{a}\hat{b} = \hat{a}^r = \hat{a}^{\frac{n}{2}-1} = \hat{a}^{-1}$$

Esto implica que G/Z_1 es isomorfo a $D_{\frac{n}{2}}$, en particular no es abeliano. El centro de ese grupo cociente es $< \hat{a}^{\frac{n}{4}}, \hat{b} >$. Sea Z_2 el segundo término de la serie central ascendente. Es claro que $\hat{a}^{2^{m-2}} = \hat{a}^{\frac{n}{2}} \in Z(G/Z_1)$. Esto implica que $< a^{2^{m-2}}, b^2 >$ está contenido en Z_1. Ahora, sea $a^t b^u$ un elemento de Z_2. Entonces $\hat{a}^t\hat{b}^u \in Z(G/Z_1)$. Pero esto implica que t es múltiplo de $n/4$, lo que demuestra la afirmación en $j = 2$.

Ahora, sea $2 \leq k < m-1$. Supongamos que la afirmación es válida para k. La demostraremos para $j+1$. Por hipótesis de inducción, $Z_k =< a^{2^{m-k}}, b^2 >$. Entonces si $\hat{x}$ denota la clase de un elemento x de G en G/Z_j, observamos que $\hat{a}$ tiene orden 2^{m-k} y b tiene orden 2. Además, como $k > 1$, $\frac{n}{2} = 2^{m-1} \equiv_{2^{m-k}} 0$. Por lo tanto:

$$\hat{b}^{-1}\hat{a}\hat{b} = \hat{a}^r = \hat{a}^{n/2-1} = \hat{a}^{-1}$$

De esta forma, $G/Z_k \simeq D_{2^{m-k}}$, en particular es no abeliano y su centro es

$$Z(G/Z_k) =< \hat{a}^{2^{m-k-1}}, \hat{b} >=< \hat{a}^{2^{m-(k+1)}}, \hat{b} >$$

Un cálculo similar al caso $j = 2$ muestra que $Z_{k+1} =< a^{2^{m-(k+1)}}, b^2 >$. □

En particular para $k = m - 1$, se tiene que $Z_{m-1} =< a^2, b^2 >$. De esta forma $[G : Z_{m-1}]$. En consecuencia, G/Z_{m-1} es abeliano, y por lo tanto, $Z_m = G$ finaliza la serie central ascendente.

Proposición 3.1.12 $[G, G] = \langle a^2 \rangle$.

Demostración: Sean $x = a^s b^{-t}$ y $z = a^u b^{-v}$. De la misma forma que el caso primo impar, se ve que:

$$xzx^{-1}z^{-1} = a^{s(1-r^v)+u(r^t-1)} = a^{\mu}$$

Se puede ver que μ es par. Además si t y v son impares,

$$s(1-r^v) + u(r^t - 1) \equiv_n s(1-r) + u(r-1) = (r-1)(u-s) = (2^{m-1} - 2)(u-s)$$

En particular con $(u - s)$ igual al inverso multiplicativo de $2^{m-2} - 1$ módulo n, tenemos que $\mu = 2$. □

Ahora, calculemos la serie central descendente de G, llamando sus términos como G_k, y fijando $G_1 = [G, G]$:

Proposición 3.1.13 *Para todo* $2 \leq k \leq m$, *se tiene* $G_k = \langle a^{2^k} \rangle$

Demostración: Por inducción sobre k. Sea $x = a^t b^{-u} \in G$. Primero, vemos el caso $k = 2$. Sea $z = a^{2v} \in G_1$. Se ve que

$$xzx^{-1}z^{-1} = a^t b^{-u} a^{2v} b^u a^{-t} a^{-2v} = a^t a^{\nu_1^u 2v} a^{-t-2v} = a^{2v(\nu_1^u - 1)}$$

Si u es impar, $2v(\nu_1^u - 1) \equiv_n 2v(\nu_1 - 1)$, termimo que será múltiplo de 4. Con esto, concluimos que $G_2 =< a^{2^2} >$.

Supongamos que la afirmación es válida para $2 \leq k < m$. La probaremos para $k + 1$. Luego, si $a^{2^k v} \in G_j$, se tiene que:

$$xzx^{-1}z^{-1} = a^t b^{-u} a^{2^k v} b^u a^{-t} a^{-2^k v} = a^t a^{\nu_1^u 2^k v} a^{-t-2^k v} = a^{2^k v(\nu_1^u - 1)}$$

Con esto, vemos que si u es impar. el número $2^k v(\nu_1^u - 1)$ es un múltiplo de 2^{k+1}. Por lo tanto, $G_{k+1} =< a^{2^{k+1}} >$. En particular, $G_m = \{1\}$, completando así la serie central descendente. □

Ejemplo 3.1.2 *Consideremos G en un caso particular, con $n = 16$, es decir, $m = 4$. Elegimos $r = 2^3 - 1 = 7$. Así, se tienen los siguientes subgrupos calculados de acuerdo a la regla anterior:*

Grupo	*Generadores*	*Grupo*	*Generadores*	*Grupo*	*Generadores*
$N_G(B)$	b, a^8	$N_G(C)$	ab, a^8	Z_3	a^2, b^2
$B \cap C$	b^4	$Z(G)$	a^8, b^2	G_2	a^4
$[G, G]$	a^2	Z_2	a^4, b^2	G_3	a^8

Tabla 3: Subgrupos de $G_{16,1}$.

Caso $j = 2$

Recordamos que $\nu_2 = \frac{n}{2} + 1$. Primero, calculamos $Z(G)$:

Proposición 3.1.14 $Z(G) = \langle a^2, b^2 \rangle$

Demostración: Sabemos que $b^2 \in Z(G)$. Veamos que potencia de a conmuta con b. Por el lema 4.2.1, parte b), se tiene que $a^t b a^{-t} = b a^{t(\nu_2 - 1)} = b a^{t(\frac{n}{2})}$. De esto se deduce que $a^t \in Z(G)$ si y sólo si t es múltiplo de 2. En particular, si $t = 2$ se cumple dicha afirmación. □

Notamos que $|G/Z(G)| = 4$, por lo tanto es un grupo abeliano. De esta forma, la serie central ascendente tiene sólo 2 términos, $Z(G)$ y G.

Con los cálculos antes hechos podemos determinar $N_G(B)$, y de forma análoga, $N_G(C)$. Esto se resume en la siguiente proposición:

Proposición 3.1.15 $N_G(B) = \langle a^2, b \rangle$ *y* $N_G(C) = \langle a^2, ab \rangle$

Determinamos ahora las intersecciones $A \cap C$ y $B \cap C$.

Proposición 3.1.16 $A \cap C = B \cap C = \{1\}$

Demostración: Para calcular $A \cap C$, notamos que si $(ab)^t = a^u$, entonces $b^t a^{t(\nu_1+1)/2} = a^u$. Esto nos dice que $t \equiv_n 0$ y de esta forma $u \equiv_n 0$. Por lo tanto $A \cap C = \{1\}$. Para ver $B \cap C$, observamos que si $b^t = (ab)^u$, entonces t y u deben ser

pares pues $ab \notin B$, luego $b^t = b^u a^{u(\nu_2+1)/2}$. Como $(\nu_2+1)/2$ es impar, se tiene que $u \equiv_n t \equiv_n 0$. Por lo tanto, $B \cap C = \{1\}$. □

La siguiente proposición se demuestra de forma similar a casos anteriores.

Proposición 3.1.17 $[G, G] = \langle a^{n/2} \rangle$

Este grupo es de orden 2, por lo tanto, la serie central descendente es:
$G \to [G, G] \to \{1\}$.

Ejemplo 3.1.3 *Sea $n = 16$, es decir $m = 4$. Entonces $\nu_2 = 9$. La tabla de subgrupos es la siguiente:*

Grupo	*Generadores*	*Grupo*	*Generadores*
$N_G(B)$	b, a^2	$Z(G)$	a^2, b^2
$N_G(C)$	ab, a^2	$[G, G]$	a^8

Tabla 5: Subgrupos de $G_{16,2}$.

Caso $j = 3$

Recordamos que $\nu_3 = n - 1$. Calculamos los subgrupos de G de la misma forma que los casos anteriores. Empezamos por $Z(G)$, $N_G(B)$ y $N_G(C)$. Usando las mismas ideas de casos anteriores, si a^t conmuta con b, se tiene que cumplir que:

$$t(\nu_3 - 1) = t(2^m - 2) = 2t(2^{m-1} - 1)$$

Por lo que nuevamente t es múltiplo de $n/2$. Así tenemos la siguiente proposición:

Proposición 3.1.18 $Z(G) = \langle a^{\frac{n}{2}}, b \rangle$, $N_G(B) = \langle a^{\frac{n}{2}}, b \rangle$ *y* $N_G(C) = \langle a^{\frac{n}{2}}, ab \rangle$

Para las intersecciones $A \cap C$ y $B \cap C$, se pueden usar las mismas ideas que en casos anteriores y se resume en lo siguiente:

Proposición 3.1.19 $A \cap C = \{1\}$ *y* $B \cap C = \langle b^2 \rangle = \langle (ab)^2 \rangle$.

Para ver la serie central ascendente de G, vemos que se repiten esencialmente los mismos cálculos del caso $j = 1$. Por lo tanto, se tiene que:

Proposición 3.1.20

$$Z_k = \langle a^{\frac{n}{2^k}}, b^2 \rangle$$

El cálculo de $[G, G]$ y la serie central descendente es similar a los casos anteriores y se resume en lo siguiente:

Proposición 3.1.21 *$[G, G] = \langle a^2 \rangle$ y para todo $2 \leq j \leq n$, $G_j = \langle a^{2^j} \rangle$*

Ejemplo 3.1.4 *Consideremos $n = 32$ y $r = 31$, es decir, $m = 5$. La tabla de subgrupos es la siguiente*

Grupo	*Generadores*	*Grupo*	*Generadores*
$N_G(B)$	b, a^{16}	$N_G(C)$	ab, a^{16}
$B \cap C$	b^2	$Z(G)$	a^{16}, b^2
$[G, G]$	a^2	Z_2	a^8, b^2
Z_3	a^4, b^2	Z_4	a^2, b^2
G_2	a^4	G_3	a^8
G_4	a^{16}	N_1	b, a^8
N_2	b, a^4	N_3	b, a^2

Tabla 5: Subgrupos de $G_{32,3}$.

3.2. Realización de $G = \mathbb{Z}_n \rtimes \mathbb{Z}_n$ como grupo de automorfismos de una superficie de Riemann

En esta sección, determinaremos una superficie de Riemann con acción de G, aplicando el Teorema de Existencia de Riemann mediante un vector generador del tipo $(0; n, n, n)$. También determinaremos los géneros y firmas de la acción de ciertos subgrupos de G. Nuevamente dividiremos el desarrollo de este capítulo de acuerdo a si n es potencia de primo impar o de 2. Primero, daremos la siguiente definición:

Definición 3.2.1 *Sea S una superficie de Riemann compacta de género positivo y sea $n \geq 3$ un entero. Diremos que S es una* ***Curva de Tipo Fermat de grado n*** *si tiene acción de un grupo Γ de orden n^2 tal que*

1. $S_\Gamma \cong \hat{\mathbb{C}}$
2. *La firma de Γ es $(0; n, n, n)$*

Llamaremos a Γ el ***grupo asociado a S***

Ejemplo 3.2.1 *Toda curva de Fermat de grado $n \geq 3$ es una curva de tipo Fermat.*

El género de una curva de tipo Fermat se puede calcular usando la fórmula de Riemann-Hurwitz:

Lema 3.2.1 *Sea S una curva de tipo Fermat de grado n con grupo asociado Γ. El género de S es:*

$$g_S = \frac{(n-1)(n-2)}{2}$$

Demostración: Aplicando el Teorema 2.5.2. se tiene que:

$$g_S = n^2(0-1) + 1 + \frac{|G|}{2}3\left(1 - \frac{1}{n}\right) = -n^2 + 1 + \frac{3n^2 - 3n}{2} = \frac{n^2 - 3n + 1}{2}$$

Como $n^2 - 3n + 2 = (n-1)(n-2)$, se demuestra la afirmación. □

Ejemplo 3.2.2 *Para el caso de $G = \mathbb{Z}_n \rtimes \mathbb{Z}_n$, éste admite a $(a, b, (ab)^{-1})$ como vector generador con firma $(0; n, n, n)$. Por el teorema de Existencia, existe una superficie de Riemann $\mathcal{X}$ con acción de G y firma la antes indicada. Por lo tanto, $\mathcal{X}$ es una curva de tipo Fermat de grado n y su género es:*

$$\frac{(n-1)(n-2)}{2}$$

Una vez determinada la existencia de esta superficie de Riemann $\mathcal{X}$, queremos determinar los géneros de los cocientes de $\mathcal{X}$ por subgrupos de G. Para ello, presentaremos la siguiente proposición:

Teorema 3.2.1 *Recordando la notación del Teorema 2.5.2, sea S una superficie de Riemann compacta con acción de un grupo Γ, $V = (a_1, ..., a_{g_\Gamma}, b_1, ..., b_{g_\Gamma}, c_1, ..., c_t)$ un vector generador de G para dicha acción con firma $(g_G; m_1, ..., m_t)$. Sea $H_j = \langle c_j \rangle$, y sea H un subgrupo de Γ. Entonces el género de S_Γ es:*

$$g_H = [\Gamma : H](g_G - 1) + 1 + \frac{1}{2}\sum_{j=1}^{t}([\Gamma : H] - |H\backslash\Gamma/H_j|)$$

donde el número $|H\backslash\Gamma/H_j|$ es el cantidad de clases dobles H y H_j de Γ.

Demostración: se puede ver en [21], págs. 402-404

Para nuestro caso, fijamos $H_1 = A = \langle a \rangle$, $H_2 = B = \langle b \rangle$, $H_3 = C = \langle ab \rangle$. Esto lo usaremos durante el desarrollo de la siguiente sección. Primero, notamos que para cualquier caso de n se tiene lo siguiente:

Proposición 3.2.1 *La superficie cociente $\mathcal{X}_A$ tiene género cero.*

Demostración: Como A es normal en G, se establece que:

$$|A\backslash G/A| = [G : A] = n$$
$$|A\backslash G/B| = [G : AB] = 1$$
$$|A\backslash G/C| = [G : AC] = 1$$

Luego, como $g_G = 0$, aplicando el Teorema 4.0.1. se tiene:

$$g_A = [G : A](\gamma - 1) + 1 + \frac{1}{2}\sum_{j=1}^{r}([G : A] - |A\backslash G/H_j|)$$

$$= -n + 1 + \frac{1}{2}(3n - n - 1 - 1) = -n + 1 + \frac{1}{2}(2n - 2) = -n + 1 + n - 1 = 0.\square$$

Como consecuencia de esta proposición, $\mathcal{X}$ es n-gonal, por lo tanto, es isomorfa a una curva plana afín determinada por una ecuación de la forma $y^n = f(x)$. En el Capítulo 4 determinaremos una ecuación para $\mathcal{X}$ como curva plana afín n-gonal. Respecto a los cocientes de $\mathcal{X}$ por los subgrupos de A, tenemos la siguiente proposición:

Proposición 3.2.2 *Sea $A_k = \langle a^{p^k} \rangle$. Para todo $1 \leq k \leq m-1$, el género de $\mathcal{X}_{A_k}$ es:*

$$g_{A_k} = \frac{(n-2)(p^k - 1)}{2}$$

Demostración: De la misma forma que con A, se puede ver que:

$$|A_j\backslash G/A| = [G : A] = n$$
$$|A_j\backslash G/B| = [G : A_jB] = p^k$$
$$|A\backslash G/C| = [G : A_jC] = p^k$$

Asi, aplicando el Teorema 4.0.1, obtenemos que:

$$g_A = [G : A_j](g - 1) + 1 + \frac{1}{2}\left(\sum_{j=1}^{r}([G : A] - |A_j\backslash G/H_j|\right)$$

$$= -np^k + 1 + \frac{1}{2}(3np^k - n - 2p^j) = \frac{np^k - n - 2p^k + 2}{2} = \frac{(n-2)(p^k - 1)}{2}.\square$$

Ahora calcularemos los géneros de los cocientes intermedios de $\mathcal{X}$ por otros subgrupos de G. Nos ocuparemos de cada caso particular, si p es 2 o impar, dado que

como se vió antes, G tiene propiedades distintas de acuerdo a tales casos. Previamente mencionaremos un lema y una teorema que nos servirán en algunos cálculos dentro de este capítulo.

Lema 3.2.2 *Sea G un grupo y H y K subgrupos de G. Entonces para todo x en G:*

$$x(H \cap K)x^{-1} = (xHx^{-1}) \cap (xKx^{-1})$$

Teorema 3.2.2 *Sea G un grupo y H, K subgrupos de G. Entonces:*

$$|H\backslash G/K| = \frac{[N_G(K) : K]}{|H|} \left(\sum_{x \in \Phi} |xKx^{-1} \cap H| \right)$$

donde Φ es un conjunto de representantes de las clases lateales derechas de $N_G(K)$ en G.

Demostración: La demostración del lema es directa. Para la demostración del teorema, consúltese en [21], pág. 403.

3.2.1. Géneros de Cocientes intermedios de $\mathcal{X}$, caso p impar

En esta subsección nos ocuparemos de calcular los cocientes intermedios de $\mathcal{X}$ por subgrupos de interés vistos en la sección anterior, en el caso p impar.

Proposición 3.2.3 *Para los subgrupos B y C:*

$$g_B = g_C = \frac{1}{2}(n - ((p-1)p^{j-1}(m-i) + p^j))$$

Demostración: En este caso, vemos que por normalidad de A, $|B\backslash G/A| = 1$. Para calcular $|B\backslash G/B|$ haremos un procedimiento distinto. Observamos que si $x = a^t b^v$ es un elemento de G, y consideramos BxB, entonces esa clase doble es la misma que Ba^tB. Por lo tanto, toda clase doble en $|B\backslash G/B|$ se representa por elementos de A. Además si a^t y a^v están en la misma clase doble, entonces existen l y s enteros tal que $b^{-l}a^t b^s = a^v$, de lo que deducimos que $b^{-l}a^t b^l b^{s-l} = a^v$, y con ello, $a^{tr^l}b^{s-l} = a^v$. Ésto nos dice que $s \equiv_n l$ y $v \equiv_n tr^l$. De esta forma se ve que si k es un número relativamente primo con p, se tiene que los elementos de la forma a^{kr^l} con $0 \leq l \leq p^{m-j}-1$ están dentro de la misma clase lateral doble Ba^kB y así los múltiplos de a con exponentes relativamente primos a p se dividen en diferentes clases laterales para distintos k. Así mismo, siguendo con k relativamente primo a p, los elementos de la forma a^{kpr^j} con $0 \leq l \leq p^{m-j-1} - 1$ están dentro de la misma clase doble

y así los elementos múltiplos de a con exponentes divisibles por p y no divisibles por potencias mayores se descomponen en diferentes clases. Este proceso ocurre de manera análoga con los $a^{kp^j r^i}$ hasta llegar a $j = m - j - 1$. Además, el neutro de G forma su propia clase doble aparte de las anteriores. Estas clases laterales dobles son disjuntas, pues si a^{p^l} está en la misma clase que a^{p^s}, existe un k tal que $r^k p^l$ es congruente a p^s, lo que implica que $k = 0$ y $l = s$.

Para cada $0 \leq l \leq m - j - 1$, hay exactamente $p^{m-j-1}(p-1)$ multiplos de p^l no divisibles por potencias mayores de p. Éstos se descomponen en órbitas bajo la acción por multilpicación de r. Se observa además que:

$$kp^l r^{p^{m-j-l}} = kp^l(1+p^i)^{p^{m-j-l}} = kp^l(1+p^{m-j-l}p^l + \varepsilon)$$

donde ε es múltiplo de n. Con esto, se ve que $kp^l r^{p^{m-j-l}}$ es congruente a kp^l módulo n, y por lo tanto, cada órbita contiene p^{m-j-l} elementos. Dividiendo, tenemos exactamente $p^{j-1}(p-1)$ clases para cada $0 \leq k < p^{m-j}$. En el caso de los kp^l, con $l \geq m - i$ estos son invariantes por r módulo n, pues

$$kp^l(1+p^j) = kp^l + kp^{j+l} \equiv_n kp^l$$

por lo tanto, para cada l tenemos exactamente $p^{m-j-1}(p-1)$ clases. Contando también la clase doble determinada por el neutro de G, tenemos que:

$$|B\backslash G/B| = 1 + (p-1)p^{j-1}(m-i) + (p-1)\sum_{l=m-j}^{m-1} p^{m-l-1}$$

Cambiando de variables en la sumatoria podemos reescribir esa suma como:

$$|B\backslash G/B| = 1 + (p-1)p^{j-1}(m-j+1) + (p-1)\sum_{l=1}^{i} p^{l-1}$$

$$1 + (p-1)p^{j-1}(m-j) + p^j - 1 = (p-1)p^{l-1}(m-j) + p^j$$

Para calcular $|B\backslash G/C|$ vemos que

$$|BC| = \frac{|B||C|}{|B \cap C|}$$

Como $B \cap C = \{1\}$, tenemos que $BC = G$. Luego, sólo hay una clase doble de B con C en G. Por lo tanto $|B\backslash G/C| = 1$. De esta manera, g_B es igual a:

$$g_B = -n + 1 + \frac{1}{2}(3n - 1 - ((p-1)p^{j-1}(m-i) + p^j) - 1)$$
$$= \frac{1}{2}(n - ((p-1)p^{j-1}(m-i) + p^j))$$

Finalmente calculamos g_C. Primero notamos que:

$$(ab)^{-1}a(ab) = b^{-1}a^{-1}aab = b^{-1}ab = a^r$$

De esta forma, el cálculo de $|B\backslash G/B|$ es similar al de $|C\backslash G/C|$, y por ello, $|B\backslash G/B| = |C\backslash G/C|$. Además, Es claro que $|C\backslash G/B| = |C\backslash G/A| = 1$. Por lo tanto, $g_B = g_C$. □

Ahora, obtendremos los géneros de cocientes intermedios de los subgrupos de B y C, que denotamos:

$$B_k = \langle b^{p^k} \rangle, \quad C_k = \langle (ab)^{p^k} \rangle$$

Proposición 3.2.4 *Para todo $1 \leq k \leq m-1$, los géneros de $\mathcal{X}_{B_k}$ y $\mathcal{X}_{C_k}$ son:*

$$g_{B_k} = g_{C_k} = \begin{cases} \frac{np^k - 2p^k - ((p-1)p^{j+k-1}(m-j-k)+p^j)+2}{2} & k < m-j \\ \frac{(n-2)(p^k-1)}{2} & k \geq m-j \end{cases}$$

Demostración: Es claro que $|B_k| = |C_k| = p^{m-k}$. Veamos g_{B_k}. Primero, conviene hacer la separación en si k es menor, igual o mayor a $m-j$, pues en la segunda y tercera situaciones, $B_k \subseteq Z(C)$.

Fijamos $k < m-j$. En ese caso, observamos que por normalidad de A,

$$|B_k\backslash G/A| = [G : B_k A] = p^k$$

Para calcular $|B_j\backslash G/B|$, podemos usar la misma idea que con $|B_k\backslash G/B|$. Observamos que si $x = a^t b^v$ es un elemento de G, y consideramos $B_k x B$, entonces esa clase doble es la misma que $B_k a^t B$. Por lo tanto, toda clase lateral doble en $|B_k\backslash G/B|$ se representa por elementos de A. Además si a^t y a^v están en la misma clase doble, entonces existen l y s enteros tal que $b^{-lp^k}a^t b^s = a^v$. lo que implica que $a^t b^{lp^k} b^{s-lp^k} = a^v$, y por ende, $a^{tr^{lp^k}} b^{s-lp^k} = a^v$. Esto nos dice que $s \equiv_n lp^j$ y $v \equiv_n tr^{lp^j}$. De esta forma, se da una situación parecida con $|B\backslash G/B|$. Si k es un número realtivamente primo con p, se tiene que los elementos de la forma $a^{kr^{lp^j}}$ con $0 \leq l \leq p^{m-i-j}-1$ están dentro de

la misma clase doble $B_j a^k B$ y y así los múltiplos de a con exponentes relativamente primos a p se dividen en diferentes clases dobles para distintos k. Así mismo, fijando $1 \leq t \leq m-j-k-1$ siguiendo con u relativamente primo a p, los elementos de la forma $a^{up^t r^l}$ con $0 \leq l \leq p^{m-j-k-t} - 1$ están dentro de la misma clase doble y así los elementos múltiplos de a con exponentes divisibles por p y no divisibles por potencias mayores se descomponen en diferentes clases. Repetimos este proceso con los $a^{up^t r^l}$ hasta llegar a $t = m-j-1$. Además, vemos que el neutro de G forma su propia clase doble aparte de las anteriores.

Para cada $0 \leq t \leq m-j-k-1$, hay exactamente $p^{m-j-k-t}(p-1)$ multiplos de p^t no divisibles por potencias mayores de p. Éstos se descomponen en órbitas bajo la acción por multilpicación de r. Se observa además que:

$$up^t r^{p^{m-j-k-t}} = up^k(1+p^j)^{p^{m-j-k}} = up^(1 + p^{m-j-k}p^j + \kappa)$$

donde κ es múltiplo de n. Con esto, se ve que $up^t r^{p^{m-j-k-t}}$ es congruente a up^t módulo n, y por lo tanto, cada órbita contiene $p^{m-j-k-t}$ elementos. Dividiendo, tenemos exactamente $p^{j+k-1}(p-1)$ clases para cada $0 \leq t < m-j-k$. En el caso de los up^t, con $t \geq m-j-k$ estos son invariantes por r módulo n. Para cada t tenemos exactamente $p^{m-1-t}(p-1)$ clases. Contando la clase del neutro de G, tenemos que:

$$|B_k \backslash G / B| = 1 + (p-1)p^{j+k-1}(m-j-k+1) + (p-1)\sum_{t=m-j-k}^{m-1} p^{m-t-1}$$

Nuevamente, cambiando de variables en la sumatoria podemos reescribir esa suma como:

$$|B_k \backslash G / B| = 1 + (p-1)p^{j-1}(m-j-k) + (p-1)\sum_{t=1}^{j+k} p^{t-1}$$

$$1 + (p-1)p^{j+k-1}(m-j-k) + p^{j+k} - 1 = (p-1)p^{j+k-1}(m-j-k) + p^{j+k}$$

Ahora, para calcular $|B_k \backslash G / C|$ resulta conveniente usar la fórmula del Teorema 3.2.2:

$$|H \backslash G / K| = \frac{[N_G(K) : K]}{|H|}\left(\sum_{x \in \Phi} |xKx^{-1} \cap H|\right)$$

donde Φ es un conjunto de representantes de las clases lateales derechas de $N_G(K)$ en G. Usaremos $H = B_k$ y $K = C$. Ya sabemos que $N_G(C) =< ab, b^{p^{m-j}} >$. Por lo tanto, $[N_G(C) : C] = p^j$. Sabemos además que $|B_j| = p^{m-j}$. Elegiremos

$$\Phi - \{b^t, 0 \leq t \leq m-j-1\}$$

Es claro que Φ es un conjunto de representantes de clases laterales derechas de $N_G(C)$ en G. Ese conjunto tiene cardinalidad p^{m-j}. Como $B \cap C = \{1\}$, se tiene que $B_k \cap C = \{1\}$ y usando el lema 3.2.2:

$$\{1\} = b^l(C \cap B_k)b^{-l} = (b^l C b^{-l}) \cap b^l B_k b^{-l} = (b^l C b^{-l}) \cap B_k$$

Así, usando el Teorema 3.2.2 vemos que:

$$|B_k \backslash G / C| = \frac{[N_G(K) : K]}{|H|}(\sum_{x \in \Phi} |xCx^{-1} \cap B_k|)$$

$$= \frac{p^j}{p^{m-k}}(1 + ... + 1) = \frac{p^j}{p^{m-k}}(p^{m-j}) = p^k$$

Y con ello, usando el Teorema 3.2.1, el género de $\mathcal{X}_{B_k}$ es

$$g_{B_k} = -np^k + 1 + \frac{1}{2}(3np^k - 2p^k - ((p-1)p^{j+k-1}(m-j-k) + p^{j+k}))$$

$$= \frac{1}{2}(np^k - 2p^k - ((p-1)p^{j+k-1}(m-j-k) + p^j) + 2)$$

En el caso de que $j \geq m-j$, $B_j \subseteq Z(G)$. Usando ideas similares al cálculo de g_{A_k} se puede verificar que $g_{B_k} = g_{A_k}$.

Para el caso de C_k, se tiene una situación parecida con B_k debido a que $(ab)^{-1}a(ab) = a^r$. De esta forma, vemos que $g_{B_k} = g_{C_k}$ para todo $1 \leq k \leq m-1$. □

Proposición 3.2.5 *El género de $\mathcal{X}_{Z(G)}$ es*

$$g_{Z(G)} = \frac{(p^{m-j}-1)(p^{m-j}-2)}{2}$$

Recordemos que $Z(G) = \langle a^{p^{m-j}}, b^{p^{m-j}} \rangle$. Este subgrupo es normal en G, por lo tanto:

$$|Z(G)\backslash G/A| = [G : AZ(G)] = \frac{|G|}{|AZ(G)|} = \frac{n^2}{np^j} = p^{m-j}$$

Por analogía a este cálculo:

$$|Z(G)\backslash G/B| = [G : BZ(G)] = p^{m-j}$$
$$|Z(G)\backslash G/C| = [G : CZ(G)] = p^{m-j}$$

Por lo tanto, $g_{Z(G)}$ es:

$$g_{Z(G)} = -p^{2(m-j)} + 1 + \frac{3p^{2(m-j)} - 3p^{m-j}}{2} = \frac{p^{2(m-j)} - 3p^{m-j} + 2}{2}$$
$$= \frac{(p^{m-j} - 1)(p^{m-j} - 2)}{2} \square$$

Observación 3.2.1 *Notamos, que en el caso $j \geq m - j$, $G/Z_1 \cong \mathbb{Z}_{p^{m-j}} \times \mathbb{Z}_{p^{m-j}}$. Este grupo actúa en $\mathcal{X}_{Z_1}$ que tiene género igual a*

$$\frac{(p^{m-j} - 1)(p^{m-j} - 2)}{2}$$

Esto dice que $\mathcal{X}_{Z_1}$ es un candidato a ser una curva clásica de Fermat, de grado p^{m-j}. En caso de ocurrir, tendríamos que $\mathcal{X}$ es un cubriente ramificado de una curva clásica de Fermat.

De la misma forma que con $Z(G)$, se puede demostrar lo siguiente:

Proposición 3.2.6 *Si $j < m-j$, y s es el mayor entero tal que $sj < m-j$, entonces los géneros de $\mathcal{X}_{Z_k}$ para $2 \leq k \leq s+1$, son:*

$$g_{Z_k} = \frac{(p^{m-kj} - 1)(p^{m-kj} - 2)}{2}$$

Observación 3.2.2 *En el caso particular de Z_{t+1}, se observa, de forma parecida al caso $j > m - j$, que $\mathcal{X}_{Z_{t+1}}$ es una candidato a ser una curva clásica de Fermat. También obsvervamos, de forma similar, que los cocientes de $\mathcal{X}$ por los términos anteriores de la serie central ascendente son candidatos a ser curvas de Tipo Fermat.*

Los géneros de los cocientes por los miembros de las serie central descendente se pueden obtener usando lo antes calculado con A_j, dado que $G_t = A_{tj}$:

Proposición 3.2.7 *Para $1 \leq k \leq s$, donde s es el menor entero tal que $sj \leq m$, los géneros de $\mathcal{X}_{G_k}$, y en particular de $\mathcal{X}_{[G,G]}$ son:*

$$g_{G_t} = \frac{(p^{tj}-1)(p^m-2)}{2}, \quad g_{[G,G]} = \frac{(p^j-1)(p^m-2)}{2}$$

Proposición 3.2.8 *Para todo $1 \leq l \leq m-1$, los géneros de $\mathcal{X}_{H_l}$ y $\mathcal{X}_{K_l}$ son:*

$$g_{H_l} = g_{K_l} = \begin{cases} 0 & si \quad l \leq j \\ \frac{(p^l-((p-1)p^{j-1}(m-j)+p^j))}{2} & si \quad l > j \end{cases}$$

Demostración: Si $l \leq j$, es evidente que H_l es normal en G, por lo tanto:

$$|H_k \backslash G/A| = |H_k \backslash G/C| = 1$$
$$|H_k \backslash G/B| = p^l$$

Asi, aplicando el Teorema 3.2.1, se tiene:

$$g_{H_l} = -p^l + 1 + \frac{3p^l - 1 - p^l - 1}{2} = 0$$

Si $l > j$, entonces, aplicamos una idea similar a la usada antes con $|B\backslash G/B|$ calcular $|H_k\backslash G/B|$, notando que nuevamente toda clase doble $H_l x B$ se puede representar con un elemento de A. Aún más, ese elemento de A se puede elegir como a^u con $0 \leq u < p^l$ y que si $x \in H$, $b^t \in B$, y a^u, $a^v \in A$, con $0 \leq u, v < p^l$ entonces $xa^u b^t = a^v$ es equivalente a que $a^v b^{n-t} a^{-u} \in H_l$ y a su vez con que $vr^{n-v} \equiv_{p^l} u$. De esta forma, usando un procedimiento similar al cálculo de $|B\backslash G/B|$, podemos obtener que:

$$|H_k \backslash G/B| = p^j + p^{j-1}(p-1)(l-j)$$

Para calcular $|H_k\backslash G/C|$, simplemente notamos que $H_l C$ contiene a BC, el cual ya sabemos que es todo G. Por lo tanto, $|H_k\backslash G/C| = 1$. Aplicando el Teorema 3.2.1, llegamos a lo deseado. □

Como consecuencia de esta proposición, tenemos el siguiente corolario:

Corolario 3.2.1 *Los géneros de $\mathcal{X}_{N_G(B)}$ y $\mathcal{X}_{N_G(B)}$ son:*

$$g_{N_G(B)} = g_{N_G(C)} = \begin{cases} 0 & si \quad m-j \leq j \\ \frac{(p^{m-j}-((p-1)p^{j-1}(m-j)+p^j))}{2} & si \quad m-j > j \end{cases}$$

3.2.2. Géneros de Cocientes intermedios de $\mathcal{X}$, caso $p = 2$

Como antes, dividimos los casos dependiendo de j

Caso $j = 1$

Recordamos que $\nu_1 = \frac{n}{2} - 1$.

