UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

ARITMÉTICA DE SUPERFICIES ELÍPTICAS Y APLICACIONES

Juan Pablo De Rasis

Director: Matilde Lalín

Jurado: Fernando Cukierman y Martín Mereb

14 de julio de 2020

Agradecimientos

Toda historia tiene un principio. Mi historia con las matemáticas no es la excepción a esta regla, y tiene un inicio muy bien definido. Con mucha nostalgia recuerdo aquellas clases de matemática de 2011 en el Departamento de Aplicación Docente de la Universidad Nacional de Cuyo; colegio secundario en el que cursaba el noveno grado durante ese año. ¿Quién diría que hoy estaría iniciando la sección de agradecimientos de mi tesis de licenciatura recordando a la profesora Nancy Silva, quien fuera la docente de matemática en aquel singular año de mi vida? Es con muchísima alegría y gratitud con la que encabezo mis agradecimientos con su nombre. Sus clases magistrales fueron un punto y aparte en mi vida: fue la primera persona que supo transmitirme la belleza intrínseca que subyace a las matemáticas. Fue la primera persona que supo hacerme admirar el arte de hacer matemática, y entender que mi vida no podía dedicarse a otra cosa. Aquello marcó el inicio de mi amor infinito hacia esta hermosa disciplina, y no puedo más que hacer mías las palabras que la icónica cantante y letrista argentina Jovita Díaz imprimió en una bella pieza musical cuando cantó: *Por eso, gracias; y solamente gracias, hoy he venido a decir... a mi maestra, la más querida, la que por siempre será en mi vida mi señorita.*

Otra persona que merece el más profundo de mis agradecimientos es, no podía ser de otra manera, Matilde Lalín. Lo que ha hecho por mí esta excelente matemática constituye una magnanimidad de proporciones bíblicas que es imposible exagerar en palabras. No solamente ha sido una excelente directora de tesis, sino que, desde un principio, depositó su plena confianza en mí y accedió a tomar el enorme riesgo de dirigir una tesis de licenciatura a distancia, a una persona que no conocía, de forma totalmente *ad honorem*, y sin jamás haberme pedido algo a cambio. Un acto de altruismo académico digno de las personas más honestamente apasionadas por el conocimiento matemático. Conocer mentes matemáticas brillantes es siempre un privilegio y una experiencia que deja excelentes frutos si se la sabe aprovechar; pero que una de estas personas brillantes muestre, además, una impresionante calidad humana como la de Matilde Lalín, hace que quien tuvo la fortuna de conocerla entienda que la vida le ha presentado una generosísima oportunidad. Matilde me ayudó de forma desinteresada e incondicional con la tesis, con las aplicaciones a las universidades de Estados Unidos y Canadá, con consejos y sugerencias, con toda la información que necesitara. Acciones como haber estado siempre atenta a mis dudas e inquietudes, haberse tomado el trabajo de corregir el borrador de mi *statement of purpose* estando accidentada de la muñeca, haberme escrito una carta de recomendación y haber permanecido siempre atenta para enviarla a tiempo, mostrarse siempre receptiva y con una voluntad intachable y aconsejarme siempre en todos los aspectos de mi vida académica, me hacen tener la firme convicción de que no podría haber tenido un mejor director de tesis. Por su brillantez como matemática, y por su impecable calidad humana, a ella le va un muy profundo agradecimiento.

Y si le di las gracias a Matilde, no puedo olvidar bajo ningún concepto el papel del profesor Daniel Perrucci. No solamente fue uno de los docentes que formó parte importante en mi formación como matemático al haber sido el docente de Cálculo Avanzado, sino también fue una persona que demostró una gigantesca generosidad al haber confiado y creído en mí, y haberme puesto en contacto con la que sería eventualmente mi actual directora de tesis. La actitud desinteresada de haber querido ayudarme a tomar mejores decisiones para mi vida, el haber accedido a ayudarme con los trámites burocráticos de la tesis que debía realizar a causa de tener a Matilde lejos, y el haber accedido a escribirme una carta de recomendación para las universidades a las que apliqué, lo ponen a él en este destacado lugar de mis agradecimientos. Cuánto anhelaría poder retribuirle algo más que estas modestas palabras.

Y para completar el grupo de quienes me escribieron cartas de recomendación, es menester mencionar y agradecer infinitamente a Fernando Cukierman. Un docente que no solo contribuyó a mi formación habiendo sido el docente de Geometría Proyectiva, sino también habiendo accedido, siempre que se lo solicité, a hablar conmigo y aconsejarme sobre mi futuro. En Cukierman encontré a una persona maravillosa, siempre dispuesta a escuchar atentamente mis situaciones y aconsejarme en consecuencia, y siempre con la mejor voluntad y accesibilidad. Una persona que accedió gentilmente a escribir cartas de recomendación para mí, a sugerirme cómo elegir universidad; en definitiva, una persona que supo orientarme cuando, a veces, me sentía muy perdido. Por eso, por haber accedido también a ser jurado de esta tesis y por tanto más: muchísimas gracias, profesor Cukierman.

Y es también meritorio de mis agradecimiento el profesor Martín Mereb. No solamente fue un excelente docente en las clases de Álgebra I que cursaba cuando me escapaba del CBC, y también en las clases de Álgebra Lineal. Él ha sido también una persona que, siempre con la mejor voluntad, buena disposición y simpatía, me aconsejó desinteresadamente cada vez que solicité su ayuda. Ya sea en materia de consejos o acciones concretas, siempre estuvo ahí para ayudar y apoyar, y no sé cómo agradecérselo. Como si todo esto fuera poco, accedió con mucho entusiasmo a ser jurado de esta tesis y sus contribuciones como tal fueron excelentes y muy valiosas. A él van dedicadas estas sinceras palabras: ¡muchísimas gracias!

Durante la excelente formación matemática que el Departamento de Matemática de la Universidad de Buenos Aires me ofreció, muchos fueron los excelentes profesores que tomaron su papel en ello, y por eso merecen mi más profundo agradecimiento, pues son tan parte de esto como yo mismo. Gracias: Guillermo Cortiñas, Daniel Kohen, Roberto Cignoli, Mariano Suárez Álvarez, Gabriel Larotonda, Diego Rial, Pablo Amster, Pablo Ferrari, Jorge Devoto, Julián Fernández Bónder, Andrea Solotar, Daniel Galicer, Gabriel Minian, Claudia Lederman, Miguel Walsh, Román Sasyk, Juan Manuel Menconi, Marcelo Paredes, Pablo de Nápoli, Emanuel Rodríguez Cirone, Pedro Tamaroff, Ignacio Ojea, Ariel Salort, Mauro Rodríguez Cartabia, Fernando Martín, Santiago Vega. A todos ellos, mi más sincero agradecimieto. Agradezco también a Nolwenn Gautier, Mercedes Rego Perlas, Cecilia Bonavetti, Maria Fe Bellido y Pablo Fresina, porque haber aprendido inglés con ellos fue no solamente muy fructífero, sino también fascinante.

Gracias también a Nicolás Sirolli por haberse hecho siempre un tiempo para mí a la hora de aconsejarme sobre mi futuro o ayudarme con cuestiones matemáticas. La calidad humana que encontré en él ha sido inconmensurable, y por eso quiero reconocerle esa excelente virtud en estas palabras de agradecimiento por todo lo que hizo por mí.

No puedo dejar de mencionar a una persona que marcó un punto y aparte en mi

vida, al haber sellado definitivamente mi decisión de estudiar matemática. Durante aquel bellísimo campamento científico *Expedición Ciencia* al cual tuve el honor de asistir durante el verano de 2014, conocí a una persona que se ha impreso en mi memoria para siempre: el coordinador Gustavo Vasen. Y se imprimió en mi memoria por haber sido la persona que, tras hablar conmigo respecto de las matemáticas y las formas de interpretarla, me hizo decidirme definitivamente por dedicarme a esta hermosa disciplina. Nunca terminaré de enterarme de si él se siente orgulloso o culpable por ello, pero lo cierto es que, por mi parte, yo guardo una muy profunda gratitud hacia él.

Y si hubo una persona que selló definitivamente mi decisión de estudiar matemática, hubo también una persona, a la que conocí por aquellos milagros del destino, que potenció todos mis deseos y entusiasmos por la vida de matemático y me hizo tener tal convicción por ello que terminé tomando la radical decisión de formarme en la Universidad de Buenos Aires, con todo lo que implicó tener que separarme de mi tierra natal, Mendoza, y de todos mis amigos y mi familia, con tal de perseguir un sueño. Esta persona, que conocí de casualidad en internet, es nada más ni nada menos que Agustín Damonte, a quien yo siempre me referí como *mi sensei*. Durante años nuestra relación fue puramente virtual, pero ello no impidió las charlas de horas y horas sobre la matemática y la vida del matemático. Tampoco impidió que él me "adoptara" y ocupara el papel de exolímpico que ayuda a un olímpico a prepararse para las Olimpíadas de Matemática. Ha sido tan trascendental la presencia de Agustín en mi vida, que cualquier método que emplee para decirle GRACIAS no hará justicia con él.

Recuerdo cuando, estando en Mendoza y habiendo tomado la decisión de irme a vivir a Buenos Aires para estudiar matemática, el miedo me carcomía. Dudas, inquietudes, inseguridades, todo tipo de sensaciones inherentes a un cambio tan profundo. Fue por eso que haber podido hablar con Miguel Ottina, un matemático que había estudiado en la UBA, fue una de los grandes regalos que me dio la vida. Le agradezco infinitamente a Miguel Ottina por haberle abierto las puertas de su oficina a un desconocido al que solamente había visto en sus clases *ad honorem* para preparar gente para la OMA. Ese desconocido hoy lo recuerda con infinita gratitud en esta tesis como la persona que, con la mejor de las voluntades, accedió a hablar conmigo durante bastante tiempo, respondiendo mis dudas y otorgándome excelentes sugerencias para la vida que había elegido.

Pero mi formación como matemático estuvo atravesada no solamente por personas que, desde su profesionalidad, me aportaron en materia de conocimientos académicos y sugerencias en el mismo plano. En la Universidad de Buenos Aires conocí personas, hice amigos y tuve bellísimas experiencias. Mis amigos son ese tesoro que he guardado en mi memoria para siempre, y hoy quiero manifestarles a todos mi agradecimiento por haber contribuido a hacer este proceso mucho más feliz de lo que hubiera sido sin ellos. Gracias: Bruno Staffa, Alejo Salvatore, Darío Aza, Mariano Chehebar, Pablo Perrella, Martín Blufstein, Santiago Ramírez, Dante Grevino, Ian Manuel Fleschler, Matías Saucedo, Guillermo Mosse, Ignacio Darago, Carlos Di Fiore, Ramiro Lepka, Carlos Giudice, Julián Garbulsky, Sofía Gurruchaga, Martín Vacas Vignolo, Jaqueline Girabel, Juan Cruz López, Melanie Sclar, Sebastián Castaño, Daniel Seidler, Fernando del Río, Facundo Rost, Cristian Kubrak, Ezequiel Cribioli, Mathias Castro Alagón, Ariel Zylber, Sebastián Prillo, Gabriel Sac.

Muchísimas gracias a mis amigos Bryan Malpartida, Romina D'Alessandro, Facundo Pugliese, Gonzalo Andreu, Nicolás Ansaldi. Porque nunca creí que podría reírme tanto y con tanta frecuencia hasta que una de las más maravillosas casualidades de mi vida me llevó

a conocer este bellísimo grupo. Un grupo que me integró, me aceptó y apreció, y siempre fueron amigos incondicionales para mí. Nunca escatimaron en hacerme sentir bienvenido y querido, y no podría plasmar en palabras cuánto les agradezco por cómo han sido conmigo. Nunca voy a olvidar los tantísimos ataques de risa que viví gracias a ellos, ni tampoco sus joyas anti-matemáticas para hacer enojar a mi TOC matemático interior. Gracias a ellos comprendí que «los reales son numerables; en particular, finitos», porque «los reales son los racionales, ¿o acaso vos escribís todas las cifras en la hoja de papel?». Descubrí también que «un buen físico nunca demuestra sus teoremas», que π es algebraico «porque $\pi^2 = 10$», que «el cardinal de los números reales depende de la temperatura» porque «en mecánica clásica la energía de un sistema es continua, pero cuando la temperatura tiende a cero el sistema se discretiza», así como también descubrí varias ecuaciones diferenciales resueltas por medio del tachado de diferenciales en mis cuadernos a la hora de ponerme a estudiar, puestas ahí por Dios sabe quién. Gracias por todo, chicos.

Y creo que nunca voy a encontrar palabras para agradecerle a Alison Rayssa Delgadillo, quien ha sido mi mayor cable a tierra en todo este proceso, además de haber sido la primera amistad que hice tras llegar a Buenos Aires. Una persona increíble, un ser humano maravilloso, una mujer fascinante, con la cual he sabido vivir experiencias que no voy a olvidar nunca. La persona que ha seguido muy de cerca todo este proceso, que siempre estuvo dispuesta a escucharme y acompañarme, que jamás claudicó en su apoyo incondicional hacia mí y mis proyectos, y no podría estar más agradecido. Una fidelidad de acero que pocas veces he visto en mi vida, de parte de alguien a quien conocí de milagrosa casualidad. Brindo internamente cada día por esa hermosa casualidad que la trajo a mi vida.

Un millón de gracias a Diego Rodrigo Cáceres, por TODO lo que hizo por mí. Es imposible exagerar con palabras la magnitud del valor que ha tenido Diego en mi vida, por todo el trabajo y dedicación que puso conmigo, por la brillante labor que realizó con altura y profesionalidad para ayudarme cuando más lo necesité. Hay tantas cosas del presente que no hubieran sido posibles de no ser por él, que nada de lo que diga aquí hará justicia con todo lo que él me brindó. Gracias, Diego.

Tengo que ponerme de pie a la hora de agradecer a Claudia Farías y Gustavo Villena, por haberme ayudado a descubrir, redescubrir y disfrutar la segunda gran pasión de mi vida: el canto lírico. Por más de que pasen los años, siempre recordaré que mi primer título universitario lo obtuve tras duros años de intenso estudio en los cuales siempre pude contar con mi profesora particular de canto y mi profesor del Coro de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires, para bajar a tierra en medio de tanta abstracción matemática. Ya sea cantando en el estudio de Claudia durante sus clases, o en las magistrales clases corales de Gustavo, cada nota musical que salió de mi voz, y que estos dos excelentes maestros me ayudaron a perfeccionar, me regaló momentos inolvidables disfrutando de aquello que tanto amo. Gracias, Claudia. Gracias, Gustavo. Ustedes son tan parte de esto como yo.

Y si mencioné a Gustavo Villena, profesor del coro, no puedo olvidarme de mis compañeros de coro, sin los cuales nada de lo que allí viví habría sido posible. Gracias Vera Blumenkranc, Ailen Sac Himelfarb, Sebastián Gorosito, Eduardo Luis Vallejo, Clara González Paladino, Silvestre Gonzalez, Claudio Fernando Echegaray (mi enemigo mortal), Brenda Denise Ochs, Andrea Cristina Juárez, Nadine Murillo, Micaela Soledad Romero, *Cosma Fulanita*, Fernanda Podesta, Federico Beraldo, Camila Ernst, Iván Gurovich. Gracias, por supuesto, a Martín Príncipe, por ser la mano derecha de Gustavo durante las enseñanzas de esta bella disciplina que es el canto coral.

Gracias al bellísimo grupo conformado por Mariana Cecilia Grohar, Carolina Ibáñez Padilla, Leandro Ariel Pezzente, Andrés Miguel Barbuto, Maximiliano Altamirano, Javier Alejandro Liñares, Juan Francisco Guerrero, Florencia Egert, Matías Oblak, Fiamma Liz Leites. Ellos saben por qué.

Pero las amistades no se terminan en la universidad. Y fuera de ella siempre pude contar con el apoyo y el afecto incondicional de amigos que estuvieron siempre para mí. Gracias: Leandro Pericoli, María Cristina Haug, Ignacio García Suárez, Ignacio Ruarte, Constanza Pizarro, Martín Bidegain (el "maistro"), Juliana Bocci, Yann Birnie-Scott, Kai Trombotto, Guadalupe Nahman, Facundo López Sevilla, Federico Brondo, Rocío Tarifeño, Enzo Duca, Milagros Aromataris.

No puedo olvidar a las personas junto a las cuales viví los bellísimos momentos de la Olimpíada Matemática Argentina. Muchísimas gracias a la profesora Diana Muñoz por haber estado siempre ahí con nosotros, y al grupo maravilloso con el que compartí estas experiencias: Nahuel Saavedra, Eduardo Pavéz, Martín Marone, Ivana Curci, Vanesa Curci, Facundo Reginato, Matías Chiarpotti, Lucciano Agostini, Sebastián Cuervo, Luciano Oro Alaria, Juan Manual Galdames, María Rocío Giménez Aranda, Guido Pérez Moro.

Pero existen dos personas que se merecen el agradecimiento mayor, por haber sido la causa primera de todo esto. Por su amor, por su apoyo, por haberme dado todo, por haberme enseñado a vivir la vida, por haberme dado la fortuna y el privilegio de heredar de ellos sus valores y enseñanzas. Por haber siempre confiado en mí, por haber creído en mí, por haber puesto todo de su parte para verme cumplir mis sueños. A mis padres, Pablo De Rasis y Viviana Marcela Paez, que me dieron el regalo de la vida al concebirme, y que desde ese preciso instante trabajaron juntos en un proyecto de amor que hoy muestra sus frutos y les dice, con muchísima sinceridad: muchas gracias, papá y mamá. Y, cómo no, imposible olvidarlo: a mi hermano menor Franco, con quien he compartido una vida entera, creciendo juntos y viviendo experiencias inolvidables.

Los familiares han sido un sostén emocional importantísimo a lo largo de todo este proceso. Gracias a mis tíos maternos Olindo Rodríguez y Celina Paez, y sus hijas, mis queridas primas, Estefania, Camila y Brunela. Gracias a mi tío paterno Juan De Rasis y sus hijas Florencia y Sofía, por su inclaudicable cariño. Gracias a mis dos abuelas, Nélida María Magdalena Parra y Yolanda Argilla, que en paz descanse. Gracias, por supuesto, a la familia que, desde España, nunca dejó de manifestar su amor y apoyo incondicional. Gracias a mis tíos Luis Paez y Claudia Morassutti, y sus hijos Irina, Iván y Mauro. Gracias a mis otros tíos Raúl Paez y Daniela Sosa, y a su hija Anabela. Entre primos y tíos he recibido una cantidad de amor infinita, que siempre me animó a seguir adelante. A la familia Milow-Argilla, por supuesto, también les va un muy afectivo agradecimiento. No tengo lazos familiares con la familia García-Christol, pero han sido como familiares para mí, y por eso quiero agradecerles también.

Quiero agradecer muy profundamente a Jorge Saganea, Néstor Saganea, Graciela Cacho y Viviana Allata, por jamás haber escatimado en ponerse a disposición de mí siempre y en todo lugar, como la familia de Buenos Aires con la que siempre pude contar para cualquier problema. Un cambio tan radical como irse a vivir a Buenos Aires siempre es apaciguado cuando uno dispone de familiares siempre dispuestos a estar presentes ante todo, y por eso creo que merecen este tan especial agradecimiento.

Con mi más plena sinceridad: muchas gracias a todos.

A mi maestra, la más querida,
la que por siempre será en mi vida mi señorita

Introducción

El objetivo de esta tesis es motivar desde problemas contemporáneos de la Teoría de Números el estudio de un objeto de la Geometría Algebraica, que es el que se lleva el título de este trabajo. Para introducir nuestros desarrollos, dividiremos la introducción en tres partes.

Contexto histórico y matemático

Célebre es el trabajo de Diofanto de Alejandría, matemático que vivió entre los siglos 3 y 4 antes de Cristo, y que debe su celebridad a *Arithmetica*, un tratado de 13 libros (del que solamente se conservan 6) en el que Diofanto colecciona diversos problemas y soluciones. Las *ecuaciones diofánticas* reciben su nombre precisamente en referencia a Diofanto.

El matemático Pierre de Fermat $(1601 - 1665)$ disponía de una copia de una edición del año 1621 del Libro 2 de *Arithmetica*, en cuya página 85 y junto al Problema 8, Fermat expuso una nota marginal afirmando haber encontrado una demostración de que, dado un número natural n mayor que 2, no es posible encontrar tres enteros positivos x, y, z tales que $x^n + y^n = z^n$. Lo más probable es que Fermat no haya demostrado dicho resultado, o que haya cometido un error al hacerlo, pues varios siglos y abundantes intentos fallidos debieron pasar hasta que, usando matemática muy contemporánea de la que Fermat no disponía, el problema fue finalmente resuelto. Este problema pasó a la historia como el *Último Teorema de Fermat*, aunque no adquirió legítimamente su estado de "teorema" hasta que finalmente fue demostrado a fines del siglo 20 por Andrew Wiles.

La teoría de curvas elípticas (entendidas, básicamente, como polinomios sobre un determinado cuerpo de escalares que satisfacen determinadas propiedades) se hizo mundialmente famosa, incluso fuera del círculo de matemáticos, durante el siglo 20 e incluso antes. Hoy sabemos que dicha teoría jugó un rol fundamental en la demostración del Último Teorema de Fermat que el matemático Andrew Wiles ofreció en 1995 a la comunidad matemática, aunque hacía décadas que había indicios de una posible demostración con base en dicha teoría. Es por esto que durante muchísimos años hubo importantísimos avances en materia de curvas elípticas, y hoy en día las mismas son utilizadas también en sistemas criptográficos para proteger información privada.

Se le atribuye a Fermat haber propuesto un acertijo en su época, tras haber observado una particularidad del número 26: el mismo está precedido de un cuadrado perfecto, y seguido de un cubo perfecto. En concreto, $5^2 = 25 < 26 < 27 = 3^3$. Es natural, pues, preguntarse cuáles son todos los números naturales que están precedidos de un cuadrado perfecto y seguidos de un cubo perfecto, lo cual induce naturalmente la ecuación diofántica $y^2 + 2 = x^3$, a resolverse en el conjunto de enteros. Esta ecuación es un caso particular de *curva elíptica*, aunque el método para resolver este problema en particular (con la

consecuencia de que las únicas soluciones son $(x, y) \in \{(3, 5), (3, -5)\}$) suele involucrar el hecho de que el anillo $\mathbb{Z}\left[\sqrt{-2}\right]$ es un dominio de factorización única.

Muchas de las célebres curvas elípticas que motivaron el desarrollo de una teoría general de las mismas provienen de problemas aritméticos motivados desde la geometría euclídea. El más famoso es, probablemente, el *problema del número congruente*, estudiado ya hacia el año 984 después de Cristo, que pregunta qué enteros positivos son el área de un triángulo rectángulo de lados racionales. A modo de ejemplo, 6 es el área del triángulo rectángulo cuyos catetos son 3 y 4, y su hipotenusa es 5. Decimos entonces que 6 es un número *congruente*. En el año 1225 Fibonacci estudió estos números, y encontró, por ejemplo, que el número 5 es también congruente, pues es el área de un triángulo rectángulo de lados $\frac{3}{2}$, $\frac{20}{3}$, $\frac{41}{6}$. Posteriormente, Fermat estudió el problema y demostró que 1, 2 y 3 no son congruentes.

La teoría de curvas elípticas permite demostrar, por medio de un adecuado cambio de variables en la formulación clásica del problema del número congruente, que un número natural n libre de cuadrados es congruente si y solo si la curva elíptica $y^2 = x^3 - n^2x$ admite una solución no trivial; es decir, distinta de $(-n, 0)$, $(0, 0)$ y $(n, 0)$.

Por medio de la clásica compactificación proyectiva, se le agrega exactamente una solución adicional a las curvas elípticas (conocida como la solución del infinito y notada clásicamente ∞) que permite darle a las soluciones de dicha curva una estructura natural de grupo abeliano en la que ∞ es el elemento neutro. Más aún, el célebre **Teorema de Mordell** dice que, cuando trabajamos sobre curvas elípticas sobre $\mathbb{Q}$, dicho grupo es finitamente generado. Se puede demostrar que la curva elíptica $y^2+2 = x^3$ que mencionamos al principio, por ejemplo, es un grupo abeliano libre de rango 1 generado por $(3, 5)$.

En cuanto a la curva elíptica $y^2 = x^3 - n^2x$ donde $n \in \mathbb{N}$ es libre de cuadrados, es sabido que el grupo de torsión es precisamente el conjunto de soluciones triviales, con lo cual el problema de determinar si n es congruente o no equivale a saber si la curva elíptica $y^2 = x^3 - n^2x$ admite o no un punto sin torsión. Es sabido, por ejemplo, que si $p \in \mathbb{N}$ es primo y $p \equiv 3 \pmod 8$, entonces $y^2 = x^3 - p^2x$ tiene rango 0, de donde p no es congruente.