Proposición 3.2.9 *Los géneros de $\mathcal{X}_B$ y $\mathcal{X}_C$ son:*

$$g_B = g_C = \frac{n}{8}$$

Demostración: Claramente, $|B\backslash G/A| = 1$. Para calcular $|B\backslash G/B|$ se procede de la misma forma que en el caso primo impar. Entonces, toda clase doble BxB está representada por un elemento de A. Dos elementos de A, digamos a^s y a^t, representan la misma clase doble si y solo si $s = tr^k$ para algún entero k. Si s es par, entonces t es par, y podemos ver que si $k = 1$,

$$s = tr = t2^{m-1} - t$$

Así, tenemos que s es congruente a t módulo n si y sólo si $t = 0$ ó $t = \frac{n}{2}$. Con esto, tenemos $2^{m-2} + 1$ clases de esta forma. Si s es impar, también lo es t y si $k = 1$,

$$s = tr = t2^{m-1} + t = (2k+1)2^{m-1} - t \equiv 2^{m-1} - t,$$

Por ello, una clase representada por una potencia impar de a también contiene una potencia impar distinta. Así, hay 2^{m-2} clases más. Sumando se tiene en total que

$$|B\backslash G/B| = 2^{m-2} + 2^{m-2} + 1 = \frac{n}{2} + 1$$

Ahora, calculamos $|B\backslash G/C|$. En este caso, $N_G(C) = \langle a^{n/2}, ab \langle$. Sean $x = a^t b^{-u}$, $y = a^s b^{-v}$ elementos de G. Supongamos que están en la misma clase lateral de $N_G(C)$. Esto significa que $y^{-1}x \in N_G(C)$. Pero

$$y^{-1}x = b^v a^{-s} a^t b^{-u} = b^{v-u} a^{r^u(t-s)}$$

Sabemos que b^2 normaliza C pues está en $Z(G)$. Luego, $v - u$ debe ser par. Además todo elemento de $N_G(C)$ se expresa como

$$(ab)^k a^{ln/2} = b^k a^{z_k + l\frac{n}{2}}$$

Por lo que igualando eso con $y^{-1}x$ se tiene que k debe ser par, y por ello,

$$z_k = \frac{k(r+1)}{2} = \frac{k}{2}\frac{n}{2}$$

Por lo tanto, $t - s$ es múltiplo de $\frac{n}{2}$. De esta forma, uno puede elegir como representantes de clases laterales de $N_G(C)$ el siguiente conjunto:

$$\Phi = \{b^u a^t, 0 \leq t \leq \frac{n}{2} - 1, 0 \leq u \leq 1\}$$

Recordamos la fórmula del Teorema 3.2.2:

$$|B\backslash G/C| = \frac{[N_G(C) : C]}{|B|} \left(\sum_{x \in \Phi} |xCx^{-1} \cap B| \right)$$

Sabemos que $B \cap C = \langle b^4 \rangle$. Observamos que por el Lema 3.2.2:

$$bCb^{-1} \cap B \cong C \cap b^{-1}Bb = C \cap B$$

Calculemos ahora $a^l C a^{-l} \cap B$. Notamos que si x está en dicha intersección, existen t, u enteros tales que $x = a^l(ab)^t a^{-l} = b^u$, de lo cual obtenemos que $\Rightarrow (ab)^t a^{l(r^t-1)} = b^u$ y por ello, $\Rightarrow b^t a^{s_t + l(r^t-1)} = b^u$. Esto nos dice que $t =_n u$ y que $s_t + l(r^t - 1) \equiv_n 0$. Por ello t debe ser par, y como

$$s_t + l(r^t - 1) = \frac{t}{2}(r+1) = \frac{t}{2}\frac{n}{2} \equiv_n 0$$

tenemos que que t es múltiplo de 4. Por lo tanto:

$$|a^u C a^{-u} \cap B| = \frac{n}{4}$$

Finalmente, vemos que:

$$ba^u C a^{-u} b^{-1} \cap B \simeq a^u C a^{-u} \cap b^{-u} B b = a^i C a^{-u} \cap B$$

Por lo tanto,

$$|B\backslash G/C| = \frac{2}{n}(\frac{n}{4} + ... + \frac{n}{4}) = \frac{2}{n}(\frac{n}{4}\frac{n}{2}) = \frac{n}{4}$$

Aplicando estos cálculos usando el Teorema 3.2.2, tenemos que el género de X_B es:

$$g_B = -n + 1 + \frac{(3n - 1 - \frac{n}{2} - 1 - \frac{n}{4})}{2} = \frac{n}{8}$$

De forma similar vemos que $g_C = g_B$. □

Sean $B_k = \langle b^{2^k} \rangle$, $C_k = \langle (ab)^{2^k} \rangle$.

Proposición 3.2.10 *Los géneros de $\mathcal{X}_{B_k}$ y $\mathcal{X}_{C_k}$ son:*

$$g_{B_k} = g_{C_k} = \begin{cases} \frac{n}{4} & k = 1 \\ \frac{(2^k-2)(n-1)}{2} & k > 1 \end{cases}$$

Demostración: Es claro que $|B_k\backslash G/A| = 2^k$. Para calcular $|B_k\backslash G/B|$ se sigue la misma idea del caso anterior, es decir, ver cuando dos elementos de A estan en la misma clase doble $B_j x B$. Si a^s y a^v son tales elementos, deben existir b^{t2^k} y b^u tales que:

$$a^s = b^{t2^k} a^v b^u = a^v b^{t2^k} b^u$$

De donde obtenemos que $s \equiv_n v$. Por lo tanto, hay exactamente n clases dobles del tipo $B_k x B$. Por lo tanto, $|B_k\backslash G/B| = n$.

Para calcular $|B_j\backslash G/C|$, simplemente notamos que B_k es normal en G, y distinguimos si $k = 1$ ó $k > 1$. Si $j = 1$, recordando que $B \cap C = B_2$, obsvervamos queda

$$|B_1\backslash G/C| = \frac{|G|}{|B_1 C|} = \frac{n^2}{\frac{|B_1||C|}{|B_1 \cap C|}} = \frac{n^2 |B_1 \cap C|}{\frac{n^2}{2}} = 2|B_2| = 2\frac{n}{4} = \frac{n}{2}$$

Así, tenemos que

$$g_{B_1} = -2n + 1 + \frac{6n - 2 - n - n/2}{2} = \frac{n}{4}$$

Si $k > 1$, se tiene que

$$|B_j \backslash G / C| = \frac{|G|}{|B_k C|} = \frac{n^2}{\frac{|B_k||C|}{|B_k \cap C|}} = \frac{n^2 |B_k \cap C|}{n^2/2^k} = 2^k |B_k| = 2^k \frac{n}{2^k} = n$$

Por esto, aplicando el Teorema 3.2.1, tenemos que:

$$g_{B_k} = -2^k n + 1 + \frac{3 \cdot 2^k n - 2^k - n - n}{2} = \frac{2^k n - 2^k - 2n + 2}{2} = \frac{(2^k - 2)(n-1)}{2}$$

El cálculo de g_{C_j} es análogo. □

Proposición 3.2.11 *La superficie cociente $\mathcal{X}_{Z(G)}$ tiene género cero.*

Demostración: Sabemos que $Z(G) = \langle a^{n/2}, b^2 \rangle$. En este caso, vemos que:

$$|Z(G) \backslash G / A| = [G : AZ(G)] = 2$$

$$|Z(G) \backslash G / B| = [G : BZ(G)] = \frac{n}{2}$$

$$|Z(G) \backslash G / C| = \frac{|G|}{|Z(G)C|} = \frac{|G||Z(G) \cap C|}{|Z(G)||C|}$$

Como $|Z(G)| = |C| = n$, se tiene que:

$$|Z(G) \backslash G / C| = |Z(G) \cap C|$$

Observando que $(ab)^2 = b^2 a^{n/2} \in Z(G)$, se tiene que $|Z(G) \cap C| = \frac{n}{2}$. Por lo tanto,

$$g_{Z(G)} = -n + 1 + \frac{3n - 2 - \frac{n}{2} - \frac{n}{2}}{2} = 0. \square$$

Como concecuencia de esto se desprenden los siguientes corolarios:

Corolario 3.2.2 *Para todo $1 \leq k \leq m-1$, la superficie cociente $\mathcal{X}_{Z_k}$ tiene género cero.*

Corolario 3.2.3 *Las superficies cocientes $\mathcal{X}_{N_G(B)}$ y $\mathcal{X}_{N_G(C)}$ tienen género cero.*

Caso $j = 2$

Recordamos que $\nu_2 = \frac{n}{2} + 1$.

Proposición 3.2.12 *Los géneros de $\mathcal{X}_B$ y $\mathcal{X}_C$ son:*

$$g_B = g_C = \frac{n}{8}$$

Demostración: Observamos que por normalidad de A, $|B\backslash G/A| = 1$. Para calcular $|B\backslash G/B|$ se procede de la misma forma que el caso de primo impar. Se tiene con ello, que toda clase lateral doble BxB está representada por un elemento de A y que dos elementos de A, digamos a^s y a^t, representan la misma clase doble si y solo si $s = tr^k$ para algun entero k. Si s es par, entonces t es par, y podemos ver que si $k = 1$,

$$s = tr = t2^{m-1} + t \equiv t(n)$$

Por lo tanto hay exactamente 2^{m-1} clases representadas por potencias pares de a. Si s es impar, entonces t es impar y si $k = 1$,

$$s = tr = t2^{m-1} + t = (2k+1)2^{m-1} + t \equiv 2^{m-1} + t$$

Por ello, una clase representada por una potencia impar de a también contiene una potencia impar distinta. Así, hay 2^{m-2} clases más. Sumando se tiene en total que

$$|B\backslash G/B| = 2^{m-1} + 2^{m-2} = \frac{3n}{4}$$

Finalmente calculamos, $|B\backslash G/C|$. Sabemos que $N_G(C) = \langle a^2, ab\rangle$. Usando el Teorema 3.2.2, se tiene que

$$|B\backslash G/C| = \frac{1}{2}(|B \cap C| + |B \cap aCa^{-1}|)$$

Sabemos que $|B \cap C| = 1$. Por esto, para que la fórmula anterior tenga sentido, $|B \cap aCa^{-1}| = 1$. Luego, $|B\backslash G/C| = 1$, y aplicando el Teorema 3.2.2, tenemos que:

$$g_B = -n + 1 + \frac{(3n - 2 - 3\frac{n}{4})}{2} = \frac{n}{8}$$

El género g_C es igual a g_B por analogía. □

Proposición 3.2.13 *Los géneros de $\mathcal{X}_{B_k}$ y $\mathcal{X}_{C_k}$ son:*

$$g_{B_k} = g_{C_k} = \frac{(2^k - 1)(n-2)}{2}$$

Demostración: Calculemos g_{B_k}. Primero, notamos que B_k es normal en G, y como $B \cap C = \{1\}$, se tiene:

$$|B_k \backslash G / A| = [G : AB_k] = 2^k$$
$$|B_k \backslash G / B| = [G : B_k B] = [G : B] = n$$
$$|B_k \backslash G / C| = \frac{|G|}{|B_k||C|} = \frac{n^2}{\frac{n^2}{2^k}} = 2^k$$

De esta forma:

$$g_{B_k} = -n2^k + 1 + \frac{3n2^k - n - 2 \cdot 2^k}{2} = \frac{n2^k - n - 2 \cdot 2^k + 2}{2} = \frac{(2^k - 1)(n-2)}{2}$$

Nuevamente por analogía a casos anteriores, $g_{C_k} = g_{B_k}$. □

Proposición 3.2.14 *Las superficies cocientes $\mathcal{X}_{Z(G)}$, $\mathcal{X}_{N_G(B)}$ y $\mathcal{X}_{N_G(C)}$ tienen género cero.*

Demostración: Recordamos que $Z(G) = \langle a^2, b^2 \rangle$. Como este subgrupo es normal en G, tenemos:

$$|Z(G) \backslash G / A| = [G : AZ(G)] = 2$$
$$|Z(G) \backslash G / B| = [G : BZ(G)] = 2$$

Para calcular $|Z(G) \backslash G / C|$, primero calcularemos $Z(G) \cap C$. Para ello, vemos cuando un elemento de C conmuta con a y b:

$$a(ab)^t a^{-1} = (ab)^t a^{r^t - 1}$$

De esto, concluimos que t es par. Viendo ahora con b, y como $\frac{t(r+1)}{2}$ es par:

$$b(ab)^t b^{-1} = bb^t a^{\frac{t(r+1)}{2}} b^{-1} = bb^t b^{-1} a^{\frac{t(r+1)}{2}} = b^t a^{\frac{t(r+1)}{2}}$$

Por lo tanto, $Z(G) \cap C = C_1$. Con esto:

$$|Z(G)\backslash G/C| = \frac{|G|}{|Z(G)C|} = \frac{|G||C_1|}{|Z(G)||C|} = \frac{n^3/2}{n^3/4} = 2$$

Con estos cálculos, aplicamos el Teorema 3.2.2 y obtenemos que el género de $\mathcal{X}_{Z(G)}$ es:

$$g_{Z(G)} = -4 + 1 + \frac{3 \cdot 4 - 3 \cdot 2}{2} = -3 + 6/2 = 0$$

El hecho de que $g_{N_G(B)} = g_{N_G(C)} = 0$ se deduce de que ambos contienen a $Z(G)$ como subgrupo de índice 2. □

Proposición 3.2.15 *Para todo subgrupo H de G tal que $B < H < N_G(B)$ ó $C < H < N_G(C)$, se tiene que $g_H = 0$.*

Demostración: Supongamos que $B < H < N_G(B)$. Es claro que H debe ser de la forma $\langle b, a^{2^k} \rangle$. Además, H es normal en B pues $aba^{-1} = a^{\frac{n}{2}}$. Por lo tanto:

$$|H\backslash G/A| = |H\backslash G/C| = 1, |H\backslash G/B| = 2^k$$

Aplicando el Teorema 3.2.2, tenemos que:

$$g_H = -2^k + 1 + \frac{3 \cdot 2^k - 2 - 2^k}{2} = 0$$

Caso $j = 3$

Recordamos que $\nu_3 = n - 1$.

Proposición 3.2.16 *Las superficies cocientes $\mathcal{X}_B$ y $\mathcal{X}_C$ tienen género cero.*

Demostración: Claramente $|B\backslash G/A| = 1$. Para calcular $|B\backslash G/B|$ se procede de la misma forma que antes, buscando como son s y t cuando $s = tr^k$. Si s es par, entonces t es par, y podemos ver que si $k = 1$,

$$s = tr = t2^m - t$$

De esta forma, vemos que es el mismo cálculo que en el caso $j = 1$. Por lo tanto:

$$|B\backslash G/B| = \frac{n}{2} + 1$$

El cálculo de $|B\backslash G/C|$ es esencialmente el mismo que en el caso $r = 2^{m-1} - 1$, sólamente cambia que el orden de los grupos $xCx^{-1} \cap B$ es $n/2$. Por lo tanto,

$$g_B = -n + 1 + \frac{(3n - 1 - \frac{n}{2} - 1 - \frac{n}{2})}{2} = -n + 1 + \frac{2n-2}{2} = 0$$

El cálculo de g_C es análogo. □

Proposición 3.2.17 *Los géneros de $\mathcal{X}_{B_k}$ y $\mathcal{X}_{C_k}$ son:*

$$g_{B_k} = g_{C_k} = \frac{(2^k - 2)(n-1)}{2}$$

Demostración: Vemos que por normalidad de B_k, y usando que $B \cap C = B_1$, se tiene:

$$|B_k\backslash G/A| = [G : AB_k] = 2^k, \quad |B_k\backslash G/B| = [G : BB_k] = n$$

$$|B_k\backslash G/C| = \frac{|G|}{|B_kC|} = \frac{|G||B_k \cap C|}{|B_k||C|} = \frac{n^2|B_k|}{|B_k|n} = n$$

Por lo tanto:

$$g_{B_k} = g_{C_k} = -n2^k + 1 + \frac{3n2^k - 2^k - 2n}{2}$$

$$= \frac{n2^k - 2^k - 2n + 2}{2} = \frac{(2^k - 2)(n-1)}{2}. \square$$

Proposición 3.2.18 *Las superficies cocientes $\mathcal{X}_{Z(G)}$, $\mathcal{X}_{N_G(B)}$ y $\mathcal{X}_{N_G(C)}$ tienen género cero.*

Demostración: de la proposición anterior, se tiene que si $k = 1$, entonces X_{B_1} tiene género cero. Este subgrupo está contenido en $Z(G)$, el cuál a su vez está contenido en los normalizadores de B y C. □

3.3. Cálculo de las firmas de los subgrupos de $G_{n,j}$

En esta sección nos dedicaremos a calcular las firmas de los subgrupos de $G_{n,j}$. Para ello, usaremos un resultado expuesto en [26] que explica como obtener la firma de un subgrupo conocida la firma de G. La idea en ese artículo, aplicada a nuestro grupo G, es la siguiente:

Observación 3.3.1 *Sea Γ un grupo actuando en una superficie de Riemann compacta S con firma $(g_\Gamma, m_1, ..., m_t)$ y vector generador $(a_1, ..., a_{g_\Gamma}, b_1, ..., b_{g_\Gamma}, c_1, ..., c_t)$. Sea H un subgrupo de Γ. La firma de la acción de H en S se obtiene de la siguiente forma:*

1. Primero, fijamos un subgrupo H de G.

2. Tomamos todos los elementos que forman el vector generador y los hacemos actuar por multiplicación izquierda sobre las clases laterales de H en G.

3. Contamos todas las órbitas de una cierta cardinalidad bajo la acción de dichos elementos.

4. En nuestro caso, llamamos la cantidad de órbitas de cardinalidad $u < n$ bajo la acción de a como $\alpha_{1,u}$, las bajo la acción de b como $\alpha_{2,u}$ y las bajo la acción de $(ab)^{-1}$ como $\alpha_{3,u}$.

5. Verificamos que estos números deben cumplir la siguiente fórmula:

$$2g_H - 2 + \sum_{l=1}^{3}\sum_{u=1}^{n-1}\left(\alpha_{l,u}\left(1-\frac{u}{n}\right)\right) = |G/H|\left(1-\frac{3}{n}\right)$$

6. Así la firma de H es:

$$\left(g_H, \left(\frac{n}{u_1}\right)^{(\alpha_{1,u_1}+\alpha_{2,u_1}+\alpha_{2,u_1})}, ..., \left(\frac{n}{u_{k_1}}\right)^{(\alpha_{1,u_k}+\alpha_{2,u_k}+\alpha_{3,u_k})}\right)$$

Donde u_j son todos los $u < n$ tales que al menos alguno de los α_u, β_u ó γ_u es mayor que cero.

Primero calcularemos la firma de A y sus subgrupos:

Proposición 3.3.1 *Para cualquier valor de n y j, la firma de la acción de A es $(0; n^{(n)})$ y la de A_k es*

$$\left(\frac{(p^k-1)(n-2)}{2}; (p^{m-k})^{(n)}\right)$$

Demostración: en este caso $|A| = n$. Es claro que la acción de a en G/A es trivial, y esta aportará n órbitas de largo 1, por lo que $\alpha_{1,1} = n$. Ahora bien, para b y $(ab)^{-1}$ es claro que los elementos de G/A se pueden representar de la forma b^jA

o $(ab)^l A$ por lo que tenemos exactamente una órbita de cardinalidad n en ambos casos, por lo que esto no afecta al cálculo final. Verificamos que:

$$2g_A - 2 + n\left(1 - \frac{1}{n}\right) = -2 + n - 1 = n - 3 = |G/A|\left(1 - \frac{3}{n}\right)$$

Así, la firma de A es la deseada. Calculemos ahora la firma de $A_k = \langle a^{p^k} \rangle$, $1 \leq k \leq m-1$. En este caso, un conjunto de representantes de G/A_j es $\{b^u a^l\}$ con $0 \leq u \leq n-1$ y $0 \leq l \leq p^k - 1$. También se puede elegir como conjunto de representantes $\{(ab)^u a^l\}$. Usando el primer conjunto de representantes, se ve que b forma sólo órbitas de largo n en G/A_k, mientras que usando el segundo, podemos ver que ab también forma sólo órbitas de largo n en G/A_k. Ahora, usando el primer conjunto de representantes, vemos que al actuar a en G/A_k:

$$a^t(a^l A_k) = a^{l+t} A_j$$
$$a^t(b^u a^l A_k) = a^{j+tr^{p^{m-j}-u}} A_j$$

De todas formas, vemos que en cualquier caso, $a^t(xA_j) = xA_j$. Por lo tanto, como la cardinalidad de G/A_k es np^k, este conjunto se descompone en exactamente n órbitas de largo p^j. Así, vemos que:

$$2g_{A_k} - 2 + n\left(1 - \frac{p^k}{n}\right) = (p^k - 1)(n-2) - 2 + n - p^k = np^k - n - 2p^k + 2 - 2 + n - p^k$$
$$= np^k - 3p^k = |G/A_k|\left(1 - \frac{3}{n}\right)$$

Así la firma de A_k es la deseada. □

Ahora, nuevamente dividiremos el trabajo de obtener las firmas de los otros subgrupos dependiendo de n y j:

3.3.1. Caso p impar

Proposición 3.3.2 *Las firmas para los subgrupos de G en el caso de p primo impar se especifican en la siguiente tabla:*

Subgrupo	*Firma*
A	$(0; n^{(n)})$
B, C	$\left(\frac{n-p^j-p^{j-1}(p-1)(m-j)}{2}; (p^m)^{(p^j)}, (p^{m-1})^{(p^{j-1}(p-1))}, ..., (p^j)^{(p^{j-1}(p-1))}\right)$
A_k	$\left(\frac{(p^k-1)(n-2)}{2}; p_{(n)}^{m-k}\right)$
B_k, C_k $(k < m-j)$	$\left(\frac{np^k-2p^k-((p-1)p^{j+k-1}(m-j-k)+p^{j+k})+2}{2}; (p^{m-k})^{(p^{j+k})}, ..., (p^j)^{(p^{j+k-1}(p-1))}\right)$
B_k, C_k $(k \geq m-j)$	$\left(\frac{(p^k-1)(n-2)}{2}; (p^{m-k})^{(n)}\right)$
Z_k	$\left(\frac{(p^{m-kj}-1)(p^{m-kj}-2)}{2}; (p^{kj})^{3p^{m-kj}}\right)$
$[G,G]$	$\left(\frac{(p^j-1)(n-2)}{2}; (p^{m-j})^{(n)}\right)$
G_k	$\left(\frac{(p^{kj}-1)(n-2)}{2}; (p^{m-kj})^{(n)}\right)$
H_k, $k \leq j$	$(0; n^{(p^t)}, p^{m-l}, p^{m-l})$
H_k, $k > j$	$\left(\frac{p^t-p^j-p^{j-1}(p-1)(t-j)}{2}; p^{l(p^j)}, (p^{l-1})^{(p^{j-1}(p-1))}, ..., (p^j)^{(p^{j-1}(p-1))}\right)$

Tabla 6: Firmas de los subgrupos de $G_{n,j}$ si n es potencia de primo impar.

Demostración:

I) $B = \langle b \rangle$ y $C = \langle ab \rangle$. Por simetría, basta hacer el cálculo con B. Vemos que los elementos de G/B se puede representar como $a^k B$ o como $(ab)^k$ (pues $(ab)^t$ se escribe como producto de potencias de a y b). Por ello, la acción de a y $(ab)^{-1}$ generan respectivamente una órbita de largo n.

Veamos la acción de b. Como $a^{p^{m-j}}$ conmuta con b, se tiene que b deja fijas las clases laterales de B cuyos representantes son potencias de $a^{p^{m-j}}$, y hay exactamente p^j de esas clases. Por lo tanto, $\beta_1 = p^j$.

Ahora si consideramos a^t con t no divisible por p^{m-j}. Entonces b^{-1} manda $a^t B$ a $a^{tr} B$. De esta forma, la órbita de B está formada por todos los elementos de la forma $a^{tr^l} B$. Recordando lo desarrollado en la Proposición 3.2.3, sabemos que hay exactamente $p^{j-1}(p-1)$ órbitas de esta forma, cuyo largo es una potencia de p, digamos u, cuyo exponente varía entre 1 y $m-j$, por lo que $\beta_u = p^{j-1}(p-1)$. Ahora, verificamos:

$$2g_B - 2 + p^{j-1}(p-1)\sum_{k=1}^{m-j}\left(1-\frac{p^k}{n}\right) + p^j\left(1-\frac{1}{n}\right)$$

$$= n - p^j - p^{j-1}(p-1)(m-j) - 2 + p^{j-1}(p-1)(m-j) - p^{j-1}(p-1)\sum_{k=1}^{m-j}\frac{p^k}{n} + p^j - \frac{p^j}{n}$$

$$n-2-\frac{p^{j-1}(p-1)p(p^{m-j}-1)}{(p-1)n}-\frac{p^j}{n}=n-2-1+\frac{p^j}{n}-\frac{p^j}{n}=n-3=|G/B|\left(1-\frac{3}{n}\right)$$

Por lo tanto, la firma de B (y por simetría, de C) es:

$$\left(\frac{n-p^j-p^{j-1}(p-1)(m-j)}{2};n^{(p^j)},(p^{m-1})^{(p^{j-1}(p-1))},...,(p^j)^{(p^{j-1}(p-1))}\right)$$

II) $B_k=\langle b^{p^k}\rangle$ y $C_k=\langle (ab)^{p^k}\rangle$, $1\leq k\leq m-1$. Como antes, basta hacer el cálculo con B_k. En este caso, vemos que un conjunto de representantes de G/B_k es $\{a^ub^l\}$, con $0\leq u\leq n-1$ y $0\leq l\leq p^k-1$. Primero, consideraremos el caso en que $k<m-j$.

Vemos que al actuar a se forman órbitas de largo n, pues $a^t(a^ub^lB_k)=a^{u+t}b^lB_k$. Ahora, al actuar $(ab)^{-1}$, tenemos que:

$$(ab)^{-1}(a^ub^lB_k)=b^{-1}a^{-1}a^ub^lB_k=b^{-1}a^{u-1}b^lB_k=a^{(u-1)r}b^{l-1}B_k$$

Como $(ab)^{p^{m-i}}=a^{p^{m-i}}b^{p^{m-i}}$, y p^k divide a p^{m-j}, se tiene que:

$$(ab)^{-p^{m-j}}(a^ub^lB_k)=a^{u-p^{m-j}}b^lB_k$$

Luego, repitiendo varias veces $(ab)^{-p^{m-i}}$ se comprueba que $(ab)^{-1}$ sólo genera órbitas de largo n.

Finalmente vemos la acción de b. Observamos que:

$$b^{-t}(a^ub^lB_k)=a^{ur^t}b^{l-t}B_k$$

Vemos que si t es divisible por p^k, se tiene que

$$b^{-t}(a^ub^lB_k)=a^{ur^t}b^lB_k$$

De esta manera, tenemos que analizar cuando $ur^t\equiv_n u$. Esto ya se hizo antes al calcular el género de B_j, y así, tenemos que para cada u potencia de p tal que $p^{k+1}\leq v\leq p^{m-j}$ se tienen que $\beta_v=p^{j+k-1}(p-1)$ y $\beta_{p^k}=p^{j+k}$. Ahora, verificamos que:

$$np^k-2p^k-((p-1)p^{j+k-1}(m-j-k-1)+p^{j+k})+2-2$$

$$+p^{j+k-1}(p-1)\sum_{l=k+1}^{m-j}\left(1-\frac{p^l}{n}\right)+p^{j+k}\left(1-\frac{p^k}{n}\right)$$
$$=np^k-2p^k-(p-1)p^{j+k-1}(m-j-k-1)-p^{j+k}$$
$$-p^{j+k-1}(p-1)(m-j-k)-p^{j+k-1}(p-1)\frac{p^{k+1}(p^{m-k-j}-1)}{(p-1)n}+p^{j+k}-\frac{p^{j+2k}}{n}$$
$$=np^k-2p^k-p^k+\frac{p^{j+2k}}{n}-\frac{p^{j+2k}}{n}=np^k-3p^k=|G/B_k|\left(1-\frac{3}{n}\right)$$

Por lo tanto, la firma de B_k cuando $k < m-j$ es:

$$\left(g_{B_k};(p^{m-k})^{(p^{j+k})},(p^{m-k-1})^{(p^{j+k-1}(p-1))},...,(p^j)^{(p^{j+k-1}(p-1))}\right)$$

En el caso que $k \geq m-j$, debido a que $b^{p^k} \in Z(G)$, ocurre lo siguiente:

$$(ab)^{lp^{m-j}}(a^ub^vB_k)=a^{kp^{m-j}}b^{lp^{m-j}}a^ub^vB_k=a^{u+lp^{m-j}}b^{v+lp^{m-j}}B_k$$

De esta forma, (ab) forma sólo órbitas de largo n, y es claro que a también forma órbitas de largo n. Además, $b^{lp^{m-j}}(a^ub^vB_k) = a^ub^{v+lp^{m-j}}B_k$. Luego, b sólo forma órbitas de largo p^k. Por lo tanto, la firma de B_k es

$$\left(\frac{(p^k-1)(n-2)}{2};(p^{m-k})^{(n)}\right)$$

III) $Z(G) = \langle a^{p^{m-j}}, b^{p^{m-j}}\rangle$. Observamos que un conjunto de representantes de los elementos de $G/Z(G)$ es $\langle a^ub^l\rangle$ con $0 \leq u,l \leq p^{m-i}-1$. Vemos que al actuar a, b y $(ab)^{-1}$ en ese conjunto de clases laterales tenemos:

$$a^t(a^ub^lZ(G))=a^{u+t}b^lZ(G)$$
$$b^{-t}(a^ub^lZ(G))=a^{ur^t}b^{l-t}Z(G)$$
$$(ab)^{-1}(a^ub^lZ(G))=b^{-1}a^{-1}(a^ub^lZ(G))=a^{(u-1)r}b^{l-1}Z(G)$$

Para el caso de a y b vemos claramente que cualquier clase lateral queda fija al actuar esos elementos en su p^{m-j}-ésima potencia. Para el caso de $(ab)^{-1}$ iteramos varias veces:

$$(ab)^{-2}(a^ub^lZ(G))=b^{-1}a^{-1}(a^{(u-1)r}b^{l-1}Z(G))=a^{ur^2-r^2-r}b^{l-2}Z(G)$$

$$\Rightarrow (ab)^{-t}(a^u b^l Z(G)) = b^{-1}a^{-1}(a^{(u-1)r}b^{l-1}Z(G)) = a^{ur^t - z_t}b^{l-t}Z(G)$$

En particular, si $t = p^{m-j}$, tenemos que $(ab)^t$ fija cualquier clase lateral. De esta forma, concluimos que $\alpha_{p^{m-j}} = \beta_{p^{m-j}} = \gamma_{p^{m-j}} = p^{m-j}$, pues $|G/Z(G)| = p^{2(m-j)}$. Como ya sabemos el género de $\mathcal{X}_{Z(G)}$, verificamos:

$$2g_{Z(G)} - 2 + 3p^{m-j}\left(1 - \frac{p^{m-j}}{n}\right) = (p^{m-j}-1)(p^{m-j}-2) - 2 + 3p^{m-j} - 3\frac{p^{2(m-j)}}{n}$$

$$= p^{2(m-j)} - 3p^{m-j} + 2 - 2 + 3p^{m-j} - 3\frac{p^{2(m-j)}}{n} = p^{2(m-j)} - 3\frac{p^{2(m-j)}}{n} = |G/Z(G)|\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de $Z(G)$ es $\left(\frac{(p^{m-j}-1)(p^{m-j}-2)}{2}; (p^j)^{(3p^{m-j})}\right)$.

IV) $Z_k = \langle a^{p^{m-kj}}, b^{p^{m-kj}} \rangle$ (si $k < m-j$). En este caso, la situación es parecida al caso de $Z(G)$. Notamos que un conjunto de representantes de los elementos de G/Z_k es $\langle a^u b^l \rangle$ con $0 \leq u, l \leq p^{m-jt} - 1$. Vemos que al actuar a, b y $(ab)^{-1}$ en ese conjunto de clases laterales tenemos al igual que con $Z(G)$, que:

$$a^t(a^u b^l Z_k) = a^{u+t}b^l Z_k, \quad b^{-t}(a^u b^l Z_k) = a^{ur^t}b^{l-t}Z_k, \quad (ab)^{-t}(a^u b^l Z_k) = a^{ur^t - z_t}b^{l-t}Z_k$$

En particular para $t = p^{m-kj}$, como $r^t =_{p^{m-kj}} 1$ y p^{m-kj} divide a Z_t, vemos que

$$a^{u+t}b^l Z_k = a^u b^l a^{tr^l} Z_k = a^u b^l Z_k, \quad a^{ur^t}b^{l-t}Z_k = a^u b^l Z_k, \quad a^{ur^t - s_t}b^{l-t}Z_k = a^u b^l Z_k$$

De esta forma, la firma de Z_k es $\left(\frac{(p^{m-kj}-1)(p^{m-kj}-2)}{2}; (p^{kj})^{(3p^{m-kj})}\right)$.

V) H_l y K_l, con $l \leq j$. En este caso, $g_{H_l} = g_{K_l} = 0$. Sabemos que en este caso estos subgrupos son normales en G, y por ello, G/H_l es cíclico de orden p^l y actúa en la esfera de Riemann. Como los indices de ramificación son (p^l, p^l) y la firma de G es $(0; n, n, n)$, podemos deducir que la firma de H_l es $(0; n^{(p^l)}, p^{m-l}, p^{m-l})$.

VI) H_l y K_l, con $l > j$. Se puede notar que el cálculo es similar al cálculo de la firma de B, notando que un conjunto de representantes de G/H_l es $\{a^t, 0 \leq t < p^l\}$ y que la acción de a, b y ab en las clases laterales es similar al de G/B. Así, la firma de H_l es:

$$\left(\frac{p^l - p^j - p^{j-1}(p-1)(l-j)}{2}; p^{l(p^j)}, (p^{l-1})^{(p^{j-1}(p-1))}, ..., (p^j)^{(p^{j-1}(p-1))}\right)$$

3.3.2. Caso $p = 2$, $j = 1$

Recordamos que $\nu_1 = n/2 - 1$.

Proposición 3.3.3 *Las firmas para los subgrupos de G cuando p es par y $j = 1$ se especifican en la siguiente tabla:*

Subgrupo	*Firma*
A	$(0; n^{(n)})$
B, C	$\left(\frac{n}{8}; n^{(2)}, \left(\frac{n}{2}\right)^{\left(\frac{n}{2}-1\right)}, \left(\frac{n}{4}\right)^{\left(\frac{n}{4}\right)}\right)$
A_k	$\left(\frac{(2^k-1)(n-2)}{2}; (2^{m-k})^{(n)}\right)$
B_k, C_k, $k = 1$	$\left(\frac{n}{4}; \frac{n}{2}_{(n)}, \frac{n}{4}_{\frac{n}{2}}\right)$
B_k, $k > 1$	$\left(\frac{(2^k-2)(n-1)}{2}; \left(\frac{n}{2^k}\right)^{(2n)}\right)$
Z_k	$\left(0; \left(\frac{n}{2}\right)^{\left(\frac{2n}{2^k}\right)}, (2^k)^{(2)}\right)$
$[G, G]$	$\left(\frac{(n-2)}{2}; (2^{m-1})^{(n)}\right)$
G_k	$\left(\frac{(2^k-1)(n-2)}{2}; (2^{m-k})^{(n)}\right)$
$N_G(B), N_G(C)$	$(0; n, n, 2)$

I) $B = \langle b \rangle$ Para el caso de B conviene notar que los elementos de G/B se pueden representar como $a^k B$ con $0 \leq k \leq n-1$. Al actuar a formará una sola órbita de largo n, y al actuar $(ab)^{-1}$ se ve que:

$$(ab)^{-1}(a^k B) = b^{-1}a^{-1}a^k B = a^{(k-1)r}B$$
$$(ab)^{-2}(a^k B) = (ab)^{-1}(a^{(k-1)r}B) = a^{((k-1)r-1)r} = a^{(k-1)-r}B = a^{k-\frac{n}{2}}B$$
$$\Rightarrow (ab)^{-4}(a^k B) = (ab)^{-2}(a^{k-\frac{n}{2}}B) = a^{k-n}B = a^k B$$

De esta forma, $\gamma_4 = n/4$. Mientras que al actuar b tenemos que $b(a^k B) = a^{kr}B$, de lo que obtenemos que $b(a^{kr}B) = a^{kr^2}B = a^k B$. Concluimos que si k no es cero o $n/2$, entonces la órbita de $a^k B$ tiene 2 elementos y cuando k es cero o $n/2$, entonces hay una sola órbita. Por lo tanto, $\beta_2 = 2^{m-1} - 1$ y $\beta_1 = 2$. Verificamos que:

$$2g_B - 2 + (2^{m-1} - 1)\left(1 - \frac{2}{n}\right) + 2\left(1 - \frac{1}{n}\right) + \frac{n}{4}\left(1 - \frac{4}{n}\right)$$
$$= \frac{n}{4} - 2 + 2^{m-1} - 1 - 1 + \frac{2}{n} + 2 - \frac{2}{n} + \frac{n}{4} - 1 = n - 3$$

Por lo tanto, la firma de B es

$$\left(\frac{n}{8}; n^{(2)}, \left(\frac{n}{2}\right)^{\left(\frac{n}{2}-1\right)}, \left(\frac{n}{4}\right)^{\left(\frac{n}{4}\right)}\right)$$

La firma de C se calcula de forma similar a la de B.

II) $B_k = \langle b^{2^k} \rangle$. En este caso, notamos que las clases laterales de B_k en K se pueden representar como $a^u b^l B_k$ con $0 \leq u \leq n-1$, $0 \leq l \leq 2^k - 1$. Claramente al actuar a este forma sólo órbitas de largo n. Al actuar b notamos:

$$b^2(a^u b^l B_k) = a^u b^{l+2} B_k$$

Iterando varias veces, podemos ver que b forma $n = \beta_{2^k}$ órbitas de largo 2^k. Ahora al actuar $(ab)^{-1}$, tenemos que:

$$(ab)^{-1}(a^u b^l B_k) = b^{-1}a^{-1}a^u b^l B_k = a^{(u-1)r} b^{l-1} B_k$$
$$(ab)^{-2}(a^u b^l B_k) = (ab)^{-1} = a^{((u-1)r-1)r} b^{l-2} B_k = a^{u-1-r} b^{l-2} B_k = a^{u-\frac{n}{2}} b^{l-2} B_k$$

De esta forma, tenemos que distinguir 2 situaciones, si $k = 1$ o $k > 1$. Si $k = 1$, veremos que al aplicar nuevamente $(ab)^{-2}$ tendremos queda

$$(ab)^{-4}(a^u b^l B_j) = a^u b^l B_k$$

Por lo tanto, $\gamma_4 = n/2$. Como $g_{B_1} = n/4$, verificamos que:

$$2g_{B_1} - 2 + n\left(1 - \frac{2^k}{n}\right) + \frac{n}{2}\left(1 - \frac{4}{n}\right) = \frac{n}{2} - 2 + n - 2^k + \frac{n}{2} - 2 = 2n - 6$$
$$= |G/B_1|\left(1 - \frac{3}{n}\right)$$

De esta forma, la firma de B_1 (y C_1) es $\left(\frac{n}{4}; \left(\frac{n}{2}\right)^{(n)}, \left(\frac{n}{4}\right)^{\frac{n}{2}}\right)$.

Si $k > 1$, actuando repetidamente $(ab)^{-1}$ en las clases laterales de B_k obtenemos que $(ab)^{-2^v}(a^u b^l B_j) = a^u b^{l-2^v} B_k$. En particular, cuando $v = k$, concluimos que $\gamma_{2^k} = n$. Verificamos:

$$2g_{B_k} - 2 + 2n\left(1 - \frac{2^k}{n}\right) = (2^k - 2)(n-1) - 2 + 2n - 2 \cdot 2^k$$

$$= n2^k - 2n - 2^k + 2 - 2 + 2n - 2 \cdot 2^k = n2^j - 3 \cdot 2^k = |G/B_k|\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de B_k es

$$\left(\frac{(2^k-2)(n-1)}{2}; \left(\frac{n}{2^k}\right)^{(2n)}\right)$$

III) $Z_k = \langle a^{\frac{n}{2^k}}, b^2\rangle$. En este caso, las clases laterales de Z_k en G se pueden representar como $a^u b^l Z_k$ con $0 \leq u \leq n/2^j - 1$, $l \in \{0,1\}$. Vemos que al actuar a, por la representación indicada, genera 2 órbitas de largo $\frac{n}{2^k}$ ($\alpha_{\frac{n}{2^k}} = 2$). Al actuar b, notamos que $b(a^u b^l Z_k) = a^{ur} b^{l+1} Z_k$, de lo que obtenemos que $b(a^{ur} b^{l+1} Z_k) = a^{ur^2} b^{l+2} Z_j = a^u b^l Z_k$. Así, se forman $\frac{n}{2^k}$ órbitas de largo 2 ($\beta_2 = \frac{n}{2^k}$). Finalmente, vemos la acción de $(ab)^{-1}$:

$$(ab)^{-1}(a^u b^l Z_k) = b^{-1}a^{-1}a^u b^l Z_k = a^{(u-1)r} b^{l-1} Z_k$$
$$(ab)^{-1}(a^{(u-1)r} b^{l-1} Z_k) = a^{u-\frac{n}{2}} b^{l-2} Z_k = a^{u-\frac{n}{2}} b^l Z_k$$

Así, como $a^{n/2} \in Z(G)$ vemos que se forman $\frac{n}{2^k}$ órbitas de largo 2 ($\gamma_2 = \frac{n}{2^k}$). Como $g_{Z_k} = 0$, verificamos:

$$-2 + 2\left(1 - \frac{\frac{n}{2^k}}{n}\right) + \frac{2n}{2^k}\left(1 - \frac{2}{n}\right)$$

$$= -2 + 2 - \frac{2}{2^k} + \frac{2n}{2^k} - \frac{4}{2^k} = \frac{2n}{2^k} - \frac{6}{2^k} = |G/Z_k|\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de Z_k es:

$$\left(0; \left(\frac{n}{2}\right)^{\left(\frac{2n}{2^k}\right)}, (2^k)^{(2)}\right)$$

IV) $N_G(B) = \langle b, a^{\frac{n}{2}}\rangle$. En este caso, observamos que $Z(G) < N_G(B)$ y que esa contención es de índice 2. Por lo tanto, el cubriente $\mathcal{X}_{Z(G)} \to \mathcal{X}_{N_G(B)}$ es cíclico de grado 2, y ramifica en 2 puntos con multiplicidad 2. Como $N_G(B)$ tiene un generador

de orden n, necesariamente esos dos puntos de ramificación deben ser 2 puntos de $\mathcal{X}_{Z(G)}$ marcados con $\frac{n}{2}$. Eso indica que la firma de $N_G(B)$ es $(0; n, n, 2)$. □

3.3.3. Caso $p = 2$, $j = 2$

Recordamos que $\nu_2 = \frac{n}{2} + 1$

Proposición 3.3.4 *Las firmas para los subgrupos de G cuando p es par y $j = 2$ se especifican en la siguiente tabla:*

Subgrupo	*Firma*
A	$(0; n^{(n)})$
B, C	$\left(\frac{n}{8}; n^{\left(\frac{n}{2}\right)}, \left(\frac{n}{2}\right)^{\left(\frac{n}{4}\right)}\right)$
A_k, B_k, C_k	$\left(\frac{(2^k-1)(n-2)}{2}; (2^{m-k})^{(n)}\right)$
$Z(G)$	$\left(0; \left(\frac{n}{2}\right)^{(6)}\right)$
$[G, G]$	$\left(\frac{(n-2)^4}{4}; 2^{(n)}\right)$
$N_G(B)$, $N_G(C)$	$\left(0; n^{(2)}, \left(\frac{n}{2}\right)^{(2)}\right)$

Demostración:

I) B y C. Por simetría, basta calcular la firma de B que de todas formas será también la firma de C. Podemos elegir como transversal izquierda de B el conjunto $\{a^k\}$ con $0 \leq k \leq n-1$. Si actúa a, sólo genera una órbita de largo n. Si actúa b, vemos que si k es par, a^k conmuta con b y por tanto, la órbita de $a^k B$ sólo contiene dicha clase lateral. Si k es impar, vemos que como b^2 conmuta con a^k, tenemos que la clase lateral $a^k B$ forma una órbita de 2 elementos. Como son $n/2$ pares y $n/2$ impares módulo n, tenemos que $\beta_1 = \frac{n}{2}$ y $\beta_2 = \frac{n}{4}$. Si actúa $(ab)^{-1}$, vemos que:

$$(ab)^{-1}(a^k B) = b^{-1}a^{-1}a^k B = a^{(k-1)r}$$
$$(ab)^{-2}(a^k B) = (ab)^{-1}(a^{(k-1)r} B) = (a^{k-1-r} B)$$

Esto nos dice que si t es par, $(ab)^{-t}(a^k B) = a^{k-t(r+1)^2} B$. Como $(r+1) = 2^{m-1}+2$, $(r+1)/2$ es impar, y por lo tanto, ab genera una órbita de largo n. Como $g_B = n/8$ verificamos:

$$2g_B - 2 + \frac{n}{2}\left(1 - \frac{1}{n}\right) + \frac{n}{4}\left(1 - \frac{2}{n}\right) = \frac{n}{4} - 2 + \frac{n}{2} - \frac{1}{2} + \frac{n}{4} - \frac{1}{2} = n - 3$$

Por lo tanto, la firma de B (y C) es

$$\left(\frac{n}{8}; n^{(\frac{n}{2})}, \left(\frac{n}{2}\right)^{(\frac{n}{4})}\right)$$

II) B_k y C_k. Nuevamente por simetría, basta ver la firma de B_k. Una transversal izquierda de B_k en G es $\{a^u b^l\}$ con $0 \leq u \leq n-1$ y $0 \leq u \leq 2^k - 1$. Es claro que la acción de a sólo genera órbitas de largo n. Recordando los otros casos, vemos que la acción de b genera n órbitas de largo 2^k. Para la acción de $(ab)^{-1}$, recordando cálculos anteriores en el caso $r = 2^{m-1} - 1$, tenemos que $(ab)^{-2}(a^u b^l B_k) = a^{u-1-r} b^{l-2} B_k$, de lo que obtenemos que $(ab)^{-t}(a^u b^l B_k)$. Verificamos que

$$(2^k - 1)(n-2) - 2 + n\left(1 - \frac{2^k}{n}\right) = n2^k - n - 2 \cdot 2^k + 2 - 2 + n - 2^k$$

$$= n2^k - 3 \cdot 2^k = |G/B_k|\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de B_k (y C_k) es:

$$\left(\frac{(2^k - 1)(n-2)}{2}; (2^{m-k})^{(n)}\right)$$

III) $Z(G) = \langle a^2, b^2 \rangle$. En este caso, una transversal lateral de $Z(G)$ en G es $\{1, a, b, ab\}$. Al actuar a, este mueve 1 en a, b en ab a en a^2 que es congruente con 1 módulo $Z(G)$, y ab en $a^2 b$ que es equivalente con b módulo $Z(G)$. Al actuar b mueve 1 a b, a en $ba = a^r b$ que es congruente a ab módulo $Z(G)$, b en $b^2 \equiv 1$ y ab a $bab = a^r b^2 \equiv a$. Finalmente, ab manda 1 en ab, a en $aba = a^{r+1} b \equiv b$, b en $abb \equiv a$ y ab en $(ab)^2 \equiv 1$. Entonces vemos que se forman 6 órbitas de largo 2. Como $g_{Z(G)} = 0$, verificamos:

$$-2 + 6\left(1 - \frac{2}{n}\right) = 4 - \frac{12}{n} = 4\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de $Z(G)$ es $(0; (\frac{n}{2})^6)$.

IV) $N_G(B)$ y $N_G(C)$. Como ambos subgrupos tienen un generador de orden n, y además contienen a $Z(G)$, de la firma de este último vemos que dos de los puntos marcados con n ramifican bajo el cubriente cíclico respectivo y los otros se agrupan en dos imágenes bajo dicho cubriente. Por lo tanto, la firma de ambos subgrupos es

$(0; n^{(2)}, \left(\frac{n}{2}\right)^{(2)})$. □

3.3.4. Caso $p = 2$, $j = 3$

Recordamos que $\nu_3 = n - 1$.

Proposición 3.3.5 *Las firmas para los subgrupos de G cuando p es par y $j = 3$ se especifican en la siguiente tabla:*

Subgrupo	*Firma*
A	$(0; n_{(n)})$
B, C	$\left(0; n^{(2)}, \left(\frac{n}{2}\right)^{(n-1)}\right)$
A_k	$\left(\frac{(2^k-1)(n-2)}{2}; (2^{m-k})^{(n)}\right)$
B_k, C_k	$\left(\frac{(2^k-2)(n-1)}{2}; (2^{m-k})^{(2n)}\right)$
$Z(G)$	$\left(0; \left(\frac{n}{2}\right)^{n)}, (2^k)^{(2)}\right)$
Z_k	$\left(0; \left(\frac{n}{2}\right)^{\left(\frac{n}{2^{k-1}}\right)}, (2^k)^{(2)}\right)$
$[G, G]$	$\left(\frac{(n-2)}{2}; (2^{m-1})^{(n)}\right)$

I) B y C. Nuevamente por simetría, basta calcular la firma de B pues será igual a la de C. Representamos $G/B = \{a^k, 0 \leq k \leq n-1\}$. Nuevamente vemos que la acción de a da sólo una órbita de largo n. Los cálculos de las órbitas bajo b y $(ab)^{-1}$ son análogos a casos anteriores:

$$b(a^k B) = a^{kr}, \quad (ab)^{-2}(a^k)B = a^{k-(1+r)}B$$

La acción de b fija la clase lateral sólo si $k = 0$ ó $k = n/2$, y en otros casos produce órbitas de 2 elementos. De esta forma, $\beta_1 = 2$ y $\beta_2 = n/2 - 1$. Mientras tanto, la acción de $(ab)^{-1}$ produce órbitas de 2 elementos, pues $1 + r = n$. Por lo tanto, $\gamma_2 = n/2$. Verificamos:

$$-2 + 2\left(1 - \frac{1}{n}\right) + (n-1)\left(1 - \frac{2}{n}\right) = -2 + 2 - \frac{2}{n} + n - 1 - 2 + \frac{2}{n} = n - 3$$

Por lo tanto, la firma de B y de C es $\left(0; n^{(2)}, \left(\frac{n}{2}\right)^{(n-1)}\right)$.

II) B_k y C_k. Basta calcular la firma de B_j. De la misma forma que los casos anteriores, notamos que los elementos de B_j en K se pueden representar como $a^u b^l B_k$ con $0 \leq u \leq n-1$, $0 \leq l \leq 2^k - 1$. Claramente al actuar a este forma sólo órbitas de largo n. La acción de b se vuelve a escribir como $b^t(a^k b^l B_j) = a^k b^{l+t} B_j$ para t par. En particular, notamos que $\beta_{2^u} = n$. Ahora al actuar $(ab)^{-1}$, como $(ab)^2 = b^2$, se tiene que si t es par:

$$(ab)^{-t}(a^u b^l B_k) = b^{-t}(a^u b^l B_k) = a^u b^{l-t} B_k$$

De esta forma, se tiene que $\gamma_{2^k} = n$. Verificamos:

$$2g_{B_k} - 2 + 2n\left(1 - \frac{2^k}{n}\right) = (2^k - 2)(n-1) - 2 + 2n - 2\cdot 2^k = n2^k - 2n - 2^k + 2 - 2 - 2n - 2\cdot 2^k$$

$$= n2^k - 3\cdot 2^k = |G/B_k|\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de B_k y C_k es

$$\left(\frac{(2^k-2)(n-1)}{2}; (2^{m-k})^{(2n)}\right)$$

III) $Z_k = \langle a^{\frac{n}{2^k}}, b^2 \rangle$. Igual que en el caso $r = 2^{m-1} - 1$, las clases laterales de Z_k en G se pueden representar como $a^u b^l Z_k$ con $0 \leq u \leq \frac{n}{2^k} - 1$, $l \in \{0, 1\}$. Vemos de nuevo que al actuar a, por la representación indicada, genera 2 órbitas de largo $\frac{n}{2^k}$ ($\alpha_{\frac{n}{2^k}} = 2$). Vemos que $b(a^u b^l Z_k) = a^{ur} b^{l+1} Z_k$ y $(ab)(a^u b^l Z_k) = a^{ukr} abb^l Z_k = a^{ur+1} b^{l+1} Z_k$, y usando que $b^2 = (ab)^2$, obtenemos que

$$b(a^{ur} b^{l+1} Z_k) = a^{ur^2} b^{l+2} Z_k = a^u b^l Z_k$$
$$(ab)^2(a^u b^l Z_k) = b^2(a^u b^l Z_k) = a^u b^l Z_k$$

Por lo tanto, $\beta_2 = \gamma_2 = \frac{n}{2^k}$. Verificamos:

$$-2 + 2\left(1 - \frac{\frac{n}{2^k}}{n}\right) + 2\frac{n}{2^k}\left(1 - \frac{2}{n}\right) = -2 + 2 - \frac{2}{2^k} + \frac{2n}{2^k} - \frac{4}{2^k}$$
$$= \frac{2n}{2^k} - \frac{6}{2^k} = |G/Z_k|\left(1 - \frac{3}{n}\right)$$

Por lo tanto, la firma de Z_k es:

$$\left(0; \left(\frac{n}{2}\right)^{\left(\frac{n}{2^{k-1}}\right)}, (2^k)^{(2)}\right)$$

IV) $N_G(B)$ y $N_G(C)$. Sabemos que existe un cubriente cíclico de grado 2 $\mathcal{X}_{Z(G)} \to \mathcal{X}_H$ con H igual a $N_G(B)$ o $N_G(C)$. Esta es una situación análoga al caso $j = 1$, por lo que las firmas son las mismas que en ese caso. □.

3.4. Inclusión de $G_{n,j}$ en $\mathbf{Aut}(\mathcal{X}_{n,j})$

Un tema de interés en nuestro trabajo es determinar si $G_{n,j}$ es el grupo completo de automorfismos de $\mathcal{X}_{n,j}$, es decir, determinar el índice $[Aut(\mathcal{X}_{n,j}), G_{n,j}]$. Para ello, usaremos un trabajo de David Singerman en [27], en el cual se estudian posibles extensiones de un grupo Γ que actúa en una superficie de Riemann compacta S con firma $(0; t, u, v)$. En nuestro caso, esto se reduce a lo siguiente:

Teorema 3.4.1 *Sea Γ un grupo finito actuando en una superficie de Riemann S compacta con firma $(0; t, t, t)$. Entonces las posibles contenciones de Γ en $\mathbf{Aut}(S)$ estan dadas en la siguiente tabla:*

Caso	*Firma de $\mathbf{Aut}(S)$*	$[\mathbf{Aut}(S) : \Gamma]$
N1	$(0; 2, t, 2t)$	*2*
N2	$(0; 3, 3, t)$	*3*
N3	$(0; 2, 3, 2t)$	*6*

Todas estas extensiones son normales

Para determinar si $G = \mathrm{Aut}(\mathcal{X})$, aplicaremos un resultado de [3] expresado en el siguiente teorema:

Teorema 3.4.2 *Sea Γ un grupo actuando en una superficie de Riemann compacta S con firma $(0; t, t, t)$. Sean x, y y z los generadores de Γ de orden t que cumplen $xyz = 1$. Definimos α_1, α_2, α_3 y β las siguientes indentificaciones:*

$$\alpha_1 : x \mapsto y, y \mapsto x, z \mapsto yzy^{-1}$$

$$\alpha_2 : x \mapsto y^{-1}xy, y \mapsto z, z \mapsto y$$

$$\alpha_3 : x \mapsto z, y \mapsto xyx^{-1}, z \mapsto x$$

$$\beta : a \mapsto b, b \mapsto c, c \mapsto a$$

Entonces

- *Exactamente uno de los α_i define a un automorfismo de G, y β no define automorfismo, sí y sólo si G se extiende de acuerdo al caso N1.*
- *β define un automorfismo de G y ninguno de los α_k es automorfismo, si y sólo si G se extiende de acuerdo al caso N2.*
- *β y α_1 definen automorfismos de G, si y sólo si G se extiende de acuerdo al caso N3.*

Estudiaremos las posibles extensiones de G en $\mathrm{Aut}(\mathcal{X})$ de acuerdo a si p es 2 o impar:

Teorema 3.4.3 *1. Si n es potencia de un primo impar, entonces:*

$$G_{n,j} \cong \boldsymbol{Aut}(\mathcal{X}_{n,j})$$

2. Si n es potencia de 2, para cualquier $r \in \{\nu_1, \nu_2, \nu_3\}$ se cumple que:

$$[\boldsymbol{Aut}(\mathcal{X}_{n,j}) : G_{n,j}] = 2$$

y la firma de $\boldsymbol{Aut}(\mathcal{X}_{n,j})$ es $(0; 2, n, 2n)$.

Demostración:

1. Supongamos que n es potencia de primo. Verificaremos que ninguno de los α_k ni β definen automorfismos de G.

- $\alpha_1 : a \mapsto b, b \mapsto a, c \mapsto bcb^{-1}$

Supongamos que α_1 define a un automorphismo de G. Entonces para $a^l b^s \in G$ se tendría que $\alpha_1(a^l b^s) = b^l a^s$. Sea $a^t b^v$ otro elemento de G. Entonces

$$\alpha_1(a^l b^s)\alpha_1(a^t b^v) = b^l a^s b^t a^v, \quad b^l b^t a^{sr^t} a^v = b^{l+t} a^{sr^t+v}$$

Por otra parte, $z = a^l b^s a^t b^v = a^l a^{tr^{n-s}} b^s b^v = a^{l+tr^{p^m-s}} b^{s+v}$, de lo que sigue que $\alpha_1(z) = b^{l+tr^{n-s}} a^{s+v}$. Entonces para que α_1 sea automorfismo, comparando exponentes, para todo t y s debe cumplirse que $tr^{n-s} \equiv_n t$ y $sr^t \equiv_n s$, hecho que no ocurre en caso de que s y t no son divisibles por p. Por lo tanto, α_1 no define un automorfismo de G, y asi descartamos el caso N1.

- $\alpha_2 : a \mapsto b^{-1}ab, b \mapsto c, c \mapsto b$

Ya sabemos que $b^{-1}ab = a^r$. Entonces, si α_2 define a un automorphismo de G, y $a^l b^s$ es un elemento de G, se tendría que

$$\alpha_2(a^l b^s) = a^{rl}(ab)^{-s}$$

Como por lema 3.1.2, $(ab)^s = b^s a^{z_s}$, reescribimos $\alpha_2(a^l b^s) = a^{rl-z_s} b^{-s}$.Sea $a^t b^v$ otro elemento de G. Entonces

$$\alpha_2(a^l b^s)\alpha_2(a^t b^v) = a^{rl-z_s} b^{-s} a^{rt-z_v} b^{-v} = a^{rl-z_s+r^s(rt-z_v)} b^{-s-v}$$

Por otra parte, $z = a^l b^s a^t b^v = a^l a^{tr^{n-s}} b^s b^v = a^{l+tr^{n-s}} b^{s+v}$, luego

$$\alpha_2(z) = a^{r(l+tr^{n-s})\ z_{s+v}} b^{\ s\ \ v}$$

Entonces para que α_2 sea automorfismo, comparando exponentes debe cumplirse que, $-z_s + r^s(rt - z_v) = tr^{n-s+1} - z_{s+v}$, de lo que se deduce que

$$-(z_s) + r^s(rt - z_v) = tr^{n-s+1} - (z_s + r^{s+1} + ... + r^{s+v})$$

Por ello. $r^s(rt - z_v) = tr^{n-s+1} - r^{s+1} + ... + r^{s+v} = tr^{n-s+1} - r^s z_v$, y con ello, $tr^{s+1} = tr^{n-s+1}$. Esta última igualdad debe cumplirse para todo s y t, cosa que no ocurre cuando $s = 1$ y t no es divisible por p. Por lo tanto, α_2 no define un automorfismo de G.

- $\alpha_3 : a \mapsto c, b \mapsto aba^{-1}, c \mapsto a$

Observamos que $aba^{-1} = ba^{r-1}$ Por lo tanto si α_2 define a un automorphismo de G, y $a^l b^s$ es un elemento de G, se tendría que $\alpha_3(a^l b^s) = (ab)^{-l}(ba^{r-1})^s$. El factor $(ba^{r-1})^s$ se puede reescribir con el siguiente lema cuya demostración es directa:

Lema 3.4.1 $(ba^{r-1})^s = b^s a^{r^s-1}$

Usando este lema, vemos que:

$$\alpha_3(a^l b^s) = (ab)^{-l}(ba^{r-1})^s = a^{-z_l} b^{-l} b^s a^{r^s-1} = a^{-z_l+(r^s-1)r^{s-l}} b^{s-l}$$

Sea $a^t b^v$ otro elemento de G. Entonces

$$\alpha_3(a^l b^s)\alpha_3(a^t b^v) = a^{-z_l+(r^s-1)r^{s-l}} b^{s-l} a^{-z_t+(r^v-1)r^{v-t}} b^{v-t}$$
$$= a^{-z_l+(r^s-1)r^{s-l}+r^{s-l}(-z_t+(r^v-1)r^{v-t})} b^{s-l+v-t}$$

Por otra parte, $z = a^l b^s a^t b^v = a^l a^{tr^{n-s}} b^s b^v = a^{l+tr^{n-s}} b^{s+v}$. Luego, llamando $l + tr^{n-s} = l'$, tenemos

$$\alpha_3(z) = a^{-z_l'+(r^{s+v}-1)r^{s+v-l'}} b^{s+v-l'}$$

Entonces para que α_3 sea automorfismo, comparando exponentes, para todo s y t debe cumplirse que $l' = l + tr^{n-s} = l + t \Rightarrow tr^{n-s} = t$, hecho que no ocurre en la última igualdad falla si s y t no son divisibles por p. Por lo tanto, α_3 no define un automorfismo de G. Así, se descartan el caso N3. Ahora vemos la última identificación.

- $\beta : a \mapsto b, b \mapsto c, c \mapsto a$

Supongamos que β define un automorfismo de G. Entonces tenemos que:

$$\beta(a^l b^s) = b^l (ab)^{-s} = b^l a^{-z_s} b^{-s} = b^{l-s} a^{-r^{n-s} z_s}$$

Sea $a^t b^v$ otro elemento de G. Entonces

$$\beta(a^l b^s)\beta_3(a^t b^v) = b^{l-s} a^{-r^{n-s} z_s} b^{t-v} a^{-r^{n-v} z_v} = b^{l-s+t-v} a^{-r^{t-v} r^{n-v} z_v - r^{n-s} z_s}$$

Por otra parte $z = a^l b^s a^t b^v = a^l a^{tr^{n-s}} b^s b^v = a^{l+tr^{n-s}} b^{s+v}$. Luego, llamando nuevamente $l + tr^{n-s} = l'$, tenemos que $\beta(z) = b^{l'-(s+v)} a^{-r^{n-(s+v)} z_{s+v}}$. Para que β sea automorfismo, comparando exponentes, para todo s y t debe cumplirse que $l' = l + t$. Anteriormente vimos que la última igualdad no es cierta. Por lo tanto, β no define un automorfismo de G. Así, se descarta el caso N2. □

2. Supongamos que n es potencia de 2. Por simplicidad, denominamos $r = \nu_j$ con $j = 1, 2, 3$.

Primero, verificamos con:

$$\alpha_2 : a \mapsto b^{-1}ab, b \mapsto c, c \mapsto b$$

Ya sabemos que $b^{-1}ab = a^r$. Entonces, si α_2 define a un automorphismo de G, y $a^l b^s$ es un elemento de G, se tendría que $\alpha_2(a^l b^s) = a^{rl}(ab)^{-s}$. Recordando que $z_s = \sum_{k=1}^{s} r^k$, se tiene que $\alpha_2(a^l b^s) = a^{rl-z_s} b^{-s}$. Ya vimos que

$$\alpha_2(a^l b^s)\alpha_2(a^t b^v) = a^{rl-z_s+r^s(rt-z_v)} b^{-s-v}$$

Por otra parte, si $z = a^l b^s a^t b^v$, tenemos

$$\alpha_2(z) = a^{r(l+tr^{n-s})-z_{s+v}} b^{-s-v}$$

Entonces para que α_2 sea automorfismo, comparando exponentes debe cumplirse que $tr^{s+1} = tr^{n-s+1}$, lo que es equivalente a que $tr^s = tr^s$, igualdad que se cumple para todo s y t, independiente de r. Entonces, en este caso, α_2 define un automorfismo de G.