El problema del número congruente es, quizá, el más clásico de los problemas abordados desde la teoría de curvas elípticas y motivados desde la geometría euclídea. Sin embargo, en esta tesis nos enfocaremos principalmente en otro tipo de problemas motivados desde la geometría euclídea, todos pertenecientes a una familia de resultados que ha dado mucho de qué hablar inclusive hasta nuestros días. De hecho, el inicio de los mismos es extremadamente reciente.

En el año 1995, el matemático Richard K. Guy resolvió un problema planteado por Bill Sans, que se preguntaba si era posible hallar un triángulo y un rectángulo, ambos de lados enteros, con la misma área y el mismo perímetro. Utilizando la teoría de curvas elípticas pudo demostrar que no existen tales figuras y que, en cambio, si se le permitía al triángulo ser isósceles, entonces había infinitas soluciones. Aquí y en el resto de ejemplos que expondremos, cada vez que decimos "infinitas soluciones" no distinguimos soluciones por semejanza geométrica, puesto que, de lo contrario, de una solución particular podríamos trivialmente obtener infinitas soluciones adicionales mediante un reescalamiento por factores enteros.

El trabajo de Guy fue el disparador de un sinfín de variantes del mismo problema que han dado lugar a una muy rica diversidad de resultados en esta suerte de "teoría euclídea de números". En 2006, Richard K. Guy y Andrew Bremner generalizaron el resultado original de Guy permitiendo al triángulo ser un triángulo de lados enteros y área entera. Hacia el

año 2016, el matemático Yong Zhang consideró la variante del problema original en la que se buscan un triángulo rectángulo de lados enteros y un paralelogramo de lados enteros que tengan la misma área y el mismo perímetro (lo cual consiste en hipótesis más relajadas que las originales del año 1995), encontrando que este problema admitía infinitas soluciones. En el mismo año, el matemático Shane Chern estudió las parejas conformadas por un triángulo rectángulo de lados enteros y un rombo de lados enteros, teniendo ambas figuras la misma área y el mismo perímetro, y pidiendo además que el ángulo agudo del rombo tenga seno y coseno racionales, y encontró que existen infinitas soluciones a dicho problema. En 2017, Yong Zhang y Junyao Peng demostraron que no es posible encontrar un triángulo isósceles de lados enteros y un rombo de lados enteros con ángulo agudo de seno y coseno racionales que tengan la misma área y el mismo perímetro. En el mismo año, Pradeep Das, Abishek Juyal y Dustin Moody probaron que existen infinitas parejas de un triángulo isósceles de lados enteros y un paralelogramo de lados enteros con la misma área y el mismo perímetro, y también que hay infinitas parejas de un triángulo de lados enteros y área entera y un rombo de lados enteros y ángulo agudo de seno y coseno racionales que tengan la misma área y el mismo perímetro. En el año 2018, Yong Zhang, Junyao Peng y Jiamin Wang probaron varios resultados análogos entre triángulos y trapezoides. En el mismo año, Yoshinosuke Hirakawa y Hideki Matsumura demostraron que el par formado por el triángulo rectángulo de lados $(135, 352, 377)$ y el triángulo isósceles de lados $(366, 366, 132)$ es la única solución al problema de encontrar un triángulo rectángulo de lados enteros y un triángulo isósceles de lados enteros con la misma área y el mismo perímetro.

El párrafo anterior consiste en una modesta selección del rico caudal de resultados aritméticos surgidos desde la publicación del trabajo de Richard K. Guy. Esencialmente, todos siguen la misma línea heurística: formular las ecuaciones que modelizan la situación, aplicar un adecuado cambio de variables para poder reformular el problema en términos de una curva elíptica, y aplicar la teoría de curvas elípticas para averiguar si la misma induce infinitas o finitas soluciones al problema original. Esta idea, si bien es, en principio, simple, acarrea una sutil dificultad. En general, saber si una curva tiene o no infinitas soluciones equivale a ver que tiene rango positivo. Y esto, si bien no siempre es un problema fácil, en las aplicaciones suele sortearse por medio de la utilización de una gigantesca base de datos de curvas elípticas ofrecida por John Cremona. El problema es que no todas las soluciones de la curva elíptica encontrada necesariamente aplican al problema original, pues la naturaleza euclídea de su formulación original impone condiciones adicionales sobre las variables que no necesariamente son satisfechas por todas las soluciones de la curva elíptica. La más inmediata evidencia de esto es que muchas de las variables de la formulación original han de representar números positivos, en tanto hacen referencia a longitudes de lados de figuras geométricas no degeneradas. Así, vemos que no basta con demostrar que la curva elíptica encontrada tiene infinitas soluciones. Deben ser infinitas en un determinado subconjunto dado por restricciones específicas.

El problema del anterior párrafo puede resolverse muy satisfactoriamente apelando a un resultado demostrado independientemente por Jules Henri Poincaré en 1901 y por Adolf Hurwitz en 1917, hoy conocido como *Teorema de Poincaré-Hurwitz*, que afirma que si las soluciones de una curva elíptica sobre $\mathbb{Q}$ son infinitas, entonces también son localmente infinitas en cada componente conexa del *real locus* donde haya soluciones racionales.

En vistas a que todos estos resultados parecen seguir un mismo patrón, es natural preguntarse si es posible dar un paso más allá y encontrar una forma de generalizar algunos de estos resultados y compactificarlos dentro de una teoría general. Este trabajo fue

realizado por las matemáticas Matilde Lalín y Xinchun Ma en el año 2019, cuando fueron capaces de probar la siguiente generalización de todos los resultados que involucraban triángulos y paralelogramos: Dado $\theta \in (0, \pi)$ de coseno racional, entonces para todos salvo finitos $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$ existen $\omega \in \left(0, \frac{\pi}{2}\right]$ e infinitos pares de un triángulo de lados enteros que tiene a θ como uno de sus ángulos y un paralelogramo de lados enteros que tiene a ω como uno de sus ángulos, tales que ambas figuras tienen la misma área y el mismo perímetro y tales que $\sin(\omega) = t \sin(\theta)$. Como siempre, sin distinguir por semejanza.

Este extremadamente fuerte resultado les permitió a Lalín y Ma, especializando en valores particulares del coseno de θ, redescubrir varios de los resultados expuestos con anterioridad. Naturalmente, un trabajo de estas proporciones difícilmente podría expresarse en tan pocas variables como una curva elíptica restringe. Es por eso que requirieron hacer uso de un objeto muy particular que, no siendo una curva elíptica, sí tiene estructura de tal aunque sus coeficientes resultan ser polinomios con coeficientes racionales en un parámetro adicional. Considerando ese parámetro como una variable trascendental, este objeto induce naturalmente una curva elíptica sobre $\mathbb{Q}(t)$. La aparición de esta situación es la que motiva el estudio de un concepto general del cual este tipo de objetos forma parte, que es lo que se conoce como *superficie elíptica*, y que es lo que buscamos entender en esta tesis para poder reproducir la demostración de Lalín y Ma. Si bien expondremos cómo hacer uso de la teoría de superficies elípticas para elaborar esta demostración, ha de señalarse que el principal y modesto objetivo de la tesis consiste en poder utilizar este problema de teoría de números planteado por Lalín y Ma en vistas a generalizar gran parte del cúmulo de resultados de índole aritmética-euclídea surgidos a raíz del trabajo de Guy como forma de motivar el estudio de las superficies elípticas.

Estructura de la tesis

La tesis está conformada por cuatro capítulos y dos apéndices.

El primer capítulo está pensado, en sus primeras secciones, como recordatorio de los aspectos básicos de la teoría de curvas elípticas que requeriremos tener presentes a lo largo del desarrollo de la tesis. Así, se expondrán los resultados sin entrar en profundidad en sus demostraciones, aunque sí se brindarán abundantes referencias para el lector interesado en las mismas. La más importante excepción que haremos de esta regla será el hecho de que, dado un primo $p \in \mathbb{N}$, la reducción módulo p de una $\mathbb{Q}$-curva elíptica, siempre que dicha reducción induce una $\mathbb{F}_p$-curva elíptica, es un morfismo de grupos. Probaremos este resultado con absoluto detalle, en tanto no existe en la literatura una demostración completa del mismo sin omitir detalles o cuentas. Dado que dicha demostración requiere de enrevesados cómputos que suelen dejarse como ejercicio para el lector o simplemente son omitidos, aquí expondremos una demostración acabada sin omitir cuentas ni detalles. Posteriormente, y tras mostrar cómo utilizar una computadora para ahorrarse los cálculos enrevesados que subyacen la estructura de grupo de una curva elíptica, ofreceremos una demostración del Teorema de Poincaré-Hurwitz, que es, en esta tesis, el resultado teórico más importante gracias al cual todo nuestro argumento se sostiene. Finalmente, mostraremos cómo aplicar la teoría de curvas elípticas en diversos contextos de desarrollo contemporáneo, empezando con algunos ejemplos sencillos, avanzando hacia un ejemplo donde se requiere del Teorema de Poincaré-Hurwitz, y finalizando con uno de los resultados de índole aritmética-euclídea que fueron listados en la sección anterior, a modo de introducción al tipo de problemas que buscamos encarar.

En el segundo capítulo entramos de lleno en el problema principal de esta tesis, que es el planteado y resuelto por Lalín y Ma en el año 2019. Ocuparemos este capítulo en modelizar y formular el problema, para ver cómo espontáneamente aparece un objeto que será nuestro primer acercamiento a las superficies elípticas. Asimismo, anticiparemos qué tipo de conclusiones es posible derivar utilizando la teoría de superficies elípticas, y mostraremos cómo resolver el problema con base en esas conclusiones. Quedará, pues, pendiente probar aquellas conclusiones prometidas.

El tercer capítulo es el capítulo más importante de la tesis, gracias al cual la misma recibe su nombre. Consiste en introducir las superficies elípticas y conocer las bases de su teoría. En este capítulo se expondrán observaciones y se probarán resultados estrictamente introductorios, aunque no todos serán relevantes para reproducir la demostración de Lalín y Ma, y haremos especial énfasis en la demostración del *Teorema de Mordell-Weil* para superficies elípticas. Si el Teorema de Poincaré-Hurwitz era el resultado más importante para resolver el problema planteado por Lalín y Ma, el Teorema de Mordell-Weil es el resultado conceptual más importante gracias al cual es posible hacer aritmética en superficies elípticas. En general, el principal rol de gran parte de estos desarrollos es que ofrecerán un marco conceptual que permitirá comprender en profundidad el argumento que expondremos en el último capítulo para resolver nuestro problema principal. Nos daremos por satisfechos si nuestra exposición, junto al cuarto capítulo, cumple el modesto objetivo de motivar desde la teoría de números el estudio de las superficies elípticas.

El cuarto capítulo, como ya se anticipó, consiste en aplicar varios de los resultados del tercer capítulo (y algunos resultados adicionales consultados en la literatura especializada) al problema que se deja inconcluso en el segundo capítulo, para ofrecer una demostración en la que, esencialmente, hemos seguido el desarrollo de Lalín y Ma, aunque hemos hecho unas pequeñas modificaciones. Además, finalizaremos con una sección adicional en la que expondremos de forma divulgativa algunas de las conclusiones adicionales que Lalín y Ma consiguieron demostrar en su paper, las cuales son de absoluto interés en tanto permiten comprender mejor la estructura general que subyace a los resultados que generalizaron.

En cuanto al primer apéndice, el mismo consiste en un sumario de los resultados provenientes de la Geometría Algebraica de los cuales haremos uso. Si bien en la tesis daremos por sabida la teoría básica de Geometría Algebraica, requeriremos tener enunciados diversos resultados y conceptos a los cuales hacer referencia a lo largo del desarrollo de la tesis. Asimismo, el apéndice puede servir como recordatorio de algunos de los conceptos básicos que se requieren tener asumidos por parte del lector, en especial a partir del tercer capítulo.

Por último, en el segundo apéndice expondremos una solución alternativa del problema principal, que preferimos tener aislada de la tesis en tanto hace uso del Teorema de Mazur y en razón de que involucra cómputos extremadamente enrevesados.

Requisitos

Los primeros dos capítulos pueden leerse teniendo un bagaje teórico elemental en materia de curvas algebraicas (téngase como referencia el libro *Algebraic Curves* de William Fulton, 2008), como así también conocimiento básico de los más conocidos anillos que estudia la teoría de números, como lo son el anillo de enteros p-ádicos para un primo $p \in \mathbb{N}$. Además, se recomienda muy enfáticamente haber tenido un primer curso o estudio en la teoría elemental de curvas elípticas. En cuanto a la demostración del Teorema de Poincaré-Hurwitz y su

aplicación en el segundo capítulo, es necesario un conocimiento mínimo de Geometría Diferencial y, en particular, de Grupos de Lie.

A partir del tercer capítulo, a todo lo anterior se le suma un requisito mínimo en Teoría de Retículos y una base sólida de Geometría Algebraica. Para esto, puede consultarse el primer apéndice como referencia.

Índice

Capítulo 1

Curvas elípticas

En este primer capítulo ofreceremos un sumario de la teoría más elemental de las curvas elípticas que requeriremos para el tratamiento de los principales desarrollos que llevaremos adelante a lo largo del presente trabajo. Comenzaremos haciendo un breve repaso de los aspectos básicos de dicha teoría y las herramientas de las que disponemos para computar en curvas elípticas, omitiendo algunas demostraciones y limitándonos a señalar referencias para profundizar en las mismas. Posteriormente, se demostrará el Teorema de Poincaré-Hurwitz, que jugará un rol fundamental en el desarrollo de la tesis. Finalmente, mostraremos algunas aplicaciones de esta teoría para ilustrar su utilidad en la Teoría de Números; particularmente, en los problemas de geometría euclídea en los que estamos interesados.

1.1 Resultados básicos

Dado un cuerpo perfecto $\mathbb{K}$, una $\mathbb{K}$-*curva elíptica* es un par (E, O), donde E es una $\mathbb{K}$-curva proyectiva no singular de género 1 y O es un punto en E. El **Teorema de Riemann-Roch** permite construir un isomorfismo algebraico entre E y una cúbica proyectiva plana no singular dada en la *forma de Weierstrass*, definida como la forma que tienen todas las cúbicas proyectivas planas (singulares o no) que tienen un punto de inflexión en $(0:1:0)$ cuya recta tangente es la recta del infinito. Esta forma está dada por

$$\begin{gathered} y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \\ a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}. \end{gathered} \tag{1.1}$$

y el mencionado isomorfismo algebraico puede elegirse de tal forma de identificar O con $(0:1:0)$, tal y como se demuestra en [18, pp. 47-48]. De esta manera, toda curva elíptica admite una inmersión algebraica en $\mathbb{P}^2$, de modo que la forma de Weierstrass recupera, por isomorfismo algebraico, todas los requisitos de la definición de una curva elíptica, salvo quizás por su no singularidad.

Dada una cúbica proyectiva plana en su forma de Weierstrass (sin que necesariamente la misma constituya una curva elíptica; es decir, sin suponer que la misma sea no singular), definimos las constantes

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, & c_4 &:= b_2^2 - 24b_4, \\ b_4 &:= 2a_4 + a_1a_3, & c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6, \\ b_6 &:= a_3^2 + 4a_6, & \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, & j &:= \tfrac{c_4^3}{\Delta} \text{ si } \Delta \neq 0. \end{aligned}$$

de tal forma que la constante Δ, que llamamos *discriminante*, cumple la propiedad de ser nula si y solo si la curva es singular. Naturalmente, existe una forma de expresar Δ en términos de $\{a_1, a_2, a_3, a_4, a_6\}$ (ver [9, 25.3.7]). Así, salvo equivalencias algebraicas, una *curva elíptica* puede definirse como una cúbica en forma de Weierstrass con discriminante no nulo.

Más aún: si la característica de $\mathbb{K}$ es distinta de 2, a través de un cambio de variables es posible suponer que $a_1 = a_3 = 0$. Si la característica de $\mathbb{K}$ no divide a 6, un cambio de variables permite suponer que $a_1 = a_2 = a_3 = 0$. En tal caso, la curva (afinizada) queda en la forma $y^2 = x^3 + ax + b$, con $a = -27c_4$ y $b = -54c_6$. Para una demostración de todo lo dicho en estos últimos dos párrafos, léase [12, III 2]. En general, dada una curva en la forma $y^2 = x^3 + ax + b$ con $a, b \in \mathbb{K}$, se tiene $\Delta = -16\left(4a^3 + 27b^2\right)$, de tal forma que, en característica 2, una tal curva es siempre singular, y en característica distinta de 2, la misma será singular si y solo si $4a^3 + 27b^2 = 0$. Esto demuestra que la suposición de que la característica de $\mathbb{K}$ sea distinta de 2 es una hipótesis fundamental para hacer esta reducción, pues no toda curva en la forma de Weierstrass es singular en característica 2.

Si C es una cúbica homogénea no singular en $\mathbb{K}[x, y, z]$, el **Teorema de Bézout** nos dice que, dada una recta L, se tiene

$$\sum_{P \in \mathbb{P}^2\left(\overline{\mathbb{K}}\right)} I\left(P, L \cap C\right) = 3,$$

donde $\overline{\mathbb{K}}$ es una clausura algebraica de $\mathbb{K}$ y $I\left(P, L \cap C\right)$ es la *multiplicidad de intersección* de L y C en P, de tal forma que podemos definir una aplicación $C\left(\overline{\mathbb{K}}\right) \times C\left(\overline{\mathbb{K}}\right) \to C\left(\overline{\mathbb{K}}\right)$ que a cada par $(P, Q) \in C\left(\overline{\mathbb{K}}\right) \times C\left(\overline{\mathbb{K}}\right)$ le asigna un punto en $C\left(\overline{\mathbb{K}}\right)$ (que notamos PQ) definido como el *zero-cycle* $PQ := L \bullet E - P - Q$, donde L es la recta proyectiva que pasa por P y Q si $P \neq Q$, y es la recta tangente a la curva en P si $P = Q$. $L \bullet C$ es el *intersection cycle* entre las curvas L y C.

Fijando $O \in C\left(\overline{\mathbb{K}}\right)$, el **Teorema fundamental de Max-Noether** permite demostrar, tal y como se hace en [8, pp. 63-64], que la aplicación $(P, Q) \mapsto O\left(PQ\right)$ induce una estructura de grupo abeliano en $C\left(\overline{\mathbb{K}}\right)$, donde O es el elemento neutro y la oposición aditiva queda definida como $-P := (OO)\,P$. Es posible demostrar usando Teoría de Galois (léase el Apéndice A.1) que, si $P, Q \in C\left(\mathbb{K}\right)$ (equivalentemente, $P, Q \in C\left(\overline{\mathbb{K}}\right)$ y admiten una representación de coordenadas proyectivas en $\mathbb{K}$), entonces $PQ \in \mathbb{C}\left(\mathbb{K}\right)$. Así, si elegimos $O \in \mathbb{C}\left(\mathbb{K}\right)$, entonces $C\left(\mathbb{K}\right)$ es un subgrupo de $C\left(\overline{\mathbb{K}}\right)$. De esta manera, la definición de la operación de grupos queda extendida a cúbicas proyectivas planas no singulares y no vacías que estén definidas sobre cualquier cuerpo perfecto, no necesariamente algebraicamente cerrado.

En el caso de curvas elípticas sobre $\mathbb{K}$ en forma de Weierstrass, podemos tomar como neutro al punto $O := (0 : 1 : 0)$, el único punto de inflexión de la curva. Como O es de inflexión, $OO = O$, y por lo tanto el inverso aditivo queda definido como $-P := OP$.

Sea E una curva elíptica sobre $\mathbb{Q}$ en forma de Weierstrass. El primer resultado importante y fundamental de la teoría de curvas elípticas es el **Teorema de Mordell**, que enunciamos a continuación y que permite comenzar a analizar la estructura del grupo abeliano $E\left(\mathbb{Q}\right)$, dando inicio al estudio de los aspectos aritméticos de la teoría de curvas elípticas.

Teorema 1.1.1 *$E\left(\mathbb{Q}\right)$ es finitamente generado como grupo abeliano.*

Demostración. Léase [12, IV]. ■

En el $\mathbb{K}$-plano proyectivo bidimensional, que notamos $\mathbb{P}^2(\mathbb{K})$, los cambios proyectivos de coordenadas que fijan el punto $(0:1:0)$ y la recta del infinito están inducidos, a menos de una constante no nula, por una matriz de la forma

$$\begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{K}^{3\times 3},$$

donde $u \neq 0$. Así, estos cambios de coordenadas preservan la propiedad de las cúbicas de estar en la forma de Weierstrass. Es posible demostrar ([18, Theorem 2.4]) que dos curvas elípticas son algebraicamente isomorfas si y solo si el isomorfismo es de esta forma. Llamaremos a estos isomorfismos *cambios admisibles de variable*. Teniendo clasificados los isomorfismos entre curvas elípticas, se desprende el siguiente importante teorema que da sentido a la constante j definida previamente, que se denomina *el j-invariante de la curva elíptica*.

Teorema 1.1.2 *Dadas dos curvas elípticas E y E' sobre un cuerpo perfecto $\mathbb{K}$ dadas en forma de Weierstrass, entonces las mismas son isomorfas sobre una clausura algebraica $\overline{\mathbb{K}}$ de $\mathbb{K}$ si y solo si tienen el mismo j-invariante.*

Demostración. Léase [11, Teorema 2.9]. ■

Más aún, dado un escalar j_0 en $\mathbb{K}$, siempre es posible encontrar una curva elíptica cuyo j-invariante sea j_0. En efecto, si $j_0 = 0$, podemos tomar la curva elíptica $y^2z + yz^2 = x^3$, o bien la curva elíptica $y^2z = x^3 + bz^3$ con $b \neq 0$. Si $j_0 = 1728$, podemos tomar la curva elíptica $y^2z = x^3 + axz^2$ con $a \neq 0$. Finalmente, si $j_0 \notin \{0, 1728\}$, se puede tomar la curva

$$y^2z + xyz = x^3 - \frac{36}{j_0 - 1728}xz^2 - \frac{1}{j_0 - 1728}z^3$$

cuyo j-invariante es j_0. Señálese que esta curva no sirve para el caso $j_0 = 0$, ya que en tal caso su discriminante es nulo.

Esta observación y el Teorema 1.1.2 muestran que, dado un cuerpo algebraicamente cerrado (en particular, perfecto), la función j-invariante induce una biyección bien definida entre las clases de isomorfismo de curvas elípticas sobre el cuerpo algebricamente cerrado en cuestión, y los elementos de dicho cuerpo.

1.2 Reducción módulo un número primo natural

Fijado un primo $p \in \mathbb{N}$ y un número natural n, y dado $P \in \mathbb{P}^n(\mathbb{Q})$, existe una representación de P como $(a_0 : \cdots : a_n)$, donde a_i está en el anillo $\mathbb{Z}_p$ de enteros p-ádicos para todo $i \in [0, n] \cap \mathbb{Z}$, y al menos uno de ellos tiene norma p-ádica unitaria. Una tal representación de P se dice *representación p-reducida de P*. Si $(b_0 : \cdots : b_n) \in \mathbb{P}^n(\mathbb{Q})$ es otra representación p-reducida de P, entonces existe $r \in \mathbb{Q}$ de norma p-ádica unitaria tal que $b_i = ra_i$ para cada $i \in [0, n] \cap \mathbb{Z}$.

Del párrafo anterior se deduce que, para cada primo $p \in \mathbb{N}$, tenemos una función *reducción* bien definida $r_p : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{F}_p)$ que a cada $P \in \mathbb{P}^n(\mathbb{Q})$ le asigna $(r_p(a_0) : \cdots : r_p(a_n))$, donde $(a_0 : \cdots : a_n)$ es una representación p-reducida de P y $r_p : \mathbb{Z}_p \to \mathbb{F}_p$ es la reducción módulo p.

Otra cosa que se deduce del primer párrafo es que, dada una curva proyectiva F en $\mathbb{P}^n(\mathbb{Q})$, la misma es equivalente (multiplicando por un racional adecuado) a una curva cuyos coeficientes están todos en $\mathbb{Z}_p$ y al menos uno tiene norma p-ádica unitaria. Así, tenemos definida una curva proyectiva F_p en $\mathbb{P}^n(\mathbb{F}_p)$ bien definida salvo por una multiplicación por un elemento no nulo, y por lo tanto la función r_p del párrafo anterior admite una restricción y correstricción a $F(\mathbb{Q}) \to F_p(\mathbb{F}_p)$.