Veamos que β no extiende a un automorfismo de G. Para ello, tomamos $x = ab$ y $y = ab^3$. Si β extiende a un automorfismo de G, tendríamos que:

$$\beta(xy) = \beta(abab^3) = \beta(a^{r+1}b^4) = b^{r+1}(ab)^{-4}$$

Además, $\beta(x) = \beta(ab) = a^{-1}$ y $\beta(y) = \beta(ab)\beta(b^2) = a^{-1}(ab)^{-2}$. Así, tenemos que $\beta(x)\beta(y) = a^{-2}(ab)^{-2}$. Si $\beta(x)\beta(y) = \beta(xy)$, tendriamos que $b^{r+1}(ab)^{-4} = a^{-2}(ab)^{-2}$, lo que implica que $b^{r+1}(ab)^{-2} = a^{-2}$. Luego, $b^{r+1} = a^{-2}(ab)^2 = a^{-2}b^2a^{r+1} = b^2a^{r-1}$ y por ello, $\Rightarrow b^{r-1} = a^{r-1}$.

La úlima igualdad no es posible pues $A \cap B = \{1\}$. Por lo tanto, β no extiende a un automorfismo de G. □

Observación 3.4.1 *Como consecuencia del Teorema 3.4.3, se tiene que existe un elemento d de $\mathbf{Aut}(\mathcal{X})$ tal que $d^2 = 1, dad = a^r$ y $dbd = (ab)^{-1}$.*

La firma de $\mathbf{Aut}(\mathcal{X})$ es $(0; 2, n, 2n)$. El elemento d ayuda a formar un vector generador para $\mathbf{Aut}(\mathcal{X})$ con dicha firma:

Proposición 3.4.1 *Para cualquier $1 \leq j \leq 3$ se tiene que $(d, b, (db)^{-1})$ es un vector generador de $\mathbf{Aut}(\mathcal{X})$ y la firma de ese vector generador es $(0; 2, n, 2n)$.*

Demostración: Primero, notamos que por la observación anterior, d normaliza G, por lo tanto $N_{\mathbf{Aut}(\mathcal{X})}(G)$ contiene estrictamente a G, lo que obliga a que

$N_{\mathbf{Aut}(\mathcal{X})}(G) = \mathbf{Aut}(\mathcal{X})$. Por lo tanto, $\mathbf{Aut}(\mathcal{X}) = \langle a, b, d \rangle$. Segundo, vemos que db tiene orden $2n$ pues:

$$(db)^2 = dbdb = (ab)^{-1}b = b^{-1}a^{-1}b = a^{-r}$$

y el elemento a^r tiene orden n, lo que demuestra lo pedido. □.

De lo anterior, también se desprende que d no normaliza B ni C. Esto lo resumimos en lo siguiente:

Proposición 3.4.2 *$N_{Aut(\mathcal{X})}(A) = Aut(\mathcal{X})$ y para $H \in \{B, C\}$, $N_{Aut(\mathcal{X})}(H) = N_G(H)$.*

Capítulo 4

$\mathcal{X}_{n,j}$ como curva n-gonal

En este capítulo desarrollaremos las propiedades de $\mathcal{X}_{n,j}$ como un cubrimiento cíclico de la esfera de Riemann. En particular determinaremos una ecuación algebraica que defina a $\mathcal{X}_{n,j}$ y realizaremos los generadores de $G_{n,j}$ como automorfismos explícitos de $\mathcal{X}_{n,j}$ como curva plana afín. Además, determinaremos ecuaciones para los cocientes intermedios de $\mathcal{X}_{n,j}$ por algunos subgrupos estudiados en el capítulo anterior, y si es posible, sus grupos de automorfismos. En el caso de que n es potencia de 2, también realizaremos el elemento d de $\mathbf{Aut}(\mathcal{X}_{n,j})$ como automorfismo explícito.

De acuerdo a lo estudiado en la sección 2.7, se establece que los pasos para encontrar la ecuación para una superficie n-gonal son los siguientes:

1. Determinar el normalizador N del grupo cíclico n-gonal C_n en G y el grupo $K = N/C_p$.

2. Determinar las firmas de G y C_n.

3. Determinar una identificación de $\mathcal{X}_{C_n}$ con la esfera de Riemann de modo que el grupo K sea un grupo de automorfismos de $\widehat{\mathbb{C}}$ y usar los puntos de alguna órbita bajo K como los puntos rama de la proyección cociente π_{C_p}.

4. Estudiar la acción de K en C_n.

5. Aplicar el Teorema 2.6.2.

Usando estas ideas demostraremos el siguiente teorema:

Teorema 4.0.1 *Sea $n = p^m$ una potencia de primo con $m \geq 3$, y consideremos $G_{n,j}$ actuando en $\mathcal{X}_{n,j}$:*

1. Si n es potencia de un primo impar, entonces

$$y^n = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t}$$

es una ecuación para $\mathcal{X}$ como curva n-gonal, donde $\lambda = e^{2\pi i/p^{m-j}}$.

2. Si n es potencia de 2, entonces

$$y^n = (x^{\frac{n}{2}} - 1)(x^{\frac{n}{2}} + 1)^{\nu_j}$$

es una ecuación para $\mathcal{X}$ como curva n-gonal.

Demostración: En nuestro caso, $C_n = A$, y $K = G/A$ es un grupo cíclico. Así, por lo explicado en la Sección 2.6, y por Proposición 3.3.1, este método se puede aplicar a nuestro caso. Ya tenemos listos los pasos (i) y (ii). Para el paso (iii), usando la Tabla 1, vemos que K actúa en $\hat{\mathbb{C}}$ como grupo de automorfismos, por ello deja dos puntos fijos. Sin perder generalidad, podemos elegi dichos puntos como 0 e ∞. Además $K = \langle [b] \rangle$ donde $[b]$ denota la clase de b en ese grupo cociente. Entonces podemos ver $[b]^{-1}$ como una funcion de la forma $\phi(z) = \omega z + \mu$, donde ω y μ son números complejos. Pero ϕ debe ser una transformación de Möbius de orden finito, lo que obliga a que $\mu = 0$ y ω debe ser una raiz n-ésima primitiva de la unidad. Como la firma de A es $(0; n^{(n)})$, la proyección cociente $\mathcal{X} \to \mathcal{X}_A$ tiene exactamente n puntos rama con indices de ramificación n. Estos puntos al ser vistos como elementos de $\hat{\mathbb{C}}$, serán las raices del polinomio $f(x)$ tal que $y^n = f(x)$ es una ecuación para $\mathcal{X}$. Moviendo adecuadamente por una transformación de Mobius, podemos suponer que uno de esos puntos es 1.

Ahora vemos la acción de K en C_n. Esta acción se denota por:

$$[b].a = bab^{-1}$$

Entonces $[b]^{-1}.a = a^r$, donde $r = r_j$ en el caso p impar, o $r = \nu_j$ en el caso $p = 2$. Aplicando la parte (v), usando $[b]^{-1}$ como generador de K, vemos que el factor $(x - \omega^k)$ de $f(x)$ tiene multiplicidad ρ_k donde $1 \leq rho_k \leq n-1$ y $\rho_k \equiv_n r^k$. Dependiendo de n, esto nos dice lo siguiente:

1. Si n es potencia de un primo impar, tenemos que hay exactamente p^{m-j} números de la forma ρ_k. Además si $\rho_k = \rho_l$, entonces $r^k \equiv_n r^l$, lo que implica que $l - k \equiv_n p^{m-j}$. De esta forma, se ve que hay exactamente p^j factores que tienen multiplicidad ρ_k, y estos factores son de la forma $(x - \omega^{l+tp^{m-j}})$ donde $0 \leq l \leq p^{m-j} - 1$. Además:

$$\prod_{t=0}^{p^j-1}(x-\omega^{l+tp^{m-j}}) = x^{p^j} - \omega^{lp^j+\chi}$$

donde

$$\chi = \sum_{t=0}^{p^j-1}(tp^{m-j}) = p^{m-j}\sum_{t=0}^{p^j-1} t = \frac{p^{m-j}(p^j-1)p^j}{2} = \frac{(p^j-1)n}{2}$$

es un divisor de n.

2. Si n es potencia de 2, vemos que si k es impar, $\rho_k = r$ y si k es par, $\rho_k = 1$, de esta forma vemos que los factores $(x-\omega^k)$ se agrupan de acuerdo si k es par o no. Además:

$$\prod_{t=0}^{\frac{n}{2}-1}(x-\omega^{2t}) = x^{\frac{n}{2}} - 1, \quad \prod_{t=0}^{\frac{n}{2}-1}(x-\omega^{2t+1}) = x^{\frac{n}{2}} + 1$$

Esto demuestra el teorema. □

A continuación mostramos algunos ejemplos de este teorema:

Ejemplo 4.0.1 *Si consideramos $p = m = 3$ y $j = 2$, es decir $r = r_2 = 1 + 3^2 = 10$, tenemos que el orden de r_2 módulo 27 es 3. Además $\rho_1 = 10$, $\rho_2 = r^2 = 100 \equiv_{27} 3$. Denotando $\lambda = e^{2\pi i/3}$, tenemos que $\mathcal{X}_{27,2}$ es isomorfa a la curva definida por:*

$$y^{27} = (x^9-1)(x^9-\lambda)^{10}(x^9-\lambda^2)^{19}$$

Ejemplo 4.0.2 *Si consideramos $p = 2$, $m = 4$ y $j = 3$, es decir $r = \nu_3 = 2^4 - 1 = 15$, entonces $X\_16, 3$ tiene como ecuación a:*

$$y^{16} = (x^8-1)(x^8+1)^{15}$$

Es claro que la curva plana afín determinada por tal ecuación es singular, pero resolviendo sus singularidades se obtiene una superficie de Riemann que es isomorfa a $\mathcal{X}$.

Haremos ahora un estudio de la curva, sus propiedades como curva plana, sus automorfismos y los cocientes interemedios por algunos subgrupos. Este estudio se divide según el caso de p impar o $p = 2$.:

4.1. Caso p impar

En este caso nuestra ecuación para $\mathcal{X}$ es:

$$y^n = f(x) = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t}$$

Denotemos $g(x) = y^n - f(x)$. Las singularidades de la ecuación se pueden determinar viendo cuales son los factores de $f(x)$ con multiplicidad mayor a 1. Esto se resume en:

Lema 4.1.1 *Las singularidades de $\mathcal{X}$ son de la forma $(\xi, 0)$ donde ξ es una raiz de*

$$\prod_{t=1}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t} = \frac{f(x)}{x^{p^j} - 1}$$

Para las posibles singularidades en la clausura proyectiva de $\mathcal{X}$, tenemos lo siguiente:

Lema 4.1.2 *En la clausura projectiva de la curva plana definida por $g(x)$, las singularidades son $[0:1:0]$ y los puntos de la forma $[\xi:0:1]$ donde ξ es una raiz de $f(x)/(x^{p^j}-1)$.*

Demostración: Primero calculemos la homogeneización de g. Antes de ello, notamos que los ρ_k, módulo n forman el subgrupo H de la observación 3.0.1, por ello, usando el Lema A.0.6 se ve que:

$$\sum_{k=0}^{p^{m-j}-1} \rho_k \equiv_n p_{m,j} = \frac{n(p^{m-j}+1)}{2}$$

Es claro que el grado de g es $p^i p_{m,j}$. Esto lo usaremos al calcular la homogeneización de g. Esta se define, de acuerdo a la Definición 2.2.4 por:

$$H_g(x,y,z) = z^{p^i p_{m,j}} g\left(\frac{x}{z}, \frac{y}{z}\right)$$

$$= z^{p^j p_{m,j}} \left(\frac{y^n}{z^n} - \prod_{t=0}^{p^{m-j}-1} \left(\frac{x^{p^j}}{z^{p^j}} - \lambda^t \right)^{\rho_t} \right) = z^{p^j p_{m,j}} \left(\frac{y^n}{z^n} - \prod_{t=0}^{p^{m-j}-1} \left(\frac{x^{p^j} - \lambda^t z^{p^j}}{z^{p^j}} \right)^{\rho_t} \right)$$

$$= z^{p^j p_{m,j}} \left(\frac{y^n}{z^n} - \frac{\prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t z^{p^j})^{\rho_t}}{z^{p^j p_{m,j}}} \right) = z^{p^i p_{m,j} - n} y^n - \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t z^{p^j})^{\rho_t}$$

Observando que:

$$p^j p_{m,j} - n = p^j \left(p^{m-j} + \frac{n(p^{m-j}+1)}{2} \right) - n$$

$$= n - \frac{p^j n(p^{m-j}+1)}{2} - n = \frac{n(n+p^j)}{2}$$

y denotando este último número por n_j se tiene que H_g es igual a:

$$H_g(x,y,z) = z^{n_j} y^n - \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t z^{p^j})^{\rho_t}$$

Notamos que si $y = 0$, entonces:

$$\prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t z^{p^j})^{\rho_t} = 0$$

Lo que hace que si $z = 1$, entonces x es una raiz n-ésima de la unidad. Entonces en la clausura proyectiva de S no hay singlaridades aparte de las ya encontradas si $y = 0$. Supongamos entonces que $y \neq 0$. Al calcular la derivada parcial de H_g en y nos queda:

$$\frac{\partial H_g}{\partial y} = n z^{n_j} y^{n-1}$$

Esa derivada sólo se anula si $z = 0$. Pero esto implica, por la ecuación $H_g(x,y,z) = 0$, que $x = 0$. Es claro que las otras derivadas parciales son polinomios homogéneos no constantes que se anulan en $[0:1:0]$. □

Nos interesa determinar el tipo de dichas singularidades:

Lema 4.1.3 *Una singularidad de la forma $(\xi, 0)$ en la curva definida por $y^n - f(x)$ es de tipo (n, ρ_k) para algún entero positivo k.*

Demostración: Debemos representar $y^n - f(x)$ como una suma de potencias de series de potencias en torno a $(\xi, 0)$ sin término constante. Elegimos $h_1(x-\xi, y) = y$. Ese nos dará una serie elevada a n. Ahora hay que encontrar otra serie elevada a ρ_k para algún k. Elegimos ρ_k como la multiplicidad de ξ en $f(x)$.

Sea $f_\xi(x) = f(x)/(x-\xi)^{\rho_k}$. Este polinomio no se anula en una vecindad simplemente conexa en $\mathbb{C}$ de ξ, por lo tanto, existe $h_\xi(x-\xi)$ serie de potencias en torno a ξ tal que $f_\xi(x) = (h_\xi(x-\xi))^{\rho_k}$. Así,

$$f(x) = f_\xi(x)(x-\xi)^{\rho_k} = (h_\xi(x-\xi))^{\rho_k}(x-\xi)^{\rho_k}$$

Eligiendo $h_2(x-\xi,y)=(x-\xi)h_\xi(x-\xi)$ obtenemos el resultado deseado. □.

Lema 4.1.4 *El punto* $[0:1:0]$ *es una singularidad de tipo* (n,n_j) *en* $\mathcal{X}$.

Demostración: Sea $A_{H,y}$ la deshomogeneización de H_g en y. Se ve que:

$$A_{H,y}(x,z)=z^{n_j}-\prod_{t=0}^{p^{m-j}-1}(x^{p^j}-\lambda^t z^{p^j})^{\rho_t}$$

por lo tanto, la afinización de la clausura proyectiva de $y^n-f(x)$ en y es la curva plana de ecuación:

$$z^{n_j}=\prod_{t=0}^{p^{m-j}-1}(x^{p^j}-\lambda^t z^{p^j})^{\rho_t}$$

Queremos ver el lado derecho de esta ecuación como una serie de potencias elevada a n. Primero notamos que si dividimos ambos lados de la ecuación por $z^{p^j p_{m,j}}$ obtenemos:

$$z^{n_j-p^j p_{m,j}}=\prod_{t=0}^{p^{m-j}-1}\left(\frac{x^{p^j}}{z^{p^j}}-\lambda^t\right)^{\rho_t}$$

Recordando un cálculo anterior, $p^j p_{m,j}-n=n_j$, por lo que:

$$\frac{1}{z^n}=\prod_{t=0}^{p^{m-j}-1}\left(\frac{x^{p^j}}{z^{p^j}}-\lambda^t\right)^{\rho_t}$$

Si (x,z) tiende a $(0,0)$, el lado izquierdo de la ecuación tiende a ∞ por lo que x/z tiende a ∞, o equivalentemente, z/x tiende a 0. Por ello, reescribimos la ecuación

$$z^{n_j}=\prod_{t=0}^{p^{m-j}-1}(x^{p^j}-\lambda^t z^{p^j})^{\rho_t}$$

factorizando $x^{p^j p_{m,j}}$ en el segundo lado:

$$z^{n_j}=x^{p^j p_{m,j}}\prod_{t=0}^{p^{m-j}-1}\left(1-\lambda^t\frac{z^{p^j}}{x^{p^j}}\right)^{\rho_t}$$

Sea $\theta(z)$ definida por

$$\theta(z)=\prod_{t=0}^{p^{m-j}-1}(1-\lambda^t z^{p^j})^{\rho_t}$$

Esta función no se anula en una vecindad de 0, por lo que existe una serie de potencias $\vartheta(z)$ tal que $\theta(z) = \vartheta(z)^n$. Ahora, la función $\eta(x,z) = \theta(z/x)$ no se define en $(0,0)$ pero tiene una singularidad removible en ese punto pues z/x tiende a cero cuando (x,z) tiende a (0,0). De esta forma, existe una serie $\kappa(x,z)$ en torno a (0,0) tal que $\eta(x,z) = \kappa(x,z)^n = \vartheta(z/x)^n$. Así, la ecuación:

$$z^{n_j} = x^{p^j p_{m,j}} \prod_{t=0}^{p^{m-j}-1} \left(1 - \lambda^t \frac{z^{p^j}}{x^{p^j}}\right)^{\rho_t}$$

queda como:

$$z^{n_j} = x^{p^j p_{m,j}} \kappa(x,z)^n = (x^{p^j p_{m,j}/n} \kappa(x,z))^n$$

Lo que demuestra la afirmación. □.

Como consecuencia de esto, aplicando lo establecido en la Sección 2.4, se obtiene el siguiente corolario:

Corolario 4.1.1 *Considérese lo establecido en los lemas 4.1.3. y 4.1.4. La resolución de las singularidades de la clausura proyectiva de S agrega un punto por cada singularidad de la forma $[\xi, 0, 1]$ y n puntos por la singularidad $[0:1:0]$.*

Ahora, estamos en condiciones de calcular el género de nuestra curva plana afín:

Proposición 4.1.1 *El género de la curva plana afín definida por la ecuación del Teorema 4.0.1 en el caso de primo impar es:*

$$\frac{(n-1)(n-2)}{2}$$

Demostración: Definimos $\phi : \mathcal{X} \to \mathbb{C}$ por:

$$\phi(x,y) - x$$

Esta función es holomorfa y se extiende a una aplicación $\varphi : \mathcal{X} \to \hat{\mathbb{C}}$. Evidentemente la preimagen de ∞ bajo φ consta de los puntos que se agregan al remover la singularidad $[0:1:0]$. Si (x,y) no es singularidad de S, entonces es un punto de ramificación sí y sólo si la derivada de g en y es cero. Vemos que la derivada de g en y es ny^{n-1}. Así, si $y = 0$ entonces x debe ser una raiz p^j-ésima de la unidad.

Si $x = 0$, entonces $(0,y)$ no es singularidad, y hay exactamente n preimágenes de 0, debido a que si $(0,y) \in \mathcal{X}$,

$$y^n = \prod_{t=0}^{p^{m-j}-1} (0-\lambda^t)^{\rho_t} = (-1)^{p_{m,j}}\lambda^{\chi}$$

donde $\chi = \sum_{t=0}^{p^{m-j}-1} t\rho_t$. En el caso de las singularidades en $\mathcal{X}$, por el corolario 4.1.1 se tiene que los puntos que reemplazan a las singularidades del lema 4.1.3 son puntos de ramificación de φ con multiplicidad n. En total, tenemos n puntos de ramificación con multiplicidad n. Aplicamos todo esto a la fórmula de Riemann-Hurwitz:

$$g = -n+1+\frac{n(n-1)}{2} = \frac{n^2-n-2n+2}{2} = \frac{n^2-3n+2}{2} = \frac{(n-1)(n-2)}{2}$$

Lo que demuestra la proposición. □

Verificado el género de $\mathcal{X}$, nos interesa realizar G como su grupo de automorfismos. Previamente, notamos que si $0 \leq k \leq p^{m-j}-2$,

$$\rho_k r - \rho_{k+1} \equiv_n r^k r - r^{k+1} \equiv_n 0$$
$$\rho_{p^{m-j}-1} r - 1 \equiv_n r^{p^{m-j}-1} r - 1 \equiv r^{p^{m-1}} - 1 \equiv_n 0$$

Definición 4.1.1 *Para $0 \leq k \leq p^{m-j}-1$ se definen los siguientes números:*

$$t_k = \begin{cases} \frac{r\rho_k - \rho_{k+1}}{n} & k \neq p^{m-j}-1 \\ \frac{r\rho_k - 1}{n} & k = p^{m-j}-1 \end{cases}$$

Por conveniencia se puede extender esta definición a todo $\mathbb{N}$ diciendo que si k es congruente a l módulo n, $t_k = t_l$

Como consecuencia de ésto tenemos el siguinete corolario:

Corolario 4.1.2 $\sigma = \sum_{k=0}^{p^{m-j}-1} t_k \equiv_{p^j} 1$

Demostración: Por el apéndice A, tenemos que el número $p_{m,j} = \sum_{k=1}^{p^{m-j}} r^k = p^{m-j} + \frac{n(p^{m-j}+1)}{2}$. Con esto, tenemos que:

$$\sum_{k=0}^{p^{m-j}-1} t_k = \sum_{k=0}^{p^{m-j}-1} \frac{r\rho_k - \rho_{k+1}}{n} = \frac{1}{n}\left(r\sum_{k=0}^{p^{m-j}-1} \rho_k - \sum_{k=0}^{p^{m-j}-1} \rho_{k+1} \right)$$
$$= \frac{1}{n}(r-1)p_{m,j} = \frac{p^{m-j} + \frac{n(p^{m-j}+1)}{2}}{p^{m-j}} = 1 + \frac{p^j(p^{m-j}+1)}{2}$$

Lo que demuestra el lema. □

Asi, podemos realizar los generadores de G como automorfismos de $\mathcal{X}$ de la siguiente forma:

Teorema 4.1.1 *Sean α, β definidas por.*

$$\alpha(x,y) = (x,\omega y), \quad \beta(x,y) = \left(\omega x, \frac{y^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{t_k}}\right)$$

Entonces α y β son automorfismos de $\mathcal{X}$ y $\bar{G} = \langle \alpha, \beta \rangle \cong G$

Demostración: es evidente que α define un automorfismo de $\mathcal{X}$. En el caso de β, tenemos que ver que $g(\beta(x,y)) = 0$ si $(x,y) \in \mathcal{X}$:

$$g(\beta(x,y)) = g\left(\omega x, \frac{y^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{t_k}}\right)$$

$$= \left(\frac{y^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{t_k}}\right)^n - \prod_{k=0}^{p^{m-j}-1}((\omega x)^{p^j}-\lambda^k)^{\rho_k}$$

$$= \frac{y^{nr}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{nt_k}} - \prod_{k=0}^{p^{m-j}-1}(\lambda x^{p^j}-\lambda^k)^{\rho_k}$$

$$= \frac{y^{nr}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{nt_k}} - \prod_{k=0}^{p^{m-j}-1}\lambda(x^{p^j}-\lambda^{k-1})^{\rho_k}$$

Haciendo un cambio de variables en el segundo producto y denotando $\rho_{p^{m-j}} = \rho_0 = 1$, la escribimos como:

$$= \frac{y^{nr}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{nt_k}} - \lambda^{p_{m,j}} \prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{\rho_{k+1}}$$

Como $p_{m,j}$ es múltiplo de p^{m-j}, $\lambda^{p_{m,j}} = 1$. Ahora dejamos todo en una sola fracción:

$$= \frac{y^{nr} - \prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{\rho_{k+1}+nt_k}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{nt_k}}$$

Observamos que

$$\rho_{k+1} + nt_k = \rho_{k+1} + r\rho_k - \rho_{k+1} = r\rho_k$$

. Luego, la expresión anterior queda

$$\frac{y^{nr} - \prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{\rho_{k+1}+nt_k}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{nt_k}} = \frac{y^{nr} - \prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{r\rho_{k+1}}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{nt_k}}$$

$$= \frac{y^{nr} - (\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{\rho_k})^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{nt_k}}$$

El numerador de la expresión es divisible por $g(x)$, por lo tanto, β define un automorfismo de $\mathcal{X}$.

Debemos ver ahora que α y β cumplen con las relaciones que definen a $G_{n,j}$. Es claro que α tiene orden n. Para ver que β también tiene oren n requerimos un trabajo más largo, apoyándonos en el siguiente lema:

Lema 4.1.5 *Para todo $2 \leq l \leq n$, se tiene que:*

$$\beta^l(x,y) = \left(\omega^l x, \frac{y^{r^l}}{\lambda^{q_l}\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{u_{k,l}}}\right)$$

Donde

$$q_l = \sigma\sum_{v=1}^{l}(v-1)r^{l-v}, \quad u_{k,l} = \sum_{v=0}^{l-1} r^{l-1-v}t_{k+v}$$

Demostración del lema: Por inducción sobre l. Vemos primero que para $l = 2$ se cumple, pues $u_{k,1} = t_k$ y $q_1 = 0$. Supongamos que se cumple para $1 \leq l < n$. La demostraremos para $l+1$:

$$\beta^{l+1}(x,y) = \beta\left(\omega^l x, \frac{y^{r^l}}{\lambda^{q_l}\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{u_{k,l}}}\right)$$

$$= \left(\omega\omega^l x, \frac{\left(\frac{y^{r^l}}{\lambda^{q_l}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{u_{k,l}}}\right)^r}{\prod_{k=0}^{p^{m-j}-1}((\omega^l x)^{p^j} - \lambda^k)^{t_k}}\right) = \left(\omega^{l+1}x, \frac{\frac{y^{r^{l+1}}}{\lambda^{rq_l}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{ru_{k,l}}}}{\prod_{k=0}^{p^{m-j}-1}(\lambda^l x^{p^j} - \lambda^k)^{t_k}}\right)$$

$$= \left(\omega^{l+1}x, \frac{\frac{y^{r^{l+1}}}{\lambda^{rq_l}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{ru_{k,l}}}}{\lambda^{l\sigma}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^{k-l})^{t_k}} \right)$$

Reordenando el denominador la expresión queda:

$$= \left(\omega^{l+1}x, \frac{\frac{y^{r^{l+1}}}{\lambda^{rq_l}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{ru_{k,l}}}}{\lambda^{l\sigma}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{t_{k+l}}} \right) = \left(\omega^{l+1}x, \frac{y^{r^{l+1}}}{\lambda^{rq_l+l\sigma}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{ru_{k,l}+t_{k+l}}} \right)$$

Observamos que

$$rq_l + l\sigma = r\sigma\sum_{v=1}^{l}(v-1)r^{l-v} + l\sigma = \sigma(\sum_{v=1}^{l}(v-1)r^{l+1-v} + l) = \sigma\sum_{v=1}^{l+1}(v-1)r^{l-v} = q_{l+1}$$

$$ru_{k,l} + t_{k+l} = \sum_{v=0}^{l-1} r^{(l-v}t_{k+v} + t_{k+l} = \sum_{v=0}^{l} r^{l-v}t_{k+v} = u_{k,l+1}$$

De esta forma,

$$\beta^{l+1}(x,y) = \left(\omega^{l+1}x, \frac{y^{r^{l+1}}}{\lambda^{q_{l+l}}\prod_{k=0}^{p^{m-j}-1}(x^{p^j}-\lambda^k)^{u_{k,l+1}}} \right)$$

Completando la demostración. □

Continuación de la demostración del Teorema 4.1.1: Aplicando el Lema 4.1.5 con $l = p^{m-j}$, notamos que cambiando de variables obtenemos:

$$q_{p^{m-j}} = \sigma\sum_{v=1}^{p^{m-j}}(v-1)r^{p^{m-j}-v} = \sum_{v=0}^{p^{m-j}-1}(p^{m-j}-1-v)r^v \equiv_{p^{m-j}} -\sigma\sum_{v=0}^{p^{m-j}-1}(v+1)r^v$$

La suma se reescribe usando:

$$\sum_{v=0}^{p^{m-j}-1}(v+1)x^v = \frac{d}{dx}\left(\sum_{v=0}^{p^{m-j}-1}x^{v+1}\right)$$

$$= \frac{d}{dx}\left(\frac{x^{p^{m-j}+1}-x}{x-1}\right) = \frac{((p^{m-j}+1)x^{p^{m-j}}-1)(x-1)-x^{p^{m-j}+1}+x}{(x-1)^2}$$

De lo que deducimos que

$$\sum_{v=0}^{p^{m-j}-1}(v+1)r^v = \frac{((p^{m-j}+1)r^{p^{m-j}}-1)(r-1)-r^{p^{m-j}+1}+r}{(r-1)^2}$$

$$= \frac{(p^{m-j}r^{p^{m-j}}+r^{p^{m-j}}-1)(r-1)-r(r^{p^{m-j}}-1)}{(r-1)^2}$$

$$= \frac{p^{m-j}r^{p^{m-j}}(r-1)+(r^{p^{m-j}}-1)(r-1)-r(r^{p^{m-j}}-1)}{(r-1)^2}$$

$$= \frac{nr^{p^{m-j}}-(r^{p^{m-j}}-1)}{(r-1)^2}$$

Examinamos primero el numerador de la anterior expresión. Usando el lema A.0.6, lo podemos reescribir como:

$$nr^{p^{m-j}}-(r^{p^{m-j}}-1) = nr^{p^{m-j}}-p^j(1+r+...+r^{p^{m-j}-1})$$

$$nr^{p^{m-j}}-p^j\left(p^{m-j}+\frac{n(p^{m-j}+1)}{2}\right) = nr^{p^{m-j}}-n+\frac{np^j(p^{m-j}+1)}{2}$$

$$= n(r^{p^{m-j}}-1)+\frac{np^j(p^{m-j}+1)}{2}$$

Esto nos dice que el numerador es divisible por p^{2j}, lo que obliga a que la expresión $q_{p^{m-j}}$ sea divisible por p^{m-j}. A continuación, examinamos la suma $u_{k,p^{m-j}}$:

$$u_{k,p^{m-j}} = \sum_{v=0}^{p^{m-j}-1} r^{p^{m-j}-1-v}t_{k+v}$$

Si $k=0$, usando $\rho_0 = 1$, tenemos:

$$u_{0,p^{m-j}} = \sum_{v=0}^{p^{m-j}-1} r^{p^{m-j}-1-v}t_v = \sum_{v=0}^{p^{m-j}-1} r^{p^{m-j}-1-v}\left(\frac{r\rho_v-\rho_{v+1}}{n}\right)$$

$$= r^{p^{m-j}-1}\left(\frac{r\rho_0-\rho_1}{n}\right)-...-r\left(\frac{r\rho_{p^{m-j}-2}-\rho_{p^{m-j}-1}}{n}\right)-\frac{r\rho_{p^{m-j}-1}-\rho_0}{n}$$

$$= \frac{r^{p^{m-j}} - r^{p^{m-j}-1}\rho_1 + r^{p^{m-j}-1}\rho_1 + r^{p^{m-j}-2}\rho_2 + ...}{n}$$

$$\frac{... + r^2\rho_{p^{m-j}-2} - r\rho_{p^{m-j}-1} + r\rho_{p^{m-j}-2} - 1}{n} = \frac{r^{p^{m-j}} - 1}{n}$$

Si $k \neq 0$, vemos que:

$$u_{k,p^{m-j}} = \sum_{v=0}^{p^{m-j}-1} r^{p^{m-j}-1-v} t_{k+v} =$$

$$\sum_{v=0}^{p^{m-j}-1} r^{p^{m-j}-1-v} t_{k+v} + \sum_{v=0}^{k-1} r^{p^{m-j}-1-v+k} t_v - \sum_{v=0}^{k-1} r^{p^{m-j}--v+k} t_v$$

Separando sumas, vemos que:

$$= \sum_{v=0}^{p^{m-j}-k-1} r^{p^{m-j}-1-v} t_{k+v} + \sum_{v=p^{m-j}-k}^{p^{m-j}-1} r^{p^{m-j}-1-v} t_{k+v} ...$$

$$... + \sum_{v=0}^{k-1} r^{p^{m-j}-1-v+k} t_v - \sum_{v=0}^{k-1} r^{p^{m-j}--v+k} t_v$$

Cambiando de variables de v a $k+v$ en el primer sumando y de v a $v-(p^{m-j}-k$ en el segundo sumando las sumatorias quedan:

$$= \sum_{v=k}^{p^{m-j}-1} r^{p^{m-j}-1-v+k} t_v + \sum_{v=0}^{k-1} r^{k-1-v} t_{v+p^{m-j}} ...$$

$$... + \sum_{v=0}^{k-1} r^{p^{m-j}-1-v+k} t_v - \sum_{v=0}^{k-1} r^{p^{m-j}-1-v+k} t_v$$

Juntando el primer y tercer sumandos, juntando el segundo con el cuarto, e identificando $t_{v+p^{m-j}}$ con t_v, se tiene:

$$= \sum_{v=0}^{p^{m-j}-1} r^{p^{m-j}-1-v+k} t_v + \sum_{v=0}^{k-1} (r^{k-1-v} t_v - r^{p^{m-j}-1-v+k} t_v)$$

$$= r^k u_{0,p^{m-j}} + (1 - r^{p^{m-j}}) \sum_{v=0}^{k-1} r^{k-1-v} t_v$$

La sumatoria $\sum_{v=0}^{k-1} r^{k-1-v} t_v$ se calcula de la misma forma que $u_{0,p^{m-j}}$ y es igual a

$$= \frac{r^{k-1}(r-\rho_1) - r^{k-2}(r\rho_1 - \rho_2) + \ldots + \rho_{k-1} - \rho_k}{n} = \frac{r^k - \rho_k}{n}$$

De esta forma:

$$u_{k,p^{m-j}} = r^k \frac{r^{p^{m-j}} - 1}{n} - (r^{p^{m-j}} - 1)\frac{r^k - \rho_k}{n}$$
$$\frac{(r^{p^{m-j}} \quad 1)(r^k \quad r^k \mid \rho_k)}{n} = \frac{(r^{p^{m-j}} \quad 1)\rho_k}{n}$$

Juntando los cálculos anteriores, vemos que:

$$\beta^{p^{m-j}}(x,y) = \left(\omega^{p^{m-j}} x, \frac{y^{r^{p^{m-j}}}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{(r^{p^{m-j}}-1)\rho_k/n}}\right)$$
$$= \left(\omega^{p^{m-j}} x, \frac{y y^{r^{p^{m-j}}-1}}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{(r^{p^{m-j}}-1)\rho_k/n}}\right)$$
$$= \left(\omega^{p^{m-j}} x, \frac{y(y^n)^{(r^{p^{m-j}}-1)/n}}{(\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)\rho_k)^{(r^{p^{m-j}}-1)/n}}\right)$$
$$= \left(\omega^{p^{m-j}} x, y\left(\frac{y^n}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} \quad \lambda^k)\rho_k}\right)^{(r^{p^{m-j}}-1)/n}\right) = (\omega^{p^{m-j}} x, y)$$

Es claro que $\beta^{p^{m-j}}$ tiene orden p^j, por lo tanto, β tiene orden n. Veamos que α y β cumplen con la relación restante. Esto es equivalente a que $\beta\alpha = \alpha^r\beta$:

$$\beta(\alpha(x,y)) = \beta(x,\omega y) = \left(\omega x, \frac{(wy)^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{t_k}}\right) = \left(\omega x, \frac{\omega^r y^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{t_k}}\right)$$

$$\alpha^r(\beta(x,y)) = \alpha^r\left(\omega x, \frac{y^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{t_k}}\right) = \left(\omega x, \omega^r \frac{y^r}{\prod_{k=0}^{p^{m-j}-1}(x^{p^j} - \lambda^k)^{t_k}}\right)$$

Finalmente notando que ninguna potencia de α está contenida en el grupo generado por β, concluimos que $\bar{G} = \langle \alpha, \beta \rangle$ es isomorfo a $G_{n,j}$. □

Ejemplo 4.1.1 *Consideremos $p = 3$, $m = 4$ y $j = 2$, de modo que $r = 3^2 + 1 = 10$. Entonces los números ρ_k y t_k son los siguientes:*

k	ρ_k	t_k
0	1	0
1	10	1
2	19	2
3	28	3
4	37	4
5	46	5
6	55	6
7	64	7
8	73	8

Fijando $\lambda = e^{2\pi i/9}$, tenemos que una ecuación para $X_{81,2}$ es

$$y^{81} = f_1(x)f_2(x)$$
$$f_1(x) = (x^9-1)(x^9-\lambda)^{10}(x^9-\lambda^2)^{19}(x^9-\lambda^3)^{28}(x^9-\lambda^4)^{37}$$
$$f_2(x) = (x^9-\lambda^5)^{46}(x^9-\lambda^6)^{55}(x^9-\lambda^7)^{64}(x^9-\lambda^8)^{73}$$

Los automorfismos α y β se pueden ver como:

$$\alpha(x,y) = (x, e^{2\pi i/81}y), \quad \beta(x,y) = \left(e^{2\pi i/81}x, \frac{y^{10}}{g_1(x)g_2(x)}\right)$$
$$g_1(x) = (x^9-\lambda)^1(x^9-\lambda^2)^2(x^9-\lambda^3)^3(x^9-\lambda^4)^4$$
$$g_2(x) = (x^9-\lambda^5)^5(x^9-\lambda^6)^6(x^9-\lambda^7)^7(x^9-\lambda^8)^8$$

El número σ se calcula como:

$$\sigma = 1 + \frac{3^2(3^{4-2}+1)}{2} = 1 + 45 = 46$$

Si tomamos $l = 8$, entonces

$$q_8 = 46(10^6 + 2\cdot 10^5 + 3\cdot 10^4 + 4\cdot 10^3 + 5\cdot 10^2 + 6\cdot 10 + 7) = 56790082 \equiv_9 1$$

Los $u_{k,8}$ se expresan en la siguiente tabla

k	$u_{k,8}$
0	80123456
1	1234567
2	12345678
3	23456780
4	34567801
5	45678012
6	56780123
7	67801234
8	78012345

Observación 4.1.1 *De lo anterior se ve que $\beta\alpha\beta^{-1} = \alpha^r$. Recordemos que los elementos a y b de G cumplen que $b^{-1}ab = a^r$. Entonces a se corresponde con α, b con β^{-1}, y $c = (ab)^{-1}$ con $\gamma = \beta\alpha^{-1}$. Con esto se verifica que que $\gamma^{p^{m-j}} = \beta^{p^{m-j}}\alpha^{-p^{m-j}}$. Notamos que $\beta^{p^{m-j}}(x,y) = (\omega^{p^{m-j}}x, y)$ es coherente con el hecho de que $b^{p^{m-j}} \subset Z(G)$.*

Proposición 4.1.2 *El género de $\mathcal{X}_{\langle\alpha\rangle}$ es cero.*

Demostración: Calculemos los puntos fijos de α. Si (x,y) es punto fijo bajo α, debe cumplir que $(x,y) = (x,\omega y)$, lo que obliga a que $y = 0$, y por ende, los puntos de la forma $(\xi, 0)$ con ξ raíz n-ésima de la unidad son puntos fijos de α. Como algunos de estos puntos son singularidades, se establece que los puntos que resuelven dichas singularidades son los puntos fijos de α al verlos en X. Por la fórmula de Riemann-Hurwitz, llamando g' al género de $X_{\langle\alpha\rangle}$, existe un entero no negativo R que:

$$\frac{(n-1)(n-2)}{2} = n(g'-1) + 1 + \frac{n}{2}\left(n(1-\frac{1}{n}\right) + R$$

$$\Rightarrow \frac{(n\quad 1)(n\quad 2)}{2} = n(g'-1) + 1 + \frac{n(n\quad 1)}{2} + R$$

$$\Rightarrow \frac{(n-1)(n-2)}{2} = ng' - n + 1 + \frac{n(n-1)}{2} + R$$

$$\Rightarrow \frac{(n-1)(n-2)}{2} = ng' + \frac{(n-1)(n-2)}{2} + R$$

Lo que obliga a que $ng' = -R$. Como R es no negativo, esto fuerza a que $R = 0$ y con ello, $g' = 0$. Por lo tanto, no hay más puntos fijos, lo que confirma la n-gonalidad cíclica de $\mathcal{X}$. □

De la proposición anterior concluimos que $\mathcal{X}_{\bar{G}}$ es de género 0. Por lo tanto, la proyección $\mathcal{X}_{\langle\alpha\rangle} \to \mathcal{X}_{\bar{G}}$ es un cubriente cíclico de grado n con dos puntos rama de multiplicidad n. Evidentemente esos dos puntos rama no pueden venir de los puntos rama de la proyección cociente $\mathcal{X} \to \mathcal{X}_{\langle\alpha\rangle}$ pues β mueve los puntos fijos de α de modo que estos forman una sóla orbita de largo n (dado que $\beta(\xi, 0) = (\omega\xi, 0)$. De esta forma, la composición de dichas proyecciones envía $\mathcal{X}$ a $\hat{\mathbb{C}}$ con tres puntos marcados con índices n, realizando la firma de $\bar{G}$ como $(0; n, n, n)$. Esto se resume en el siguiente teorema:

Teorema 4.1.2 *Sea $n = p^m$ una potencia de un primo impar con $m \geq 3$. Sea $r = 1 + p^i$ con $1 \leq i \leq m-1$. Sea G el grupo definido por la siguiente presentación:*

$$G = G_{n,j} = \langle a, b | a^n = b^n = 1, b^{-1}ab = a^{r^j} \rangle$$

Entonces G actúa en una superficie de Riemann compacta $\mathcal{X}_{n,j}$ de género

$$\frac{(n-1)(n-2)}{2}$$

con firma $(0; n, n, n)$ y ecuación algebraica de la forma:

$$y^n = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t}$$

donde ρ_j son números entre 1 y $n-1$ tales que ρ_k es congruente a r_j^k módulo n, y λ es una raiz p^j-ésima primitiva de la unidad. Los elementos a y b se realizan en $Aut(\mathcal{X})$ como α y β definidos en el Teorema 4.1.1. Además, $G_{n,j} \cong Aut(\mathcal{X}_{n,j})$.

4.1.1. Ecuaciones para cocientes intermedios

Ahora, determinaremos ecuaciones para los cocientes de $\mathcal{X}$ por ciertos subgrupos de G.

1. **Centro de G y serie central ascendente:** Recordemos que $\alpha^{p^{m-j}}$ y $\beta^{p^{m-j}}$ generan $Z(G)$ y la firma de dicho subgrupo es:

$$\left(\frac{(p^{m-j}-1)(p^{m-j}-2)}{2}, p^j_{(3p^{m-j})}\right)$$

Para los términos de la serie central ascendente, que llamamos Z_k, en el caso en que $j < m-j$, con $1 \leq k \leq s+1$ y s denota el mayor entero positivo tal que $sj < m-j$, la firma de Z_k es:

$$\left(\frac{(p^{m-kj}-1)(p^{m-kj}-2)}{2}, (p^{kj})^{(3p^{m-kj})}\right)$$

Proposición 4.1.3 *Considerando la notación del Teorema 4.1.2 y la Observación 4.1.4.*

- *Si $j \geq m-j$ entonces $\mathcal{X}_{Z(G)}$ es una curva de Fermat de grado p^j.*
- *Si $j < m-j$ y $s = \left[\frac{m}{j}\right] - 1$, entonces $\mathcal{X}_{Z_{s+1}}$ es una curva de Fermat de grado $p^{(s+1)j}$, y los cocientes $\mathcal{X}_{Z_k}$ con $1 \leq k \leq s$ son curvas de tipo Fermat de grado p^{kj}.*

Demostración: Existe una proyección natural $\pi_{k,k+1} : \mathcal{X}_{Z_k} \to \mathcal{X}_{Z_{k+1}}$ originada por la acción de Z_{k+1}/Z_k en $\mathcal{X}_{Z_k}$. Tal grupo cociente es abeliano, por ser cociente de grupos consecutivos en una serie central ascendente. En particular, si $k = s+1$, $Z_{k+1}/Z_k = G/Z_k$ es abeliano y $\pi_{s+1,s+2}$ es una proyección de $\mathcal{X}_{Z_{s+1}}$ en la esfera de Riemann. La firma de ese término es:

$$\left(\frac{(p^{m-(s+1)j}-1)(p^{m-(s+1)j}-2)}{2}, (p^{(s+1)j})^{(3p^{m-(s+1)j})}\right)$$

Como la firma de G es $(0; n, n, n)$, necesariamente los $3p^{m-(s+1)j}$ puntos de $\mathcal{X}_{Z_{s+1}}$ marcados con $p^{(s+1)j}$ deben ser las preimágenes de los tres puntos marcados con n en la esfera. El orden de G/Z_{s+1} es $p^{2(m-(s+1)j)}$ y es isomorfo a un producto directo de $\mathbb{Z}_{p^{m-(s+1)j}}$ consigo mismo. Como consecuencia de esto, la firma de la acción de G/Z_{s+1} en $\mathcal{X}_{Z_{s+1}}$ es $(0; p^{m-(s+1)j}, p^{m-(s+1)j}, p^{m-(s+1)j})$

Esta situación ocurre también si $j \geq m-j$, en ese caso la situación de Z_{s+1} se da con $Z(G)$ pues en ese caso $G/Z(G)$ es abeliano.

Lo anterior es un caso particular de una situación más general: fijando k entre 1 y $s+1$ inclusive, la función ψ_k definida como

$$\psi_k = \pi_{s+2,s+1} \circ \ldots \circ \pi_{k,k+1}$$

es una projección de $\mathcal{X}_{Z_k}$ en la esfera dada por la acción de G/Z_k que es un producto semidirecto de $\mathbb{Z}_{p^{kj}}$ consigo mismo. De forma análoga a $k = s+1$, se ve que la firma de esta acción en $\mathcal{X}_{Z_k}$ es $(0; p^{m-kj}, p^{m-kj}, p^{m-kj})$. □

Como consecuencia de esto, obtenemos el siguiente corolario:

Corolario 4.1.3 *Considerando la notación de la proposición anterior:*

- *Si $j \geq m-j$ entonces una ecuación que define a $\mathcal{X}_{Z(G)}$ es:*

$$y^{p^{m-j}} = x^{p^{m-j}} \quad 1$$

- *Si $j < m-j$ y $s = \left[\frac{m}{j}\right] - 1$, entonces para $1 \leq k \leq s+1$, una ecuación que define a $\mathcal{X}_{Z_k}$ es:*

$$y^{p^{m-kj}} = \prod_{t=0}^{p^{m-(k+1)j}-1} (x^{p^j} - \zeta^t)^{\tau_t}$$

Donde los τ_t son números con $1 \leq t \leq p^{m-kj}-1$ tal que τ_t es congruente a r_j^t módulo p^{m-kj} y $\zeta = e^{2\pi i/p^{m-2j}}$.

Mostraremos como obtener la ecuación para $\mathcal{X}_{Z(G)}$ a partir de la de $\mathcal{X}$. Consideremos Y como la curva algebraica definida por

$$y^{p^{m-kj}} = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \zeta^t)^{\tau_t}$$

de acuerdo al corolario anterior. Primero extendemos la definición de τ_t para todo entero no negativo diciendo que si $t \equiv_{p^{m-2j}} k$ y $0 \leq k \leq p^{m-2j}-1$, $\tau_t = \tau_k$. Notamos también que $\rho_t - \tau_t$ es divisible por p^{m-j}

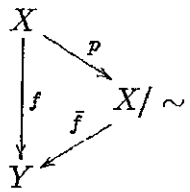
Lema 4.1.6 *La aplicación $\pi_{\mathcal{Y}} : \mathcal{X} \to \mathcal{Y}$ definida por*

$$\pi_{\mathcal{Y}}(x,y) = \left(x^{p^j}, \frac{y^{p^j}}{\prod_{t=0}^{p^{m-j}-1}(x^{p^j} - \lambda^t)^{(\rho_t - \tau_t)/p^j}} \right)$$

es holomorfa e induce un isomorfismo entre $\mathcal{Y}$ y $\mathcal{X}_{Z(G)}$

Demostración: Esta demostración requiere el siguiente lema:

Lema 4.1.7 *Sea $f : X \to Y$ una aplicación continua y sobre entre espacios topológicos y sea $\sim$ una relación de equivalenca en X. Suponga que $x \sim y$ sí y solo si $f(x) = f(y)$. Entonces f induce un homeomorfismo $\bar{f} : X/\sim \to Y$ tal que el siguiente diagrama es conmutativo:*



(4.1)

donde p denota la proyección cociente de X en X/ ∼

Demostración del lema 4.1.8: se puede ver en [19], págs 142-143.

Demostración del lema 4.1.7: Debemos verificar que $\pi_{\mathcal{Y}}$ está bien definida y respeta la relación de equivalencia en el sentido del lema 7.1.8. Veamos primero que $\pi_{\mathcal{Y}}$ está bien definida. Si $\pi_{\mathcal{Y}}(x,y) = (z,w)$, entonces

$$w^{p^{m-j}} = \left(\frac{y^{p^j}}{\prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{(\rho_t - \tau_t)/p^{m-j}}} \right)^{p^{m-j}} = \frac{y^n}{\prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t - \tau_t}}$$

$$= \frac{\prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t}}{\prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t - \tau_t}} = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} \quad \lambda^t)^{\tau_t} = \prod_{t=0}^{p^{m-j}-1} (z \quad \lambda^t)^{\tau_t}$$

Notamos que el último producto se puede reescribir como:

$$\prod_{t=0}^{p^{m-2j}-1} \prod_{k=0}^{p^j-1} (z - \lambda^{t+kp^{m-2j}})^{\tau_t} = \prod_{t=0}^{p^{m-2j}-1} (z^{p^j} - \lambda^{tp^j})^{\tau_t} = \prod_{t=0}^{p^{m-j}-1} (z^{p^j} - \zeta^t)^{\tau_t}$$

Por lo tanto, $\pi_{\mathcal{Y}}$ está bien definida. Claramente es una aplicación holomorfa de $\mathcal{X}$ en $\mathcal{Y}$. Finalmente, notamos que si $\pi_{\mathcal{Y}}(z,w) = \pi_{\mathcal{Y}}(x,y)$, entonces $x^{p^j} = z^{p^j}$ y de ello se deriva que $y^{p^j} = w^{p^j}$. De esta forma, vemos que $x = \varpi z$ y $w = \varpi' y$ donde ϖ y ϖ' son raices p^j-ésimas de 1. Esto implica que dichos puntos (x,y) y (z,w) pertenecen a la misma órbita bajo la acción de $Z(G)$. De esta forma, se induce una aplicación holomorfa $\mathcal{X}_{Z(G)} \to \mathcal{Y}$ que es inyectiva, y como ambas superficies son compactas, es un isomorfismo.

Ahora, para tratar el caso más general $\mathcal{X}_{Z_k}$, se hace el mismo procedimiento, esta vez sustituyendo $\mathcal{X}$ por $\mathcal{X}_{Z(G)}$ y $\mathcal{X}_{Z(G)}$ por $\mathcal{X}_{Z_2}$, y así sucesivamente. Con esto, el corolario queda demostrado. □

Ejemplo 4.1.2 *Consideremos $p = 5$, $m = 3$ y $j = 2$, es decir, $r = 5^2 + 1 = 26$. En*

este caso, el centro de $G_{125,2}$ es $\langle a^5, b^5\rangle$ y el cociente que genera es isomorfo a Z_5^2. De acuerdo al Corolario 7.1.2, $X_{Z(G)}$ tiene como ecuación:

$$y^5 = x^5 - 1$$

si consideramos $j = 1$, es decir, $r = 5 + 1 = 6$, entonces $Z(G) = \langle a^{25}, b^{25}\rangle$ y $Z_2 = \langle a^5, b^5\rangle$. Primero, verificamos los números τ_k que están entre 1 y $5^2 - 1 = 24$:

k	τ_k
0	1
1	6
2	11
3	16
4	21

Así, fijando $\lambda = e^{2\pi i/5}$, las ecuaciones para $\mathcal{X}_{Z(G)}$ y $\mathcal{X}_{Z_1}$ respectivamente son:

$$y^{25} = (x^5 - 1)(x^5 - \lambda)^6(x^5 - \lambda^2)^{11}(x^5 - \lambda^3)^{16}(x^5 - \lambda^4)^{21}$$
$$y^5 = x^5 - 1$$

2. B, sus subgrupos y H_j, si $j \geq m - j$. Notamos que $\mathcal{X}_B$ no tiene género cero, pero en este grupo actúa $L = N/B \cong \mathbb{Z}_{p^{m-j}}$ donce $N = N_G(B)$. Este grupo cíclico tiene orden p^j. Sea z la clase de a en L. De acuerdo al Corolario 3.2.1, como $N = H_{m-j}$, se tiene que $\mathcal{X}_N$ es cero, y además N contiene a H_j como subgrupo propio normal. Consideremos $H = H_{j+1}$ si $j < m - 1$ o $H = B$ si $j = m - 1$. Vemos que este subgrupo es normal en N. Por la proposición antes mencionada, el género de $\mathcal{X}_H$ es

$$\frac{p^l - p^j - p^{j-1}(p-1)(l-j)}{2}$$

De esta forma, vemos que $\mathcal{X}_H$ es una curva p-gonal. El número ε de los puntos de ramificación de la proyección de $\mathcal{X}_H$ a la esfera se calcula usando la fórmula de Riemann-Hurwitz:

$$\frac{p^l \quad p^j \quad p^{j-1}(p \quad 1)(m \quad j)}{2} = -p + 1 + \frac{1}{2}(\varepsilon(p-1))$$
$$\Rightarrow \frac{p^l - p^j - p^{j-1}(p-1)(m-j)}{2} = \frac{1}{2}((\varepsilon - 2)(p-1))$$

$$\Rightarrow \frac{p^l - p^j - p^{j-1}(p-1)(m-j)}{p-1} = \varepsilon - 2$$
$$\Rightarrow \frac{p^l - p^j - p^{j-1}(p-1)(m-j)}{p-1} + 2 = \varepsilon$$

Más aún, N/H es cíclico de orden mayor a p y por la Proposición 5.3.2, deducimos que todo subgrupo intermedio U entre N y H es tal que $\mathcal{X}_U$ es de género cero. Como consecuencia de esto, el cociente de $\mathcal{X}_H$ por cualquier subgrupo de N/H es de género cero. En base a esto, podemos citar el siguiente resultado demostrado en [16], pág. 13:

Proposición 4.1.4 *Sea S una superficie de Riemann de género g bajo la acción de $\mathbb{Z}_{p^u}$, p un primo cualquiera, $u > 1$. Suponga que para cualquier subgrupo H no trivial de $\mathbb{Z}_{p^u}$ se cumple que S_H tiene género cero. Entonces S es isomorfa a una curva plana afín definida por la ecuación:*

$$y^p = x^l \prod_{k=1}^{\iota} (x^{p^{u-1}} - \lambda_k)^{l_k}$$

donde l y l_k son números entre 1 y $p-1$ tales que su suma no es divisible por p, los λ_k son números complejos distintos entre sí. El género de S es

$$g = \frac{\iota(p^{u-1}(p-1))}{2}$$

donde ι es tal que la firma de la acción es $(0; p_{(\iota)}, p^u, p^u)$. La acción de $\mathbb{Z}_{p^u}$ viene dada por el siguiente automorfismo:

$$\varphi(x, y) = (\lambda x, \mu y)$$

con $\lambda = e^{2\pi i/p^{j-1}}$ y μ tal que $\mu^p = \lambda^a$

Esto implica que si $j > m - j$, $\mathcal{X}_H$ tiene un modelo afin como el que describe la proposición anterior.

En nuestro caso, vemos que ι se puede calcular como:

$$\frac{p^l - p^j - p^{j-1}(p-1)(m-j)}{2} = \frac{\iota(p^{j-1}(p-1))}{2}$$

De lo que obtenemos que $\iota = \frac{p^{l-j+1}-p}{p-1} - m + j$. Comparando el cálculo de ε con el de ι podemos ver que $\iota p^{j-1}(p-1) = (\varepsilon-2)(p-1)$de lo que obtenemos que $\varepsilon = p^{j-1}\iota + 2$. Reexpresamos ι como:

$$\iota = \frac{p^{l-j+1}-p}{p-1} - l + j = p^{l-j} + ... + p - l + j$$

De esto obtenemos que $\varepsilon = p^{j-1}\iota + 2 = p^{m-1} + ...p^j - (m-j)p^{j-1} + 2$.

Queremos determinar algunas propiedades de $\mathbf{Aut}(\mathcal{X}_H)$. Para ello, podemos usar la siguiente proposición:

Proposición 4.1.5 *Sea S una curva plana definida por una ecuación $y^p = f(x)$ con $f(x)$ un polinomio con v raices. Si $v > 2p$, entonces $\boldsymbol{Aut}(S)$ es una extensión de $\mathbb{Z}_p$ por un subgrupo finito de $\boldsymbol{Aut}(\hat{C})$.*

Demostración: ver [15], pág. 11.

Con esta proposición, podemos deducir lo siguiente

Proposición 4.1.6 *$\boldsymbol{Aut}(\mathcal{X}_H)$ es una extensión normal de $\mathbb{Z}_p$ por un subgrupo finito de $\boldsymbol{Aut}(\hat{C})$.*

En nuestro caso, $v = \varepsilon$. Observamos que si $j \neq 1$

$$\varepsilon = p^{m-1} + ... + p^j - (m-j)p^{j-1} + 2 > (m-j)p^j - (m-j)p^{j-1} = (m-j)p^j(p-1)$$

Es claro que $(m-j)p^j(p-1) \geq 2p$. Si $j = 1$

$$\varepsilon = p^{l-1} + ... + p - l - 1 + 2 \geq p^{l-1} + ... + p + 1 - m$$

Usando que $p^{l-1} - (l-1) > p$, obtenemos que $\varepsilon > 2p$. Por lo tanto, el grupo $\mathbb{Z}_p \trianglelefteq \mathbf{Aut}(\mathcal{X}_H)$.

La condición $\varepsilon > 2p$ implica que $g > (p-1)^2$ pues:

$$g = \frac{(\varepsilon-2)(p-1)}{2} > \frac{(2p-2)(p-1)}{2} = (p-1)^2$$

El siguiente teorema establece las posibles grupos a los cuales $\mathbf{Aut}(\mathcal{X}_H)$ es isomorfo:

Teorema 4.1.3 *Sea S una superficie de Riemann cíclica p-gonal para un primo p impar. Supongamos que el género de S es mayor a $(p-1)^2$. Entonces $\boldsymbol{Aut}(S)$ sólo puede ser isomorfo a uno de los siguientes:*

- *a)* $\mathbb{Z}_{pn}$, $n \geq 1$.
- *b)* D_{pn}, $n \geq 1$.
- *c)* $\mathbb{Z}_p \rtimes Z_n$, $n \geq 1$.
- *d)* $\mathbb{Z}_p \rtimes D_n$, $n \geq 1$.
- *e)* $\mathbb{Z}_p \times A_4$
- *f)* $(\mathbb{Z}_p \times A_4) \rtimes \mathbb{Z}_2$
- *g)* $\mathbb{Z}_p \rtimes S_4$
- *h)* $\mathbb{Z}_p \times A_5$
- *i)* $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_9$ *si* $p = 3$ *y* $Aut(X)/\mathbb{Z}_p \cong A_4$.
- *j)* $(\mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3$ *si* $p \equiv_6 1$ *y* $\boldsymbol{Aut}(X)/\mathbb{Z}_p \cong A_4$.
- *k)* $((\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_9) \rtimes \mathbb{Z}_2$ *si* $p = 3$ *y* $\boldsymbol{Aut})/\mathbb{Z}_p \cong S_4$.

Demostración: ver [1], págs 63-65.

Ejemplo 4.1.3 *Para $p = m = 3$, y $j = 2$ se tiene que:*

$$\iota - \frac{3^{3-2+1}-1}{3-1} - 3 + 2 - \frac{9-1}{2} - 1 - 3, \quad \epsilon - 3^{3-1} \cdot 3 + 2 - 29$$

De esta forma, una ecuación para $\mathcal{X}_B$ es dada por:

$$y^3 = x^l(x^3 - \lambda_1)^{l_1}(x^3 - \lambda_2)^{l_2}(x^3 - \lambda_3)^{l_3}$$

donde l y l_k son enteros positivos y los λ_k son números complejos distintos entre sí.

3. **Subgrupos de A, parte I:** Consideremos $\mathcal{X}_{A_k}$ donde $A_k = \langle a^{p^k} \rangle$ con $k \leq j$. Tenemos lo siguiente:

Proposición 4.1.7 *Una ecuación para $\mathcal{X}_{A_k}$ es de la forma:*

$$y^{p^k} + x^n = 1$$

Demostración: Sabemos que $A_k \trianglelefteq G$ y $K = G/A_j$ es abeliano, pues $b^{-1}ab = a^r = aa^{p^j}$ y $p^k|p^j$. Además, vemos que K es generado por las clases de a y b en ese cociente, y la clase de a tiene orden p^k mientras que la clase de b tiene orden n. De esta forma, $K \cong \mathbb{Z}_{p^k} \times \mathbb{Z}_n$. Además $Z_{p^k} \cong A/A_k$ y con ello

$$(\mathcal{X}_{A_k})_{\mathbb{Z}_{p^k}} \cong \mathcal{X}_A \cong \hat{\mathbb{C}}$$

De esta forma, $\mathcal{X}_{A_k}$ es p^k-gonal. Usando el mismo argumento del cálculo de ecuación para $\mathcal{X}$, se puede encontrar una ecuación para X, usando que $\mathbb{K} = K/\mathbb{Z}_k$ es un grupo de automorfismos cíclico de orden n que actúa en la esfera. Los puntos rama del cubriente cíclico $\mathcal{X}_{A_k} \to \hat{\mathbb{C}}$ son imágenes de los puntos rama de $\mathcal{X} \to \mathcal{X}_{A_k}$ que de hecho, son los n puntos que fija a. De esta forma tenemos n puntos rama del cubriente $\mathcal{X}_{A_k} \to \hat{\mathbb{C}}$. Usando ideas similares a las usadas al encontrar una ecuación para $\mathcal{X}$, se determina la ecuación deseada. □

Más aún, uno puede determinar el grupo completo de automorfismos de esa curva, usando la siguiente proposición:

Proposición 4.1.8 *Si S es una superficie de Riemann compacta definida por una ecuación de la forma*

$$x^t + y^u = 1$$

con $t|u$, $t < u$, entonces $\boldsymbol{Aut}(S) \cong (\mathbb{Z}_t \times \mathbb{Z}_u) \rtimes Z_2$

Demostración: ver [15], pág. 21.

De esto, obtenemos lo siguiente:

Proposición 4.1.9 *$\boldsymbol{Aut}(\mathcal{X}_{A_k})$ es isomorfo a un producto semidirecto $(\mathbb{Z}_{p^k} \times \mathbb{Z}_n) \rtimes Z_2$.*

4. **Subgrupos de A, parte II:** Ahora consideremos $\mathcal{X}_{A_k}$ con $k > j$. En ese caso tenemos lo siguiente:

Proposición 4.1.10 *Si $k > j$, entonces $\mathcal{X}_{A_k}$ tiene como ecuación:*

$$y^{p^k} = \prod_{t=0}^{p^{k-j}-1} (x^{p^{m-k+j}} - \lambda^t)^{\rho_t}$$

Donde $\rho_t \equiv_{p^k} r^t$ es un entero positivo menor a p^k y $\lambda = e^{2\pi i/p^{k-j}}$.