En el caso de curvas elípticas, podemos hacer algo mejor. Dado un cambio admisible de variables de la forma $\begin{pmatrix} u^2 & 0 & 0 \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, este cambio de variables genera que los coeficientes a_i, $i \in \{1,2,3,4,6\}$ de la forma original queden multiplicados por u^{-i} una vez efectuado el cambio de variables. Exactamente lo mismo ocurre con los escalares b_i, $i \in \{2,4,6,8\}$ y los escalares c_i, $i \in \{4,6\}$. De hecho, esta es la motivación para la aparentemente arbitraria elección de subíndices.

Esto demuestra que, si R es un anillo tal que $\mathbb{K}$ es su cuerpo de fracciones, entonces toda curva elíptica en forma de Weierstrass con coeficientes en $\mathbb{K}$, mediante una adecuada elección de u, es isomorfa a una curva elíptica en forma de Weierstrass sobre $\mathbb{K}$ cuyos coeficientes están en R. En particular, podemos trabajar con curvas elípticas sobre $\mathbb{Q}$ con coeficientes enteros, y dado que el coeficiente de x^3 es 1 (cuya norma p-ádica es 1), entonces tenemos una curva elíptica sobre $\mathbb{Q}$ cuyos coeficientes son todos enteros (en particular, están en $\mathbb{Z}_p$) y tal que al menos uno de sus coeficientes tiene norma p-ádica unitaria. En otras palabras, dada una $\mathbb{Q}$-curva elíptica E, a menos de un cambio de variables admisible podemos suponer que sus coeficientes son enteros, de tal forma que E_p consiste en reducir módulo p los coeficientes enteros de E, sin necesidad de multiplicarlos por algún racional adecuado. Sea Δ_p el discriminante de E_p. Entonces $\Delta_p = 0$ si y solo si $p \mid \Delta$. Así, si $p \nmid \Delta$, entonces E_p es una $\mathbb{F}_p$-curva elíptica. Dado que en la literatura no está demostrado con todos los detalles y sin omisiones, probaremos cuidadosamente que $r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ es un morfismo de grupos. Para esto, requeriremos un lema previo.

Lema 1.2.1 *Sea $p \in \mathbb{N}$ un número primo y sea $m \in \mathbb{N}$. Sea F una curva proyectiva plana no singular de grado m sobre $\mathbb{Q}$. Sea L una recta en $\mathbb{P}^2(\mathbb{Q})$. Sea $k \in \mathbb{N}_0$ y sean $P_0, \cdots, P_k$ puntos distintos de $L \cap F$ con la misma reducción módulo p. Si F_p y L_p son las reducciones módulo p de F y L, entonces*

$$\min\{m, I(P_0, L \cap F) + k\} \leq I(r_p(P_0), L_p \cap F_p).$$

Demostración. Para cada $i \in [0,k] \cap \mathbb{Z}$, sea $(x_i : y_i : z_i)$ una representación p-reducida de P_i. Multiplicando por un entero coprimo con p adecuado, podemos suponer que $x_i, y_i, z_i \in \mathbb{Z}$ para cada $i \in [0,k] \cap \mathbb{Z}$. Sabemos que, para estos valores de i, $r_p(P_0) = r_p(P_i)$, con lo cual existe $a_i \in \mathbb{Z}$ no divisible por p tal que $a_i(x_i, y_i, z_i) \equiv (x_0, y_0, z_0) \pmod{p}$. Cambiando el sistema de representantes multiplicando por a_i, podemos suponer sin pérdida de generalidad que $(x_i, y_i, z_i) \equiv (x_0, y_0, z_0) \pmod{p}$ para cada $i \in [0,k] \cap \mathbb{Z}$.

Sea $P' \in \mathbb{P}^2(\mathbb{Q})$ un punto de L con $r_p(P') \neq r_p(P_0)$ (en particular, se tiene que $P' \neq P_i$ para todo $i \in [0,k] \cap \mathbb{Z}$). Veamos que un tal P' existe. En efecto, por hipótesis, $x_0, y_0, z_0 \in \mathbb{Z}$ y al menos uno es coprimo con p. Supongamos que $p \nmid z_0$ (los otros casos son análogos). En particular $z_0 \neq 0$ y, como $P_0 \in L$, entonces L no es la recta $\{z = 0\}$. Por lo tanto, tomando el único punto de intersección $P' \in \mathbb{P}^2(\mathbb{Q})$ entre L y $\{z = 0\}$, es claro que P' funciona, ya que la última coordenada en cualquier representación p-reducida de P' es nula, lo cual no ocurre con P_0 pues $p \nmid z_0$.

Sea $(x' : y' : z')$ una representación p-reducida de P' con coordenadas enteras. Reescalando F para que todos sus coeficientes sean enteros y al menos uno de ellos sea coprimo con p, definimos $\psi \in \mathbb{Z}[t]$ como

$$\psi(t) := F\left(x_0 + tx', y_0 + ty', z_0 + tz'\right) = \sum_{j=r}^{m} \widetilde{F}_j t^j \tag{1.2}$$

donde $r \in \mathbb{N}_0$ es tal que $\widetilde{F}_r \neq 0$. Sabemos entonces que $I(P_0, L \cap F) = r$ (aquí usamos que F es no singular, pues en tal caso un tal r debe existir, o de lo contrario $L \mid F$).

Supongamos que $k = 0$. Entonces $I(P_0, L \cap F) \leq \deg(L)\deg(F) = 1 \cdot m = m$, por lo tanto debemos ver que $I(P_0, L \cap F) \leq I(r_p(P_0), F_p \cap L_p)$, lo cual se ve fácilmente reduciendo 1.2 módulo p. Supongamos entonces que $k \geq 1$ y probemos que $p \mid \widetilde{F}_i$ para todo $i \in [r, \min\{m, r+k-1\}] \cap \mathbb{Z}$, lo cual probará el lema.

Como L es una recta proyectiva y, para cada $i \in [1,k] \cap \mathbb{Z}$, $P_i \neq P'$, existe un conjunto de k racionales distintos $\{t_i : i \in [1,k] \cap \mathbb{Z}\}$ tal que

$$(x_i : y_i : z_i) = \left(x_0 + t_i x' : y_0 + t_i y' : z_0 + t_i z'\right)$$

para cada $i \in [1,k] \cap \mathbb{Z}$. Como, para estos valores de i, se tiene $P_i \neq P_0$, entonces $t_i \neq 0$ y existe $c_i \in \mathbb{Q}^\times$ tal que

$$(x_i, y_i, z_i) = c_i\left(x_0 + t_i x', y_0 + t_i y', z_0 + t_i z'\right).$$

Como $r_p(P_i) = r_p(P_0) \neq r_p(P')$, alguna submatriz de 2×2 de $\begin{pmatrix} x' & y' & z' \\ x_i & y_i & z_i \end{pmatrix}$ tiene determinante no divisible por p. Veamos que $t_i \in \mathbb{Z}_p$. Supongamos sin pérdida de generalidad que $\det \begin{pmatrix} x' & y' \\ x_i & y_i \end{pmatrix} = y_i x' - x_i y'$ no es divisible por p (los otros casos son análogos). Como $c_i \neq 0$, $x_i = c_i(x_0 + t_i x')$ e $y_i = c_i(y_0 + t_i y')$, entonces

$$x_i\left(y_0 + t_i y'\right) = x_i \frac{y_i}{c_i} = y_i \frac{x_i}{c_i} = y_i\left(x_0 + t_i x'\right),$$

de donde $x_i y_0 - y_i x_0 = t_i(y_i x' - x_i y')$. Como $y_i x' - x_i y'$ no es divisible por p, resulta que $t_i \in \mathbb{Z}_p$, como queríamos. Más aún, como $x_i \equiv x_0 \pmod{p}$ e $y_0 \equiv y_i \pmod{p}$ pues $(x_i, y_i, z_i) \equiv (x_0, y_0, z_0) \pmod{p}$, entonces $p \mid x_i y_0 - y_i x_0$, de donde $\|t_i\|_p < 1$.

Escribimos

$$0 = F(x_i, y_i, z_i) = c_i^m F\left(x_0 + t_i x', y_0 + t_i y', z_0 + t_i z'\right) = c_i^m \sum_{j=r}^{m} \widetilde{F}_j t_i^j,$$

de donde, usando que $c_i \neq 0 \neq t_i$, obtenemos

$$\sum_{j=r}^{m} \widetilde{F}_j t_i^{j-r} = 0.$$

Como esto lo probamos para cada $i \in [1,k] \cap \mathbb{Z}$, tenemos un sistema de k ecuaciones en las $m - r + 1$ incógnitas $\widetilde{F}_r, \cdots, \widetilde{F}_m$, cuya forma matricial es

$$A \begin{pmatrix} \widetilde{F}_r \\ \vdots \\ \widetilde{F}_m \end{pmatrix} = 0,$$

donde $A \in \mathbb{Q}^{k\times(m-r+1)}$ es tal que $A_{ij} = t_i^{j-1}$. Si $k \geq m-r+1$, podemos quedarnos con las primeras $m-r+1$ ecuaciones y obtenemos un sistema homogéneo de Vandermonde; que es, en consecuencia, inversible, y por lo tanto solamente admite la solución trivial; es decir, $\widetilde{F}_i = 0$ para todo $i \in [r,m] \cap \mathbb{Z}$. En particular $p \mid \widetilde{F}_i$ para estos valores de i. Como $k \geq m-r+1$, entonces $\min\{m, r+k-1\} = m$, con lo cual hemos probado el lema para este caso.

Supongamos entonces que $k < m-r+1$. Escribimos $A = (V \mid U)$, con $V \in \mathbb{Q}^{k\times k}$, de tal forma que $U \in \mathbb{Q}^{k\times(m-r-k+1)}$. Sea $F_1 := \begin{pmatrix} \widetilde{F}_r \\ \vdots \\ \widetilde{F}_{r+k-1} \end{pmatrix}$ y sea $F_2 := \begin{pmatrix} \widetilde{F}_{r+k} \\ \vdots \\ \widetilde{F}_m \end{pmatrix}$. Como V es una matriz de Vandermonde inversible, multiplicando la expresión $VF_1 + UF_2 = 0$ por V^{-1} obtenemos $F_1 + V^{-1}UF_2 = 0$. Sea $D \in \mathbb{Q}^{k\times k}$ la matriz diagonal definida como $D_{ij} = \delta_{ij}t_i$, donde δ es la *función delta de Kronecker*. Sean $\{\sigma_i : i \in [1,k] \cap \mathbb{N}\}$ las funciones elementales simétricas en $\{t_i : i \in [1,k] \cap \mathbb{N}\}$, de tal forma que

$$\prod_{j=1}^{k}(X - t_j) = X^k + \sum_{s=1}^{k}(-1)^{k+1-s}\,\sigma_{k+1-s}X^{s-1} \in \mathbb{Q}[X].$$

En particular, evaluando en $X = t_i$ para algún $i \in [1,k] \cap \mathbb{N}$, tenemos

$$\sum_{s=1}^{k}(-1)^{k+1-s}\,\sigma_{k+1-s}t_i^{s-1} = -t_i^k.$$

Definimos $W \in \mathbb{Q}^{k\times k}$ como

$$W_{ij} = \delta_{i,j+1} + \delta_{kj}\,(-1)^{k-i}\,\sigma_{k+1-i}.$$

Es claro que $(DV)_{ij} = t_i^j$. Por otra parte,

$$(VW)_{ij} = \sum_{s=1}^{k} V_{is}W_{sj} = \sum_{s=1}^{k} t_i^{s-1}\left(\delta_{s,j+1} + \delta_{kj}\,(-1)^{k-s}\,\sigma_{k+1-s}\right) =$$

$$= \left(\sum_{s=1}^{k}\delta_{s,j+1}t_i^{s-1}\right) - \delta_{kj}\sum_{s=1}^{k}(-1)^{k+1-s}\,\sigma_{k+1-s}t_i^{s-1} = \left(\sum_{s=1}^{k}\delta_{s,j+1}t_i^{s-1}\right) + \delta_{kj}t_i^k.$$

Si $k \neq j$ entonces $j < k$, de modo que existe $s \in [1,k] \cap \mathbb{N}$ tal que $s = j+1$, luego la anterior expresión es igual a t_i^j. Si $k = j$, no existe un tal s, de donde la anterior expresión es igual a t_i^j también. Esto demuestra que $DV = VW$, de donde $V^{-1}D = WV^{-1}$.

Para cada $\ell \in \mathbb{N}_0$, definimos $C_\ell := \begin{pmatrix} t_1^\ell \\ \vdots \\ t_k^\ell \end{pmatrix}$. Es claro que $C_{\ell+1} = DC_\ell$ para todo $\ell \in \mathbb{N}_0$.

Así, como $V^{-1}D = WV^{-1}$,

$$V^{-1}C_{\ell+1} = V^{-1}DC_\ell = WV^{-1}C_\ell.$$

Si $\ell = k-1$, C_ℓ es la última columna de V, por lo tanto $V^{-1}C_{k-1}$ es la última columna e_k de la identidad en $\mathbb{Q}^{k\times k}$.

Probaremos que, para todo $\ell \in \mathbb{N}_0$ tal que $\ell \geq k-1$, $V^{-1}C_\ell = W^{\ell-k+1}e_k$. En efecto, para $\ell = k-1$ lo probamos en el párrafo anterior. Si vale para un $\ell \in \mathbb{N}_{\geq k-1}$ genérico, entonces

$$V^{-1}C_{\ell+1} = WV^{-1}C_\ell = WW^{\ell-k+1}e_k = W^{(\ell+1)-k+1}e_k,$$

lo cual completa el paso inductivo.

Dado $n \in \mathbb{N}$ y un vector $X \in \mathbb{Q}^k$ que cumpla que su i-ésima entrada es homogénea de grado $k+n-i$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$, entonces WX cumple que su i-ésima entrada es homogénea de grado $k+(n+1)-i$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$. En otras palabras, el grado de homogeneidad aumenta en 1. Esto es así porque, en efecto,

$$(WX)_i = \sum_{j=1}^{k} W_{ij}X_j = \sum_{j=1}^{k} \left(\delta_{i,j+1} + \delta_{kj}\,(-1)^{k-i}\,\sigma_{k+1-i}\right) X_j.$$

Si $i=1$, $\delta_{i,j+1} = 0$ para todo $j \in [1,k] \cap \mathbb{N}$ y la expresión queda igual a $(-1)^{k-i}\,\sigma_{k+1-i}X_k$, la cual es homogénea de grado $(k+1-i)+(k+n-k) = k+(n+1)-i$. Si $1 < i < k$, la expresión queda igual a X_{i-1}, cuyo grado de homogeneidad es $k+n-(i-1) = k+(n+1)-i$. Finalmente, si $i=k$, la expresión queda igual a $X_{k-1}+\sigma_1 X_k$, lo cual es suma de elementos de grado de homogeneidad $n+1 = k+(n+1)-i$. En efecto, X_{k-1} tiene grado de homogeneidad $k+n-(k-1) = n+1$ y $\sigma_1 X_k$ tiene grado de homogeneidad $1+(k+n-k) = n+1$.

De esto se deduce que, para todo $n \in \mathbb{N}$, la i-ésima entrada de la última columna de W^n es homogénea de grado $k+n-i$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$. En efecto, para $n=1$, la i-ésima entrada de la última columna de W es homogénea de grado $k+1-i$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$, pues σ_i es homogénea de grado i en dichas variables. Inductivamente, si vale para un $n \in \mathbb{N}$ genérico, se tiene que la última columna de W^{n+1} es igual a WX, donde X es la última columna de W^n. Por hipótesis inductiva, X cumple que su i-ésima entrada es homogénea de grado $k+n-i$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$. Aplicando lo probado en el anterior párrafo, WX, que es la última columna de W^{n+1}, cumple que su i-ésima entrada es homogénea de grado $k+(n+1)-i$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$, lo cual completa el paso inductivo. Fijando $\ell \in \mathbb{N}$ tal que $\ell \geq k$, y aplicando lo probado para $n = \ell-k+1$, sabemos que la i-ésima entrada de la última columna de $W^{\ell-k+1}$, que es igual a $W^{\ell-k+1}e_k = V^{-1}C_\ell$, es homogénea de grado $k+(\ell-k+1)-i = \ell+1-i \geq k+1-i \geq 1$ en las variables $t_1, \cdots, t_k$ para cada $i \in [1,k] \cap \mathbb{N}$. Por lo tanto, dado que las columnas de U son de la forma C_ℓ con $\ell \in \mathbb{N}_{\geq k}$, resulta que $V^{-1}U$ es una matriz cuyas entradas son homogéneas de grado mayor o igual que 1 en las variables $t_1, \cdots, t_k$.

De la expresión $F_1 + V^{-1}UF_2 = 0$ obtenemos que, para todo $n \in [r, r+k-1] \cap \mathbb{N}_0$, $\widetilde{F}_n$ es combinación lineal de algunas de las entradas de $-V^{-1}U$ con coeficientes en las entradas de F_2, que son enteras. Como las entradas de $-V^{-1}U$ son homogéneas de grado positivo en $t_1, \cdots, t_k$, y cada uno de estos números racionales tiene norma p-ádica menor que 1, se sigue de la propiedad ultramétrica de la norma p-ádica que, para todo $n \in [r, r+k-1] \cap \mathbb{Z}$, $p \mid \widetilde{F}_n$. Como $k < m-r+1$ entonces $\min\{m, r+k-1\} = r+k-1$, por lo tanto $p \mid \widetilde{F}_i$ para todo $i \in [r, \min\{m, r+k-1\}] \cap \mathbb{Z}$, lo cual termina de probar el lema en este último caso y finaliza la demostración. ■

Ahora estamos en condiciones de probar lo que queríamos.

Proposición 1.2.2 *Dada una $\mathbb{Q}$-curva elíptica E con coeficientes enteros y $p \in \mathbb{N}$ un número primo tal que el discriminante de E no es divisible por p, el morfismo reducción $r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ es un morfismo de grupos.*

Demostración. Sea L una recta proyectiva en $\mathbb{P}^2(\mathbb{Q})$. Como E es no singular, existen puntos no necesariamente distintos $P_0, P_1, P_2 \in E \cap L$ tales que $E \bullet L = P_0 + P_1 + P_2$. Probaremos que $L_p \bullet E_p = r_p(P_0) + r_p(P_1) + r_p(P_2)$.

Supongamos que r_p induce una biyección entre $\{P_0, P_1, P_2\}$ y $\{r_p(P_0), r_p(P_1), r_p(P_2)\}$. Entonces $I(P_j, E \cap L) \leq I(r_p(P_j), E_p \cap L_p)$ para cada $j \in \{0,1,2\}$, por el Lema 1.2.1 con $k = 0$. Como E_p es no singular, $L_p \bullet E_p$ es un *zero-cycle* de grado 3, de donde, para cada $j \in \{0,1,2\}$, $I(P_j, L \cap E) = I(r_p(P_j), L_p \cap E_p)$ y $L_p \bullet E_p = r_p(P_0) + r_p(P_1) + r_p(P_2)$. Obsérvese que este argumento funciona incluso si el cardinal de $\{P_0, P_1, P_2\}$ no es 3.

Supongamos ahora que r_p no es inyectiva en $\{P_0, P_1, P_2\}$. Como primer caso, asumimos que el cardinal de $\{P_0, P_1, P_2\}$ es 3 y que $r_p(P_0) = r_p(P_1) \neq r_p(P_2)$. Usando $k = 1$ en el Lema 1.2.1, $I(r_p(P_0), L_p \cap E_p) \geq I(P_0, L \cap E) + 1 = 2$ y, nuevamente por el Lema 1.2.1 pero con $k = 0$, $I(r_p(P_2), L_p \cap E_p) \geq I(P_2, L \cap E) = 1$. Como $L_p \bullet E_p$ debe necesariamente tener grado 3, obtenemos $L_p \bullet E_p = 2r_p(P_0) + r_p(P_2) = r_p(P_0) + r_p(P_1) + r_p(P_2)$.

Como segundo caso, seguimos suponiendo que el cardinal de $\{P_0, P_1, P_2\}$ es 3, y asumimos que $r_p(P_0) = r_p(P_1) = r_p(P_2)$. Entonces, por el Lema 1.2.1 con $k = 2$, obtenemos $I(r_p(P_0), L_p \cap E_p) \geq I(P_0, L \cap E) + 2 = 3$, de donde, como $L_p \bullet E_p$ debe tener grado 3, $L_p \bullet E_p = 3r_p(P_0) = r_p(P_0) + r_p(P_1) + r_p(P_2)$.

Como tercer caso, supongamos que $P_0 = P_2 \neq P_1$, es decir, $I(P_0, L \cap E) = 2$. Como estamos bajo el caso general de que r_p no es inyectiva en $\{P_0, P_1, P_2\}$, necesariamente debe ser $r_p(P_0) = r_p(P_1)$. Haciendo uso del Lema 1.2.1 con $k = 1$ obtenemos que $I(r_p(P_0), L_p \cap E_p) \geq I(P_0, L \cap E) + 1 = 2 + 1 = 3$. Al igual que en el párrafo anterior, esto implica que $L_p \bullet E_p = 3r_p(P_0) = r_p(P_0) + r_p(P_1) + r_p(P_2)$.

No quedan más casos por analizar, ya que el caso en que $P_0 = P_1 = P_2$ no permite suponer que r_p no es inyectiva en $\{P_0, P_1, P_2\}$. Esto demuestra que, dados dos puntos P y Q en E, $r_p(PQ) = r_p(P)\, r_p(Q)$. Como además $r_p(0:1:0) = (0:1:0)$; entonces, llamando O al neutro en E y O_p al neutro en E_p,

$$r_p(O(PQ)) = r_p(O)\, r_p(PQ) = O_p(r_p(P)\, r_p(Q))$$

que es precisamente la propiedad de ser un morfismo de grupos para las estructuras consideradas. ■

La importancia del morfismo reducción radica en que, gracias al mismo, es posible desarrollar un algoritmo para calcular el grupo de torsión de una $\mathbb{Q}$-curva elíptica. Como el único punto de la curva sobre la recta del infinito es $(0:1:0)$, que es de torsión por ser el elemento neutro, el resto de los puntos de torsión serán de la forma $(x:y:1)$ con $x, y \in \mathbb{Q}$. El **Teorema de Lutz-Nagell**, que enunciamos a continuación, nos da condiciones sobre x e y que reducen la lista de posibilidades a un número finito de candidatos. Concretamente, tenemos el siguiente teorema.

Teorema 1.2.3 *Sea E una curva elíptica sobre $\mathbb{Q}$ en la forma de Weierstrass y con coeficientes en $\mathbb{Z}$, y sea Δ su discriminante.*

a) Si $(x:y:1) \in E(\mathbb{Q})_{\text{tors}}$, entonces $4x$ y $8y$ son enteros.

b) Si $(x : y : 1) \in E(\mathbb{Q})_{\text{tors}}$ *y* $a_1 = 0$*, entonces* x *e* y *son enteros.*

c) Si $p \in \mathbb{N}$ *es un primo impar tal que* $p \nmid \Delta$*, entonces la restricción* $r_p : E(\mathbb{Q})_{\text{tors}} \to E_p(\mathbb{F}_p)$ *es inyectiva. Si* $p = 2$*, esto también vale si* $2 \nmid \Delta$ *y* $a_1 = 0$*.*

d) Si E *está dada en la forma (afinizada)* $y^2 = x^3 + ax + b$ *(es decir,* $a_1 = a_2 = a_3 = 0$*), entonces, dado* $(x : y : 1) \in E(\mathbb{Q})_{\text{tors}}$*, se tiene* $y = 0$ *(de donde el punto* $(x : y : 1)$ *tiene orden 2) o bien* $y^2 \mid 4a^3 + 27b^2$*.*

Demostración. Léase [12, V 4]. ■

Veamos cómo hacer uso de este teorema para encontrar el grupo de torsión de $E(\mathbb{Q})$. El ítem (c) del Teorema 1.2.3 permite acotar el orden de dicho grupo por el máximo común divisor entre los números naturales de la forma $|E_p(\mathbb{F}_p)|$, donde $p \in \mathbb{N}$ es un primo impar tal que $p \nmid \Delta$ (si $a_1 = 0$ y Δ es impar, podemos agregar $p = 2$). En la práctica, es posible elegir algunos de estos primos p, encontrar el valor de $|E_p(\mathbb{F}_p)|$ y calcular el máximo común divisor entre los números encontrados.

Una vez obtenida la cota para el orden del grupo de torsión, es posible usar los ítems (b) y (d) para hallar una lista finita de los posibles valores de y para un punto de torsión de la forma $(x : y : 1)$. Para cada uno de estos valores, se resuelve la ecuación en x que resulta de sustituir y por estos valores obtenidos, obteniendo así una lista finita de puntos $(x : y : 1)$ que son candidatos a ser puntos de torsión.