Demostración: Vemos que $K = G/A_k$ no es abeliano, de hecho es un producto semidirecto $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_n$ con presentación:

$$K = \langle a, b | a^{p^k} = b^n = 1, b^{-1}ab = a^r \rangle$$

El orden de r módulo p^k es p^{k-j}. Aplicamos la misma idea de la observación anterior, notando que la acción de K en $Aut(\mathbb{Z}_{p^k})$ es de la forma $b \to (a \to b^{-1}ab = a^r)$. □

Ejemplo 4.1.4 *Consideremos ahora $\mathcal{X}_{27,1}$ ($p = m = 3$, $j = 1$ de modo que $r = 3+1 = 4$). En este caso, las ecuaciones para $\mathcal{X}_{A_1}$ y $\mathcal{X}_{A_2}$ son, respectivamente:*

$$y^3 = x^{27} - 1$$
$$y^9 = (x^9 - 1)(x^9 - e^{2\pi i/3})^4(x^9 - e^{4\pi i/3})^7$$

4.2. Caso $p = 2$

Recordemos que en este caso, $\mathcal{X}$ es isomorfa a

$$y^n = f(x) = (x^{\frac{n}{2}} - 1)(x^{\frac{n}{2}} + 1)^{\nu_j}$$

Haremos el mismo estudio hecho en el caso anterior. Denotamos $g(x,y) = y^n - f(x)$. En adelante, llamaremos $r = \nu_j$. El siguiente lema se deduce de inmediato de la ecuación de S:

Lema 4.2.1 *Las singularidades de $\mathcal{X}$ son de la forma $(\chi, 0)$ donde χ es una raiz de $x^{\frac{n}{2}} + 1$ y las singularidades de la clausura proyectiva de $\mathcal{X}$ son de la forma $[\chi : 0 : 1]$ donde χ es una raiz de $x^{\frac{n}{2}} + 1$, más el punto $[0 : 1 : 0]$.*

Demostración: notamos que la homogeneización de g es:

$$H_g(x,y,z) = z^{\frac{n(r+1)}{2}} \left(\left(\frac{y}{z}\right)^n - \left(\left(\frac{x}{z}\right)^{\frac{n}{2}} - 1 \right) \left(\left(\frac{x}{z}\right)^{\frac{n}{2}} + 1 \right)^{r+1} \right)$$
$$= z^{\frac{n(r-1)}{2}} y^n - z^{n(r+1)} \frac{(x^{\frac{n}{2}} - z^{\frac{n}{2}})(x^{\frac{n}{2}} + z^{\frac{n}{2}})^r}{z^{\frac{n(r+1)}{2}}}$$
$$= z^{\frac{n(r-1)}{2}} y^n - (x^{\frac{n}{2}} - z^{\frac{n}{2}})(x^{\frac{n}{2}} + z^{\frac{n}{2}})^r$$

Vemos que la derivada parcial de H_g en y es igual a $nz^{\frac{n(r+1)}{2}}y^{n-1}$. Para que se anule, z o y deben ser cero. Si y es cero, vemos que tenemos las mismas singularidades de S. Si z es cero, se ve por la ecuación de $H_g = 0$ que $x = 0$. Evidentemente cuando x y z son cero, se anulan las otras derivadas de primer orden, dada la forma de H_g. Esto demuestra el lema. □

Notamos que el procedimiento de resolver esas singularidades es el mismo que aplicamos en el caso de primo impar. Esto se resume en:

Lema 4.2.2 *Las singularidades de la forma* $[\chi : 0 : 1]$ *son de tipo* (r, n) *y la singularidad* $[0 : 1 : 0]$ *es de tipo* $(n, \frac{n(r+1)}{2})$. *Las primeras singularidades aportan 1 punto al resolverlas, mientras que la última aporta n puntos en su resolución.*

De la misma forma que en el caso de p impar, usando lo anterior obtenemos el siguiente resultado:

Proposición 4.2.1 *El género de la superficie de Riemann* $\mathcal{X}$ *obtenida al resolver las singularidades de la clausura proyectiva de la curva plana afín definida por* $g(x)$ *es:*

$$\frac{(n-1)(n-2)}{2}$$

Ahora, realizaremos los generadores de G como automorfismos de $\mathcal{X}$:

Teorema 4.2.1 *Sean* α, β *definidas por.*

$$\alpha(x,y) = (x, \omega y), \quad \beta(x,y) = \left(\omega x, \frac{y^r}{(x^{n/2}+1)^{(r^2-1)/n}}\right)$$

Entonces α *y* β *definen automorfismos de* $\mathcal{X}$ *y el grupo* $\bar{G}$ *que generan es isomorfo a* $G_{n,j}$

Demostración: Es claro que α define un automorfismo de $\mathcal{X}$. Para ver el caso de β, notamos que si $\beta(x,y) = (z,w)$, entonces:

$$w^n = \left(\frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}}\right)^n = \frac{y^{nr}}{(x^{n/2}+1)^{(r^2-1)}} = \frac{(x^{\frac{n}{2}}-1)^r(x^{\frac{n}{2}}+1)^{r^2}}{(x^{\frac{n}{2}}+1)^{(r^2-1)}}$$

$$= (x^{\frac{n}{2}}+1)(x^{\frac{n}{2}}-1)^r = ((\omega^{-1}w)^{\frac{n}{2}}+1)((\omega^{-1}w)^{\frac{n}{2}}-1)^r = (-w^{\frac{n}{2}}+1)(-w^{\frac{n}{2}}-1)^r$$

$$= (-1)^{r+1}(w^{\frac{n}{2}}-1)(w^{\frac{n}{2}}+1)^r$$

Como $r+1$ es par, se cumple que β está bien definida. Para ver que es inyectiva, notamos que si $\beta(x,y)=\beta(t,u)$ es inmediato que $x=t$ y que $y^r=u^r$, lo que obliga a que $y=wu$ con w una raíz r-ésima de la unidad. Como $x=t$, necesariamente $y^n=u^n=w^nu^n$. Como r y n son primos relativos, forzadamente $w=1$. De esta manera, β define un automorfismo de $\mathcal{X}$.

Verificamos $\langle\alpha,\beta\rangle$ es isomorfo a G. Es evidente que α tiene orden n. Para verificar lo mismo con β, vemos que:

$$\beta(\beta(x,y))=\beta\left(\omega x,\frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}}\right)=\left(\omega^2x,\frac{\frac{y^{r^2}}{(x^{\frac{n}{2}}+1)^{\frac{r(r^2-1)}{n}}}}{((\omega x)^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}}\right)$$

$$=\left(\omega^2x,\frac{y^{r^2}}{(-x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}(x^{\frac{n}{2}}+1)^{\frac{r(r^2-1)}{n}}}\right)$$

$$=\left(\omega^2x,\frac{y^{r^2}}{(-1)^{\frac{r^2-1}{n}}(x^{\frac{n}{2}}-1)^{\frac{r^2-1}{n}}(x^{\frac{n}{2}}+1)^{\frac{r(r^2-1)}{n}}}\right)$$

$$=\left(\omega^2x,(-1)^{\frac{r^2-1}{n}}y\frac{y^{r^2-1}}{((x^{\frac{n}{2}}-1)(x^{\frac{n}{2}}+1)^r)^{\frac{r^2-1}{n}}}\right)$$

$$=\left(\omega^2x,(-1)^{\frac{r^2-1}{n}}y\left(\frac{y^n}{(x^{n/2}-1)(x^{\frac{n}{2}}+1)^r}\right)^{\frac{r^2-1}{n}}\right)$$

$$=(\omega^2x,(-1)^{\frac{r^2-1}{n}}y)$$

De esta forma, vemos que β^2 tiene orden $\frac{n}{2}$, lo que implica que β tiene orden n. Finalmente, debemos ver que β normaliza α, situación que es evidentemente análoga al caso de primo impar. □

Con esto, realizamos el grupo G como grupo de automorfismos de $\mathcal{X}$. Además, tenemos que el género de $\mathcal{X}$ es $\frac{(n-1)(n-2)}{2}$. El cálculo para realizar la firma de G es el mismo que en el caso de primo impar. Sin embargo, falta verificar la extensión de G por un automorfismo de orden 2. Para ello, usaremos la siguiente proposición:

Proposición 4.2.2 *La siguiente función:*

$$\gamma(x,y)=\left(\frac{1}{x},\frac{\zeta y}{x^{\frac{r+1}{2}}}\right)$$

donce $\zeta = e^{\pi i/n}$, define un automorfismo de $\mathcal{X}$ de orden $2n$ que no está en $\langle \alpha, \beta \rangle$.

Demostración: Si $\gamma(x,y) = (z,w)$, entonces:

$$w^n = \left(\frac{\zeta y}{x^{\frac{r+1}{2}}}\right)^n = \frac{\zeta^n y^n}{x^{n\frac{r+1}{2}}} = \frac{-y^n}{x^{n\frac{r+1}{2}}} = \frac{-(x^{\frac{n}{2}}-1)(x^{\frac{n}{2}}+1)^r}{x^{n\frac{r+1}{2}}}$$
$$= \frac{(1-x^{\frac{n}{2}})(x^{\frac{n}{2}}+1)^r}{x^{n\frac{r+1}{2}}} = \left(\frac{1}{x^{\frac{n}{2}}}-1\right)\left(\frac{1}{x^{\frac{n}{2}}}+1\right)^r = (z^{\frac{n}{2}}-1)(z^{\frac{n}{2}}+1)^r$$

Por lo tanto, γ está bien definida. Además:

$$\gamma(\gamma(x,y)) = \gamma\left(\frac{1}{x}, \frac{\zeta y}{x^{\frac{r+1}{2}}}\right) = \left(\frac{1}{\frac{1}{x}}, \frac{\zeta \frac{\zeta y}{x^{\frac{r+1}{2}}}}{\frac{1}{x^{\frac{r+1}{2}}}}\right) = (x, \zeta^2 y) = (x, \omega y) = \alpha(x,y)$$

Esto demuestra que γ tiene orden $2n$. Como $\langle \alpha, \beta \rangle$ es isomorfo un producto semidirecto $\mathbb{Z}_n \rtimes \mathbb{Z}_n$, no puede tener elementos de orden $2n$. Por lo tanto, δ no pertenece a ese grupo. □

A continuación, determinaremos los elementos de $\mathbf{Aut}(\mathcal{X})$ que realizan la firma $(0; 2, n, 2n)$. Para ello, usaremos el siguiente lema:

Lema **4.2.3** *Sea $\delta = \gamma^r \beta$. Entonces δ tiene orden 2.*

Demostración: Como r es impar, usando la proposición anterior, vemos que

$$\gamma^r \beta(x,y) = \gamma^r\left(\omega x, \frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}}\right) = \gamma^r\left(\omega x, \frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}}\right)$$
$$= \left(\frac{1}{\omega x}, \zeta^r \frac{\frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}}}{(\omega x)^{\frac{r+1}{2}}}\right) = \left(\frac{1}{\omega x}, \zeta^r \frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}(\omega x)^{\frac{r^2-1}{n}}}\right)$$

Al evaluar δ en lo anteriormente calculado obtenemos que:

$$\delta(\delta(x,y)) = \delta\left(\frac{1}{\omega x}, \zeta^r \frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}}(\omega x)^{\frac{r^2-1}{n}}}\right)$$

$$= \left(\frac{1}{\omega^{\frac{1}{\omega x}}}, \zeta^{-r} \frac{\left(\zeta^r \frac{y^r}{(x^{\frac{n}{2}}+1)^{\frac{r^2-1}{n}} (\omega x)^{\frac{r^2-1}{n}}} \right)^r}{\left(\frac{1}{(\omega x)^{\frac{n}{2}}} + 1 \right)^{\frac{r^2-1}{n}} \left(\frac{w}{wx} \right)^{\frac{r^2-1}{n}}} \right) = \left(x, \zeta^r \frac{\zeta^{r^2} \frac{y^{r^2}}{(x^{\frac{n}{2}}+1)^{r\frac{r^2-1}{n}} (\omega x)^{r\frac{r^2-1}{n}}}}{\left(\frac{x^{\frac{n}{2}}-1}{x^{\frac{n}{2}}} \right)^{\frac{r^2-1}{n}} \left(\frac{1}{x} \right)^{\frac{r^2-1}{n}}} \right)$$

$$= \left(x, \zeta^{(r^2+r)} y \frac{\frac{y^{r^2-1}}{(x^{\frac{n}{2}}+1)^{r\frac{r^2-1}{n}} (\omega x)^{r\frac{r^2-1}{n}}}}{(x^{\frac{n}{2}}-1)^{\frac{r^2-1}{n}} \left(\frac{1}{x} \right)^{\frac{r^2-1+r+1}{2}}} \right)$$

Como $\zeta^2 - \omega$, las potencias de ζ y ω se cancelan y así la expresión anterior queda:

$$= \left(x, y \frac{y^{r^2-1}}{(x^{\frac{n}{2}}-1)^{\frac{r^2-1}{n}} (x^{\frac{n}{2}}+1)^{r\frac{r^2-1}{n}}} \right) = \left(x, y \left(\frac{y^n}{(x^{\frac{n}{2}}-1)(x^{\frac{n}{2}}+1)^r} \right)^{\frac{r^2-1}{n}} \right) = (x, y)$$

Lo que demuestra la afirmación. □

Ejemplo 4.2.1 *Sea $n = 32$ y $j = 1$, con esto, $r = 16 - 1 = 15$. Una ecuación para $X_{32,1}$ es:*

$$y^{32} = (x^{16} - 1)(x^{16} + 1)^{15}$$

Los automorfismos α, β, γ y δ se expresan como:

$$\alpha(x, y) = (x, e^{\frac{2\pi i}{32}} y), \quad \beta(x, y) = \left(e^{\frac{2\pi i}{32}} x, \frac{y^{15}}{(x^{16}+1)^7} \right)$$

$$\gamma(x, y) = \left(\frac{1}{x}, \frac{e^{\frac{2\pi i}{32}} y}{x^8} \right), \quad \delta(x, y) = \left(\frac{1}{e^{\frac{2\pi i}{32}} x}, \frac{e^{\frac{-\pi i}{32}} y^{15}}{(x^{16}+1)^7 x^8} \right)$$

Aplicando el Teorema 4.2.1 se obtiene la siguiente proposición:

Proposición 4.2.3 *La firma de $\langle \alpha, \beta \rangle$ es $(0; n, n, n)$. Además, $(\delta, \beta^{-1}, \gamma^{-r})$ es un vector generador de $Aut(\mathbb{S})$ con firma $(0; 2, n, 2n)$*

Finalmente resumimos todo esto en el siguiente Teorema:

Teorema 4.2.2 *Sea $n = 2^m$ una potencia de 2 con $m \geq 3$. Sea $r = \nu_j$ con $1 \leq j \leq 3$ donde ν_j se define de acuerdo al Lema A.0.7. Sea G el grupo definido por la siguiente presentación:*

$$G = G_{n,j} = \langle a, b | a^n = b^n = 1, b^{-1}ab = a^r \rangle$$

Entonces G actúa en una superficie de Riemann compacta $\mathcal{X}_{n,j}$ de género

$$g = \frac{(n-1)(n-2)}{2}$$

con firma $(0; n, n, n)$ y ecuación algebraica de la forma:

$$y^n = (x^{\frac{n}{2}} - 1)(x^{\frac{n}{2}} + 1)^r$$

Los elementos a y b se realizan en $\mathbf{Aut}(\mathcal{X}_{n,j})$ como α y β definidos en el Teorema 4.1.3. Además, $[\mathbf{Aut}(\mathcal{X}_{n,j}) : G_{n,j}] = 2$, y la firma de $\mathbf{Aut}(\mathcal{X}_{n,j})$ es $(0; 2, n, 2n)$.

4.2.1. Ecuaciones para cocientes intermedios

Ahora, determinaremos ecuaciones para cocientes interemedios de la misma forma que en el caso de p impar:

1. B: en los casos $j = 1$ y $j = 2$, se ve que $\mathcal{X}_B$ es una curva hiperelíptica, pues B contiene un subgrupo de indice 2 en G de modo que al cortar X por dicho subgrupo se obtiene $\hat{\mathbb{C}}$. En el caso $j = 1$, vemos que ese subgrupo es $N_G(B)$ y en el caso $j = 2$, ese grupo es $H = \langle b, a^{n/2} \rangle$. Por lo tanto, la cantidad de puntos fijos por la involución hiperelíptica es $n/4 + 2$. En particular, si $j = 2$, con ayuda de la proposición 3.2.15, que $\mathcal{X}_B$ es una curva con acción de $N_G(B)/B \cong \mathbb{Z}_{\frac{n}{2}}$ de modo que al cortar $\mathcal{X}_B$ por todos sus subgrupos da género cero. Así, la proposición 5.1.3 es también válida en este caso, y de ella obtenemos el siguiente corolario:

Corolario 4.2.1 *Si $n = 2^m$ y $r = \frac{n}{2} + 1$, entonces $\mathcal{X}_B$ es isomorfa a la curva plana afín definida por una ecuación de la forma:*

$$y^2 = x(x^{n/4} - 1)$$

Demostración: Notamos que hay exactamente $n/4$ factores de la forma $(x - a_l)$ en la ecuación, por ser $\mathcal{X}_B$ hiperelíptica, con multiplicidad 1, y por la proposición 7.1.3 estos deben agruparse en factores de la forma $x^{2^{m-2}} - \lambda = x^{\frac{n}{4}} - \lambda$. Pero vemos que de hecho sólo puede haber un factor de ese tipo. Amplificando x e y por constantes adecuadas podemos suponer que $\lambda = 1$. □

Además, podemos determinar el grupo completo de automorfismos de X_B en el caso $j = 2$:

Corolario 4.2.2 *Considerando la notación del corolario anterior.*

- *Si $n = 8$, entonces $\mathcal{X}_B$ tiene un grupo de automorfismos de orden infinito que incluye a $\mathbb{Z}_4$.*
- *Si $n > 8$, entonces $\boldsymbol{Aut}(\mathcal{X}_B) \cong \boldsymbol{V}_{\frac{n}{2}}$ donde*

$$\boldsymbol{V}_t = \langle a, b | a^4 = b^t = (ab)^2 = (a^{-1}b) = 1 \rangle$$

Demostración: Sea $\lambda = e^{4\pi i/n}$ una raiz primitiva $n/2$-ésima de la unidad. Primero definimos el automorfismo h_1 de $\mathcal{X}_B$ definido por $h_1(x, y) = (\lambda^2 x, \lambda y)$. Vemos que está bien definido. Si $h_1(x, y) = (z, w)$, entonces

$$w^2 = \lambda^2 y^2 = \lambda^2 x(x^{\frac{n}{2}} - 1) = z((\lambda^2/x)^{\frac{n}{2}} - 1) = z(z^{\frac{n}{2}} - 1)$$

Por lo tanto, h define un automorfismo de $\mathcal{X}_B$. Claramente tiene orden $n/2$. De esto se establece que si $n = 8$, entonces $\mathcal{X}_B$ es una curva elíptica, por ello tiene un grupo de automorfismos infinito que contiene un grupo cíclico de orden 4.

Supongamos ahora que $n > 8$. Definimos ahora el siguiente automorfismo de $\mathcal{X}_B$:

$$h_2(x, y) = \left(\frac{-1}{x}, \frac{y}{x^{\frac{n}{8}+1}} \right)$$

Primero vemos que está bien definido, de hecho, si $h_2(x, y) = (z, w)$, tenemos:

$$w^2 = \frac{y^2}{x^{\frac{n}{4}+2}} = \frac{x(x^{\frac{n}{4}} - 1)}{x^{\frac{n}{4}+2}} = \left(\frac{1}{x}\right)\left(1 - \frac{1}{x^{\frac{n}{4}}}\right) = -z(1 - (-z)^{\frac{n}{4}}) = z(z^{\frac{n}{4}} - 1)$$

Entonces, h_2 está bien definida y es un automorfismo de $\mathcal{X}_B$. Lo siguiente es verificar que h_2 con h_1 cumplen las relaciones que definen a $V_{n/4}$. Lo primero es ver el orden de h_2. Observamos que:

$$h_2(h_2(x, y)) = h_2\left(\frac{-1}{x}, \frac{y}{x^{n/8+1}} \right) = \left(\frac{-1}{\frac{-1}{x}}, \frac{\frac{y}{x^{\frac{n}{8}+1}}}{(\frac{-1}{x})^{\frac{n}{8}+1}} \right) = (x, -y)$$

Es decir, h_2^2 es la involución hiperelíptica σ. De esta forma, h_2 tiene orden 4. Ahora, debemos ver que h_2 normaliza h_1. Vemos que $h_2h_1(x,y) = h_2(\lambda^2 x, \lambda y) = \left(\frac{-1}{\lambda^2 x}, \frac{\lambda y}{(\lambda^2 x)^{\frac{n}{8}+1}}\right)$. Además, $(\lambda^2)^{\frac{n}{8}+1} = \lambda^{\frac{n}{4}}\lambda^2 = -\lambda^2$, luego, $h_2h_1(x,y) = \left(\frac{-1}{\lambda^2 x}, \frac{-y}{\lambda x^{\frac{n}{8}+1}}\right)$. Por otra parte:

$$h_1^{-1}h_2(x,y) = h_1\left(\frac{-1}{x}, \frac{y}{x^{\frac{n}{8}+1}}\right) = \left(\frac{-1}{\lambda^2 x}, \frac{y}{\lambda x^{\frac{n}{8}+1}}\right) = \sigma h_2h_1$$

$$\Rightarrow h_2h_1 = \sigma h_1^{-1}h_2 = h_1^{-1}\sigma h_2 = h_1^{-1}h_2^{-1} = (h_2h_1)^{-1}(x,y)$$

Por lo tanto, h_2h_1 tiene orden 2. Además $(h_2^{-1}h_1)^{-1} = h_1^{-1}h_2 = \sigma h_2h_1 = h_2^{-1}h_1$, con lo que se concluye que $h_2^{-1}h_1$ tiene orden 2. Por lo tanto, el grupo L generado por h_1 y h_2 es isomorfo a $V_{\frac{n}{2}}$. Para ver que es efectivamente $\mathbf{Aut}(\mathcal{X}_B)$, recordamos que por el Ejemplo 2.7.1 la involución hiperelíptica está en $Z(\mathbf{Aut}(\mathcal{X}_B))$. Luego, el cociente $L/\langle\sigma\rangle$ está bien definido, es isomorfo a $D_{\frac{n}{4}}$ (pues $\sigma h_2h_1 = h_2^{-1}h_1$) y actúa en los $\frac{n}{4}+2$ puntos rama del cubriente de $\mathcal{X}_B$ a la esfera dado por σ. Dos de esos puntos son 0 e ∞ y quedan fijos por la clase de h_1 módulo σ y se mueven uno al otro por la clase de h_2. Los otros puntos son las raices $\frac{n}{4}$ ésimas de la unidad que se mueven bajo las clases de h_1 y h_2. Usando que la firma de $D_{\frac{n}{4}}$ en la esfera es $(2,2,\frac{n}{4})$, obtenemos que la firma de $V_{\frac{n}{2}}$ es $(0;2,4,\frac{n}{2})$. En [4] se establece que $V_{\frac{n}{2}}$ es grupo completo de automorfismos de una superficie hiperelíptica, con la firma encontrada. □

Ejemplo 4.2.2 *Si $n = 16$ y $j = 2$, entonces $r = 8+1 = 9$. Una ecuación para X_B es $y^2 = x(x^4-1)$. Los automorfismos h_k son*

$$h_1(x,y) = (-x, iy), \quad h_2(x,y) = \left(\frac{-1}{x}, \frac{y}{x^3}\right)$$

2. **Subgrupos de A:** Consideramos ahora X_{A_k}, donde $A_k = \langle a^{2^k}\rangle$. De la misma forma que en el caso de p impar, se pueden encontrar ecuaciones para este cociente, lo que expresamos en el siguiente teorema:

Proposición 4.2.4 *Considerando la notación de la observación anterior:*

- *Si $j = 2$, entonces una ecuación para X_{A_k} es $y^{2^{m-k}} = x^n - 1$.*
- *Si $j \neq 2$, entonces una ecuación para X_{A_k} es $y^{2^{m-k}} = (x^{\frac{n}{2}}-1)(x^{\frac{n}{2}}+1)^{2^{m-k}-1}$.*

Primero, notamos que G/A_k es isomorfo a un producto semidirecto de $\mathbb{Z}_{2^k}$ con $\mathbb{Z}_n$. Como $b^{-1}ab = a^{\nu_j}$, notamos que si $j = 2$, $\nu_2 = \frac{n}{2}+1$, de modo que como $a^{n/2} \in$

A_k,$b^{-1}ab = a^{\frac{n}{2}}a$. De esta forma, si $j = 2$, G/A_k es abeliano y de esa forma se procede igual que el caso p impar (cuando $k \leq j$). Supongamos que $j \neq 2$. Si $j = 1$, $\nu_1 = n/2-1$ y se tiene que $b^{-1}ab = a^{\frac{n}{2}}a^{-1} = a^{-1}$, y si $j = 3$, $\nu_3 = n-1$ y se tiene que $b^{-1}ab = a^n a^{-1} = a^{-1}$. De esta forma, en el cociente, a^{-1} es igual a a^{2m-k-1}. Usamos las mismas ideas de la sección anterior para calcular la ecuación de X_{A_k}. □

4.3. Cuerpos de Definición para $\mathcal{X}_{n,j}$

En esta sección, veremos el menor cuerpo de definición posible para $\mathcal{X}$ como curva plana definida por la ecuación determinada en este capítulo. También daremos algunos indicios de cómo $\mathcal{X}$ se define sobre este cuerpo de definición minimal. Nos concentraremos en el caso primo impar, pues es claro que en el caso de $p = 2$, la curva se define sobre $\mathbb{Q}$. Cuando $p > 2$, vemos que un cuerpo de definición de $\mathcal{X}$ es $Q(e^{2\pi i/p^{m-j}})$, recordando que se define por la ecuación:

$$y^n = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t}$$

donde $\lambda = e^{2\pi i/p^{m-j}}$

Primero, notamos que G es imagen homomorfa de un grupo fuchsiano de la forma:

$$\Gamma = \langle c_1, c_2, c_3 | c_1^n = c_2^n = c_3^n = c_1c_2c_3 = 1 \rangle$$

bajo el homomorfismo $c_1 \to a, c_2 \to b, c_3 \to (ab)^{-1}$, el cual se extiende a todo Γ.

A continuación presentamos ideas de [6], adaptadas al grupo G que nos permitirán determinar el menor cuerpo de definición de $\mathcal{X}_{n,j}$.

Definición 4.3.1 *Diremos que una tupla de enteros (u, v, w) determina un homomorfismo $\phi : \Gamma \to G$ con núcleo sin torsión si*

$$\phi(c_1) = b^u a^{s_1}, \phi(c_2) = b^v a^{s_2}, \phi(c_1) = b^w a^{s_3}$$

En ese caso, diremos que ϕ es del tipo (u, v, w)

En nuestro caso, vemos que el homomorfismo mostrado antes es del tipo $(1, 0, -1)$, usando que $b^{-1}a^{-1} = a^{-r}b^{-1}$. El siguiente teorema establece que un homomorfismo $\Gamma \to G$ del tipo (u, v, w) determina el menor cuerpo de definición de $\mathcal{X}_{n,j}$ (demostrado en [6], pág. 293):

Teorema 4.3.1 *Sea X una superficie de Riemann compacta con acción de $G_{n,j}$ uniformizada por el nucleo de un homomorfismo $\Gamma \to G$ determinado por la tupla (u,v,w). Si exactamente uno de lo tres números u, v o W es congruente a 0 módulo p^{m-j}, entonces el menor cuerpo de definición de X es $\mathbb{Q}(\cos(2\pi i/p^{m-j}))$.*

De esto, deducimos el siguiente corolario:

Corolario 4.3.1 *Para cualquier j, El menor cuerpo de definición de $\mathcal{X}_{n,j}$ es $\mathbb{Q}(cos(2\pi i/p^{m-j}))$.*

Definición 4.3.2 *Sea K una extensión galoisiana de $\mathbb{Q}$ y $H = Gal(K|\mathbb{Q})$.*

1. Para $f \in K[x,y]$ y $\sigma \in H$ sea f^σ el polinomio obtenido al aplicar σ a los coeficientes de f.

*2. Para $X \subset \mathbb{C}^2$ una curva plana afín definida por un polinomio $f \in K[x,y|$ sea X^σ el polinomio definido por f^σ. Considere $L = \{\sigma \in H | X^\sigma \cong X\}$. El cuerpo $M_K(X) = Fix_L(K)$ se llama **cuerpo de Móduli** de X.*

En [10] se estudia en detalle el concepto de cuerpo de Móduli de forma más general. Se puede ver que todo cuerpo de definición de X contenido en K contiene a $M_K(X)$ y existen condiciones para cuando $M_K(X)$ es un cuerpo de definición de X, propiedad que se tiene en ciertos casos como en las curvas quasiplatónicas. Como $\mathcal{X}_{n,j}$ es una curva quasiplatónica (pues $\mathcal{X}_{n,j}/\mathbf{Aut}(\mathcal{X}_{n,j}) \cong \mathbb{P}^1$ con 3 puntos de ramificación), se establece que $\mathcal{X}_{n,j}$ se define sobre su cuerpo de móduli. De esta forma, $\mathbb{Q}(\cos(2\pi i/p^{m-j}))$ es el cuerpo de móduli de $\mathcal{X}_{n,j}$.

Para encontrar una ecuación, o un conjunto de ecuaciones para $\mathcal{X}_{n,j}$ en nos apoyaremos en resultados de [11] que dan una forma constructiva de encontrar las ecuaciones para $\mathcal{X}_{n,j}$, usando lo mencionado en el párrafo anterior. Primero, vemos que:

$$\left\{(x,y) \in \mathbb{C}^2 | y^n = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^t)^{\rho_t}\right\} \cong \left\{(x,y) \in \mathbb{C}^2 | y^n = \prod_{t=0}^{p^{m-j}-1} (x^{p^j} - \lambda^{-t})^{\rho_t}\right\}$$

donde un isomorfismo es dado por

$$h(x,y) = \left(\frac{1}{x}, \frac{y}{x^{p_{m,j}p^j/n}}\right)$$

Este isomorfismo está definido sobre $\mathbb{Q}$. Además, si σ es el elemento de $Gal(\mathbb{Q}(\lambda)|\mathbb{Q}(cos(2\pi i/p^{m-j})))$ tal que $\sigma(\lambda) = \lambda^{-1}$, este automorfismo de cuerpos

cambia el polinomio que define $\mathcal{X}_{n,j}$ en el polinomio que define su imagen bajo h. Consideremos ahora la siguiente aplicación inyectiva de $\mathbb{C}^2$ a $\mathbb{C}^4$ definida por:

$$\Phi(x,y) = (x, y, h(x,y))$$

A continuación definimos los siguientes polinomios en $\mathbb{C}[x_1, x_2, x_3, x_4]$:

$$g_1(x_1,x_2,x_3,x_4) = x_1x_3, \quad g_2(x_1,x_2,x_3,x_4) = x_2x_4$$
$$g_3(x_1,x_2,x_3,x_4) = x_1 + x_3, \quad g_4(x_1,x_2,x_3,x_4) = x_2 + x_4$$
$$g_5(x_1,x_2,x_3,x_4) = x_1x_2 + x_3x_4$$

Escribamos $\Psi(\hat{x}) = (g_1(\hat{x}), g_2(\hat{x}), g_3(\hat{x}), g_4(\hat{x}), g_5(\hat{x}))$ y $F = \Psi \circ \Phi$, donde $\hat{x} = (x_1, x_2, x_3, x_4)$.

Proposición 4.3.1 *La función F es inyectiva y la imagen de $\mathcal{X}_{n,j}$ bajo F está definida sobre $\mathbb{Q}(cos(2\pi i/p^m \ ^j))$.*

De esta forma, la curva algebraica obtenida estará definida en el menor cuerpo de definición de $\mathcal{X}$. Debido al grado del polinomio que define a $\mathcal{X}$, la determinación de las ecuaciones en el nuevo cuerpo de definición es una tarea que incluso con ayuda de programas computacionales es complicada. Eventualmente, si podemos encontrar las ecuaciones, que serían 4, sería también interesante poder determinar los generadores de G como automorfismos de la nueva curva algebraica obtenida.

Capítulo 5

Representaciones Irreducibles de $G_{n,j}$ y la Variedad Jacobiana de $\mathcal{X}_{n,j}$

En este capítulo estudiaremos algunas aplicaciones de los resultados obtenidos anteriormente. Especiificamente, estudiaremos las representaciones irreducibles complejas y racionales de G y usaremos esto para determinar la descomposición isotípica de la Jacobiana de $\mathcal{X}$. También determinaremos ecuaciones para los cocientes intermedios dados por los núcleos de las representaciones complejas de G. Además, determinaremos variedades de Prym de $\mathcal{X}$ asociadas a subgrupos de G. Finalmente, mencionaremos brevemente algunos hechos sobre el menor cuerpo de definición de $\mathcal{X}$, es decir, el menor cuerpo en el cual $\mathcal{X}$ se puede definir como curva plana.

5.1. Representaciones irreducibles de $G_{n,j}$

El método de determinar las representaciones complejas irreducibles de G se basa en lo expuesto en la Sección 8.2 de [23] sobre representaciones de productos semidirectos de la forma $G = A \rtimes B$ donde A es abeliano. Esto se resume en lo siguiente:

1. Como A es abeliano, sus representaciones irreducibles son todas de dimensión 1.

2. Para la acción de G en $irr(A)$ por $z.\chi(a) = \chi(z^{-1}az)$, determinamos los estabilizadores y las órbitas bajo esta acción.

3. Para cada representante χ de los estabilizadores H, se construye la representación inducida ξ^G

4. $\xi^G \in irr(G)$

De esta forma, se obtienen todas las representaciones irreducibles complejas de G. Para obtener las representaciones irreducibles racionales, se determina para cada representación sus conjugadas de acuerdo a su cuerpo de caracteres K, y se suman cada representación con sus respectivas conjugadas por $Gal(K|\mathbb{Q})$, multiplicadas por su respectivo índice de Schur para obtener las representaciones racionales. Esto se basa en lo expuesto en [7], capítulo X.

En nuestro caso, $A = \langle a \rangle$, $B = \langle b \rangle$, son grupos cíclicos de orden n, por lo que ambos sólo tienen representaciones irreducibles de dimensión 1.

Ahora, haremos la distinción de acuerdo a cada caso:

5.1.1. Caso p impar

Especificamos el siguiente teorema respecto a las representaciones complejas y racionales irreducibles de G;

Teorema 5.1.1 *El número de representaciones complejas irreducibles de G es*

$$np^j + p^{j-1}(p-1)\sum_{v=j}^{m-1} p^v = np^j + p^{j-1}(p^m - p^j)$$

y el número de representaciones racionales irreducibles de G es

$$(m-j)p^j + \sum_{t=0}^{m-j-1}\sum_{l=0}^{t}(p^{l+1}-1) + (m-j+1)p^j + 2\frac{\frac{p^j-1}{p-1} - j + 2}{p-1} + p^{j-1} + 1$$

Todas estas representaciones tienen índices de Schur iguales a 1.