Finalmente, dado un punto P en la lista obtenida, verificar que sea un punto de torsión consiste en chequear si existe $n \in \mathbb{N}$ menor o igual que la cota obtenida para el orden de $E(\mathbb{Q})_{\text{tors}}$ tal que $nP = (0 : 1 : 0)$. Para esto, requeriremos de descripciones explícitas de la operación de grupo en $E(\mathbb{Q})$. Esto es el tema de la próxima sección.

Un teorema muy relacionado, cuya demostración excede los objetivos y alcances del presente trabajo, es el conocido **Teorema de Mazur**. El mismo expone todas las posibilidades para la estructura del grupo de torsión de una $\mathbb{Q}$-curva elíptica. Concretamente, se tiene lo siguiente.

Teorema 1.2.4 *Sea* E *una* $\mathbb{Q}$*-curva elíptica. Entonces* $E(\mathbb{Q})_{\text{tors}}$ *es isomorfo a* $\mathbb{Z}/n\mathbb{Z}$ *donde* $n \in \mathbb{N}_{\leq 12}$ *y* $n \neq 11$*, o bien es isomorfo a* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$*, donde* $n \in \mathbb{N}_{\leq 4}$*.*

Finalmente, una vez calculado el grupo de torsión de una $\mathbb{Q}$-curva elíptica, es natural preguntarse por la estructura que tiene su parte libre. El problema de calcular el rango de esta parte libre es un problema abierto de la matemática, dado que, a día de hoy, no existen algoritmos eficientes para computar el rango de una $\mathbb{Q}$-curva elíptica.

1.3 Cómputo explícito en curvas elípticas

Sea $\mathbb{K}$ un cuerpo perfecto. Sea E una $\mathbb{K}$-curva elíptica en la forma 1.1. Sea $P_0 \in E(\mathbb{K})$ tal que $P_0 \neq O = (0 : 1 : 0)$. Como $(0 : 1 : 0)$ es el único punto en $E(\mathbb{K}) \cap \{z = 0\}$, podemos escribir $P_0 := (x_0 : y_0 : 1)$ con $x_0, y_0 \in \mathbb{K}$. Veamos cómo calcular $-P_0 = OP_0$. La recta $L : x - x_0 z$ pasa por O y por P_0, con lo cual L es la recta por O y P_0. Buscamos el tercer punto en $L \cap E$. Para esto, sustituimos $x = x_0 z$ en 1.1. Más aún; como $P_0 \neq O$ entonces $-P_0 \neq O$, con lo cual podemos también sustituir $z = 1$ y obtener

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

Sabemos que $y = y_0$ es una raíz de esta ecuación. Como la suma de las raíces de una ecuación cuadrática mónica coincide con el opuesto aditivo del coeficiente lineal de la misma, resulta que la otra raíz está dada por $-y_0 - a_1x_0 - a_3$. Así, hemos demostrado que

$$-P_0 = (x_0 : -y_0 - a_1x_0 - a_3 : 1). \tag{1.3}$$

Sabiendo cómo operar con el elemento neutro y con inversos aditivos, veamos cómo operar en el resto de los casos. Sean $P_1, P_2, P_3 \in E(\mathbb{K})$ tales que $P_i \neq (0:1:0)$ para todo $i \in \{1,2,3\}$ y $P_1 + P_2 = P_3$. Como $(0:1:0)$ es el único punto en $E(\mathbb{K}) \cap \{z = 0\}$, para cada $i \in \{1,2,3\}$ tenemos definida la afinización (x_i, y_i) de P_i, de tal forma que $P_i = (x_i : y_i : 1)$.

Como $P_1 + P_2 = P_3$ y $P_3 \neq O$, entonces $P_1 \neq -P_2$. Es decir, $x_1 \neq x_2$ o bien $x_1 = x_2$ e $y_1 \neq -y_2 - a_1x_2 - a_3$.

Veamos que $P_1 \neq P_2$ si y solo si $x_1 \neq x_2$. Es claro que, si $x_1 \neq x_2$, entonces $P_1 \neq P_2$. Recíprocamente, supongamos que $P_1 \neq P_2$. Como, además, según vimos, $P_1 \neq -P_2$, entonces $x_1 \neq x_2$ o bien $x_1 = x_2$ e $y_1 \neq -y_2 - a_1x_2 - a_3$. Veamos que $x_1 \neq x_2$. Esto es claro si $y_1 = y_2$, pues $P_1 \neq P_2$ por hipótesis. Supongamos entonces que $y_1 \neq y_2$. Si fuera $x_1 = x_2$, entonces $y_1 \neq -y_2 - a_1x_2 - a_3$ y, además,

$$C := y_1^2 + a_1x_1y_1 + a_3y_1 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6 =$$

$$= x_2^3 + a_2x_2^2 + a_4x_2 + a_6 = y_2^2 + a_1x_2y_2 + a_3y_2 = y_2^2 + a_1x_1y_2 + a_3y_2,$$

de donde y_1, y_2 son dos raíces distintas de la cuadrática $y^2 + (a_1x_1 + a_3)\, y - C$, de donde $y_1 + y_2 = -(a_1x_1 + a_3)$, lo cual contradice que $y_1 \neq -y_2 - a_1x_2 - a_3$.

Ahora veamos que si $P_1 = P_2$ entonces $2y_1 + a_1x_1 + a_3 \neq 0$. Como $P_1 = P_2$ entonces $x_1 = x_2$ e $y_1 = y_2$. Como $P_2 \neq -P_1$ y $x_1 = x_2$, entonces $y_2 \neq -y_1 - a_1x_1 - a_3$, pero $y_1 = y_2$, de donde $2y_1 + a_1x_1 + a_3 \neq 0$, como queríamos.

Estos últimos dos párrafos nos permiten definir

$$m := \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P_1 \neq P_2, \\[2ex] \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & P_1 = P_2. \end{cases}$$

$$b := \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}, & P_1 \neq P_2, \\[2ex] \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & P_1 = P_2. \end{cases}$$

Haciendo el cálculo explícito, se ve que $y = mx + bz$ es la recta L que pasa por P_1 y P_2, que es tangente a E en P_1 si $P_1 = P_2$. Afinizando y sustituyendo en la ecuación de la curva elíptica, es posible hallar los valores de x_3 e y_3, obteniendo

$$x_3 = m^2 + a_1m - a_2 - x_1 - x_2,$$
$$y_3 = -(m + a_1)\, x_3 - b - a_3.$$

Para un desarrollo detallado de estos cálculos, léase [12, III 4]. Con esto tenemos completamente descripta la operación de grupo en $E(\mathbb{K})$.

Esta descripción ofrece una demostración alternativa de lo demostrado en A.1 con Teoría de Galois, y permite demostrar, mediante la comparación de expresiones explícitas, la asociatividad de la operación de grupo en $E(\mathbb{K})$ de forma completamente elemental, sin apelar al Teorema Fundamental de Max-Noether ni a ningún concepto de la geometría algebraica. Hemos preferido exponer o referenciar las otras demostraciones dada la riqueza conceptual que subyace a las mismas, lo cual no ocurre con las aquí mencionadas.

1.4 Uso computacional de PARI/GP

No es necesario hacer los cómputos a mano, dado que tenemos a nuestra disposición el sistema de álgebra computacional `PARI/GP` y, específicamente, el paquete `elldata`, a través del cual podemos utilizar `PARI/GP` para realizar cómputos de forma rápida y sencilla en nuestras curvas elípticas[1]. El objetivo de esta sección es mostrar cómo utilizar las funciones básicas de `PARI/GP` para el cálculo en curvas elípticas. De aquí en adelante, prácticamente cualquier cálculo que involucre curvas elípticas será computado por medio de los procedimientos que detallamos a continuación.

Dada una $\mathbb{Q}$-curva elíptica en la forma 1.1, en la terminal de `PARI/GP` podemos introducir

`v=[a1,a2,a3,a4,a6]`

para generar el vector $(a_1, a_2, a_3, a_4, a_6) \in \mathbb{Q}^5$. Hecho esto, la curva elíptica 1.1 puede guardarse como

`e=ellinit(v,1)`,

lo cual nos devolverá el vector

$$(a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, b_8, c_4, c_6, \Delta, j)$$

correspondiente a las constantes que hemos definido con esas notaciones.

Para calcular el grupo de torsión, introducimos el comando

`elltors(e)`.

De esta manera, el programa nos devolverá un vector de tres coordenadas, donde la primera coordenada será el orden del grupo de torsión de la curva elíptica, la segunda coordenada ofrecerá la estructura de dicho grupo como producto de grupos cíclicos, y la tercera coordenada será el conjunto de generadores. Dichos generadores estarán dados como vectores en dos coordenadas, lo cual debe interpretarse como las coordenadas afines de los puntos en cuestión.

Para sumar dos puntos de la curva distintos del neutro, tomamos sus formas afinizadas $(a : b : 1)$ y $(c : d : 1)$ e introducimos el comando

`elladd(e,[a,b],[c,d])`.

Así, el programa nos devolverá un vector de dos coordenadas que, como siempre, debemos interpretar como las coordenadas afines de un punto de la curva. En cuanto al neutro, el mismo se representa a través del vector de una coordenada `[0]`.

Finalmente, podemos introducir el comando

`ellgenerators(e)`.

Esto nos devuelve una base de la parte libre del grupo de soluciones de la curva elíptica. Para calcular esto, `PARI/GP` hace uso de una gigantesca base de datos de curvas elípticas hecha por John Cremona[2], que está incorporada en el paquete `elldata`.

[1] Acceder a http://pari.math.u-bordeaux.fr/ para descargar `PARI/GP` y, si no viene incorporado por defecto, el paquete `elldata`.

[2] http://johncremona.github.io/ecdata/

1.5 Teorema de Poincaré-Hurwitz

La diferencia entre una curva elíptica de rango cero y una de rango positivo radica en la cantidad de soluciones que admite: una curva elíptica tiene finitas soluciones si y solo si es de rango cero. En consecuencia, muchos problemas de la teoría de números que consisten en saber si un planteo admite o no un número infinito de soluciones se resuelven modelizando dicho planteo con base en una curva elíptica para ver si existe en ella un elemento sin torsión.

En determinadas ocasiones, se requiere de algo más. Dado que varios planteos, como algunos que veremos en esta tesis, provienen de situaciones donde a las variables se les imponen condiciones adicionales, muchas veces es necesario saber si las soluciones son infinitas localmente. El Teorema de Poincaré-Hurwitz, que probaremos en esta sección, nos dice básicamente que si tenemos infinitas soluciones, dicha infinidad vale también localmente.

Requeriremos un lema previo.

Lema 1.5.1 *Todo subgrupo multiplicativo infinito de* $\mathbb{S}^1$ *es denso en* $\mathbb{S}^1$.

Demostración. Sea G un subgrupo infinito de $\mathbb{S}^1$. Sea $z \in \mathbb{S}^1$ y sea $\varepsilon > 0$. Entonces basta ver que existe un elemento $w \in G$ que está separado de z por un arco de $\mathbb{S}^1$ de longitud menor que ε; es decir, que el ángulo que forman z y w es menor que ε.

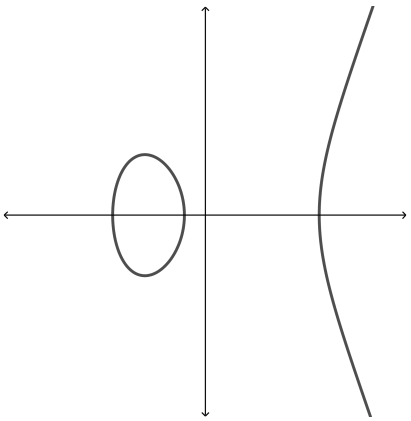
Sea $n \in \mathbb{N}$ tal que $n > \max\left\{4, \frac{\pi}{\varepsilon}\right\}$. Como G es infinito, existe un subconjunto $G' \subseteq G$ de cardinal n. En consecuencia, dispuestos los n elementos de G' en el círculo unitario, la suma de los ángulos que forman los pares adyacentes es igual a 2π. Así, existen dos elementos adyacentes $a, b \in G'$ que forman un ángulo menor o igual que $\frac{2\pi}{n}$. Más aún, como $a, b \in G$ y $a \neq b$, entonces $w := ab^{-1} \in G \setminus \{1\}$ y además es un elemento que forma un ángulo menor o igual que $\frac{2\pi}{n}$ con 1. Cambiando w por $w^{-1} = \overline{w}$ de ser necesario, supondremos que w está en el primer cuadrante, lo cual es posible pues $n > 4$. Tomamos $M \in \mathbb{N}$ tal que $M \arg(w) > 2\pi$. Entonces el conjunto $\left\{w^j : j \in [0, M] \cap \mathbb{Z}\right\}$ particiona $\mathbb{S}^1$ en arcos de longitud menor o igual que $\arg(w) \leq \frac{2\pi}{n}$, de donde z debe estar alejado de uno de estos elementos por un ángulo de longitud menor o igual que $\frac{\arg(w)}{2} \leq \frac{\pi}{n} < \varepsilon$. ■

Requeriremos, asimismo, tener presente el siguiente resultado de la geometría diferencial. Dado un grupo de Lie G, llamamos G_0 a la componente conexa de G a la cual pertenece el elemento neutro, que llamaremos 1_G. Entonces G_0 es un subgrupo de Lie de G. En efecto, es abierto por ser una componente conexa de un espacio topológico localmente conexo (toda variedad diferencial lo es), por lo tanto es una subvariedad diferencial de G. Como $G_0 \times G_0$ es conexo por ser producto de conexos, y como la función de multiplicación de grupo $\mu : G \times G \to G$ es continua, entonces la imagen por μ de $G_0 \times G_0$ es un conjunto conexo que contiene a la identidad, pues $(1_G, 1_G) \in G_0 \times G_0$ y $\mu(1_G, 1_G) = 1_G$. Como la imagen por μ de $G_0 \times G_0$ es un conjunto conexo que contiene a 1_G, necesariamente debe estar incluida en la componente conexa que contiene a 1_G, es decir, en G_0. Del mismo modo, llamamos $\iota : G \to G$ a la función de inversión de G, la cual es continua y cumple que $\iota(1_G) = 1_G$, de donde la imagen por ι de G_0 es un conjunto conexo que contiene a 1_G y por lo tanto está contenida en G_0.

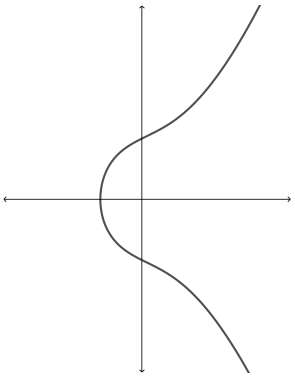
Sea E una $\mathbb{Q}$-curva elíptica dada en su forma de Weierstrass. Como la ecuación de Weierstrass de E es no singular, $E(\mathbb{R})$ define una variedad diferencial de dimensión 1. Al ser un subconjunto cerrado del espacio topológico compacto $\mathbb{P}^2(\mathbb{R})$ (recordar que $\mathbb{P}^2(\mathbb{R})$ es

homeomorfo a un cociente de $\mathbb{S}^2$ vía una acción de grupo de $\mathbb{Z}/2\mathbb{Z}$), resulta que $E(\mathbb{R})$ es compacto. Por otra parte, de los resultados en 1.3 vemos que la operación de grupo de E sobre $\mathbb{R}$ es continuamente diferenciable, con lo cual $E(\mathbb{R})$ resulta ser un grupo de Lie de dimensión 1 abeliano y compacto. Es sabido que todo grupo de Lie abeliano y conexo es isomorfo a $\mathbb{R}^m \oplus \left(\mathbb{S}^1\right)^n$ para algunos $m, n \in \mathbb{N}_0$ (léase [22, p. 87]). Como la componente conexa de $E(\mathbb{R})$ que contiene el punto del infinito es un grupo de Lie abeliano, conexo, compacto y de dimensión 1, entonces la única posibilidad es que sea isomorfa a $\mathbb{S}^1$.

Un sencillo argumento de gráfico permite ver que, transformando E vía un cambio admisible de variables en la forma $y^2 = x^3 + ax + b$, $E(\mathbb{R})$ tiene una o dos componentes conexas, dependiendo de si el polinomio $x^3 + ax + b$ tiene exactamente una o tres raíces reales, respectivamente (léase [28, p. 20]). Una forma sencilla de discriminar entre ambos casos es mirando el discriminante Δ de la curva, el cual será un número real no nulo. $E(\mathbb{R})$ será conexo si y solo si $\Delta < 0$ (léase [12, p. 60]). En tal caso, el grupo de Lie $E(\mathbb{R})$ es isomorfo a $\mathbb{S}^1$. En caso contrario (es decir, cuando $E(\mathbb{R})$ tiene dos componentes conexas), el grupo de Lie $E(\mathbb{R})$ es isomorfo a $\mathbb{S}^1 \oplus \mathbb{Z}/2\mathbb{Z}$. Esta será la próxima proposición que probaremos. Para una demostración alternativa, léase [27, p. 420].



Discriminante positivo



Discriminante negativo

Antes de demostrarla, obsérvese que el argumento de gráfico referenciado en [28] permite ver, además, que si x_0, x_1, x_2 son las tres raíces reales de $x^3 + ax + b$, entonces no es cierto que todos los puntos (afinizados) $(x_0, 0)$, $(x_1, 0)$, $(x_2, 0)$ están en la misma componente

conexa de $E(\mathbb{R})$. Debe, pues, al menos uno de esos puntos estar en la componente conexa de $E(\mathbb{R})$ que no contiene al punto del infinito. Por lo desarrollado en 1.3 (particularmente la expresión 1.3), se ve que todos estos puntos son iguales a sus opuestos aditivos. En otras palabras, hemos demostrado con esto que existe un elemento de orden 2 en la componente conexa de $E(\mathbb{R})$ que no contiene al punto del infinito. Esto será crucial para la demostración de la proposición que buscamos probar. Antes, veamos dos lemas previos.

Lema 1.5.2 *Sea E una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{R})$ admite dos componentes conexas. Sea $E_0(\mathbb{R})$ la componente conexa que contiene al punto del infinito, y sea $E_1(\mathbb{R})$ la otra componente conexa. Dados $P, Q \in E_1(\mathbb{R})$, se tiene que $P+Q \in E_0(\mathbb{R})$ y $-P \in E_1(\mathbb{R})$.*

Demostración. Fijamos $P \in E_1(\mathbb{R})$. Veamos que $P+Q \in E_0(\mathbb{R})$ para todo $Q \in E_1(\mathbb{R})$. En efecto, es claro que $-P \in E_1(\mathbb{R})$, pues de lo contrario, como $E_0(\mathbb{R})$ es un subgrupo de $E(\mathbb{R})$, se tendría $P = -(-P) \in E_0(\mathbb{R})$, contrario a nuestras hipótesis. Así, la función $\psi : E(\mathbb{R}) \to E(\mathbb{R})$ que a cada $Q \in E(\mathbb{R})$ le asigna $P+Q \in E(\mathbb{R})$ es una función diferenciable y, además, cumple que $\psi(-P) = (0:1:0) \in E_0(\mathbb{R})$. Es decir, le asigna a un elemento de $E_1(\mathbb{R})$ un valor en $E_0(\mathbb{R})$. Como $E_1(\mathbb{R})$ es conexo, su imagen por ψ es un conjunto conexo que deberá, en consecuencia, estar incluido en alguna de las componentes conexas de $E(\mathbb{R})$, y como $\psi(P) \in E_0(\mathbb{R})$, entonces la imagen por ψ de $E_1(\mathbb{R})$ está contenida en $E_0(\mathbb{R})$, como queríamos. ■

Lema 1.5.3 *Sea E una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{R})$ admite dos componentes conexas. Sea $E_0(\mathbb{R})$ la componente conexa que contiene al punto del infinito, y sea $E_1(\mathbb{R})$ la otra componente conexa. Dados $P \in E_0(\mathbb{R})$ y $Q \in E_1(\mathbb{R})$, se tiene que $P+Q \in E_1(\mathbb{R})$.*

Demostración. Si fuera $P+Q \in E_0(\mathbb{R})$, entonces, como $E_0(\mathbb{R})$ es un subgrupo de $E(\mathbb{R})$, se tendría $Q = (P+Q) - P \in E_0(\mathbb{R})$, contrario a nuestras hipótesis. ■

Veamos, pues, cómo hallar la estructura de grupo de Lie de $E(\mathbb{R})$ para una $\mathbb{Q}$-curva elíptica E de discriminante positivo.

Proposición 1.5.4 *Sea E una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{R})$ admite dos componentes conexas. Entonces existe un isomorfismo de grupos de Lie $E(\mathbb{R}) \cong \mathbb{S}^1 \oplus \mathbb{Z}/2\mathbb{Z}$ que identifica la componente conexa que contiene al punto del infinito con $\mathbb{S}^1 \times \{0\}$ e identifica la otra componente conexa con $\mathbb{S}^1 \times \{1\}$.*

Demostración. Sea $E_0(\mathbb{R})$ la componente conexa que contiene al punto del infinito, y sea $E_1(\mathbb{R})$ la otra componente conexa. Sabemos que existe un isomorfismo de grupos de Lie $\varphi : E_0(\mathbb{R}) \to \mathbb{S}^1$. Sabemos también que existe un punto $P \in E_1(\mathbb{R})$ de orden 2.

Por el Lema 1.5.2 tenemos una función $\Psi : E(\mathbb{R}) \to \mathbb{S}^1 \oplus \mathbb{Z}/2\mathbb{Z}$ bien definida como

$$\Psi(Q) := \begin{cases} (\varphi(Q), 0), & Q \in E_0(\mathbb{R}), \\ (\varphi(P+Q), 1), & Q \in E_1(\mathbb{R}). \end{cases}$$

Veamos que Ψ es inyectiva. En efecto, mirando la coordenada de $\mathbb{Z}/2\mathbb{Z}$ vemos que el valor por Ψ de un punto de $E_0(\mathbb{R})$ jamás puede igualar al valor por Ψ de un elemento de $E_1(\mathbb{R})$. Dos puntos distintos $Q, Q' \in E_0(\mathbb{R})$ no pueden tener el mismo valor por Ψ pues la biyectividad de φ nos diría que $Q = Q'$. Dos puntos distintos $R, R' \in E_1(\mathbb{R})$ no pueden

tener el mismo valor por Ψ pues la biyectividad de φ nos diría que $P+R=P+R'$, de donde $R=R'$.

Veamos que Ψ es sobreyectiva. Dado $(x,0)\in\mathbb{S}^1\oplus\mathbb{Z}/2\mathbb{Z}$, existe $Q\in E_0(\mathbb{R})$ tal que $\varphi(Q)=x$, luego $\Psi(Q)=(x,0)$. Por otro lado, dado $(y,1)\in\mathbb{S}^1\oplus\mathbb{Z}/2\mathbb{Z}$, existe $R\in E_0(\mathbb{R})$ tal que $\varphi(R)=y$. Por el Lema 1.5.2 se tiene $-P\in E_1(\mathbb{R})$, y por el Lema 1.5.3 se tiene $R-P\in E_1(\mathbb{R})$. Así, $\Psi(R-P)=(y,1)$.

Veamos que Ψ es diferenciable. Basta ver que componiendo Ψ con las proyecciones de $\mathbb{S}^1\oplus\mathbb{Z}/2\mathbb{Z}$ a $\mathbb{S}^1$ y $\mathbb{Z}/2\mathbb{Z}$ obtenemos funciones diferenciables. En cuanto a la composición con la proyección a $\mathbb{Z}/2\mathbb{Z}$, la función resulta constante en cada componente conexa de $E(\mathbb{R})$, por lo tanto es trivialmente diferenciable. Por otro lado, en cuanto a la composición con la proyección a $\mathbb{S}^1$, por el lema del pegado basta ver que la función resultante restringida a cada elemento de un cubrimiento por abiertos de $E(\mathbb{R})$ es diferenciable. Como $E(\mathbb{R})$ es una variedad diferencial, es un espacio topológico localmente conexo, con lo cual podemos tomar el cubrimiento por abiertos dado por sus componentes conexas. Restringiéndonos a $E_0(\mathbb{R})$ obtenemos la función φ, que es diferenciable por ser un isomorfismo de grupos de Lie. Restringiéndonos a $E_1(\mathbb{R})$, obtenemos la composición entre φ y la traslación por P, los cuales son ambos diferenciables.