Demostración: denotamos los caracteres de A por χ_k, con $0 \leq k \leq n-1$. Estos caracteres se expresan como

$$\chi_k(a^t) = e^{2\pi ikt/n}$$

Calculemos $L_k = Stab_B(\chi_k)$. Si $b^u \in L_k$, se tiene que:

$$\chi_k(a) = b^u.\chi_k(a) = \chi_k(b^{-u}ab^u) = \chi_k(a^{r^u}) = \chi_{r^u k}(a)$$

Esto nos lleva de nuevo a ver el cálculo de la órbita de k módulo n bajo la acción de multiplicar por r. De esta forma, tenemos que:

- Si $mcd(k,n) = p^v$ con $0 \leq v < m-j$, entonces $L_k = \langle b^{p^{m-j-v}} \rangle$.
- Si $mcd(k,n) \geq p^{m-j}$ entonces $L_k = B$.

Así, si $mcd(k,n) \geq p^{m-j}$, y ζ_l es una representación compleja irreducible de B, donde

$$\zeta_l(a^t) = e^{2\pi i l t/n}$$

entonces $\xi_{k,l} = \chi_k \otimes \zeta_l$ es una representación irreducible de G de dimensión 1. Hay exactamente $p^j n$ representaciones de este tipo.

Si $mcd(k,n) = p^v < p^{m-j}$, llamando $\zeta_{l,v}$ una representación irreducible de L_k, obtenemos que $\xi_{k,l,v} = \chi_k \otimes \zeta_{l,v}$ es una representación irreducible de $A \rtimes L_k$ que induce una representación $\theta_{k,l,v}$ de dimensión p^{m-j-v}. En total para cada v, hay exactamente $p^{j-1}(p-1)p^{j+v}$ representaciones complejas irreducibles de dimensión p^{m-j-v}. De esta forma, el número de representaciones complejas irreducibles de G es:

$$np^j + p^{j-1}(p-1)\sum_{v=j}^{m-1} p^v = np^j + p^{j-1}(p^m - p^j)$$

Estas representaciones tienen índice de Schur igual a 1 pues G es un grupo nilpotente de orden impar (se puede consultar este hecho en [22]). Las representaciones de dimensión mayor a 1 se pueden ver matricialmente como las siguientes matrices para a y b:

$$a = Diag(w^k, w^{kr}, ..., w^{kr^{p^{m-j-v}-1}})$$

$$b = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & w^{lp^{m-j-v}} \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & \vdots & 1 & 0 \end{bmatrix}$$

La matriz de a tiene traza igual a cero, pues se puede comprobar directamente que las componentes de su diagonal son distintas. Si se suman, tenemos

$$\sum_{l=0}^{p^{m-j-v}-1} w^{kr^l} = w^k \sum_{l=0}^{p^{m-j-v}-1} w^{k(r^l-1)}$$

Los sumandos de la suma del segundo lado de la igualdad anterior son raices p^{m-j-v}-ésimas de la unidad, distintas entre sí, por lo que esa suma es cero. Al elevar la matriz a $t = p^{m-j-v}$, vemos que $p^{m-j-v}kr \equiv_n p^{m-v}k$, por lo tanto, $a^t = w^{tk}I_{p^{m-j-v}}$. Además, $b^t = w^{kp^{m-j-v}}I_{p^{m-j-v}}$. Así, llamando $K_{k,l,v}$ el cuerpo de caracteres de $\theta_{k,l,v}$ tenemos que ese cuepo es igual a $\mathbb{Q}(w^{p^{\bar{z}}})$, donde $\bar{z} = min(m-j, m-j-v+u)$ con $p^u = mcd(l,n)$. Aplicando esto, podemos obtener la siguiente tabla de representaciones racionales obtenidas (tomando en cuenta que $0 \leq v \leq m-j-1$ y $0 \leq u \leq j+v$:

v	u	Cantidad de $\theta_{k,l,v}$	rep. obtenidas
t	Todo $l \geq t$	$p^{2j-1}(p-1)$	p^j
t	$l < t$	$(p^{j+t} - p^{j+t-l-1})(p-1)$	$p^{j-1}(p^{l+1}-1)$

Sumando los términos de la cuarta columna, tenemos que el número de representaciones racionales obtenidas de las complejas de dimensión mayor a 1 es:

$$(m-j)p^j + \sum_{t=0}^{m-j-1} \sum_{l=0}^{t-1} (p^{l+1}-1)$$

representaciones racionales de G derivadas de las complejas de dimensión mayor a 1.

En el caso de las representaciones racionales obtenidas a partir de las complejas de dimensión 1, haremos el análisis dependiendo de $k = p^{m-j}\bar{k}$ y l con $0 \leq \bar{k} \leq p^j - 1$ y $0 \leq l \leq n-1$. Para $mcd(l,n) = p^u$ con $0 \leq u \leq m-j$, verificamos que

$$\xi_{k,l}(a^{t_1}b^{t_2}) = w^{kt_1+lt_2}$$

al ser conjugado por el generador de $Gal(K_{k,l}|\mathbb{Q})$, con $K_{k,l}$ el cuerpo de caracteres de $\xi_{k,l}$, modifica el caracter de acuerdo a la imagen de w. De esta forma se construyen órbitas cuyo largo depende de k y l en cuanto a su divisibildad por potencias de p. Esto lo resumimos en la siguiente tabla, denominando $mcd(k,n) = p^{v_1}$ y $(l,n) = p^{v_2}$. Se cuentan cuantos k y l cumplen con los valores de v_1 y v_2, se establece cual de ellos aporta con las raices de mayor grado, se cuentan las combinaciones posibles de $\xi_{k,l}$ y se divide por los conjugados posibles de las raices en cuestión por $Gal(K_{k,l}|\mathbb{Q})$ para obtener las representaciones racionales, siendo la primera tabla para el caso en que $j > 1$, y la segunda en el caso de $j = 1$:

v_1	v_2	Cantidad de $\xi_{k,l}$	rep. obtenidas
Todos	$0 \leq t \leq m-j$	$p^j p^{t-1}(p-1)$	p^j
$m-j+1 \leq t < m$	todo $u > t$	$p^{m-u}p^{m-t-1}(p-1)$	p^{m-u}
$m-j+1 \leq t < m$	t	$p^{m-t-1}(p-1)p^{m-t-1}(p-1)$	$p^{m-t-1}(p-1)$
$u > t$	$m-j+1 \leq t < m$	$p^{m-u}(p-1)p^{m-t-1}(p-1)$	$p^{m-u}(p-1)$
m	m	1	1

Haciendo la suma de estas de los números de la cuarta columna se obtiene:

$$(m-j+1)p^j + 2\frac{\frac{p^j-1}{p-1} - j + 2}{p-1} + p^{j-1} + 1$$

Que es el número total de representaciones racionales derivadas de las complejas de dimensión 1. □

Ejemplo 5.1.1 *Consideremos $p = m = 3$, $j = 2$, es decir, $r = 10$. En este caso $b^3 \in Z(G)$, por lo que las representaciones complejas irreducibles de G sólo tienen dimensión 1 ó 3. El número total de estas representaciones es:*

$$27 \cdot 9 + 3(27-9) = 297$$

que originan en total 35 representaciones racionales de G.

5.1.2. Caso $p = 2$, $j = 1$

En este caso $r = \nu_1 = \frac{n}{2} - 1$.

Teorema 5.1.2 *La cantidad de representaciones irreducibles complejas de G es:*

$$\frac{n^2}{4} + \frac{3n}{2}$$

Y la cantidad de representaciones racionales irreducibles es:

$$6 + 2^{m-1} + \sum_{t=1}^{m-2} t2^{m-t-2} + m$$

Hay exactamente $\frac{n}{2}$ representaciones complejas irreducibles con índice de Schur igual a 2.

Demostración: Denotamos χ_k de forma análoga al caso anterior. Recordando el cálculo de las órbitas de $\mathbb{Z}/n\mathbb{Z}$ bajo la multiplicación por r, podemos hacer el mismo procedimiento que en el caso anterior y se tiene que

- Si k es divisible por $\frac{n}{2}$, entonces $L_k = B$.

- Si k no es divisible por $\frac{n}{2}$, entonces $L_k = \langle b^2 \rangle$.

De esta forma, cuando k es divisible por $\frac{n}{2}$, y ζ_l se define de la misma forma que en el caso anterior, $\xi_{k,l} = \chi_k \otimes \zeta_l$ es una representación compleja irreducible de dimensión 1. Hay en total $2n$ representaciones de este tipo. Si k no es divisible por $\frac{n}{2}$ y $\zeta_{l,1}(a^t) = e^{4\pi i l t/n}$ define una representación irreducible de L_k, entonces $\xi_{k,l,1} = \chi_k \otimes \zeta_{l,1}$ induce una representación $\theta_{k,l,1}$ de G de dimensión 2. En total hay $\frac{n}{2}(\frac{n}{2}-1)$ representaciones de este tipo y así, el número de representaciones complejas irreducibles de G es:

$$2n + \frac{n^2}{4} - \frac{n}{2} = \frac{n^2}{4} + \frac{3n}{2}$$

Las representaciones de dimensión 2 se ven matricialmente como:

$$a = Diag(w^k, w^{rk}), \quad b = \begin{bmatrix} 0 & w^{2l} \\ 1 & 0 \end{bmatrix}$$

Para calcular el indice de Schur de estas representaciones, que es menor o igual a 2, nos apoyaremos en el siguiente teorema demostrado en [14]:

Teorema 5.1.3 *Sea Γ un grupo cuyo orden es una potencia de 2, y sea θ una representación de Γ de dimensión 2 sobre $\mathbb{C}$. θ tiene índice de Schur igual a 2 si y sólo si para todo $x \in \Gamma$, $Det(\Theta(x)) - 1$.*

Aplicando este teorema, observamos que los determimante de a y b son $Det(a) = w^{(r+1)k} = w^{k\frac{n}{2}}$, $Det(b) = -w^{2l}$. Esto nos dice que para que el índice de Schur sea 2, k tiene que ser par y $l \in \{\frac{n}{4}, 3\frac{n}{4}\}$.

Sobre el cuerpo de caracteres de $\theta_{k,l,1}$, que denotamos por $K_{k,l,1}$, podemos decir que la traza de la matriz de a es $w^k + w^{rk}$, mientras que la matriz de b^2 tiene como traza $2w^{2l}$. Si k es impar, observando que $w^{\frac{n}{2}} = -1$, la traza de a es igual a $w^k - w^{-k}$, el cual es un número complejo puramente imaginario. De esto, podemos establecer que $K_{k,l,1} = \mathbb{Q}(w^k - w^{-k}, w^{2l})$. Si k es par, tenemos que $rk \equiv_n -k$, por lo que la traza de a es $w^k + w^{-k}$, que es un número real. Por lo tanto, $K_{k,l,1} = \mathbb{Q}(w^k + w^{-k}, w^{2l})$. Aplicando estas ideas, la agrupación de las representaciones complejas para formar las racionales se expresa en la siguiene tabla

u_1	u_2	Cantidad de $\theta_{k,l,1}$	Cantidad de rep. obtenidas
0	$t \leq m-3$	$2^{m-2} \cdot 2^{m-t-2}$	2^{m-t-3}
0	$t > m-3$	2^{m-2}	1
$t>0$	$l \leq t-1$	$2^{m-t-2} \cdot 2^{m-l-2}$	2^{m-t-2}
$t>0$	$t-1 < l \leq m-3$	$2^{m-t-2} \cdot 2^{m-l-2}$	2^{m-l-3}
$t>0$	$l > m-3$	2^{m-t-2}	1

Entonces la cantidad de representaciones racionales irreducibles obtenidas de esta forma es:

$$\sum_{t=0}^{m-3} 2^{m-t-3} + 2 + \sum_{t=1}^{m-2}\sum_{l=0}^{t-1} 2^{m-t-2} + \sum_{t=1}^{m-2}\sum_{l=t}^{m-3} 2^{m-l-3} + 2$$

$$= 3 + 2^{m-2} + \sum_{t=1}^{m-2} t2^{m-t-2} + \sum_{t=1}^{m-2} (2^{m-t-2} - 1)$$

$$= 3 + 2^{m-2} + \sum_{t=1}^{m-2} t2^{m-t-2} + 2^{m-2} - 1 - (m-2)$$

$$= 4 + 2^{m-1} + \sum_{t=1}^{m-2} t2^{m-t-2} - m$$

A continuación, consideramos las representaciones complejas de dimensión 1. Estas son de la forma $\xi_{k,l} = \chi_k \otimes \zeta_l$ donde k es múltiplo de $n/2$ y $0 \leq l \leq n-1$. La forma de obtener las racionales derivadas de éstas es de la misma forma que el caso de p impar y las resumimos en la siguiente tabla, llamando u_1, u_2 tales que $(k,n) = 2^{u_1}$ y $(l,n) = 2^{u_2}$:

u_1	u_2	Cantidad de $\xi_{k,l}$	Cantidad de rep. obtenidas
$m-1$ o m	$u \leq m-2$	2^{m-u-1}	1
$m-1$ o m	$m-1$ o m	1	1

De esta forma se tienen en total $2(m+1)$ representaciones racionales. □

5.1.3. Caso $p = 2$, $j = 2$

En este caso $r = \nu_2 = \frac{n}{2} + 1$.

Teorema 5.1.4 *La cantidad de representaciones complejas irreducibles de G es:*

$$\frac{5n^2}{8}$$

y la cantidad de representaciones racionales irreducibles de G es:

$$n + \sum_{u=1}^{m-2}(u-1)2^{m-u-1} + 2^m - 2 + 2m$$

Denotamos χ_k como antes. Recordando el cálculo de las órbitas de $\mathbb{Z}/n\mathbb{Z}$ bajo la multiplicación por r, podemos obtener lo siguiente:

- Si k es par, entonces $L_k = B$.
- Si k es impar, entonces $L_k = \langle b^2 \rangle$.

De esta forma, cuando k es par y ζ_l se define de la misma forma que en el caso anterior, $\xi_{k,l} = \chi_k \otimes \zeta_l$ es una representación compleja irreducible de dimensión 1. Hay en total $\frac{n^2}{2}$ representaciones de este tipo. Si k es impar y $\zeta_{l,1}(a^t) = e^{4\pi i l t/n}$, define una representación irreducible de L_k, entonces $\xi_{k,l,1} = \chi_k \otimes \zeta_{l,1}$ induce una representación $\theta_{k,l,1}$ de G de dimensión 2. En total hay $\frac{n}{2} \cdot \frac{n}{4}$ representaciones de este tipo. Por lo tanto, el número de representaciones complejas irreducibles de G es:

$$\frac{n^2}{2} + \frac{n^2}{8} = \frac{5n^2}{8}$$

Las representaciones de dimensión 2 se ven matricialmente como:

$$a = Diag(w^k, w^{rk}), \quad b = \begin{bmatrix} 0 & w^{2l} \\ 1 & 0 \end{bmatrix}$$

Para racionalizar las representaciones complejas, se hace de una forma similar a los casos anteriores. Sea $K_{k,l,1}$ el respectivo cuerpo de caracteres. La traza de a es $w^k - -w^k = 0$, la de a^2 es w^{2k}, mientras que la de b^2 es $2w^{2l}$. Por lo tanto, $K_{k,l,1} = \mathbb{Q}(w^2)$. Como hay en total $\frac{n^2}{8}$ representaciones de dimensión 2, se obtienen $\frac{n}{2}$ representaciones racionales.

Viendo la matriz de a, vemos que su determimante es $w^{(\frac{n}{2}+2)k}$ que nunca es 1 pues k es impar. Aplicando el teorema 8.1.1, se tiene que todas las representaciones complejas irreducibles de dimensión 2 de G tienen índice de Schur 1.

En el caso de las de dimensión 1, se hace de nuevo como en los otros casos, fijando $\xi_{k,l} = \chi_k \otimes \zeta_l$ las representaciones de dimensión 1, k par y $0 \leq l \leq n-1$, u_1 y u_2 tales que $(k,n) = 2^{u_1}$ y $(l,n) = 2^{u_2}$. De esta forma se tiene la siguiente tabla:

u_1	u_2	Cantidad de $\xi_{k,l}$	Cantidad de rep. obtenidas
Todos	0	$2^{m-1} \cdot 2^{m-1}$	2^{m-1}
$t < u$	$1 \leq u \leq m-2$	$(2^{m-t-1}) \cdot 2^{m-u-1}$	2^{m-u-1}
$u \leq t < m-1$	$1 \leq u \leq m-2$	$2^{m-t-1} \cdot 2^{m-u-1}$	2^{m-t-1}
$t \geq m-1$	$1 \leq u \leq m-2$	2^{m-u-1}	1
$t \leq m-2$	$m-1$ ó m	2^{m-t-1}	1
$m-1$ ó m	$m-1$ ó m	1	1

Por lo tanto, la cantidad de representaciones racionales de G derivadas de las complejas de dimensión 1 es:

$$2^{m-1} + \sum_{u=1}^{m-2}\sum_{t=1}^{u-1} 2^{m-u-1} + \sum_{u=1}^{m-2}\sum_{t=u}^{m-2} 2^{m-t-1} + 4(m-2) + 4$$

$$= 2^{m-1} + \sum_{u=1}^{m-2}(u-1)2^{m-u-1} + \sum_{u=1}^{m-2}(2^{m-u} - 2) + 4(m-2) + 4$$

$$= 2^{m-1} + \sum_{u=1}^{m-2}(u-1)2^{m-u-1} + 2^m - 4 + 2m. \square$$

5.1.4. Caso $p = 2$, $j = 3$

En este caso $r = \nu_3 = n - 1$. Denotamos χ_k de forma análoga al caso anterior. Repitiendo la misma idea de los otros dos casos, podemos establecer los siguientes teoremas:

Teorema 5.1.5 *La cantidad de representaciones irreducibles complejas de G es:*

$$\frac{n^2}{4} + \frac{3n}{2}$$

y la cantidad de representaciones racionales irreducibles es:

$$6 + 2^{m-1} + \sum_{t=1}^{m-2} t2^{m-t-2} + m$$

Hay exactamente $\frac{n}{2}$ representaciones complejas irreducibles con índice de Schur igual a 2.

Demostración: El cálculo de las cantidades de representaciones similar al caso $p = 2$, $j = 1$. Las representaciones de dimensión 2 se ven matricialmente como:

$$a = Diag(w^k, w^{rk}), \quad b = \begin{bmatrix} 0 & w^{2l} \\ 1 & 0 \end{bmatrix}$$

Se puede ver que la matriz de a tiene determinante 1 independiente de k pues $r+1 = n$. Entonces, observando la matriz de b, concluimos que $\theta_{k,l,1}$ tiene índice de Schur 2 si y solo si $(l, n/2) = n/4$. □

5.2. Descomposición Isotípica de $J\mathcal{X}_{n,j}$

Después de lo desarrollado en la sección anterior, podemos obtener las dimensiones de los factores de la descomposición isotípica de $J\mathcal{X}_{n,j}$. Como ha sido usual en este trabajo, dividiremos esta sección según si p es impar o igual a 2:

5.2.1. Caso p impar

Teorema 5.2.1 *Las dimensiones de los factores de la descomposición isotípica de $J\mathcal{X}_{n,j}$ se especifican en las siguientes tablas, siendo la primera para los factores asociados a representaciones complejas de dimensión mayor a 1 y la segunda para los factores asociados a representaciones complejas de dimensión 1:*

d_1	d_2	$K(\theta_{k,l,v})$	$\dim(D_{k,l,j})$
0	1	$p^{j-1}(p-1)$	$\frac{p^{j-1}(p-1)(p^{m-j-v-1}-1)}{2}$
1	0	$p^{j-1}(p-1)$	$\frac{p^{j-1}(p-1)(p^{m-j-v-1}-1)}{2}$
0	0	$p^{j+v-u-1}(p-1)$, $0 \leq u < v$	$\frac{p^{m-u-1}(p-1)}{2}$

donde $d_1 = \dim(Fix_b(\theta_{k,l,v}))$ *y* $d_2 = \dim(Fix_{ab}(\theta_{k,l,v}))$

v_1	v_2	ϑ	$K(\xi_{k,l})$	$Dim(E_{k,l})$
$t < m$	$u \leq m-j$	(0,0,0)	$p^{m-u-1}(p-1)$	$\frac{p^{m-1}(p-1)}{2}$
$t = m-j$	$m-j+1$	(0,0,0)	$p^{j-1}(p-1)$	$\frac{p^{j-1}(p-1)}{2}$
$m-j \leq t < m$	$m-j+1$	(0,0,0)	$p^{j}(p-1)$	$\frac{p^{j-1}(p-1)}{2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$t < m-1$	$m-1$	(0,0,0)	$p^{m-t-1}(p-1)$	$\frac{p^{m-t-1}(p-1)}{2}$
$t = m-1$	$m-1$	(0,0,0)	$(p-1)$	$\frac{p-1}{2}$
$t-m$	$u < m$	(1,0,0)	$p^{m-u-1}(p-1)$	0
$t < m$	m	(0,1,0)	$p^{m-t-1}(p-1)$	0
t	u *tal que* $n \mid (p^j t + u)$	(0,0,1)	$p^{m-j-1}(p-1)$	0

donde $mcd(k,n) = p^{v_1}$ y $mcd(l,n) = p^{v_2}$.
El factor de la descomposición isotípica asociado a la representación trivial de G tiene dimensión cero.

Demostración: Para determinar que factores aportan en la descomposición de $J\mathcal{X}$, necesitamos determinar la existencia de subespacios de cada representación fijos por a, b y ab, así como las extensiones de $\mathbb{Q}$ obtenidas al adjuntar los caracteres evaluados en cada elemento de G.

Empezando con las representaciones complejas de dimensión mayor a 1, una observación es que a no tiene subespacios fijos no triviales salvo si $kr \equiv_n k$, es decir, cuando k es múltiplo de p^{m-j}. Como $v < m-j$, a no aporta puntos fijos no triviales en ningun caso. Para ver si b aporta subespacios fijos no triviales, eso ocurre sólo si $l = 0$. De esta forma, vemos que hay sólo una representación racional derivada de complejas de esta forma. En el caso de ab, podemos ver que su matriz es igual a:

$$ab = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & w^{p^{m-j-v}l+k} \\ w^{r^k} & 0 & 0 & \dots & 0 & 0 \\ 0 & w^{r^{2k}} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & \vdots & w^{r^{p^{m-j-v}-1}k} & 0 \end{bmatrix}$$

Para que esa matriz tenga subespacios fijos no triviales es necesario que

$$(1 + r + \dots + r^{p^{m-j-v}-1})k + p^{m-j-v}l \equiv_n \left(p^{m-j-v} + \frac{p^{m-v}(p^{m-j-v}+1)}{2}\right)k + p^{m-j-v}l$$

sea congruente a cero módulo n. Como k es múltiplo de p^v esa expresión es congruente módulo n a $p^{m-j-v}(k+l)$. Es claro que para cada k existe un único $l > 0$ que satisface esa ecuación, el cual debe ser múltiplo de p^v. Además si esa matriz tiene puntos fijos no triviales, sus conjugadas por $Gal(\mathbb{Q}(w)|\mathbb{Q})$ también. De esta forma, existe una única representación racional en cuyas complejas asociadas $Fix_{ab}(\theta_{k,l,v})$ es no trivial. Claramente esos espacios fijos son de dimensión 1. Y en ese caso, la extensión asociada debe ser $\mathbb{Q}(w^{p^{m-j}})$.

Para las otras representaciones racionales de G, $\xi_{k,l}$ sean v_1 y v_2 tales que . Primero, notamos que en el caso de las representaciones no triviales (es decir, k y l no idénticamente cero), exactamente uno de a, b y ab sólo tienen subespacios fijos sí y sólo si $k = 0$ (en el cual $\dim Fix_a > 0$), o bien $l = 0$ ($\dim(Fix_b) > 0$), o cuando $p^j k + l$ es congruente a 0 módulo n. En este último caso es evidente que para cada

k existe un único l que cumple eso, por lo que hay exactamente 3 representaciones racionales en las cuales sus complejas asociadas tienen espacios fijos no triviales por algunos de a, b o ab. De todo esto, usando el Teorema 2.8.1, se obtienen las tablas antes indicadas.

Finalmente, como $g_G = 0$, tenemos que el factor asociado a la representación trivial de G es de dimensión cero. □

Ejemplo 5.2.1 *Usando el Teorema anterior, la Jacobiana de $\mathcal{X}_{27,2}$ es isógena a el siguiente producto de subvariedades:*

$$J\mathcal{X} \sim \prod_{k=1}^{7} T_k^3 \times \prod_{k=1}^{2} U_k^3 \times \prod_{k=8}^{15} T_k \times \prod_{k=1}^{9} V_k \times E$$

donde $\dim(T_k) = 9$, $\dim(U_k) = 6$, $\dim(V_k) = 3$ *y* $\dim(E) = 1$. *Las T_k con $k \leq 7$ y las U_k se corresponden con representaciones complejas irreducibles de dimensión 3 y las restantes con representaciones de dimensión 1.*

5.2.2. Caso $p = 2$

Los siguientes teoremas para la descomposición isotípica de $J\mathcal{X}$ en $p = 2$ se demuestran de forma similar a lo desarrollado en la subsección anterior:

Teorema 5.2.2 *Las dimensiones para los factores de la descomposición isotípica $J\mathcal{X}_{n,j}$ con $j = 1$ se especifican en las siguientes tablas, siendo la primera correspondiente a factores asociados a representaciones complejas de dimensión 2 y la segunda a factores asociados a representaciones complejas de dimensión 1:*

u_1	u_2	ϑ	$K(\theta_{k,l,1})$	$m(\theta_{k,l,1})$	$\dim(E_{k,l})$
0	$< m-2$	$(0,0)$	2^{m-1}	1	2^{m-1}
$0 < t < m-2$	$0 \leq u < t$	$(0,0)$	2^{m-u-2}	1	2^{m-u-2}
$0 < t < m-2$	$t \leq u < m-2$	$(0,0)$	2^{m-t-1}	1	2^{m-u-2}
$0 < t < m-2$	$m-2$	$(0,1)$	2^{m-t-2}	2	2^{m-t-2}
$m-2$	$u < m-2$	$(0,0)$	2^{m-u-1}	1	2^{m-u-1}
$m-2$	$m-2$	$(0,0)$	2	2	4
0	$m-1$	$(0,1)$	2^{m-2}	1	2^{m-2}
$t > 0$	$m-1$	$(0,1)$	2^{m-t-2}	2	2^{m-t-2}

donde $\vartheta = (\dim(Fix_b), \dim(Fix_{ab}))$, $m(\theta_{k,l,1})$ *el índice de Schur de* $\theta_{k,l,1}$ *y* u_1, u_2 *son tales que* $(k,n) = 2^{u_1}$ *y* $(l,n) = 2^{u_2}$.

u_1	u_2	ϑ	$K(\xi_{k,l})$	$\dim(E_{k,l})$
$m-1$	$u<m-2$	$(0,0,0)$	2^{m-u-1}	2^{m-u-2}
$m-1$	$m-1$	$(0,0,1)$	1	0
$m-1$	m	$(0,1,0)$	2^{m-u-1}	0
m	$u<m$	$(1,0,0)$	2^{m-u-1}	0
m	$m-1$	$(1,0,0)$	2^{m-u-1}	0

donde $\vartheta=(\dim(Fix_a),\dim(Fix_b),\dim(Fix_{ab}))$ *y* u_1, u_2 *son tales que* $(k,n)=2^{u_1}$ *y* $(l,n)=2^{u_2}$.

El factor de la descomposición isotípica asociado a la representación trivial de G *tiene dimensión cero.*

Teorema 5.2.3 *Las dimensiones de los factores de la descomposición isotípica de* $JX_{n,j}$ *con* $j=2$ *asociados a las representaciones complejas irreducibles de* G *se especifican en las siguientes tablas, siendo la primera correspondiente a factores asociados a representaciones complejas de dimensión 2 y la segunda a factores asociados a representaciones complejas de dimensión 1:*

u	ϑ	$K(\theta_{k,l,1})$	$\dim(E_{k,l})$
$u<m-2$, $(r+1)k+2l\equiv_n 0$	$(0,1)$	2^{m-2}	2^{m-3}
$u<m-2$, $n\nmid(r+1)k+2l$	$(0,0)$	2^{m-2}	2^{m-2}
$m-2$	$(0,0)$	2^{m-2}	2^{m-2}
$m-1$	$(1,0)$	2^{m-2}	2^{m-3}

donde u *es tal que* $(l,\frac{n}{2})=2^u$ *y* $\vartheta=(\dim(Fix_b),\dim(Fix_{ab}))$.

u_1	u_2	ϑ	$K(\xi_{k,l})$	$\dim(E_{k,l})$
Todos	*0*	$(0,0,0)$	2^{m-1}	2^{m-2}
$t<u$, $n\nmid(k+l)$	$1\le u\le m-2$	$(0,0,0)$	2^{m-t-1}	2^{m-t-2}
$u\le t<m-1$, $n\nmid(k+l)$	$1\le u\le m-2$	$(0,0,0)$	2^{m-u-1}	2^{m-u-2}
$m-1$	$1\le u\le m-2$	$(0,0,0)$	2^{m-u-1}	2^{m-u-2}
$t<u$, $n\mid(k+l)$	$1\le u\le m-2$	$(0,0,0)$	2^{m-t-1}	2^{m-t-2}
$u\le t<m-1$, $n\mid(k+l)$	$1\le u\le m-2$	$(0,0,1)$	2^{m-u-1}	*0*
$m-1$	$m-1$	$(0,0,1)$	2^{m-u-1}	*0*
m	*cualquiera*	$(1,0,0)$	2^{m-u-1}	0
cualquiera	m	$(0,1,0)$	2^{m-u-1}	0

donde $\vartheta=(\dim(Fix_a),\dim(Fix_b),\dim(Fix_{ab}))$ *y* u_1, u_2 *son tales que* $(k,n)=2^{u_1}$ *y* $(l,n)=2^{u_2}$.

El factor de la descomposición isotípica asociado a la representación trivial de G tiene dimensión cero.

Teorema 5.2.4 *Las dimensiones de los factores de la descomposición isotípica de $J\mathcal{X}_{n,j}$ con $j = 3$ asociados a las representaciones complejas irreducibles de G se especifican en las siguientes tablas, siendo la primera correspondiente a factores asociados a representaciones complejas de dimensión 2 y la segunda a factores asociados a representaciones complejas de dimensión 1:*

u_1	u_2	ϑ	$K(\theta_{k,l,1})$	$m(\theta_{k,l,1})$	$\dim(E_{k,l})$
0	$t < m-2$	$(0,0)$	2^{m-2}	1	2^{m-2}
$0 < t < m-2$	$0 \leq u < t$	$(0,0)$	2^{m-u-2}	1	2^{m-u-2}
$0 < t < m-2$	$t \leq u < m-2$	$(0,0)$	2^{m-t-2}	1	2^{m-t-2}
$0 < t < m-2$	$m-2$	$(0,0)$	2^{m-t-2}	2	2^{m-t-1}
$m-2$	$u < m-2$	$(0,0)$	2^{m-u-2}	1	2^{m-u-2}
$m-2$	$m-2$	$(0,0)$	2	2	4
0	$m-1$	$(1,1)$	2^{m-2}	1	0
$0 < t < m-2$	$m-1$	$(1,1)$	2^{m-t-2}	1	0
$m-1$	$u < m-2$	$(0,0)$	1	2^{m-u-2}	1
$m-1$	$m-2$	$(0,0)$	1	2	1
$m-1$	$m-1$	$(1,1)$	1	1	0

donde $\vartheta = (\dim(Fix_b), \dim(Fix_{ab}))$, $m(\theta_{k,l,1})$ el índice de Schur de $\theta_{k,l,1}$ y u_1, u_2 son tales que $(k,n) = 2^{u_1}$ y $(l,n) = 2^{u_2}$.

u_1	u_2	ϑ	$K(\xi_{k,l})$	$\dim(E_{k,l})$
$m-1$	$u < m-2$	$(0,0,0)$	2^{m-u-1}	2^{m-u-2}
$m-1$	$m-1$	$(0,0,1)$	1	0
$m-1$	m	$(0,1,0)$	2^{m-u-1}	0
m	$u < m$	$(1,0,0)$	2^{m-u-1}	0
m	$m-1$	$(1,0,0)$	2^{m-u-1}	0

donde $\vartheta = (\dim(Fix_a), \dim(Fix_b), \dim(Fix_{ab}))$ y u_1, u_2 son tales que $(k,n) = 2^{u_1}$ y $(l,n) = 2^{u_2}$.

El factor de la descomposición isotípica asociado a la representación trivial de G tiene dimensión cero.

Ejemplo 5.2.2 *Consideremos $m = 3$, Entonces la Jacobiana de $\mathcal{X}_{8,2}$ es isógena al siguiente producto de subvariedades:*

$$J\mathcal{X}_{8,2} \sim U_1^2 \times U_2^2 \times U_3 \times U_4 \times U_5 \times E_1^2 \times E_2^2 \times E_3 \times E_4 \times E_5$$

donde $\dim(U_k) = 2$, $\dim(E_k) = 1$.