Finalmente, veamos que Ψ es un morfismo de grupos. Sean $Q,R\in E(\mathbb{R})$. Queremos ver que $\Psi(Q+R)=\Psi(Q)+\Psi(R)$. Separaremos en casos.

Si $Q,R\in E_0(\mathbb{R})$, entonces $Q+R\in E_0(\mathbb{R})$, pues $E_0(\mathbb{R})$ es un subgrupo de $E(\mathbb{R})$. Así,

$$\Psi(Q+R)=(\varphi(Q+R),0)=(\varphi(Q)+\varphi(R),0)=(\varphi(Q),0)+(\varphi(R),0)=\Psi(Q)+\Psi(R),$$

donde hemos usado que $\varphi(Q+R)=\varphi(Q)+\varphi(R)$ pues φ es un isomorfismo de grupos.

Si $Q\in E_0(\mathbb{R})$ y $R\in E_1(\mathbb{R})$, por el Lema 1.5.3 se tiene $Q+R\in E_1(\mathbb{R})$, luego

$$\Psi(Q+R)=(\varphi(P+Q+R),1)=(\varphi(P+R)+\varphi(Q),1)=$$
$$=(\varphi(Q),0)+(\varphi(P+R),1)=\Psi(Q)+\Psi(R),$$

donde hemos escrito $\varphi(P+Q+R)=\varphi(P+R)+\varphi(Q)$ porque φ es un morfismo de grupos y $P+R\in E_0(\mathbb{R})$ por el Lema 1.5.2.

Finalmente, si $Q,R\in E_1(\mathbb{R})$, por el Lema 1.5.2 se tiene $Q+R\in E_0(\mathbb{R})$, luego

$$\Psi(Q+R)=(\varphi(Q+R),0)=(\varphi(P+Q+P+R),0)=(\varphi(P+Q)+\varphi(P+R),0)=$$
$$=(\varphi(P+Q),1)+(\varphi(P+R),1)=\Psi(Q)+\Psi(R),$$

donde hemos escrito $Q+R=P+Q+P+R$ porque P tiene orden 2 por definición. Además, como $P+Q,P+R\in E_0(\mathbb{Q})$ por el Lema 1.5.2, entonces que φ sea morfismo de grupos justifica la igualdad $\varphi(P+Q+P+R)=\varphi(P+Q)+\varphi(P+R)$. ■

Supongamos que E es una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{R})$ admite dos componentes conexas. Sea $E_0(\mathbb{R})$ la componente conexa que contiene al punto del infinito, es decir, la que se identifica con $\mathbb{S}^1\times\{0\}$; y sea $E_1(\mathbb{R})$ la otra componente conexa, es decir, la que se identifica con $\mathbb{S}^1\times\{1\}$. Entonces $E_0(\mathbb{R})$ es un subgrupo de $E(\mathbb{R})$, mientras que $E_1(\mathbb{R})$ no lo es. Sin embargo, la estructura de grupo de $\mathbb{S}^1\oplus\mathbb{Z}/2\mathbb{Z}$ nos dice que ambos conjuntos son cerrados por tomar inverso aditivo en la operación de cúbicas de E.

Dados $i,j\in\{0,1\}$ se tiene, por la estructura de grupo de $\mathbb{S}^1\oplus\mathbb{Z}/2\mathbb{Z}$,

$$E_i(\mathbb{R})+E_j(\mathbb{R})\subseteq\begin{cases}E_0(\mathbb{R}), & i=j,\\ E_1(\mathbb{R}), & i\neq j.\end{cases}\tag{1.4}$$

Dado $i \in \{0,1\}$, definimos $E_i(\mathbb{Q}) := E_i(\mathbb{R}) \cap E(\mathbb{Q})$. Como $E(\mathbb{Q})$ es un subgrupo de $E(\mathbb{R}) = E_0(\mathbb{R}) \cup E_1(\mathbb{R})$, entonces $E(\mathbb{Q}) = E_0(\mathbb{Q}) \cup E_1(\mathbb{Q})$.

Llamemos *componente principal de* E al conjunto $E_0(\mathbb{R})$, y llamemos *componente secundaria de* E al conjunto $E_1(\mathbb{R})$.

Nuestro primer resultado importante para demostrar el Teorema de Poincaré-Hurwitz será ver que si $E(\mathbb{Q})$ es infinito, entonces $E_0(\mathbb{Q})$ también lo es.

Lema 1.5.5 *Sea E una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{R})$ admite dos componentes conexas y el grupo $E(\mathbb{Q})$ es infinito. Entonces $E_0(\mathbb{Q})$ es infinito.*

Demostración. Como $E(\mathbb{Q}) = E_0(\mathbb{Q}) \cup E_1(\mathbb{Q})$ es infinito, existe $i \in \{0,1\}$ tal que $E_i(\mathbb{Q})$ es infinito. Si $i = 0$, no hay nada que probar. Si $i = 1$, fijamos $P \in E_1(\mathbb{Q})$. Por 1.4 y el hecho de que $E(\mathbb{Q})$ es un subgrupo de $E(\mathbb{R})$, tenemos una función $E_1(\mathbb{Q}) \to E_0(\mathbb{Q})$ bien definida que a cada $Q \in E_1(\mathbb{Q})$ le asigna $P + Q \in E_0(\mathbb{Q})$. Esta función es inyectiva por ser una traslación de grupo; por lo tanto, como $E_1(\mathbb{Q})$ es infinito, $E_0(\mathbb{Q})$ lo es. ■

En principio, no podemos decir que ocurra lo mismo con las componentes secundarias. Considérese, por ejemplo, la curva en forma de Weierstrass $y^2z = x^3 - 12xz^2 - z^3$, cuyo discriminante es $110160 > 0$. Esta curva elíptica tiene grupo de torsión trivial y parte libre de rango 1 generada por $(5:8:1)$, el cual está en la componente principal de la curva. Así, todos los puntos de $\mathbb{P}^2(\mathbb{Q})$ en dicha curva están sobre la componente principal, y la componente secundaria no tiene ningún punto en $\mathbb{P}^2(\mathbb{Q})$.

Sin embargo, sí es posible demostrar lo siguiente.

Lema 1.5.6 *Sea E una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{R})$ admite dos componentes conexas y el grupo $E(\mathbb{Q})$ es infinito. Entonces $E_1(\mathbb{Q})$ es o bien vacío o bien infinito.*

Demostración. Si $E_1(\mathbb{Q})$ no es vacío, fijamos $P \in E_1(\mathbb{Q})$. Por el Lema 1.5.5 sabemos que $E_0(\mathbb{Q})$ es infinito, de donde la función inyectiva $E_0(\mathbb{Q}) \to E_1(\mathbb{Q})$ que a cada $Q \in E_0(\mathbb{Q})$ le asigna $P + Q \in E_1(\mathbb{Q})$ (bien definida por 1.4) nos garantiza que $E_1(\mathbb{Q})$ es infinito. ■

Estamos, finalmente, en condiciones de probar el Teorema de Poincaré-Hurwitz.

Teorema 1.5.7 *Sea E una $\mathbb{Q}$-curva elíptica tal que $E(\mathbb{Q})$ es infinito, y sea $\Delta \in \mathbb{R}$ su discriminante.*

(a) Si $\Delta < 0$, entonces $E(\mathbb{Q})$ es denso en $E(\mathbb{R})$.

(b) Si $\Delta > 0$ y $E_1(\mathbb{Q})$ es vacío, entonces $E(\mathbb{Q})$ es denso en $E_0(\mathbb{R})$.

(c) Si $\Delta > 0$ y $E_1(\mathbb{Q})$ es infinito, entonces $E(\mathbb{Q})$ es denso en $E(\mathbb{R})$.

En particular, dado un abierto U de $\mathbb{P}^2(\mathbb{R})$ tal que $U \cap E(\mathbb{Q}) \neq \emptyset$, se tiene que $U \cap E(\mathbb{Q})$ es un conjunto infinito.

Demostración. Veamos cada uno de los ítems.

(a) Si $E(\mathbb{R})$ admite exactamente una componente conexa, $E(\mathbb{R})$ es isomorfo a $\mathbb{S}^1$ como grupo de Lie. Así, $E(\mathbb{Q})$ se identifica con un subgrupo infinito de $\mathbb{S}^1$, de donde resulta denso por el Lema 1.5.1.

(b) Si $E(\mathbb{R})$ admite dos componentes conexas y $E_1(\mathbb{Q})$ es vacío, entonces $E(\mathbb{Q})$ es un subgrupo infinito de $E_0(\mathbb{R})$, que es isomorfo a $\mathbb{S}^1$ como grupo de Lie. Nuevamente, el Lema 1.5.1 nos da el resultado buscado.

(c) Si $E(\mathbb{R})$ admite dos componentes conexas y $E_1(\mathbb{Q})$ es infinito, por el Lema 1.5.5 $E_0(\mathbb{Q})$ es un subgrupo infinito de $E_0(\mathbb{R})$, que es isomorfo a $\mathbb{S}^1$ como grupo de Lie. Así, por el Lema 1.5.1 se tiene que $E_0(\mathbb{Q})$ es denso en $E_0(\mathbb{R})$. Finalmente, sea $P \in E_1(\mathbb{R})$ y veamos que existe una sucesión $\{P_n\}_{n\in\mathbb{N}} \subseteq E_1(\mathbb{Q})$ tal que $\lim_{n\to+\infty} P_n = P$. Sea $R \in E_1(\mathbb{Q})$. Como $P \in E_1(\mathbb{R})$, entonces 1.4 nos dice que $P+R \in E_0(\mathbb{R})$. Como $E_0(\mathbb{Q})$ es denso en $E_0(\mathbb{R})$, existe una sucesión $\{Q_n\}_{n\in\mathbb{N}} \subseteq E_0(\mathbb{Q})$ tal que $\lim_{n\to+\infty} Q_n = P+R$. Por 1.4 y el hecho de que las componentes principal y secundaria son cerradas por tomar inverso, para cada $n \in \mathbb{N}$ se tiene $P_n := Q_n - R \in E_1(\mathbb{Q})$ y $\lim_{n\to+\infty} P_n = P+R-R = P$. ■

Para finalizar, veamos la última parte del teorema. Sea U un abierto de $\mathbb{P}^2(\mathbb{R})$ que admite al menos un punto de $E(\mathbb{Q})$. Como $E(\mathbb{R})$ es una variedad diferencial de dimensión 1 y $\widetilde{U} := U \cap E(\mathbb{R})$ es un abierto no vacío de la misma, entonces $\widetilde{U}$ es una subvariedad diferencial de dimensión 1. Así, admite infinitos elementos. Separaremos en casos.

Si $E(\mathbb{R})$ admite exactamente una componente conexa, por el ítem (a) $\widetilde{U} \cap E(\mathbb{Q})$ es denso en $\widetilde{U}$. Si $\widetilde{U} \cap E(\mathbb{Q})$ fuera finito, en particular sería cerrado. Pero un cerrado finito no puede ser denso en un conjunto infinito. En consecuencia, $\widetilde{U} \cap E(\mathbb{Q})$ debe ser infinito; es decir, hay infinitos puntos de $E(\mathbb{Q})$ en $\widetilde{U} \subseteq U$.

Si $E(\mathbb{R})$ admite dos componentes conexas, definimos $\widetilde{U}_i := \widetilde{U} \cap E_i(\mathbb{R})$ para $i \in \{0,1\}$. Como $E(\mathbb{R})$ es una variedad diferencial, es un espacio topológico localmente conexo, de donde sus componentes conexas son abiertas. Así, $\widetilde{U}_1$ y $\widetilde{U}_2$ son abiertos de $E(\mathbb{R})$ y $\widetilde{U} = \widetilde{U}_1 \cup \widetilde{U}_2$. Como $\widetilde{U} \cap E(\mathbb{Q}) = U \cap E(\mathbb{R}) \cap E(\mathbb{Q}) = U \cap E(\mathbb{Q}) \neq \emptyset$, entonces alguno de los conjuntos $\widetilde{U}_1$ y $\widetilde{U}_2$ tiene intersección no vacía con $E(\mathbb{Q})$. Sea $i \in \{0,1\}$ tal que $\widetilde{U}_i \cap E(\mathbb{Q}) \neq \emptyset$. En particular, $\widetilde{U}_i$ es una subvariedad diferencial de dimensión 1 de $E(\mathbb{R})$, y por lo tanto es un conjunto infinito. Según sea el caso, aplicamos el ítem (b) ó (c) para afirmar que $\widetilde{U}_i \cap E(\mathbb{Q})$ es denso en $\widetilde{U}_i$. Esto implica que $\widetilde{U}_i \cap E(\mathbb{Q})$ no puede ser un conjunto finito, pues sería cerrado y, por lo tanto, no sería denso en el conjunto infinito $\widetilde{U}_i$. Se sigue que debe haber infinitos puntos de $E(\mathbb{Q})$ en $\widetilde{U}_i \subseteq \widetilde{U} \subseteq U$. ■

1.6 Ejemplos de aplicación

En esta sección veremos algunas de las aplicaciones inmediatas de la teoría elemental de curvas elípticas. Ofreceremos dos aplicaciones puramente aritméticas y, dado el interés principal de esta tesis, mostraremos, a modo de introducción, una aplicación al tipo de problemas geométricos que buscamos atacar.

1.6.1 El Último Teorema de Fermat para exponente 3

Conocido es el *Último Teorema de Fermat*, en virtud del cual no es posible hallar $(a,b,c) \in \mathbb{N}^3$ y $n \in \mathbb{N}_{\geq 3}$ tales que

$$a^n + b^n = c^n.$$

La teoría de curvas elípticas jugó un rol fundamental en la demostración que a fines del siglo XX Andrew Wiles ofreció a la comunidad matemática. Veremos aquí cómo resolver el caso particular de este resultado en el que $n = 3$.

En otras palabras, buscamos probar que no es posible que la suma de dos cubos perfectos positivos iguale a un cubo perfecto. Dado que la ecuación $a^3 + b^3 = c^3$ es homogénea en las variables a, b, c, este problema equivale a mostrar que no es posible hallar $a, b, c \in \mathbb{Q}_{>0}$ tales que $a^3 + b^3 = c^3$. En particular, es posible pensar esta ecuación en $\mathbb{P}^2(\mathbb{Q})$.

Afinizando la ecuación respecto de la variable c; lo cual es válido pues buscamos soluciones con coordenadas estrictamente positivas, obtenemos la ecuación $X^3 + Y^3 = 1$, de la cual buscamos soluciones en los racionales positivos. El siguiente resultado nos dice que esto no es posible.

Proposición 1.6.1 *Si $X, Y \in \mathbb{Q}$ y $X^3 + Y^3 = 1$, entonces $XY = 0$.*

Demostración. Sean $X, Y \in \mathbb{Q}$ tales que $X^3 + Y^3 = 1$. Si $Y = 1$, entonces $X = 0$ y no hay nada que probar. Suponemos entonces que $Y \neq 1$ y definimos

$$x := \tfrac{3X}{1-Y}, \qquad y := \tfrac{9}{1-Y}. \tag{1.5}$$

De esto se sigue que $X = \frac{1-Y}{3}x = \frac{3x}{y}$ y que $1 - Y = \frac{9}{y}$, de donde $Y = 1 - \frac{9}{y} = \frac{y-9}{y}$. Sustituyendo en la expresión $X^3 + Y^3 = 1$ obtenemos

$$\left(\frac{3x}{y}\right)^3 + \left(\frac{y-9}{y}\right)^3 = 1$$

$$27x^3 + y^3 - 27y^2 + 243y - 729 = y^3$$

$$x^3 - y^2 + 9y - 27 = 0$$

$$y^2 - 9y = x^3 - 27. \tag{1.6}$$

La ecuación 1.6 está en la forma de Weierstrass afinizada y su discriminante es $-19683 \neq 0$. Esta curva elíptica tiene rango nulo y grupo de torsión

$$\{(0:1:0), (3:9:1), (3:0:1)\}.$$

Por consiguiente, $(x, y) \in \{(3, 9), (3, 0)\}$. Pero la segunda expresión en 1.5 implica trivialmente que $y \neq 0$, por lo tanto $(x, y) = (3, 9)$. Pero entonces $Y = \frac{y-9}{9} = 0$, y por lo tanto $XY = 0$, como queríamos. ■

Observación 1.6.2 La elección de los cambios de variable definidos en 1.5 no es arbitraria: puede obtenerse por medio de una elección adecuada de cambios proyectivos de coordenadas que transformen la curva $\left\{(x:y:z) \in \mathbb{P}^2(\mathbb{Q}) : x^3 + y^3 = z^3\right\}$ en una cúbica que tenga un punto de inflexión en $(0:1:0)$ y cuya recta tangente en dicho punto sea $\{z = 0\}$, en vistas a obtener una cúbica en la forma 1.1. Para más detalles, léase [12, pp. 50-52].

1.6.2 Una variante de la Conjetura de Euler

En el año 1769 Euler conjeturó que no es posible hallar $n \in \mathbb{N}_{\geq 3}$ y un conjunto de n números naturales $\{a_i : i \in [1, n] \cap \mathbb{N}\} \subseteq \mathbb{N}$ tales que

$$\sum_{i=1}^{n-1} a_i^n = a_n^n$$

Esto se conoce como la *Conjetura de Euler*. Obsérvese que el caso en que $n = 3$ corresponde al caso particular del *Último Teorema de Fermat* que resolvimos en la sección anterior.

Es sabido que la conjetura es falsa para $n = 4$ y que, de hecho, hay infinitos contraejemplos. En cuanto a $n = 5$, también se han encontrado contraejemplos para la conjetura. Sin embargo, para exponente $n \geq 6$ continúa siendo un problema abierto.

En el año 2013 los matemáticos Tianxin Cai y Yong Zhang [5] intentaron encontrar un contraejemplo de la Conjetura de Euler para exponente 6 considerando el siguiente problema: determinar si existen $n, b \in \mathbb{N}$ tales que $n \geq 2$ y un conjunto de n números naturales $\{a_i : i \in [1, n] \cap \mathbb{N}\} \subseteq \mathbb{N}$ tales que

$$\left(\prod_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} a_i\right) = b^{n+1}.$$

Está claro que, si tomamos un contraejemplo de la Conjetura de Euler para exponente $n+1$, digamos, $\{b_i : i \in [1, n+1] \cap \mathbb{N}\} \subseteq \mathbb{N}$ tal que $\sum_{i=1}^{n} b_i^{n+1} = b_{n+1}^{n+1}$, entonces podemos tomar $a_i := b_i^{n+1}$ para cada $i \in [1, n+1] \cap \mathbb{N}$ y $b := \prod_{i=1}^{n+1} b_i$, obteniendo así una solución al problema planteado por Tianxin Cai y Yong Zhang.

En el artículo referenciado, si bien no lograron dar con el buscado contraejemplo, Tianxin Cai y Yong Zhang lograron probar, mediante la utilización de la teoría de curvas elípticas, que su problema no admite solución para $n = 2$ y que admite infinitas soluciones para $n \in \mathbb{N}_{\geq 3}$. Mostraremos aquí una demostración ligeramente distinta a la presentada por Tianxin Cai y Yong Zhang para la primera aserción.

Teorema 1.6.3 *No es posible hallar $a_1, a_2, b \in \mathbb{N}$ tales que $a_1 a_2 (a_1 + a_2) = b^3$.*

Demostración. Supongamos que existen $a_1, a_2, b \in \mathbb{N}$ tales que $a_1 a_2 (a_1 + a_2) = b^3$.

Reescribimos la expresión como

$$\frac{a_1}{b}\frac{a_2}{b}\left(\frac{a_1}{b} + \frac{a_2}{b}\right) = 1.$$

Para $i \in \{1, 2\}$ definimos $b_i := \frac{a_i}{b}$, de modo que $b_1 b_2 (b_1 + b_2) = 1$; o, equivalentemente,

$$\left(\frac{b_1}{b_2}\right)^2 + \frac{b_1}{b_2} = \frac{1}{b_2^3}.$$

Definimos $u := \frac{b_1}{b_2}$ y $v := \frac{1}{b_2}$, de donde $u^2 + u = v^3$. Finalmente, definiendo $y := 8u + 4$ y $x := 4v$, obtenemos

$$\left(\frac{y-4}{8}\right)^2 + \frac{y-4}{8} = \left(\frac{x}{4}\right)^3$$
$$y^2 - 8y + 16 + 8(y-4) = x^3$$
$$y^2 = x^3 + 16.$$

Esta curva elíptica afinizada tiene rango 0 y discriminante $-110592 \neq 0$, y su grupo de torsión es

$$\{(0:1:0), (0:4:1), (0:-4:1)\}.$$

En cualquier caso se tiene $x = 0$, de donde $v = 0$. Pero $v = \frac{1}{b_2}$, por lo tanto estamos ante un absurdo. ■

1.6.3 Ternas de naturales con igual suma y producto

Decimos que un conjunto $S \subseteq \mathbb{N}^3$ es *primitivo* si el máximo común divisor entre todas las coordenadas de todos sus elementos es igual a 1. Dado $n \in \mathbb{N}$, nos preguntamos si es posible hallar infinitos subconjuntos primitivos de $\mathbb{N}^3$ de cardinal n tales que todos sus elementos tengan la misma suma y el mismo producto de sus coordenadas. Este fue un problema abierto hasta el año 1996, cuando el matemático Andrzej Schinzel resolvió el problema utilizando técnicas de curvas elípticas [23].

El primer paso consiste en trasladar el problema hacia una formulación que nos permita realizar cambios de variable para obtener curvas elípticas. En esto radica el corazón de la demostración de A. Schinzel.

Lema 1.6.4 *Existen infinitos* $(x_1, x_2, x_3) \in \mathbb{Q}^3_{>0}$ *tales que*

$$x_1 + x_2 + x_3 = x_1x_2x_3 = 6$$

Demostración. La ecuación en forma de Weierstrass afinizada $E : y^2 = x^3 - 9x + 9$ tiene discriminante $11664 > 0$. Esta curva elíptica tiene rango 1, siendo su grupo libre generado por $(-3 : 3 : 1)$. En particular, E admite infinitas soluciones. Alternativamente, el punto afinizado $(7, 17)$ pertenece a E y, como $0 \neq 17^2 \nmid 11664$, por el ítem (d) del Teorema 1.2.3 se sigue que $(7, 17)$ es un punto sin torsión.

Sea (x_0, y_0) una solución afinizada de E tal que $|y_0| < 6 - 3x_0$. En particular, se tiene $0 \leq |y_0| < 6 - 3x_0$, de donde $x_0 < 2 < 3$. Definimos

$$x_1 := \tfrac{6}{3-x_0}, \quad x_2 := \tfrac{6-3x_0+y_0}{3-x_0}, \quad x_3 := \tfrac{6-3x_0-y_0}{3-x_0}$$

y observamos que, como $|y_0| < 6 - 3x_0$ y $x_0 < 3$, entonces $6 - 3x_0 \pm y_0 > 0$ y $3 - x_0 > 0$, luego $x_j > 0$ para todo $j \in \{1, 2, 3\}$. Además,

$$x_1 + x_2 + x_3 = \frac{6 + 6 - 3x_0 + y_0 + 6 - 3x_0 - y_0}{3 - x_0} = \frac{6\,(3 - x_0)}{3 - x_0} = 6,$$

$$x_1x_2x_3 = \frac{6\,(6 - 3x_0 + y_0)\,(6 - 3x_0 - y_0)}{(3 - x_0)^3} = \frac{6\left[(6 - 3x_0)^2 - y_0^2\right]}{(3 - x_0)^3} =$$

$$= \frac{6\left[(6 - 3x_0)^2 - \left(x_0^3 - 9x_0 + 9\right)\right]}{(3 - x_0)^3} = \frac{6\,(3 - x_0)^3}{(3 - x_0)^3} = 6.$$

En otras palabras, para cada punto de E en el abierto inducido por la inecuación $|y| < 6-3x$, obtenemos una solución del sistema del enunciado. Además, dos puntos distintos de E en dicho abierto inducen, de esta forma, dos soluciones distintas del sistema del enunciado. En efecto, si (x_0', y_0') es otra solución afinizada de E tal que $|y_0'| < 6 - 3x_0'$ y

$$\left(\frac{6}{3 - x_0}, \frac{6 - 3x_0 + y_0}{3 - x_0}, \frac{6 - 3x_0 - y_0}{3 - x_0}\right) = \left(\frac{6}{3 - x_0'}, \frac{6 - 3x_0' + y_0'}{3 - x_0'}, \frac{6 - 3x_0' - y_0'}{3 - x_0'}\right),$$

entonces, mirando la primera coordenada, se tiene $x_0 = x_0'$ y, usando esta igualdad y mirando la segunda coordenada, obtenemos $y_0 = y_0'$.

Como el punto afinizado $(0, 3)$ pertenece a E y pertenece al abierto determinado por la inecuación $|y| < 6 - 3x$, en virtud del Teorema 1.5.7 concluimos que E admite infinitas soluciones en dicho abierto. De lo anterior se sigue que cada una de ellas induce una solución diferente del sistema de ecuaciones del enunciado. ■

El teorema buscado resulta un corolario elemental del lema anterior.

Teorema 1.6.5 *Sea $n \in \mathbb{N}$. Existen infinitos subconjuntos primitivos de $\mathbb{N}^3$ con n elementos tales que todos sus elementos tienen la misma suma de coordenadas y tienen el mismo producto de coordenadas.*

Demostración. Para cada $m \in \mathbb{N}$ tomamos un conjunto $S_m \subseteq \mathbb{Q}^3_{>0}$ de exactamente n soluciones del sistema $x_1 + x_2 + x_3 = x_1x_2x_3 = 6$, de tal forma que los conjuntos tomados son distintos dos a dos. En virtud del Lema 1.6.4, esto es posible.

Para cada $m \in \mathbb{N}$ numeramos el conjunto S_m de la forma

$$S_m = \{(x_{mi1}, x_{mi2}, x_{mi3}) : i \in [1, n] \cap \mathbb{N}\}$$

y definimos d_m como el mínimo común múltiplo de los denominadores de las coordenadas de todos los elementos de S_m escritos como fracción irreducible, de tal forma que, cualquiera sea $i \in [1, n] \cap \mathbb{N}$ y cualquiera sea $j \in \{1, 2, 3\}$, se tiene $x_{mij} = \frac{a_{mij}}{d_m}$ para algún $a_{mij} \in \mathbb{N}$. Así, los elementos del conjunto $\{d_m\} \cup \{a_{mij} : i \in [1, n] \cap \mathbb{N}, j \in \{1, 2, 3\}\}$ son coprimos. Se cumple, entonces, para cada $i \in [1, n] \cap \mathbb{N}$,

$$\sum_{j=1}^{3} a_{mij} = 6d_m, \quad \prod_{j=1}^{3} a_{mij} = 6d_m^3. \tag{1.7}$$

Definimos $T_m := \{(a_{mi1}, a_{mi2}, a_{mi3}) : i \in [1, n] \cap \mathbb{N}\} \subseteq \mathbb{N}^3$ para cada $m \in \mathbb{N}$. Estos son conjuntos de cardinal n que, por 1.7, cumplen que todos sus elementos tienen la misma suma de coordenadas y el mismo producto de coordenadas. Si existieran $m, k \in \mathbb{N}$ tales que $T_m = T_k$, entonces por 1.7 se tendría $d_m = d_k$, de donde $S_m = S_k$ y por lo tanto $m = k$. En consecuencia, solamente nos falta demostrar que T_m es primitivo para todo $m \in \mathbb{N}$.

En efecto, supongamos que existe $m \in \mathbb{N}$ y un primo $p \in \mathbb{N}$ tal que $p \mid a_{mij}$ para todo $i \in [1, n] \cap \mathbb{N}$ y $j \in \{1, 2, 3\}$. Por 1.7 se tiene $p^3 \mid 6d_m^3$, de donde $p \mid d_m$ pues 6 es libre de cubos. Pero los elementos del conjunto $\{d_m\} \cup \{a_{mij} : i \in [1, n] \cap \mathbb{N}, j \in \{1, 2, 3\}\}$ son coprimos, por lo tanto esto es imposible. ■

Observación 1.6.6 Del último párrafo de la demostración anterior se ve que la importancia del número 6 del Lema 1.6.4 radica en que 6 es libre de cubos. Si pudiese demostrarse un análogo del Lema 1.6.4 cambiando el número 6 por algún otro número natural libre de cubos, la demostración anterior seguiría funcionando perfectamente.

1.6.4 Aplicación aritmética-euclídea

En vistas al objetivo de esta tesis, veamos una (restrictiva) variante de nuestro resultado principal para ilustrar el uso de la teoría de curvas elípticas en aspectos aritméticos de la geometría euclídea. Seguiremos a Shane Chern en [6], haciendo unos leves cambios.

Un polígono se dice *entero* si la longitud de sus lados es entera. Análogamente, un polígono se dice *racional* si la longitud de sus lados es racional. Obsérvese que todo polígono racional es semejante a un polígono entero.

Sea $ABCD$ un rombo y sea $\theta \in \mathbb{R}$ tal que $0 < \theta < \frac{\pi}{2}$. Decimos que $ABCD$ es *θ-entero* si $ABCD$ es entero, $\angle BAD = \theta$ y, además, $\sin(\theta), \cos(\theta) \in \mathbb{Q}$. Análogamente, decimos que $ABCD$ es *θ-racional* si $ABCD$ es racional, $\angle BAD = \theta$ y, además, $\sin(\theta), \cos(\theta) \in \mathbb{Q}$. Obsérvese que en ambos casos se pide $\sin(\theta), \cos(\theta) \in \mathbb{Q}$.

En atención al tipo de resultados que perseguimos, es natural preguntarse si es posible encontrar un triángulo rectángulo entero y un rombo θ-entero para algún $\theta \in \left(0, \frac{\pi}{2}\right)$, de tal forma que ambas figuras tengan la misma área y el mismo perímetro.

En caso de existir, es también natural preguntarse si la cantidad de soluciones a este problema es finita o infinita. En principio, está claro que, en caso de existir una solución, existen infinitas; pues basta con reescalar las figuras por un factor entero para obtener soluciones con figuras semejantes a la solución original. Esto no resulta muy interesante. En consecuencia, podemos trabajar con soluciones sin distinguir semejanzas, y volver a preguntarnos si las soluciones son finitas o infinitas.

En esta sección veremos que estas soluciones existen y son infinitas. Concretamente, modelizaremos el problema de tal forma que el hecho de no distinguir soluciones por semejanza se traducirá en trabajar con coordenadas proyectivas, y la cuestión de la cantidad de soluciones se verá por medio de un análisis del rango de una curva elíptica adecuada.

Obsérvese que encontrar estos pares de polígonos enteros equivale a encontrar pares definidos de forma análoga pero cambiando la hipótesis de *polígonos enteros* por *polígonos racionales*, dada nuestra consideración sobre las semejanzas. Comenzaremos, pues, buscando una forma de describir los triángulos rectángulos racionales.

Triángulos rectángulos racionales

Por el Teorema de Pitágoras, podemos identificar a los triángulos rectángulos racionales con aquellos $(x, y, z) \in \mathbb{Q}^3_{>0}$ tales que $x^2 + y^2 = z^2$, suponiendo ordenados los catetos.

Dado que nos interesa analizar dichos triángulos a menos de semejanza, podemos identificar estas clases de semejanza con elementos $(x : y : z) \in \mathbb{P}^2(\mathbb{Q})$ que admiten una representación en coordenadas proyectivas donde todas estas son positivas, y que cumplen la ecuación homogénea $x^2 + y^2 = z^2$.

En tal caso, dado que trabajamos sobre el plano proyectivo, podemos suponer sin pérdida de generalidad que $x, y, z \in \mathbb{N}$. Entonces, hemos reducido nuestro problema al conocido problema de las ternas pitagóricas, que consiste en hallar todos los $(x, y, z) \in \mathbb{N}^3$ tales que $x^2 + y^2 = z^2$. Más aún: nuevamente, como trabajamos sobre el plano proyectivo, podemos suponer que x, y, z son coprimos. Es claro que, entonces, han de ser coprimos dos a dos, puesto que si un primo divide a dos de ellos, se sigue de la relación $x^2+y^2 = z^2$ que también divide al tercero. Una terna pitagórica donde sus coordenadas son coprimas se conoce como *terna pitagórica primitiva*. Obsérvese que, en una terna pitagórica primitiva (x, y, z), no pueden ser las tres coordenadas impares; puesto que, en tal caso, se tendría que z es par, al ser su cuadrado suma de dos impares. No puede, asimismo, haber dos coordenadas pares, pues las coordenadas son coprimas dos a dos. En consecuencia, exactamente un elemento de cada terna pitagórica primitiva es par. Además, dicho elemento no puede ser z, pues de lo contrario $4 \mid z^2$, y como todo cuadrado perfecto impar tiene resto 1 en la división por 4, obtenemos

$$0 \equiv z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4,$$

lo cual es absurdo. En consecuencia, el número par debe ser x o y. Sin pérdida de generalidad, supongamos que y es par.

Es sabido que (x, y, z) es una terna pitagórica primitiva donde y es par si y solo si existen $p, q \in \mathbb{N}$ coprimos y de paridades opuestas tales que $p > q$ y $(x, y, z) = \left(p^2 - q^2, 2pq, p^2 + q^2\right)$. Este clásico resultado puede derivarse de muchas formas distintas. Existe una forma de derivarlo usando las propiedades de los enteros gaussianos (ver [16, cap. 1]), por medio del

Método de Diofanto (ver [12, Theorem 1.2]) e inclusive de forma completamente elemental (ver [9, Theorem 225]). En cualquier caso, es sencillo usar este resultado para ver que, entonces, podemos parametrizar

$$\left\{(x:y:z)\in\mathbb{P}^2(\mathbb{Q}):x^2+y^2=z^2\right\}=$$

$$=\left\{\left(m^2-n^2:2mn:m^2+n^2\right)\in\mathbb{P}^2(\mathbb{Q}):m,n\in\mathbb{Q}\wedge(m,n)\neq(0,0)\right\}.$$

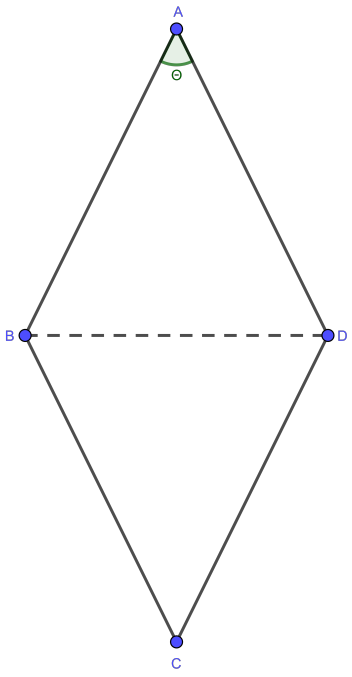
Observemos que no es necesario agregar otra parametrización que intercambie las expresiones de las primeras dos coordenadas, pues si $m,n\in\mathbb{Q}$ no son ambos nulos, entonces $a:=m+n$ y $b:=m-n$ no son ambos nulos y $\left(m^2-n^2:2mn:m^2+n^2\right)=\left(2ab:a^2-b^2:a^2+b^2\right)$. Por otra parte, $\left(m^2-n^2:2mn:-m^2-n^2\right)=\left(n^2-(-m)^2:2n(-m):n^2+(-m)^2\right)$, con lo cual tampoco es necesario corregir signos en la última coordenada.

Incluso, reescalando, podemos tomar $m,n\in\mathbb{Z}$. Dado que, más adelante (ver 2.1), utilizaremos el Método de Diofanto para resolver el problema, más general, de caracterizar los triángulos racionales, sin pedir que sean necesariamente triángulos rectángulos, omitiremos la demostración de esto por el momento.

Como buscamos triángulos rectángulos, podemos suponer que $mn\neq 0<m^2-n^2$. De tal forma, definiendo $u:=\frac{n}{m}$ y reescalando, podemos quedarnos con los triángulos rectángulos de lados $1-u^2$, $2u$, $1+u^2$ donde $0<u<1$ y $u\in\mathbb{Q}$, como representativos de todas las clases de semejanza de los triángulos rectángulos racionales.

Modelización del problema

Por lo visto en 1.6.4, reescalando, podemos suponer que tenemos un triángulo rectángulo de lados $1-u^2$, $2u$, $1+u^2$ donde $0<u<1$ y $u\in\mathbb{Q}$. Supongamos que tenemos un rombo $ABCD$ que es θ-racional, de tal forma que $0<\theta<\frac{\pi}{2}$, $\theta=\angle BAD$ y $\cos(\theta),\sin(\theta)\in\mathbb{Q}$. Llamemos p a la longitud de los lados AB, BD, CD, DA del rombo.



El triángulo ABD tiene área igual a

$$\frac{AB \cdot AD \cdot \sin(\theta)}{2} = \frac{p^2 \sin(\theta)}{2}$$

y, por lo tanto, el área de $ABCD$ es igual a $p^2 \sin(\theta)$. Por otra parte, nuestro triángulo tiene área igual a $\frac{2u(1-u^2)}{2} = u\left(1-u^2\right)$. Por lo tanto, el triángulo y el rombo tendrán la misma área si y solo si $u\left(1-u^2\right) = p^2 \sin(\theta)$.

En cuanto a los perímetros, el perímetro del triángulo es $1-u^2+2u+1+u^2 = 2+2u$, y el perímetro del rombo es $4p$, de tal forma que ambas figuras tendrán el mismo perímetro si y solo si $2+2u = 4p$. Así, nuestras figuras cumplirán las condiciones buscadas si y solo si se satisface el sistema

$$\begin{cases} u\left(1-u^2\right) = p^2 \sin(\theta), \\ 1+u = 2p. \end{cases}$$

Como $0 < \theta < \frac{\pi}{2}$ y $\sin(\theta), \cos(\theta) \in \mathbb{Q}$, la identidad pitagórica nos dice que el triángulo de lados $\sin(\theta), \cos(\theta), 1$ es un triángulo rectángulo racional. Por lo visto en la sección 1.6.4, podemos escribir, para algún $v \in (0,1) \cap \mathbb{Q}$,

$$(\cos(\theta) : \sin(\theta) : 1) = \left(1-v^2 : 2v : 1+v^2\right) = \left(\frac{1-v^2}{1+v^2} : \frac{2v}{1+v^2} : 1\right),$$

de tal forma que $\sin(\theta) = \frac{2v}{1+v^2}$. El sistema a considerar es, entonces,

$$\begin{cases} u\left(1-u^2\right)\left(1+v^2\right) = 2vp^2, \\ 1+u = 2p. \end{cases}$$

Sustituyendo $p = \frac{1+u}{2}$ en la primera ecuación, obtenemos

$$2u\left(1-u^2\right)\left(1+v^2\right) = v(1+u)^2$$

$$2u(1-u)\left(1+v^2\right) = v(1+u)$$

$$2u^2v^2 + 2u^2 - 2uv^2 + uv - 2u + v = 0. \tag{1.8}$$

De esta forma, nuestro problema es equivalente a encontrar una solución de 1.8 con $u, v \in (0,1) \cap \mathbb{Q}$; y, en segunda instancia, saber si la cantidad de soluciones es finita o infinita.

Shane Chern consideró las transformaciones inversas

$$\begin{aligned} (x,y) &= \left(-\frac{4uv^2+4u+4v-4}{v^2}, -\frac{8uv^2-4v^2+8u+8v-8}{v^3}\right), \\ (u,v) &= \left(-\frac{x^3+4x^2+2xy-y^2+4x+4y}{4x^2+y^2+16x+16}, \frac{2x+4}{y}\right), \end{aligned} \tag{1.9}$$

que transforman 1.8 en la curva elíptica

$$E : y^2 - 3xy - 12y = x^3 + 6x^2 + 8x, \tag{1.10}$$

la cual está en la forma de Weierstrass afinizada, y cuyo discriminante es $-18368 \neq 0$. Así, buscamos una solución (x,y) de 1.10 tal que $u, v \in (0,1) \cap \mathbb{Q}$.

Solución del problema

Estamos, pues, en condiciones de probar el resultado principal de esta sección.

Teorema 1.6.7 *Existen infinitos pares de polígonos tales que uno de ellos es un triángulo rectángulo entero, y el otro es un rombo θ-entero para algún $\theta \in \left(0, \frac{\pi}{2}\right)$, tales que ambos tienen la misma área y el mismo perímetro, y tales que no hay dos pares de la lista infinita con sus triángulos o sus rombos semejantes.*

Demostración. De acuerdo a 1.6.4, esto es equivalente a encontrar infinitas soluciones en la curva elíptica 1.10 cuyas transformaciones vía 1.9 inducen vectores (u, v) con $u, v \in (0,1) \cap \mathbb{Q}$.

El grupo de torsión de $E(\mathbb{Q})$ tiene orden 2 y está generado por $(-4:0:1)$. Como no nos interesan las soluciones con $y = 0$, miramos la parte libre de $E(\mathbb{Q})$. Este grupo tiene rango 1 y está generado por $P := (-2:6:1)$. Por consiguiente, para encontrar una solución válida, hemos de buscar una solución de 1.10 de la forma nP con $n \in \mathbb{N}$ que genere una solución (u, v) adecuada. Una breve inspección muestra que

$$P = (-2:6:1), \qquad 2P = \left(-\frac{32}{9} : -\frac{28}{27} : 1\right),$$

$$3P = \left(\frac{316}{49} : -\frac{4416}{343} : 1\right), \quad 4P = \left(\frac{5920}{4761} : \frac{557678}{328509} : 1\right),$$

y que $(x, y) = \left(\frac{5920}{4761}, \frac{557678}{328509}\right)$ induce, vía 1.9,

$$(u, v) = \left(\frac{552}{1105}, \frac{483}{1264}\right),$$

que cumple con nuestros requisitos para inducir una solución válida.

Finalmente, el abierto $(0,1)^2 \subseteq \mathbb{R}^2$ se transforma a un abierto de $\mathbb{P}^2(\mathbb{R})$ vía la extensión de 1.9 y la inmersión natural de $\mathbb{R}^2$ en $\mathbb{P}^2(\mathbb{R})$. En este abierto tenemos la solución $4P \in E(\mathbb{Q})$, y toda otra solución en el mismo abierto inducirá una solución válida a nuestro problema. Por el Teorema 1.5.7, tenemos infinitas soluciones en dicho abierto, lo cual termina de probar lo que queríamos. ■

Capítulo 2

Introducción al problema principal

El paper citado de Shane Chern [6] forma parte de una extensa lista de resultados aritméticos de índole euclídea muy similares, que constituyen una serie de teoremas que lleva varios años estudiándose y desarrollándose. En el año 2019 las matemáticas Matilde Lalín y Xinchun Ma realizaron un estudio sistemático de estos resultados y dieron con una fuerte generalización y formalización de los mismos [13]. El análisis de dicho resultado será nuestra motivación para introducir la teoría de superficies elípticas.

2.1 Triángulos racionales

Comenzaremos este capítulo describiendo por medio de coordenadas proyectivas los triángulos racionales tal que el coseno de uno de sus ángulos es racional.

Sea ABC un triángulo racional tal que $\cos(\angle ACB) \in \mathbb{Q}$ y sean $x := BC$, $y := AC$, $z := AB$, $a := \cos(\angle ACB)$. La Ley del Coseno nos dice que

$$AB^2 = BC^2 + AC^2 - 2 \cdot BC \cdot AC \cdot \cos(\angle ACB)$$

$$z^2 = x^2 + y^2 - 2axy. \tag{2.1}$$

Para nuestros propósitos, supondremos que trabajamos sobre triángulos no degenerados, de tal forma que $0 < \angle ACB < \pi$ y por lo tanto $|a| < 1$.

Si pensamos la ecuación 2.1 como una ecuación en las variables x, y, z, obtenemos una ecuación homogénea de grado 2 que podemos resolver por medio del **Método de Diofanto**, que consiste en parametrizar las soluciones a través de una solución particular por medio del trazado de rectas que pasen por la solución particular en cuestión y buscando un segundo punto de intersección entre dichas rectas y la ecuación a resolver. Afinizando la ecuación, obtenemos

$$1 = x^2 + y^2 - 2axy. \tag{2.2}$$

Esta ecuación admite la solución $(x, y) = (0, -1)$. El conjunto de rectas en $\mathbb{Q}^2$ que pasan por $(0, -1)$, exceptuando la recta $y = 0$, es el conjunto de rectas de la forma $x = ty - 1$ con $t \in \mathbb{Q}$. Sustituimos en 2.2 para buscar una segunda intersección (en función de t) entre esta recta y la ecuación a resolver. De esta forma, obtenemos

$$1 = (ty - 1)^2 + y^2 - 2a(ty - 1)y$$

$$0 = t^2y^2 - 2ty + y^2 - 2aty^2 + 2ay.$$

Dado que la solución con $y = 0$ induce la solución particular $(0, -1)$, que no es la que buscamos, suponemos $y \neq 0$ y entonces obtenemos

$$0 = t^2 y - 2t + y - 2aty + 2a$$

$$2t - 2a = \left(t^2 + 1 - 2at\right) y.$$

Como $t^2 + 1 - 2at = (t - a)^2 + 1 - a^2 \geq 1 - a^2 > 0$ (pues $|a| < 1$), entonces

$$y = \frac{2t - 2a}{t^2 + 1 - 2at}.$$

Finalmente, usando que $x = ty - 1$, obtenemos $x = \frac{t^2-1}{t^2+1-2at}$. En definitiva, deshaciendo la afinización, hemos probado que si $(x : y : z) \in \mathbb{P}^2(\mathbb{Q})$ cumple la ecuación homogénea 2.1 y $z \neq 0$, entonces

$$\left(\frac{x}{z}, \frac{y}{z}\right) = \left(\frac{t^2 - 1}{t^2 + 1 - 2at}, \frac{2t - 2a}{t^2 + 1 - 2at}\right).$$

Sean $m, n \in \mathbb{Z}$ tales que $n \neq 0$ y $t = \frac{m}{n}$. Como no nos interesan las soluciones con $t \in \{-1, 1\}$ (pues las mismas inducen $x = 0$), suponemos $t^2 \neq 1$. De esta forma,

$$\frac{y}{x} = \frac{y/z}{x/z} = \frac{2t - 2a}{t^2 - 1} = \frac{2m/n - 2a}{(m/n)^2 - 1} = \frac{2mn - 2an^2}{m^2 - n^2} = \frac{2n\,(m - an)}{m^2 - n^2}.$$

De esto se sigue que

$$(x : y : z) = \left(m^2 - n^2 : 2n\,(m - an) : b\right),$$

donde $b \in \mathbb{Q}$ satisface, sustituyendo en 2.1,

$$b^2 = \left(m^2 - n^2\right)^2 + [2n\,(m - an)]^2 - 2a\left(m^2 - n^2\right)[2n\,(m - an)]$$

$$b^2 = m^4 - 2m^2n^2 + n^4 + 4n^2m^2 - 8n^3am + 4n^4a^2 + 4a^2m^2n^2 - 4a^2n^4 - 4am^3n + 4amn^3$$

$$b^2 = 4a^2m^2n^2 - 4am^3n - 4amn^3 + m^4 + 2m^2n^2 + n^4$$

$$b^2 = \left(m^2 - 2amn + n^2\right)^2.$$

Dado que nos interesan las soluciones con $z > 0$, tomamos

$$b := m^2 - 2amn + n^2 > m^2 - 2\,\mathrm{sgn}\,(mn)\,mn + n^2 = [m - \mathrm{sgn}\,(mn)\,n]^2 \geq 0,$$

donde, en la primera desigualdad, hemos usado que $|a| < 1$. Así, obtenemos

$$(x : y : z) = \left(m^2 - n^2 : 2n\,(m - an) : m^2 - 2amn + n^2\right).$$

Obsérvese que, en esta representación, si bien tenemos $m, n \in \mathbb{Z}$, podemos suponer que son variables racionales también, dado que tenemos expresiones homogéneas de grado 2 para el sistema de coordenadas proyectivas. En otras palabras, reescalando, podemos suponer $m, n \in \mathbb{Z}$ o bien $m, n \in \mathbb{Q}$. Obsérvese, asimismo, que tomando $a = 0$ obtenemos el caso de triángulos rectángulos, lo cual nos da la parametrización vista en 1.6.4.

Volviendo a nuestra situación original, hemos probado que si tenemos un triángulo rectángulo racional ABC tal que $\cos(\angle ACB) \in \mathbb{Q}$ y $a := \cos(\angle ACB)$, entonces existen $m, n \in \mathbb{Q}$ tales que ABC es semejante a un triángulo de lados $m^2 - n^2$, $2n\,(m - an)$, $m^2 - 2amn + n^2$.

2.2 Formulación y modelización del problema

Dado $\theta \in (0, \pi)$, decimos que un triángulo ABC es θ-entero si ABC es entero, $\theta = \angle ABC$ y $\cos(\theta) \in \mathbb{Q}$. Análogamente, decimos que ABC es θ-racional si ABC es racional, $\theta = \angle ABC$ y $\cos(\theta) \in \mathbb{Q}$. Obsérvese que en ambos casos se pide $\cos(\theta) \in \mathbb{Q}$.