Ejemplo 5.2.3 *Consideremos* $m = 3$, *Entonces la Jacobiana de* $\mathcal{X}_{8,1}$ *es isógena al siguiente producto de subvariedades:*

$$J\mathcal{X}_{8,1} \sim T_1^2 \times U_1^2 \times U_2 \times U_3 \times E_1^2 \times E_2^2 \times E_3$$

Donde $\dim(T_k) = 4$, $\dim(U_k) = 2$ *y* $\dim(E_k) = 1$. *El factor* U_2 *está asociado a una representación con índice de Schur igual a 2.*

5.3. Núcleos de las Representaciones Irreducibles Complejas de G

Ahora, determinaremos los núcleos de las representaciones irreducibles complejas de G. Nuevamente distinguimos caso por caso:

5.3.1. Caso p impar

Primero calculemos los núcleos de las representaciones de dimensión mayor a 1. De acuerdo a las matrices de a y b, se puede ver que como $p^v = mcd(k, n)$:

$$krp^{m-j-v} = kp^{m-j} + kp^{m-v} \equiv_n kp^{m-j}$$

De esta forma, se establece que la matriz de a tiene orden p^{m-v}. Análogamente se puede ver que la matriz de b tiene orden p^{m-u} donde $p^u = mcd(l, p^{j+v})$. Más aún, la matriz de b es un ponderado de la matriz identidad por alguna raíz de la unidad. Eligiendo $\bar{v} = max\{u, v\}$, podemos establecer lo siguiente:

Proposición 5.3.1 $N_{k,l,v} = Ker(\theta_{k,l,v}) = \{a^{p^{m-v}}, b^{p^{m-u}}, a^{p^{m-j-v}} b^{\epsilon p^{m-j-v}}\}$

Ahora, determinaremos una ecuación para $\mathcal{X}_{N_{k,l,v}}$. Llamemos $G_{k,l,v} = G/N_{k,l,v}$ y llamemos $A_{k,l,v}$ el subgrupo generado por la clase de a en ese cociente. Es claro ver que $X_{k,l,v}/A_{k,l,v}$ es de género cero. Por lo tanto, es una curva p^{m-v}-gonal. Usando métodos similares a la sección anterior, podemos determinar una ecuación para X:

Proposición 5.3.2 $\mathcal{X}_{N_{k,l,v}}$ *es isomorfa a la curva definida por la ecuación:*

$$y^{p^{m-v}} = \prod_{k=1}^{p^{m-j-u}-1} (x^{p^j} - \mu^k)^{\tau_k}$$

Donde $0 \leq \tau_k \leq p^{m-u} - 1$ *son enteros tales que*

$$\tau_k \equiv_{p^{m-u}} r^k$$

En el caso de las representaciones complejas de dimensión mayor a 1, recordamos que estas se expresan de la forma:

$$\xi_{k,l}(a^{t_1}b^{t_2}) = w^{p^{m-j}\bar{k}t_1 + lt_2}$$

En base a esto, podemos decir lo siguiente:

Proposición 5.3.3 *Sea $M_{k,l} = Ker(\xi_{k,l})$. Entonces:*

$$M_{k,l} = \langle a^{p^{s_1}}, b^{p^{s_2}}, ab^{\bar{l}} \rangle$$

donde s_i y $0 \leq \bar{l} \leq n-1$ es tales tales que $p^{s_1}k \equiv_n 0$, $p^{s_2}l \equiv_n 0$ y $k + l\bar{l} \equiv_n 0$.

Es claro que $s_1 \leq p^j$, por lo que $G/M_{k,l}$ es abeliano. De esta forma, la ecuación para $\mathcal{X}_{M_{k,l}}$ es la siguiente:

Proposición 5.3.4 *$\mathcal{X}_{M_{k,l}}$ es isomorfa a la curva definida por la siguiente ecuación:*

$$y^{n/\epsilon} - x^{p^\kappa} - 1$$

Donde $\epsilon = mcd(s_k, u_1)$ y κ es el entero tal que $p^\kappa = mcd(s_2, u_2)$.

5.3.2. Caso $p = 2$, $j \neq 2$

Empezamos con las representaciones de dimensión 2, y vemos por lo anterior que las situaciones para $j = 1, 3$ se pueden estudiar de forma similar. En estos casos observamos que la matriz de a al elevarla al cuadrado queda

$$a^2 = Diag(w^{2k}, w^{2rk}) = Diag(w^{2k}, w^{-2k})$$

Mientras que la matriz de b al hacer lo mismo queda

$$b^2 = w^{2l}I$$

donde I es la matriz identidad de 2×2. Entonces el núcleo de estas representaciones depende sólo del orden de estas matrices:

Proposición 5.3.5 *Sea $N_{k,l,1} = Ker(\theta_{k,l,1})$. Entonces:*

$$N_{k,l,1} = \langle a^{2^{s_1}}, b^{2^{s_2}} \rangle$$

donde $2^{s_1} = n/mcd(k,n)$ *y* $2^{s_2} = n/mcd(l,n)$.

Es necesario notar que $b^{\frac{n}{2}}$ pertenece a dicho núcleo pues el orden de la matriz de b es mayor o igual a 2. Vemos que $G/N_{k,l,1}$ es isomorfo a :

$$\langle a, b | a^{2^{s_1}} = b^{2^{s_2}} = 1, b^{-1}ab = a^{-1}$$

Usando ideas similares a secciones anteriores, se tiene la ecuación para $\mathcal{X}_{N_{k,l,1}}$:

Proposición 5.3.6 *$\mathcal{X}_{k,l,1}$ es isomorfa a la curva definida por la ecuación:*

$$y^{2^{m-s_1}} = (x^{2^{m-s_2-1}} - 1)(x^{2^{m-s_2-1}} + 1)^{2^{m-s_2-1}}$$

Para las representaciones de dimensión 1, recordamos que son de la forma:

$$\xi_{k,l}(a^t b^u) = w^{kt+lu}$$

De la misma forma que el caso p impar, se puede afirmar lo siguiente sobre el núcleo de $\xi_{k,l}$

Proposición 5.3.7 *Sea $M_{k,l} = Ker(\xi_{k,l})$. Entonces:*

$$M_{k,l} = \langle a^{2^{m-u_1}}, b^{2^{m-u_2}}, a^{v_1}b^{v_2} \rangle$$

donde $mcd(k,n) = 2^{u_1}$. $mcd(l,n) = 2^{u_2}$ y v_i son enteros positivos con v_1 minimal tales que $n|(kv_1 + lv_2)$:

Notamos que u_1 puede ser $m-1$ o m. Si es m, entonces $M_{k,l}$ contiene a A, por lo tanto $\mathcal{X}_{M_{k,l}}$ es de género 0. Si u_1 es $m-1$, entonces $k = \frac{n}{2}$. Esto nos dice que $G/M_{k,l}$ es abeliano pues a tiene orden 2 en ese cociente. Además

$$a^{v_1}b^{v_2}a^{v_1}b^{v_2} = b^{2v_2}a^{(r+1)v_1}$$

con lo que $M_{k,l} = \{a^2, b^{2^\kappa}\}$, donde $2^\kappa = mcd(n, u_2, v_2)$.

Sobre el género de $\mathcal{X}_{M_{k,l}}$ podemos decir lo siguiente:

Proposición 5.3.8 *Si $k = n/2$ y $mcd(l,n) < \frac{n}{2}$, entonces $\mathcal{X}_{M_{k,l}}$ es isomorfa a la curva definida por la ecuación:*

$$y^{\frac{n}{2}} = x^{2^{m-\kappa}} - 1$$

Demostración: Aplicando:

$$-2^{\kappa+1}+1+\frac{3\cdot 2^{\kappa+1}-2^{\kappa}-2-|M_{k,l}\backslash G/C|}{2}$$

Observamos que $|M_{k,l}\backslash G/C| = [G : M_{k,l}C]$. Además, si $mcd(l,n) < \frac{n}{2}$, b^2 no está en $M_{k,l}$, luego, $C \cap H = \langle b^{2^\kappa}\rangle$ y $\kappa > 1$, lo que implica que $|M_{k,l}\backslash G/C| = 2$. Por lo tanto, el género de $\mathcal{X}_{k,l}$ es

$$-2^{\kappa+1}+1+\frac{3\cdot 2^{\kappa+1}-2^{\kappa}-2-2}{2}=\frac{2^{\kappa}-2}{2}$$

Si $mcd(l,n)=\frac{n}{2}$, entonces $b^2 \in M_{k,l}$. Entonces $M_{k,l}=\langle a^2, b^2\rangle$. Si $l=0$, entonces $M_{k,l}=\langle a^2, b\rangle$. Estos grupos contienen al centro de G y por la tabla 7, sabemos que $\mathcal{X}_Z(G)$ es de género 0. □

5.3.3. Caso $p=2$, $j=2$

Empezamos con las representaciones de dimensión 2. Observamos que como $r = n/2+1$, el cuadrado de la matriz de a es $w^{2k}I$ pero su orden es n. Como el cuadrado de la matriz de b es $w^{2l}I$, esto nos dice que:

Proposición 5.3.9

$$N_{k,l,1} = Ker(\theta_{k,l,1}) = \{b^{2^{m-u}}, a^t b^2\}$$

donde $2tk$ es congruente a $2l$ módulo n y $2^u = 2mcd(l,\frac{n}{2})$

Es claro que t tiene que ser par, de esta forma, $N_{k,l,1}$ es un subgrupo de $Z(G)$. Además se puede ver que $a^t b^2$ tiene orden $n/2$.

Ese género es cero cuando $\iota = \delta - u = m - u$. En caso contrario, interesa ver la ecuación de $X_{k,l,1} = X/N_{k,l,1}$. Previamente notamos que $G/N_{k,l,1}$ no es abeliano pues $a^{n/2}$ no está en $N_{k,l,1}$. Notando que la clase de a en ese cociente tiene orden n, vemos que $X_{k,l,1}$ es n-gonal con grupo de esfera cíclico de orden 2^{m-u}. Con esto, se puede establecer lo siguiente:

Proposición 5.3.10 *El género de $\mathcal{X}_{N_{k,l,v}}$ es*

$$\frac{2^{m-u+1}-2^{\iota}-2^{\delta-u}}{2}$$

donde ι es tal que $\frac{n}{2^\iota}$ es el orden de a^t y δ es tal que $2^\delta = mcd(n, l+k)$. Además, una ecuación para $\mathcal{X}_{N_{k,l,v}}$ es

$$y^n = (x^{2^{m-u-1}} - 1)(x^{2^{m-u-1}} + 1)^r$$

Demostración: Primero notamos que:

$$|N_{k,l,1}\backslash G/A| = [G : AN_{k,l,1}] = [G : \langle a, b^2\rangle] = 2$$
$$|N_{k,l,1}\backslash G/B| = [G : BN_{k,l,1}] = [G : \langle a^t, b\rangle] = 2^\iota$$

donde $\frac{n}{2^\iota} = |a^t|$. Para calcular $|N_{k,l,1}\backslash G/C|$ usaremos la fórmula del Teorema 5.0.3.

$$\begin{aligned}|N_{k,l,1}\backslash G/C| &= \frac{[N_G(C) : C]}{|N_{k,l,1}|}(|C \cap N_{k,l,v}| + |C \cap abN_{k,l,v}(ab)^{-1}|)\\ &= 2^{m-u}(|C \cap N_{k,l,v}| + |C \cap bN_{k,l,v}b^{-1}|)\\ &= 2^{m-u}(2|C \cap N_{k,l,v}|)\end{aligned}$$

Basta ver que potencia de ab cae en el núcleo de la representación. Como se vió antes se puede ver que

$$(ab)^2 = b^2 a^{\frac{n}{2}+2}$$

Por lo que la matriz de $(ab)^2$ queda como:

$$(ab)^2 = w^{2l+(\frac{n}{2}+2)k} I$$

De lo cual se puede establecer que el orden de esa matriz es n si y sólo si $l+k$ es impar. En general, si $2^\delta = mcd(n, l+k)$ se puede ver que el orden de la matriz de ab es $\frac{n}{2^\delta}$. Por lo tanto:

$$|N_{k,l,1}\backslash G/C| = 2^{\delta-u}$$

y de esta forma, el genero de $\mathcal{X}_{N_{k,l,1}}$ es:

$$\begin{aligned}&-2^{m\ u+1} + 1 + \frac{3\cdot 2^{m-u+1} - 2 - 2^\iota - 2^{\delta-u}}{2}\\ &= \frac{2^{m-u+1} - 2^\iota - 2^{\delta-u}}{2}\end{aligned}$$

El cálculo de la ecuación de $\mathcal{X}_{N_{k,l,1}}$ se hace de forma similar a otros cocientes vistos. □

A continuación, consideremos las representaciones de dimensión 1. Estas son de la forma

$$\xi_{k,l}(a^t b^u) = w^{kt+lu}$$

donde $0 \leq k, l \leq n-1$ con k par. De forma similar a los casos anteriores podemos establecer las siguientes proposiciones:

Proposición 5.3.11

$$M_{k,l} = \langle a^{2^{m-u_1}}, b^{2^{m-u_2}}, a^{v_1} b^{v_2} \rangle$$

donde $mcd(k,n) = 2^{u_1}$. $mcd(l,n) = 2^{u_2}$ *y* v_t *son enteros positivos con* v_1 *minimal tales que* $n|(kv_1 + lv_2)$*:*

Proposición 5.3.12 $\mathcal{X}_{M_{k,l}}$ *es isomorfa a la curva definida por la ecuación:*

$$y^{2^{m-u_1}} - x^{2^{m-u_2}} - 1$$

5.4. Jaccobianas y Variedades de Prym asociadas a Cocientes Intermedios

Ahora, en ciertos casos de subgrupos H de G, interesa ver como es $J(\mathcal{X}_H)$ y $P(\mathcal{X}|\mathcal{X}_H)$. Consideremos primero los subgrupos $A_k = \langle a^{p^k} \rangle$.

Por el teorema 2.9.3 y las proposiciones 5.3.1, 5.3.3, 5.3.5, 5.3.7 y 5.3.9, podemos establecer lo siguientes resultados respecto a las Jacobianas de cocientes intermedios de $\mathcal{X}$ obtenidos en capítulos anteriores:

Proposición 5.4.1

$$A_t \leq \bigcap_{m-v \leq t} N_{k,l,v} \bigcap_{u \leq t} M_{k,l}$$

donde u *es tal que* a^{p^u} *es un generador de* $M_{k,l}$*.*

Proposición 5.4.2

$$J(\mathcal{X}_{A_t}) \sim \prod_{m-v \leq t} D_{k,l,v}^{p^{m-j-v}} \times \prod_{u \leq t} D_{k,l}, \quad P(\mathcal{X}|\mathcal{X}_{A_j}) \sim \prod_{t > m-v} D_{k,l,v}^{p^{m-j-v}} \times \prod_{u > t} D_{k,l}$$

$$P(\mathcal{X}_{A_t}|\mathcal{X}_{A_{t+1}}) \sim \prod_{t=m-v} D_{k,l,v}^{p^{m-j-v}} \times \prod_{u=tt} D_{k,l}$$

Ahora, si consideramos ahora los términos de la serie central de G, tenemos que hacer la distinción si $j < m - j$ o no. En el primer caso, recordamos que si s es el mayor entero tal que $sj < m - j$, tenemos que para $1 \leq t \leq s+1$:

$$Z_t = \langle a^{p^{m-tj}}, b^{p^{m-tj}} \rangle$$

De esto podemos establecer lo siguiente:

Proposición 5.4.3

$$Z_t \leq \bigcap_{tj \leq \bar{v}} N_{k,l,v} \bigcap_{max(s_1,s_2) \leq m-tj} M_{k,l}$$

Proposición 5.4.4

$$J(\mathcal{X}_{Z_t}) \sim \prod_{tj \leq \bar{v}} D_{k,l,v}^{p^{m-j-v}} \times \prod_{max(s_1,s_2) \leq m-tj} D_{k,l}$$

$$P(\mathcal{X}|\mathcal{X}_{Z_j}) \sim \prod_{tj\, \bar{v}} D_{k,l,v}^{p^{m-j-v}} \times \prod_{max(s_1,s_2) > m-tj} D_{k,l}$$

$$P(\mathcal{X}_{Z_t}|\mathcal{X}_{Z_{t+1}}) \sim \prod_{tj \leq \bar{v} < (t+1)j} D_{k,l,v}^{p^{m-j-v}} \times \prod_{m-(t+1)j < max(s_1,s_2) \leq m-tj} D_{k,l}$$

Para los casos de $p = 2$, se puede hacer un ejercicio similar en el caso de los subgrupos de A. Supongamos que $j \neq 2$. En ese caso, es evidente que A_t está contenido en todos los $M_{k,l}$. Esto nos dice que::

Proposición 5.4.5 *Si $p = 2$ y $j \neq 2$, entonces*

$$A_t \leq \bigcap_{v \leq t} N_{k,l,1} \bigcap_{k,l} M_{k,l}$$

donde $2^v = mcd(k, n)$

De esto se deduce que:

Proposición 5.4.6 *Si $p = 2$ y $j \neq 2$, entonces*

$$J(\mathcal{X}_{A_t}) \sim \prod_{m-v \leq t,l} D_{k,l,1}^{2/sch(\theta_{k,l,1})} \times \prod_{k,l} D_{k,l}, \quad P(\mathcal{X}|\mathcal{X}_{A_j}) \sim \prod_{t > m-v,l} D_{k,l,1}^{2/sch(\theta_{k,l,1})}$$

$$P(\mathcal{X}_{A_t}|\mathcal{X}_{A_{t+1}}) \sim \prod_{t=m-v,l} D_{k,l,1}^{2/sch(\theta_{k,l,1})} \times \prod_{u=t} D_{k,l}$$

Si $p=j=2$, tenemos lo siguiente:

Proposición 5.4.7 *Si $p=2$ y $j=2$, entonces*

$$A_t \leq \bigcap_{v\leq t,l} M_{k,l}$$

donde $2^v = mcd(k,n)$

De esto deducimos:

Proposición 5.4.8 *Si $p=2$ y $j=2$, entonces*

$$J(\mathcal{X}_{A_t}) \sim \prod_{v\leq t} D_{k,l}, \quad P(\mathcal{X}|\mathcal{X}_{A_j}) \sim \prod_{k,l} D_{k,l,1}^2 \times \prod_{v>t,l} D_{k,l}, \quad P(X_{A_t}|X_{A_{t+1}}) \sim \prod_{v=t,l} D_{k,l}$$

En general, para B y sus subgrupos se puede hacer el mismo análisis, el cual se puede resumir en las siguientes proposiciones:

Proposición 5.4.9 *Si p es impar, entonces:*

$$B_t \leq \begin{cases} \bigcap_{m-u\leq t} N_{k,l,v} \bigcap_{s_2\leq t} M_{k,l} & si \quad p>2 \\ B_t \leq \bigcap_{k,s_2\leq t} N_{k,l,1} \bigcap_{k,s_2\leq t} M_{k,l} & si \quad p=2, j\neq 2 \\ B_t \leq \bigcap_{k,m-u\leq t} N_{k,l,1} \bigcap_{k,m-u_2\leq t} M_{k,l}5 & si \quad p=2, j=2 \end{cases}$$

Con esto tenemos lo siguiente:

Proposición 5.4.10 *Si p es impar, entonces:*

$$J(\mathcal{X}_{B_t}) \sim \prod_{k,m-u\leq t} D_{k,l,v}^{p^{m-j-v}} \times \prod_{k,s_2\leq t} D_{k,l}, \quad P(\mathcal{X}|\mathcal{X}_{B_j}) \sim \prod_{k,m-u>t} D_{k,l,1}^{p^{m-j-v}} \times \prod_{k,s_2\leq t} D_{k,l}$$

Si $p=2$ y $j\neq 2$, entonces

$$J(\mathcal{X}_{B_t}) \sim \prod_{k,s_2\leq t} D_{k,l,v}^{p^{m-j-v}} \times \prod_{k,s_2\leq t} D_{k,l}, \quad P(\mathcal{X}|\mathcal{X}_{B_j}) \sim \prod_{k,m-u>t} D_{k,l,1}^{2/sch(\theta_{k,l,1})} \times \prod_{k,s_2>t} D_{k,l}$$

Si $p=2$ y $j=2$, entonces

$$J(\mathcal{X}_{B_t}) \sim \prod_{k,s_2\leq t} D_{k,l,v}^2 \times \prod_{k,s_2\leq t} D_{k,l}, \quad P(\mathcal{X}|\mathcal{X}_{B_j}) \sim \prod_{k,m-u\leq t} D_{k,l,1}^2 \times \prod_{k,m-u_2\leq t} D_{k,l}$$

Apéndice A

Grupos Cíclicos Finitos y Enteros módulo n

En este capítulo presentaremos propiedades de grupos cíclicos y del anillo de enteros módulo n que serán de utilidad para el trabajo de tesis. Nos enfocaremos en el caso en que n es una potencia de un primo.

Un hecho evidente es que todo grupo cíclico finito es isomorfo a $\mathbb{Z}/n\mathbb{Z}$ donde n es el orden de dicho grupo. En adelante usaremos la notación:

$$a \equiv_n b$$

para decir que a es congruente a b módulo n.

En el capítulo anterior mencionamos que si G es cíclico de orden primo, $Aut(G)$ es cíclico. Primero, notamos el siguiente lema cuya demostración se deja al lector:

Lema A.0.1 *Si G es un grupo cíclico finito de orden n, entonces*

$$Aut(G) \cong (\mathbb{Z}_n)^*$$

El siguiente teorema nos dice cuando $Aut(G)$ es cíclico:

Teorema A.0.1 *Sea $n > 1$ un entero positivo. Entonces $(\mathbb{Z}_n)^*$ es cíclico si y sólo si n es 2, 4, una potencia de primo impar o el doble de una potencia de primo impar.*

Demostración: puede consultarse en [25], págs. 92-95.

Esto nos dice que $Aut(G)$ es cíclico en los casos antes indicados. Supongamos que $n = p^m$ donde p es un primo impar y $m \geq 3$.

Nos fijaremos en la estructura de $\mathbb{Z}_n$ como anillo. Sea $1 \leq j \leq m-1$ y consideremos $r = 1 + p^j$. Es claro que $r \in \mathbb{Z}_n^*$. Sea U_j el subgrupo de $\mathbb{Z}_n^*$ generado por r.

Lema A.0.2 *El orden de r en $(\mathbb{Z}_n)^*$ es p^{m-j}*

Demostración: Se puede hacer usando teorema del binomio y propiedades de coeficientes binomiales. Se deja al lector.

Con esto, consideremos lo siguiente:

Observación A.0.1 *sea H el subgrupo de $(\mathbb{Z}_n)^*$ formado por los elementos de la forma $1 + kp^j$. Es un subgrupo, pues:*

$$(1 + kp^j)(1 + lp^j) = (1 + (k + l + klp^j)p^j)$$

y el inverso de $(1+kp^j)$ es $(1+kp^j)^{n-1}$ que por la igualdad anterior es un elemento de H. Hay exactamente p^{m-j} elementos de este subgrupo. Pero sabemos que $\langle r \rangle$ es un subgrupo de orden p^{m-j} por lo que $H = \langle r \rangle$.

Con esto, podemos obtener el siguiente lema:

Lema A.0.3

$$\sum_{k=1}^{p^{m-j}} r^k = p^{m-j} + \frac{n(p^{m-j}+1)}{2}$$

Demostración: La suma del lado izquierdo es igual, por la observación anterior, a:

$$\sum_{k=0}^{p^{m-j}-1} (1 + kp^j) = \sum_{k=0}^{p^{m-j}-1} 1 + p^j \sum_{k=0}^{p^{m-j}-1} k = p^{m-j} + p^j \frac{(p^{m-j}-1)p^{m-j}}{2}$$

Con lo que se llega a demostrar el lema. □

En lo que sigue el número

$$p^{m-j} + \frac{n(p^{m-j}+1)}{2}$$

se denotará por $p_{m,j}$.

Ahora, supongamos que n es una potencia de 2, digamos $n = 2^m$ con $m \geq 3$. En este caso, $(\mathbb{Z}_n)^*$ no es cíclico, pero se tiene lo siguiente:

Lema A.0.4 *Sean ν_1, ν_2 y ν_3 los siguientes elementos de $(\mathbb{Z}/n\mathbb{Z})^*$:*

$$\nu_1 = \frac{n}{2} - 1$$
$$\nu_2 - \frac{n}{2} + 1$$
$$\nu_3 = n - 1$$

Entonces el orden de estos elementos módulo n es 2 y el subgrupo generado por estos tres elementos es isomorfo al grupo de Klein

Demostración: Obvia.

Ahora, estudiaremos acciones de $(\mathbb{Z}_n)^*$ en sí mismo, considerando su estructura de grupo, con el objeto de definir la estructura de los grupos que nos interesan. Para ello, recordamos la siguiente proposición.

Proposición A.0.11 *Si $n = q^m$ es potencia de un primo q, entonces*

$$|\mathbb{Z}/n\mathbb{Z}^*| = (q-1)q^{m-1}$$

Demostración: Ver [25], pág. 69.

De esto, se establece que en el caso de primo impar, si $\mathbb{Z}_n = \langle 1 \rangle$ actúa en sí mismo de forma no trivial, entonces el automorfismo de $\mathbb{Z}_n$ determinado por la acción de 1 debe tener orden una potencia de p, siempre que la acción no sea trivial. Vamos a ver que el producto semidirecto $\mathbb{Z}_n \rtimes \mathbb{Z}_n$ determinado por la acción dada por elementos del mismo orden en $\mathbb{Z}_n$ es esencialmente la misma, por ser $\mathbb{Z}_n$ y $\mathbb{Z}_n^*$ cíclicos.

En el caso $p = 2$, la acción es de todas formas debe ser una potencia de 2, pero nos concentraremos en las acciones dadas por los ν_1. De todas formas vamos a ver que las acciones que generan son diferentes

Para ver esto, primero supongamos que n es potencia de primo impar. Consideremos $\phi : \mathbb{Z}_n \to \mathbb{Z}_n^*$ y denotemos por $\phi_k = \phi(k)$. Veremos ahora que en nuestro caso, si k y l son tales que ϕ_k y ϕ_l son elementos del mismo orden u en $Aut(\mathbb{Z}_n)$ entonces los productos semidirectos $\mathbb{Z}_n$ determinados respectivamente por esos automorfismos son isomorfos. Esto se ve porque existen $\bar{k}$ y $\bar{l}$ en $\mathbb{Z}_n^*$ tales que:

$$\phi_k(x) = \bar{k}x, \phi_l(x) = \bar{l}x$$

Sea $t \in \mathbb{Z}_n^*$ tal que $t\bar{k} = \bar{l}$. Entonces el orden de t es el mismo que $\bar{k}$ y $\bar{l}$ y además:

$$\phi_l(x) = \bar{l}x = t\bar{k}x = t\phi_k(x)$$

Sea t^{-1} el inverso de t módulo n. Definimos:

$$h : \mathbb{Z}_n \rtimes_{\phi_k} \mathbb{Z}_n \to \mathbb{Z}_n \rtimes_{\phi_l} \mathbb{Z}_n$$
$$h(x,y) = (tx, t^{-1}y)$$

Claramente es biyectiva. Es un homomorfismo de grupos pues:

$$h(x,y) + h(z,w) = (tx, t^{-1}y) + (tz, t^{1}w) = (tx + \phi_l(t^{-1}y)tz, t^{-1}(y+w))$$
$$= (t(x + \bar{l}t^{-1}yz), t^{-1}(y+w)) = (t(x + \bar{k}yz), t^{-1}(y+w)) = h(x + \phi_k(y)z, y+w)$$
$$= h((x,y) + (z,w))$$

Por lo tanto, $\mathbb{Z}_n \rtimes_{\phi_k} \mathbb{Z}_n \cong \mathbb{Z}_n \rtimes_{\phi_l} \mathbb{Z}_n$. En particular, todo producto semidirecto de esa forma esta determindado de forma única salvo isomorfismo por la acción dada por los r_j.

En el caso n potencia de 2, observamos que las acciones definidas por ν_j son diferentes una de otra pues el grupo que forman es isomorfo al grupo de Klein, lo que hace que una acción no se pueda describir en terminos de otra de las dos ponderando por un impar que no este en ese grupo. De esta forma, los productos semidirectos que determinan no son isomorfos a pares.

Otra propiedad que cumplen ν_j es la siguiente, la cual se deja al lector:

Lema A.0.5 *Si k es par, entonces*

$$\sum_{l=1}^{k} \nu_j^l = \frac{k(\nu_j + 1)}{2}$$

Si k es impar, entonces

$$\sum_{l=1}^{k} \nu_j^l = \frac{(k+1)(\nu_j + 1)}{2} - 1$$

Bibliografía

[1] G. Bartolini, A.F. Costa, y M. Izquierdo. *On Automorphisms Groups of Cyclic p-gonal Riemann Surfaces. Journal of Symbolic Computation*, 57:61–69, 2013.

[2] S.A. Broughton. *Classifying Finite Group Actions on Surfaces of Low Genus. Journal of Pure and Applied Algebra*, 69:233–270, 1991.

[3] E. Bujalance, F.J. Cirre, y M. Conder. *On Extendability of Group Actions on Compact Riemann Surfaces. Transactions of the A.M.S.*, 355:1537–1557, 2002.

[4] E. Bujalance, J. Gamboa, y G. Gromadzki. *The Full Automorphism Groups of Hyperelliptic Riemann Surfaces. Manuscripta Math.*, 79:267–282, 1993.

[5] A. Carocca y R. Rodríguez. *Jacobians with Group Actions and Rational Idempotents. J. Algebra*, 306:322–343, 2006.

[6] A.D. Coste, G.A. Jones, M. Streit, y J. Wolfart. *Generalised Fermat H ypermaps and Galois Orbits . Glasgow Math. J.*, 51:289–299, 2009.

[7] C.W. Curtis y I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* John Wiley and Sons Inc., 1962.

[8] J. Dodziuk y L. Keen. *Lipa's Legacy: Proceedings of the Bers Colloquium.* A.M.S., 1995.

[9] W. J. Harvey. *On Branch Loci in Teichmüller Space. Trans. Amer. Math. Soc.*, 15:387–399, 1971.

[10] R. Hidalgo. *Cuerpos de Móduli y Cuerpos de Definición.* U.T.F.S.M, 2000.

[11] R. Hidalgo y S. Reyes. *Weil's Galois Descent Theorem: a Computational Point of View. arXiv*, 1203.6294:1–13, 2014.

[12] R. Hidalgo y R. Rodríguez. *Introducción a las Variedades Abelianas y Grupos Kleinianos.* U.T.F.S.M., 2005.

[13] J. Hillman. *Singularities of Plane Algebraic Curves. Expositiones Mathematicae,* 23:233–254, 2005.

[14] Y. Iida. *A Note on the Schur Index of an Irreducible Character of a 2-Group. Soochow Journal of Mathematics,* 24:163–165, 1998.

[15] S. Kallel y D. Sjerve. *On the Group of Automorphisms of Cyclic Covers of the Riemann Sphere. arXiv:math/0310053v1,* págs. 1–23, 2003.

[16] S. Kallel, D. Sjerve, y Y. Song. *On Cyclic Covers of the Riemann Sphere and a Related Class of Curves. Advances in Topological Quantum Field Theory,* 179:327–353, 2004.

[17] I. Kuribayashi & A. Kuribayashi. *On Automorphism Groups of Compact Surfaces of Genus 4. Proc. Japan Acad.,* 62:65–68, 1986.

[18] R. Miranda. *Algebraic Curves and Riemann Surfaces.* A.M.S., 1995.

[19] J. Munkres. *Topology (Second Edition).* Pearson, 2000.

[20] J. Pinto. *Ecuaciones para Superficies de Riemann correspondientes a cubrimientos cíclicos primos. Tesis de Magíster.* Universidad de Chile, 2012.

[21] A. Rojas. *Group Actions on Jacobian Varieties. Rev. Mat. Iberoamericana,* 23:397–420, 2007.

[22] P. Roquette. *Archiv. der Math,* págs. 241–250.

[23] J-P. Serre. *Linear Representations of Finite Groups.* Springer-Verlag, 1977.

[24] I. Shafarevich. *Basic Algebraic Geometry.* Springer-Verlag, 1977.

[25] D. Shanks. *Solved and Unsolved Problems in Number Theory.* Chelsea Publishing Company, 1978.

[26] D. Singerman. *Subgroups of Fuchsian Groups and Finite Permutation Groups. Bull. London Math. Soc.,* 2:319–323, 1970.

[27] D. Singerman. *Finitely Maximal Fuchsian Groups. J. London Math. Soc.,* 6:29–38, 1972.

[28] P. Tzermias. *The Group of Automorphisms of the Fermat Curve. Journal of Number Theory,* 53:173–178, 1995.

[29] A. Wootton. *Defining Equations for Cyclic Prime Covers of the Riemann Sphere. Israel Journal of Mathematics,* 157:103–122, 2007.