Por otra parte, dado $\omega \in \left(0, \frac{\pi}{2}\right]$, un paralelogramo $ABCD$ se dice *un ω-paralelogramo* si $\angle BAD = \omega$. En las funciones trigonométricas sobre este valor no impondremos hipótesis, de tal manera que, si decimos que un paralelogramo es *un ω-paralelogramo racional* o *un ω-paralelogramo entero*, solamente estamos imponiendo condiciones sobre las longitudes de los lados de un ω-paralelogramo.

De aquí en adelante, al referirnos al concepto de *polígono*, excluiremos los polígonos degenerados. Dado un polígono $\mathfrak{A}$, notamos $\ell(\mathfrak{A})$ a su perímetro.

Dados dos polígonos semejantes $\mathfrak{A}$ y $\mathfrak{B}$, definimos el *factor de semejanza de $\mathfrak{A}$ respecto de $\mathfrak{B}$* como

$$\mathscr{C}_{\mathfrak{AB}} := \frac{\ell(\mathfrak{A})}{\ell(\mathfrak{B})}.$$

Así, la constante $\mathscr{C}_{\mathfrak{AB}}$ cuantifica el factor por el que se debe reescalar el polígono $\mathfrak{B}$ para obtener el polígono $\mathfrak{A}$.

Dados cuatro polígonos $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, decimos que el par $(\mathfrak{A}, \mathfrak{C})$ es *indistinguible por semejanza* del par $(\mathfrak{B}, \mathfrak{D})$ si y solo si $\mathfrak{A}$ y $\mathfrak{B}$ son semejantes, $\mathfrak{C}$ y $\mathfrak{D}$ son semejantes, y además $\mathscr{C}_{\mathfrak{AB}} = \mathscr{C}_{\mathfrak{CD}}$.

Observación 2.2.1 Si $\ell(\mathfrak{A}) = \ell(\mathfrak{C})$ y $\ell(\mathfrak{B}) = \ell(\mathfrak{D})$, entonces $(\mathfrak{A}, \mathfrak{C})$ es indistinguible por semejanza del par $(\mathfrak{B}, \mathfrak{D})$ si y solo si $\mathfrak{A}$ y $\mathfrak{B}$ son semejantes y $\mathfrak{C}$ y $\mathfrak{D}$ son semejantes. En efecto, si $\mathfrak{A}$ y $\mathfrak{B}$ son semejantes y $\mathfrak{C}$ y $\mathfrak{D}$ son semejantes, entonces $\mathscr{C}_{\mathfrak{AB}} = \frac{\ell(\mathfrak{A})}{\ell(\mathfrak{B})} = \frac{\ell(\mathfrak{C})}{\ell(\mathfrak{D})} = \mathscr{C}_{\mathfrak{CD}}$. La implicación recíproca es trivial.

En [13], Lalín y Ma lograron demostrar que, fijado $\theta \in (0, \pi)$ tal que $a := \cos(\theta) \in \mathbb{Q}$, para todos salvo finitos $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$ existen $\omega \in \left(0, \frac{\pi}{2}\right]$ e infinitos pares de un triángulo θ-entero y un ω-paralelogramo entero que tienen la misma área y el mismo perímetro, tales que $\sin(\omega) = t\sin(\theta)$, y tales que no hay dos de estos pares que sean indistinguibles por semejanza.

El hecho de que no distingamos soluciones por semejanza y tengamos esta imposición sobre los perímetros nos permite aplicar la Observación 2.2.1 para modelizar el problema en coordenadas proyectivas: representar a los triángulos como puntos en $\mathbb{P}^2(\mathbb{Q})$ tal y como hicimos en 2.1, y representar a los paralelogramos como puntos en $\mathbb{P}^1(\mathbb{Q})$ que admiten una representación proyectiva con sus dos coordenadas positivas.

Veamos cómo modelizar nuestro problema concreto. Como antes, podemos suponer que nuestras figuras son racionales y no enteras, dado que, por medio de un reescalamiento, podemos hacer que sus lados sean enteros y así obtener, de una solución con figuras racionales, una solución con figuras enteras indistinguible por semejanza a la original.

Sea $\theta \in (0, \pi)$ tal que $a := \cos(\theta) \in \mathbb{Q}$ y sea $\mathfrak{A}$ un triángulo θ-racional. Entonces, por lo visto en 2.1, existen $m, n \in \mathbb{Q}$ tales que $\mathfrak{A}$ tiene lados de longitud $n^2 - m^2$, $2m(n - am)$, $m^2 - 2amn + n^2$. Por la Identidad Pitagórica se tiene $\sin(\theta) = \sqrt{1-a^2}$, de donde el área de nuestro triángulo es

$$2m(n - am)\left(n^2 - m^2\right)\sqrt{1-a^2}.$$

Por otra parte, el perímetro de nuestro triángulo es

$$\left(n^2-m^2\right)+\left[2m\left(n-am\right)\right]+\left(m^2-2amn+n^2\right)=2\left(n-am\right)\left(n+m\right).$$

Sea $\omega\in\left(0,\frac{\pi}{2}\right]$ y sea $ABCD$ un ω-paralelogramo racional. Sean p y q las longitudes de los lados AB y AD, de tal forma que su área es $pq\sin\left(\omega\right)$ y su perímetro es $2p+2q$. En consecuencia, tenemos el siguiente sistema de ecuaciones:

$$\begin{cases}\sqrt{1-a^2}\left(n^2-m^2\right)m\left(n-am\right)=pq\sin\left(\omega\right)\\ \\ \left(n-am\right)\left(n+m\right)=p+q\end{cases}. \tag{2.3}$$

Como $m,n,p,q\in\mathbb{Q}$, la primera ecuación de 2.3 nos dice que existe $t\in\mathbb{Q}_{>0}$ tal que $\sin\left(\omega\right)=t\sqrt{1-a^2}$, de forma que

$$\begin{cases}\left(n^2-m^2\right)m\left(n-am\right)=tpq\\ \\ \left(n-am\right)\left(n+m\right)=p+q\end{cases}. \tag{2.4}$$

Al igual que en 1.6.4, un cambio de variables adecuado para este sistema nos llevará a una curva elíptica correspondiente a partir de la cual podremos obtener el resultado buscado. Concretamente, tenemos la siguiente proposición:

Proposición 2.2.2 *Sea $a\in\mathbb{Q}$, sea $t\in\left(0,\frac{1}{\sqrt{1-a^2}}\right]\cap\mathbb{Q}$ y sea $\theta\in(0,\pi)$ tal que $\cos\left(\theta\right)=a$. Si la ecuación*

$$E_{a,t}:y^2=x^3+t\left[\left(1+a\right)^2t+4\left(a-3\right)\right]x^2+32\left(1-a\right)t^2x \tag{2.5}$$

admite infinitas soluciones $(x,y)\in\mathbb{Q}^2$ que satisfacen las condiciones

$$4\left(1-a\right)t<x<8t,\qquad |y|<\left(1+a\right)tx, \tag{2.6}$$

entonces existen infinitos pares de un triángulo θ-entero y un ω-paralelogramo entero tales que $\sin\left(\omega\right)=t\sin\left(\theta\right)$, para algún $\omega\in\left(0,\frac{\pi}{2}\right]$, y tales que ambos tienen la misma área y el mismo perímetro, sin distinción por semejanza.

Demostración. Del sistema 2.4 obtenemos

$$\left(p-q\right)^2=\left(p+q\right)^2-4pq=\left(n-am\right)^2\left(n+m\right)^2-\frac{4}{t}\left(n^2-m^2\right)m\left(n-am\right).$$

Lalín y Ma consideraron el cambio de variables

$$\begin{cases}Y=4\left(1-a^2\right)t^2\frac{p-q}{\left(n-am\right)^2}\\ \\ X=4\left(1-a\right)t\frac{n+m}{n-am}\end{cases},$$

de donde puede tomarse

$$\begin{cases}m=X-4\left(1-a\right)t\\ \\ n=aX+4\left(1-a\right)t\end{cases},\qquad \begin{cases}p=2\left(1-a^2\right)\left[\left(1+a\right)tX+Y\right]\\ \\ q=2\left(1-a^2\right)\left[\left(1+a\right)tX-Y\right]\end{cases}.$$

Este cambio de variables induce la ecuación

$$Y^2 = X^3 + t\left[(1+a)^2 t + 4(a-3)\right] X^2 + 32(1-a)t^2 X,$$

que coincide con la ecuación de Weierstrass 2.5.

Dado que estamos trabajando con figuras geométricas, requerimos que sus lados sean positivos. En consecuencia, llamando $x := n^2 - m^2$, $y := 2m(n - am)$, buscamos que $x, y, p, q \in \mathbb{Q}_{>0}$.

En cuanto a p y q, dado que $|a| < 1$, entonces $2\left(1-a^2\right) > 0$, de donde $p, q \in \mathbb{Q}_{>0}$ si y solo si $(1+a)tX \pm Y > 0$, que equivale a $|Y| < (1+a)tX$.

En cuanto a x e y, obsérvese que, de las identidades $x = n^2 - m^2$, $y = 2m(n - am)$, obtenemos

$$x = [aX + 4(1-a)t]^2 - [X - 4(1-a)t]^2 = \left(1-a^2\right) X(8t - X),$$

$$y = 2[X - 4(1-a)t][aX + 4(1-a)t - a(X - 4(1-a)t)] = 8\left(1-a^2\right) t[X - 4(1-a)t].$$

De $|a| < 1$ y $t > 0$ obtenemos $1 - a^2 > 0$ y $8\left(1-a^2\right)t > 0$. Por consiguiente, $x, y \in \mathbb{Q}_{>0}$ si y solo si $X(8t - X) > 0$ y $X - 4(1-a)t > 0$. Veremos que estas dos condiciones equivalen a la desigualdad $4(1-a)t < X < 8t$.

Si $X(8t - X) > 0$ y $X - 4(1-a)t > 0$, entonces, de la segunda desigualdad, tenemos $X > 4(1-a)t$. Como $|a| < 1$ entonces $1 - a > 0$, de donde esta última desigualdad nos dice que $X > 0$. En consecuencia, la desigualdad $X(8t - X) > 0$ nos dice que $8t - X > 0$, de donde $4(1-a)t < X < 8t$. Recíprocamente, si $4(1-a)t < X < 8t$, entonces, como $1 - a > 0$, se tiene $X > 0$. Así, multiplicando por X la desigualdad $X < 8t$ obtenemos $X(8t - X) > 0$. La desigualdad $X - 4(1-a)t > 0$ se sigue trivialmente de $4(1-a)t < X$.

Con esto tenemos probada la necesidad de las condiciones. En cuanto a la suficiencia, deshaciendo el cambio de variables tenemos todo reconstruido, salvo ω. Del hecho de que $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right]$, $\sin(\theta) = \sqrt{1-a^2}$ y $|a| < 1$ se obtiene $0 < t\sin(\theta) \leq 1$, por lo tanto existe $\omega \in \left(0, \frac{\pi}{2}\right]$ tal que $\sin(\omega) = t\sin(\theta)$. ■

2.3 Nuestra primera superficie elíptica

Naturalmente, las condiciones 2.6 de la Proposición 2.2.2 inducirán un abierto en $\mathbb{P}^2(\mathbb{R})$ tal que, de encontrar allí una solución de $E_{a,t}$ (suponiendo que la misma constituye una curva elíptica de rango positivo), podremos aplicar el Teorema 1.5.7 para afirmar que existen infinitas soluciones allí, de donde la Proposición 2.2.2 nos garantizará que tenemos infinitas soluciones a nuestro problema inicial. Lo que probaron Matilde Lalín y Xinchun Ma en [13] es que, en efecto, fijado el valor de a, para todos salvo finitos valores de $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$ se tiene que $E_{a,t}$ es una curva elíptica de rango positivo que admite una solución en el abierto inducido por 2.6.

Por lo pronto, señálese que $E_{a,t}$ es una ecuación en forma de Weierstrass afinizada. Su discriminante está dado por

$$\Delta_{a,t} = 2^{14}\left(1-a^2\right)^2 t^6\left[(1+a)^2 t^2 + 8(a-3)t + 16\right],$$

de donde, al ser un polinomio no nulo en t (pues $a \notin \{-1, 1\}$ y $0 < 1 - |a| \leq 1 + a$), $E_{a,t}$ será una curva elíptica para todos salvo finitos valores de t.

Es decir, tenemos un conjunto de curvas elípticas definidas por un parámetro en sus coeficientes. Este fenómeno será nuestra primera aproximación, y motivación principal, para la introducción y el estudio de superficies elípticas.

Obsérvese que $(x,y) = \left(8t, 8\left(1+a\right)t^2\right)$ satisface la ecuación $E_{a,t}$ y, además, está en el borde del abierto inducido por 2.6, dado que $|y| = y = (1+a)\,t \cdot 8t = (1+a)\,tx$ (recuérdese que $1+a>0$), y además $8t = x > 4\left(1-a\right)t$, puesto que esta desigualdad equivale a $a > -1$, lo cual vale pues $|a|<1$. Notaremos este punto como $P_{a,t} := \left(8t : 8\left(1+a\right)t^2 : 1\right)$.

La teoría de superficies elípticas nos permitirá demostrar que, para todos salvo finitos $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$, $E_{a,t}\left(\mathbb{Q}\right)$ será una curva elíptica de rango positivo.

Por lo pronto, finalizaremos este capítulo viendo cómo valernos de este resultado para resolver el problema. Fijamos t tal que $E_{a,t}\left(\mathbb{Q}\right)$ es una curva elíptica de rango 1. Sabemos que $P_{a,t}$ es un punto de $E_{a,t}\left(\mathbb{Q}\right)$. El Teorema 1.5.7 nos dice que $E_{a,t}\left(\mathbb{Q}\right)$ es denso, al menos, en la componente conexa de $E_{a,t}\left(\mathbb{R}\right)$ a la cual $P_{a,t}$ pertenece.

Como $|a|<1$ entonces $1-a>0$ y $1-a<2$, de donde $0<\frac{1-a}{2}<1$. Además, como

$$\lim_{\delta\to 1^-}\left[\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)\left(\delta-1\right) + \left(1+a\right)^2 t^2\right] = \left(1+a\right)^2 t^2 > 0,$$

entonces existe $\delta \in \mathbb{R}$ tal que $\frac{1-a}{2} < \delta < 1$ y

$$\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)\left(\delta-1\right) + \left(1+a\right)^2 t^2 > 0.$$

Definimos $X_0 := 8\delta t$ y tomamos $Y_0 \in \mathbb{R}$ tal que (X_0, Y_0) satisface la ecuación $E_{a,t}$. Para ver que un tal Y_0 existe, debemos ver que

$$X_0^3 + t\left[\left(1+a\right)^2 t + 4\left(a-3\right)\right]X_0^2 + 32\left(1-a\right)t^2 X_0 \geq 0.$$

Veremos que, de hecho, vale la desigualdad estricta. Como $X_0 = 8\delta t \neq 0$, esto es equivalente a ver que

$$\frac{X_0^3 + t\left[\left(1+a\right)^2 t + 4\left(a-3\right)\right]X_0^2 + 32\left(1-a\right)t^2 X_0}{X_0^2} > 0$$

$$X_0 + t\left[\left(1+a\right)^2 t + 4\left(a-3\right)\right] + \frac{32\left(1-a\right)t^2}{X_0} > 0$$

$$8\delta t + t\left[\left(1+a\right)^2 t + 4\left(a-3\right)\right] + \frac{32\left(1-a\right)t^2}{8\delta t} > 0$$

$$8\delta t + 4t\left(a-3\right) + \frac{4\left(1-a\right)t}{\delta} + \left(1+a\right)^2 t^2 > 0$$

$$\frac{8t}{\delta}\left(\delta^2 + \frac{a-3}{2}\delta + \frac{1-a}{2}\right) + \left(1+a\right)^2 t^2 > 0$$

$$\frac{8t}{\delta}\left(\delta^2 + \frac{a-3}{2}\delta + \frac{1-a}{2}\right) + \left(1+a\right)^2 t^2 > 0$$

$$\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)\left(\delta-1\right) + \left(1+a\right)^2 t^2 > 0,$$

y esto último es cierto por nuestra elección de δ. En particular, podemos tomar

$$Y_0 := 8\delta t\sqrt{\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)(\delta-1) + (1+a)^2 t^2}.$$

Obsérvese que, si fuese $\delta = 1$, obtendríamos $(X_0, Y_0) = P_{a,t}$. Sin embargo, elegir $\frac{1-a}{2} < \delta < 1$ nos garantiza que $(X_0, Y_0) \in E_{a,t}(\mathbb{R})$ satisface las condiciones 2.6. En efecto, multiplicando la desigualdad $\frac{1-a}{2} < \delta < 1$ por $8t > 0$ obtenemos $4(1-a)t < X_0 < 8t$. En cuanto a $|Y_0| < (1+a)tX_0$, como $Y_0 > 0$, esta desigualdad equivale a

$$8\delta t\sqrt{\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)(\delta-1) + (1+a)^2 t^2} < (1+a)t \cdot 8\delta t$$

$$\sqrt{\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)(\delta-1) + (1+a)^2 t^2} < (1+a)t.$$

Esta desigualdad es cierta pues, como $t > 0$ y $0 < \frac{1-a}{2} < \delta < 1$, entonces

$$\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)(\delta-1) < 0,$$

y por lo tanto

$$\sqrt{\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)(\delta-1) + (1+a)^2 t^2} < \sqrt{(1+a)^2 t^2} = (1+a)t.$$

ya que $1 + a > 0$, al ser $|a| < 1$.

Otra observación a realizar es que (X_0, Y_0) pertenece a la misma componente conexa de $E_{a,t}(\mathbb{R})$ que $P_{a,t}$. Una manera topológica de ver esto, sin apelar a la teoría de curvas elípticas, es viendo que los ceros de $E_{a,t}$ en $\mathbb{R}^2$, al ser $E_{a,t}$ no singular, forman una variedad diferencial; en particular, un espacio topológico localmente conexo. Así, como

$$\lim_{\delta \to 1^-}\left(8\delta t, 8\delta t\sqrt{\frac{8t}{\delta}\left(\delta - \frac{1-a}{2}\right)(\delta-1) + (1+a)^2 t^2}\right) = P_{a,t},$$

entonces existe δ lo suficientemente cercano a 1 tal que el argumento del anterior límite pertenece a la misma componente conexa de $E_{a,t}(\mathbb{R})$ que $P_{a,t}$. Por arcoconexión, esto valdrá también para todo valor de $\delta \in \left(\frac{1-a}{2}, 1\right)$; en particular, para el valor que tomamos al definir (X_0, Y_0), ya que el argumento del límite anterior como función de δ es continuo en el intervalo abierto $\left(\frac{1-a}{2}, 1\right)$.

Concluimos que $(X_0, Y_0) \in E_{a,t}(\mathbb{R})$ satisface las condiciones 2.6 y pertenece a la misma componente conexa de $E_{a,t}(\mathbb{R})$ que $P_{a,t}$. Por la primera parte del Teorema 1.5.7, tenemos una solución de $E_{a,t}(\mathbb{Q})$ lo suficientemente cerca de (X_0, Y_0) de tal forma que pertenece al abierto definido por 2.6. Aplicando la segunda parte del Teorema 1.5.7, tendremos allí infinitas soluciones, lo cual resuelve el problema.

Capítulo 3

Superficies elípticas

Este capítulo pretende introducir el concepto de *superficie elíptica* con la motivación expuesta en el Capítulo 2, y exponer la teoría básica, con el objetivo de ofrecer el marco conceptual adecuado para una lectura crítica de los argumentos del próximo capítulo.

A partir de aquí, supondremos al lector familiarizado con los conceptos básicos de geometría algebraica. En caso de necesidad, en el Apéndice A hemos expuesto, a modo de recordatorio rápido, (algunos de) los conceptos y resultados de la geometría algebraica más significativos para el desarrollo de nuestro trabajo. Al mismo tiempo, ofreceremos referencias adicionales con cierta regularidad para poder ampliar la información de estos conceptos.

3.1 Definición y primeras observaciones

Tal y como vimos en 2.3, podemos hacer surgir espontáneamente de un problema de Teoría de Números un objeto consistente en, básicamente, una parametrización de un conjunto de curvas elípticas con base en un parámetro escalar, con finitas excepciones. Más generalmente, buscamos parametrizar una familia de curvas elípticas con base en una curva fijada previamente, admitiendo (y, de hecho, requiriendo positivamente) finitas excepciones. Esto es lo que entenderemos como el concepto general de superficie elíptica.

Para hacer más preciso este concepto, fijamos una curva proyectiva no singular C sobre un cuerpo algebraicamente cerrado k. Para cada k-superficie proyectiva no singular S y cada morfismo algebraico $f : S \to C$, decimos que f es una *fibración de la superficie S con base en la curva C* si f es un morfismo algebraico sobreyectivo y de fibras conexas. Decimos que f es una *fibración de género g* si solamente finitas de sus fibras son curvas singulares de S (reducibles o no), y el resto son curvas de S no singulares de género g. Obsérvese que, entonces, tenemos naturalmente inducida una curva de género g sobre el cuerpo de funciones $k(C)$ de la curva C, la cual es la fibra inducida por el punto genérico de la curva de base C y recibe el nombre de *fibra genérica*. Recuérdese que, en general, dado un esquema integral (en particular, irreducible), cada abierto afín de su espacio topológico subyacente (es decir, un abierto dado por el espectro de un anillo) cumple que el cuerpo de fracciones de ese anillo es isomorfo al anillo local asociado al punto genérico de dicho esquema. En particular, el anillo local asociado al punto genérico de C es un cuerpo isomorfo a $k(C)$.

Dada una fibración $f : S \to C$, una *sección de f* es un morfismo $\sigma : C \to S$ tal que $f \circ \sigma$ es el morfismo identidad en C. Con todo esto definido, procedemos a dar una definición de superficie elíptica.

Definición 3.1.1 *Sea k un cuerpo algebraicamente cerrado. Una* k-superficie elíptica *es un par (f, σ_0) tal que $f : S \to C$ es una fibración de género 1, donde S es una k-superficie proyectiva no singular y C es una k-curva proyectiva no singular, y tal que σ_0 es una sección de f, de modo que se cumplen las siguientes condiciones:*

i) Ninguna componente irreducible de una f-fibra es una (-1)-curva (esta condición recibe el nombre de minimalidad relativa*).*

ii) Al menos una de las fibras de f es singular.

Una tal fibración f (incluyendo la existencia de una sección) recibirá el nombre de fibración elíptica*.*

Recordemos que, dada una k-superficie proyectiva no singular S, tenemos definido su *pairing de intersección* $\langle \cdot, \cdot \rangle : \mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}$ (consultar A.3), y que una subvariedad irreducible $\mathfrak{C}$ de codimensión 1 en S se dice *una* (-1)*-curva* si $\langle \mathfrak{C}, \mathfrak{C} \rangle = -1$.

Ha de observarse que no toda la literatura sobre el tema adopta esta definición. No siempre se requiere que se cumpla la condición (i), no siempre se requiere que se cumpla la condición (ii), no siempre se requiere de la existencia de una sección, etc. En consecuencia, tenemos buenas razones para introducir un análisis cuidadoso de la anterior definición para justificar metodológicamente su adopción en vistas a nuestros objetivos. Procedemos a hacerlo a continuación.

Sean $k, (f, \sigma_0)$ como en 3.1.1.

Recordemos que habíamos definido una curva elíptica como una curva proyectiva no singular de género 1 que admite al menos un punto solución. En consecuencia, pedir que la fibración sea una fibración de género 1 recupera la primera de las condiciones para tener una curva elíptica. Por otra parte, dado $v \in C$, la existencia de la sección σ_0 nos dice que $\sigma_0(v)$ pertenece a la f-fibra inducida por v, con lo cual tenemos garantizada la segunda condición de la definición de curva elíptica. Así, hemos recuperado la idea intuitiva original de parametrizar una familia de curvas elípticas con base en una curva fijada.

La imposición de la condición (ii) se concreta para excluir casos triviales como el que sigue. Considérese una k-curva elíptica E y supongamos que $S = E \times C$; es decir, S es la superficie dada por el producto entre las curvas E y C. Si f es la proyección $S \to C$, obtenemos una fibración de género 1 de S sobre la curva base C con sección, de tal forma que todas las fibras son algebraicamente isomorfas a E. Aquí, la fibra genérica es E vista como curva elíptica sobre $k(C)$ (o, más precisamente, la fibra genérica es $E \otimes_k k(C)$), y por lo tanto tiene a su conjunto de puntos k-racionales como subconjunto y, de hecho, como subgrupo, por lo visto en A.1. Esto implica que $E(k(C))$ tiene un cardinal mayor o igual que el de $E(k)$. Si, por ejemplo, fuera $k = \mathbb{C}$, entonces $E(k(C))$ sería no numerable, lo cual hace imposible que sea un grupo finitamente generado. En consecuencia, sin la condición (ii), no podemos tener esperanzas de probar un análogo del Teorema de Mordell, lo cual elimina desde el principio una de las posibilidades naturales de hacer aritmética.

La condición (i) es la más llamativa, pero encuentra una debida justificación en el contexto de modelos minimales. Recuérdese que, dado un *blow-up* $\pi : \widetilde{S} \to S$ de la superficie S en un punto $P \in S$, entonces el divisor excepcional $\pi^{-1}(P)$ de $\widetilde{S}$ tiene *self-intersection* igual a -1 (léase [2, Proposition II.3 (ii)]). Así, de no existir la condición (i), podríamos tomar $\widetilde{f} := f \circ \pi$, de tal forma que, bajo esta nueva fibración, todas las fibras se mantienen isomorfas con la excepción de la fibra de $f(P)$. Esta condición recibe el nombre de *minimalidad relativa* dado que la misma, si bien es implicada por la condición

de minimalidad, no garantiza la implicación recíproca. La razón es que S puede admitir (-1)-curvas sin que necesariamente las mismas sean alcanzadas por las fibras de f. Para ver un ejemplo concreto, léase [25, pp. 83-85].

Finalmente, hagamos un comentario respecto de la definición de fibración elíptica, y su diferencia con el concepto de superficie elíptica. En virtud de nuestra definición, la diferencia entre una superficie elíptica y una fibración elíptica radica en el hecho de que en la superficie elíptica tenemos fijada una sección, en tanto que en la fibración elíptica simplemente conocemos la existencia de alguna. En este sentido estricto y formal, una fibración elíptica induce diferentes superficies elípticas en virtud de las diferentes secciones que admite. Está claro, sin embargo, que se trata de una mera diferencia formal que no tendrá mucha relevancia en la práctica, aunque nos veremos en la necesidad de discriminar entre ambos conceptos en tanto, a partir de una fibración elíptica, veremos cómo inducir una sección de forma canónica. La forma de hacer esto requerirá de un importante resultado que probaremos a continuación, que nos permite relacionar el conjunto de secciones de una fibración elíptica con los puntos de su fibra genérica; lo cual, a su vez, da una primera idea de la importancia de esta fibra genérica. Antes, requeriremos de un sencillo lema al que necesitaremos hacer referencia en diversas ocasiones de aquí en adelante.

Lema 3.1.2 *Sea k un cuerpo algebraicamente cerrado y sea $f : S \to C$ un morfismo algebraico, donde S es una k-superficie proyectiva no singular y C es una k-curva proyectiva no singular. Sea $\sigma : C \to S$ un morfismo algebraico tal que $f \circ \sigma$ es la identidad en C. Entonces la imagen de σ es una curva en S isomorfa a C que intersecta cada fibra de f en un único punto, y de manera transversal.*

Demostración. Sean $a, b \in C$ tales que $\sigma(a) = \sigma(b)$. Aplicando f obtenemos $a = b$, de donde σ es inyectiva. Por otra parte, la expresión $f \circ \sigma = \mathrm{id}_C$ nos dice que, para todo $c \in C$, se tiene $d_{\sigma(c)} f \circ d_c \sigma = \mathrm{id}_{T_c(C)}$, y por un argumento análogo se tiene que $d_c\sigma$ es inyectiva. Por consiguiente, σ es una inmersión algebraica cerrada (léase [31, Theorem 19.1.1]), de donde define un isomorfismo algebraico con su imagen.

Dado $v \in C$, sea $x \in \sigma(C) \cap f^{-1}(v)$. Entonces existe $s \in C$ tal que $x = \sigma(s)$, luego $v = f(x) = f(\sigma(s)) = s$, de donde $x = \sigma(v)$, y por lo tanto $\sigma(C) \cap f^{-1}(v) = \{\sigma(v)\}$. Solamente falta ver que la intersección entre $\sigma(C)$ y $f^{-1}(v)$ en $\sigma(v)$ se da transversalmente.

Veamos que la imagen de $d_v\sigma$ está dada por $d_v\sigma(T_v(C)) = T_{\sigma(v)}(\sigma(C))$. En efecto, se tiene por definición que $d_v\sigma(T_v(C)) \subseteq T_{\sigma(v)}(\sigma(C))$. Como C es no singular, entonces $T_v(C)$ tiene dimensión 1. Como $d_v\sigma$ es un monomorfismo, entonces $d_v\sigma(T_v(C))$ es también de dimensión 1. Además, como C es no singular y $C \cong \sigma(C)$, entonces $\sigma(C)$ es no singular, de donde $T_{\sigma(v)}(\sigma(C))$ es también de dimensión 1. Se sigue entonces de la inclusión inicial que tenemos, de hecho, la igualdad $d_v\sigma(T_v(C)) = T_{\sigma(v)}(\sigma(C))$.

Por otro lado, $T_{\sigma(v)}\left(f^{-1}(v)\right) \subseteq \ker\left(d_{\sigma(v)}f\right)$, puesto que f es constante en $f^{-1}(v)$. Veamos, finalmente, que $T_{\sigma(v)}\left(f^{-1}(v)\right) \cap T_{\sigma(v)}(\sigma(C)) = \{0\}$, lo cual terminará de demostrar nuestro lema.

Dado $x \in T_{\sigma(v)}\left(f^{-1}(v)\right) \cap T_{\sigma(v)}(\sigma(C))$, se tiene de $x \in T_{\sigma(v)}(\sigma(C)) = d_v\sigma(T_v(C))$ que $x = d_v\sigma(y)$ para algún $y \in T_v(C)$. Usando esta última identidad y el hecho de que $x \in T_{\sigma(v)}\left(f^{-1}(v)\right) \subseteq \ker\left(d_{\sigma(v)}f\right)$, obtenemos

$$0 = d_{\sigma(v)}f(x) = d_{\sigma(v)}f(d_v\sigma(y)) = \mathrm{id}_{T_v(C)}(y) = y,$$

y por lo tanto $x = d_v\sigma(y) = d_v\sigma(0) = 0$. Como x era un punto arbitrariamente tomado de $T_{\sigma(v)}\left(f^{-1}(v)\right) \cap T_{\sigma(v)}(\sigma(C))$, entonces $T_{\sigma(v)}\left(f^{-1}(v)\right) \cap T_{\sigma(v)}(\sigma(C)) = \{0\}$. ■

Necesitaremos, también, un sencillo resultado de teoría elemental de conjuntos.

Lema 3.1.3 *Sean A y B dos conjuntos, sea $f : A \to B$ una función y sean $g_1 : B \to A$, $g_2 : B \to A$ tales que $f \circ g_1$ y $f \circ g_2$ son iguales a la identidad en B. Si g_1 y g_2 tienen la misma imagen, entonces $g_1 = g_2$.*

Demostración. Sea $x \in B$. Como $g_1(x)$ está en la imagen de g_1, que es igual a la imagen de g_2, entonces existe $y \in B$ tal que $g_1(x) = g_2(y)$. Aplicando f obtenemos

$$x = f(g_1(x)) = f(g_2(y)) = y,$$

y por lo tanto $g_1(x) = g_2(x)$. Como $x \in B$ era arbitrario, concluimos entonces que $g_1 = g_2$, como queríamos. ■

Proposición 3.1.4 *Sea k un cuerpo algebraicamente cerrado y sea $f : S \to C$ una fibración elíptica, donde S es una k-superficie proyectiva no singular y C es una k-curva proyectiva no singular. Sea E la $k(C)$-curva elíptica dada por la fibra genérica de f. Entonces hay una biyección entre $E(k(C))$ y el conjunto de secciones de f.*

Demostración. Dada una sección σ de f, la misma induce una curva $D := \sigma(C) \cong C$ dentro de S, que intersecta cada fibra en un solo punto, por el Lema 3.1.2. Tomando la clausura Zariski de D, la misma se extiende naturalmente al esquema subyacente $\mathcal{S}$ de S[1], de modo que la misma intersecta la fibra genérica $E(k(C))$ en un solo punto.

Recíprocamente, dado $P \in E(k(C))$, tomamos la clausura $\mathcal{D}$ de P en $\mathcal{S}$, que es una curva en $\mathcal{S}$, y llamamos D a su restricción a S. Por construcción, tenemos un morfismo $f_1 : D \to C$ dado por la restricción de f a D. Es claro que f_1 no es constante, dado que, si lo fuera, $D \subseteq f^{-1}(v)$ para algún $v \in C$, y por lo tanto $\mathcal{D} \subseteq f^{-1}(v)$; lo cual, usando que $P \in \mathcal{D}$, contradice que $P \in E(k(C))$. Por lo tanto la imagen de f_1 es densa.

Veamos que f_1 es un isomorfismo. Dado $w \in D$, el anillo local de D en w, que notamos $\mathcal{O}_{D,w}$, es isomorfo al anillo local de $v := f_1(w)$ en C, notado $\mathcal{O}_{C,v}$. Esto es así porque la densidad de la imagen de f_1 nos dice que $f_1^* : \mathcal{O}_{C,v} \to \mathcal{O}_{D,w}$ es inyectivo, de donde $\mathcal{O}_{C,v}$ es isomorfo a un subanillo de $\mathcal{O}_{D,w}$, de modo que la extensión de anillos resultante es una extensión integral. Pero ambos anillos tienen a $k(C)$ como su cuerpo de fracciones y $\mathcal{O}_{C,v}$ es integralmente cerrado, dado que C es una curva no singular (de donde todos sus anillos locales son anillos locales regulares; léase [10, p. 32]); en particular, normal (es decir, todos sus anillos locales son integralmente cerrados). Por lo tanto, f_1^* es sobreyectivo; ergo, biyectivo. Aquí estamos usando que todo anillo local regular es un dominio integralmente cerrado, como se prueba en [17, p. 121]. En definitiva, f_1 resulta ser localmente un isomorfismo, de donde es un isomorfismo global. La inversa de este isomorfismo nos da una sección $\sigma : C \to S$ de f cuya imagen es D.

Veamos que esta correspondencia es biyectiva. Dado $P \in E(k(C))$, el párrafo anterior nos dice que P induce una sección σ_P de f cuya imagen D_P es la restricción a S de la clausura $\mathcal{D}_P$ de P en $\mathcal{S}$. Queremos ver que, si tomamos la clausura de D_P en $\mathcal{S}$ e intersecamos con E, obtenemos P. En efecto, como $P \in D_P \subseteq \mathcal{D}_P$, tomando clausura en $\mathcal{S}$

[1] Aquí, por *esquema subyacente* de una k-variedad nos referimos, naturalmente, a la transformación de dicha variedad por el funtor *fully faithful* natural de las k-variedades a los esquemas sobre k. Esto consiste, esencialmente, en añadir de forma natural puntos genéricos a cada subespacio irreducible de una variedad para obtener un esquema. Para más detalles, léase [10, p. 78]

obtenemos que la clausura de D_P en $\mathcal{S}$ es $\mathcal{D}_P$. Este último contiene al elemento P, el cual está también en E. Como $E \cap \mathcal{D}_P$ es un conjunto de un solo punto, entonces $\mathcal{D}_P \cap E = \{P\}$.

Veamos ahora la relación inversa. Dada una sección σ de f, tomamos la clausura $\mathcal{C}_\sigma$ de $\sigma(C)$ en $\mathcal{S}$ e intersecamos la misma con E, lo cual nos dará un conjunto de un solo punto $P \in E(k(C))$. Queremos ver que, si tomamos la clausura $\mathcal{D}_P$ de P en $\mathcal{S}$ y la restricción D_P de $\mathcal{D}_P$ a S, entonces la inversa de la restricción a D_P de f (compuesta con la inclusión de D_P en S) es σ. Lo primero que hemos de observar es que $\mathcal{C}_\sigma = \mathcal{D}_P$, puesto que, en general, dado un divisor irreducible Y de S tal que la intersección entre su clausura $\mathcal{Y}$ en $\mathcal{S}$ y la fibra genérica es no vacía, entonces la clausura en $\mathcal{S}$ de cada punto de dicha intersección es igual a $\mathcal{Y}$ (léase [15, p. 349]). En nuestro caso tenemos $Y = \sigma(C)$ y $\mathcal{Y} = \mathcal{C}_\sigma$, y como $P \in \mathcal{C}_\sigma \cap E(k(C))$, usando el resultado citado obtenemos que la clausura $\mathcal{D}_P$ de P en $\mathcal{S}$ iguala a $\mathcal{Y} = \mathcal{C}_\sigma$. Así, tanto σ como la inversa de la restricción a D_P de f (compuesta con la inclusión de D_P en S) son secciones de f que tienen la misma imagen. El Lema 3.1.3 nos dice entonces que coinciden. ■

3.2 Modelo de Kodaira-Néron

La definición de superficie elíptica nos dice cómo, dado un cuerpo k algebraicamente cerrado y una k-superficie elíptica, la misma induce naturalmente una $k(C)$-curva elíptica dada por la fibra genérica de la fibración elíptica correspondiente, donde C es la curva proyectiva no singular sobre la cual tenemos definida nuestra superficie elíptica. En esta sección veremos que, recíprocamente, dada una k-curva proyectiva no singular y una curva elíptica sobre su cuerpo de funciones, es posible construir una superficie elíptica cuya fibra genérica sea esta curva elíptica tomada en primer lugar.

Proposición 3.2.1 *Sea k un cuerpo algebraicamente cerrado y sea C una k-curva proyectiva no singular. Dada una $k(C)$-curva elíptica E cuyo discriminante admite al menos una solución, existe una fibración elíptica $f : S \to C$, donde S es una k-superficie proyectiva no singular, cuya fibra genérica es E.*

Demostración. Escribimos E en forma de Weierstrass. Sea $\mathfrak{E}$ la unión entre los polos de sus coeficientes y las raíces de su discriminante, sea $C' = C \setminus \mathfrak{E}$ y sea $S' \subseteq \mathbb{P}^2(k) \times C'$ la superficie proyectiva abierta definida por la ecuación inducida por E. Sea $f' : S' \to C'$ la restricción de la proyección a C'. Si W es la clausura Zariski de S', tenemos inducido un morfismo no singular $\overline{f} : W \to C$ que extiende a f'. Además, W es una superficie proyectiva, aunque no necesariamente es no singular. En efecto, las fibras de $\overline{f}$ son o bien curvas elípticas, o bien cúbicas en forma de Weierstrass con discriminante nulo. Desingularizando estos puntos singulares y levantando $\overline{f}$ en los *blow-ups* realizados para tal fin, obtenemos un morfismo $\widetilde{f} : S'' \to C$, donde S'' es una superficie proyectiva no singular cuya fibra genérica es E por construcción, y que admite una sección inducida por una de las inyecciones naturales $C' \to S' \subseteq \mathbb{P}^2(k) \times C'$.

Si acaso alguna de las $\widetilde{f}$-fibras tuviese alguna (-1)-curva, contraemos la misma usando el **Teorema de Castelnuovo** (léase [10, p. 414]), obteniendo naturalmente una nueva fibración donde nos hemos deshecho de una de las fibras problemáticas. Repitiendo sucesivamente, proceso que finaliza en un número finito de pasos, obtenemos una k-superficie proyectiva no singular S y una fibración elíptica $f : S \to C$ cuya fibra genérica es E. La existencia de fibras singulares está garantizada en virtud de la hipótesis sobre el discriminante de E. ■

Esta fibración es, además, única a menos de isomorfismo. Esto se debe a la existencia de una propiedad universal asociada a la condición de minimalidad relativa: dadas dos fibraciones elípticas h y h' con fibras genéricas isomorfas, existe un único morfismo g entre las superficies proyectivas subyacentes tal que $h' = h \circ g$. Esencialmente, la razón de esto es que el isomorfismo entre sus fibras genéricas induce un morfismo birracional entre ambas superficies proyectivas, que a su vez se puede extender a un isomorfismo. Compárese con el resultado análogo concerniente a morfismos birracionales entre superficies minimales de dimensión de Kodaira no negativa (léase [25, p. 69]; consultar también [2, pp. 19-20]).

Lo que nos importa, al fin y al cabo, es la posibilidad de poder asociar (al menos) una superficie elíptica a cada curva elíptica definida sobre el cuerpo de fracciones de una curva proyectiva no singular, para poder aplicar la teoría de superficies elípticas sin necesitar, a priori, más que una curva elíptica sobre un determinado cuerpo.

3.3 Fibras singulares

El objetivo de esta sección es poner énfasis en el segundo ítem de la Definición 3.1.1 y analizar las fibras singulares de las superficies elípticas. Encontraremos que la estructura de dichas fibras singulares es fundamental para gran parte de la aritmética que se puede hacer en superficies elípticas. A partir de aquí, comenzaremos a centrarnos en el cuerpo $\mathbb{C}$. Si bien lo que desarrollaremos se extiende en general sobre cuerpos algebraicamente cerrados (en particular para $\overline{\mathbb{Q}}$), hemos preferido desarrollar la teoría sobre $\mathbb{C}$, en primer lugar, dada la caracterización que hemos dado del grupo de Néron-Severi en A.2; y, en segundo lugar, para mantener la fidelidad del contexto sobre el cual hicimos surgir nuestra motivación de las superficies elípticas.

Recordemos que, por el Lema A.3.9, todas las fibras de una superficie elíptica son algebraicamente equivalentes. Esto le da sentido al enunciado del siguiente lema, del cual haremos uso.

Lema 3.3.1 *Sea (f, σ_0) una $\mathbb{C}$-superficie elíptica. Sea S la superficie subyacente. Sea $g(C)$ el género de C. Entonces $\langle K_S, K_S \rangle = 0$ y*

$$K_S \approx (2g(C) - 2 + \chi(S))\, F,$$

donde F es la clase de equivalencia algebraica de las f-fibras.

No probaremos el Lema 3.3.1, pero sí exhibiremos esquemáticamente las ideas de una posible demostración del mismo, siguiendo [3]. Del Teorema A.3.3 se sigue que, dada una fibra no singular F (en particular, $p_a(F) = g(F) = 1$), $0 = \langle F, F \rangle + \langle F, K_S \rangle = \langle F, K_S \rangle$, donde en la última igualdad hemos usado el Lema A.3.1. Como el pairing de intersección es compatible con equivalencia algebraica, y todas las fibras son algebraicamente equivalentes por el Lema A.3.9, entonces esto vale también para cualquier fibra. Apelando a que K_S o $-K_S$ es efectivo, por el mismo argumento que expondremos en la Proposición 3.5.3 se sigue que K_S está generado por componentes irreducibles de f-fibras (de donde, nuevamente por el Lema A.3.1, se tiene $\langle K_S, K_S \rangle = 0$) y, usando esto y aplicando el **Lema de Zariski** (léase [1, p. 111]), se puede ver que, de hecho, K_S está generado por f-fibras. Usando que todas las fibras son algebraicamente equivalentes por el Lema A.3.9, se obtiene la expresión $K_S \approx mF$ para algún $m \in \mathbb{Z}$. El valor de m puede computarse por medio del análisis de la sucesión espectral inducida por f, obteniendo $m = 2g(C) - 2 + \chi(S)$.

Definición 3.3.2 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica y sea E su fibra genérica, la cual es una curva elíptica sobre $\mathbb{C}(C)$ que escribimos en forma de Weierstrass y, en virtud de la Proposición 3.1.4, consideramos la sección σ_0 inducida por el punto $O = (0 : 1 : 0)$, de forma que (f, σ_0) es una superficie elíptica. Notamos (O) a la imagen por σ_0 de C. Esta sección es la que conocemos como* sección cero *de la superficie elíptica. En general, notamos (P) a la imagen de C por la sección inducida por P, para cada $P \in E(\mathbb{C}(C))$. El Lema 3.1.2 nos dice que (P) es una subvariedad irreducible de codimensión 1 en S, por ser algebraicamente isomorfa a C. En particular, si $P, Q \in E(\mathbb{C}(C))$ y $P \neq Q$, entonces necesariamente se tiene $\langle (P), (Q) \rangle \geq 0$.*

Con base en la Definición 3.3.2, podemos obtener un corolario del Lema 3.3.1.

Corolario 3.3.3 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica y sea E su fibra genérica. Sea $P \in E(\mathbb{C}(C))$. Entonces $\langle (P), (P) \rangle = -\chi(S)$.*

Demostración. Por el Teorema A.3.3 se tiene $2g((P)) - 2 = \langle (P), (P) \rangle + \langle (P), K_S \rangle$. Aplicando el Lema 3.3.1 y usando que $g((P)) = g(C)$ porque $(P) \cong C$, se tiene

$$2g(C) - 2 = \langle (P), (P) \rangle + \langle (P), (2g(C) - 2 + \chi(S)) F \rangle$$

$$2g(C) - 2 = \langle (P), (P) \rangle + 2g(C) - 2 + \chi(S)$$

$$\langle (P), (P) \rangle = -\chi(S),$$

donde hemos usado que $\langle (P), F \rangle = 1$, por el Lema 3.1.2. ■

Con estos resultados a nuestra disposición, podemos comenzar un análisis de las fibras singulares de una superficie elíptica, que jugarán un rol fundamental en la solución del problema principal de esta tesis.

Definición 3.3.4 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Para cada $v \in C$, notamos $m_v \in \mathbb{N}$ al número de componentes irreducibles de la fibra $f^{-1}(v)$.*

Teorema 3.3.5 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Sea $v \in C$. Entonces:*

(i) Solamente una componente irreducible de $f^{-1}(v)$ tiene intersección no vacía con (O). Recibe el nombre de componente identidad *de $f^{-1}(v)$ y se nota $\Theta_{v,0}$. Su multiplicidad en el divisor $f^{-1}(v)$, que notamos $\mu_{v,0}$, es igual a 1.*

(ii) Si $f^{-1}(v)$ es una curva irreducible y singular (es decir, $m_v = 1$ y $f^{-1}(v) = \Theta_{v,0}$), entonces $\Theta_{v,0}$ es o bien una curva racional con un nodo, o bien una curva racional cuspidal.

(iii) Si $f^{-1}(v)$ es una curva reducible y singular (es decir, $m_v > 1$), entonces todas las componentes irreducibles de $f^{-1}(v)$ son curvas no singulares racionales cuyo número de self-intersection *es igual a -2.*

Demostración. El ítem (i) es consecuencia directa de que $(O) \cap F$ es un conjunto de un solo punto en el que ambas curvas se intersectan transversalmente, por el Lema 3.1.2.

En cuanto al ítem (ii), el mismo no es más que una reformulación sofisticada de la clasificación de curvas en forma de Weierstrass con determinante nulo (léase [12, III 5]), en vistas a que la fibra genérica de la superficie elíptica es una curva elíptica sobre $\mathbb{C}(C)$ y, por consiguiente, es irreducible.

En cuanto al ítem (iii), sea $v \in C$ tal que $m_v > 1$, y sea Θ una de las componentes irreducibles de $f^{-1}(v)$. Por el Lema A.3.1, $\langle \Theta, \Theta \rangle < 0$. Por el Teorema A.3.3 tenemos

$$2p_a(\Theta) - 2 = \langle \Theta, \Theta \rangle + \langle \Theta, K_S \rangle = \langle \Theta, \Theta \rangle < 0, \tag{3.1}$$

donde en la última igualdad hemos usado el Lema 3.3.1 para reemplazar K_S por un múltiplo de $f^{-1}(v)$ y luego aplicamos el Lema A.3.1. Como $p_a(\Theta)$ es un entero no negativo, la única forma de que $2p_a(\Theta) - 2 < 0$, que equivale a $p_a(\Theta) < 1$, es que $p_a(\Theta) = 0$. Por consiguiente, el Lema A.3.4 nos dice que Θ es no singular y racional.

La racionalidad de Θ nos dice que $g(\Theta) = p_a(\Theta) = 0$. Así, volviendo a la expresión 3.1, tenemos $-2 = \langle \Theta, \Theta \rangle$. ■

Ahora introduciremos la *Notación de Kodaira* para las fibras singulares, que será muy útil para trabajar con las mismas.

Definición 3.3.6 *En virtud del Teorema 3.3.5, dada S una $\mathbb{C}$-superficie proyectiva no singular, C una $\mathbb{C}$-curva proyectiva no singular y $f : S \to C$ una fibración elíptica, entonces para cada $v \in S$ fijamos una numeración $\{\Theta_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}\}$ de las $m_v - 1$ componentes irreducibles de $f^{-1}(v)$ distintas de la componente identidad $\Theta_{v,0}$ y, para cada $i \in [1, m_v - 1]$ y todo $v \in C$, definimos $\mu_{v,i} \in \mathbb{N}$ a la multiplicidad de $\Theta_{v,i}$ en $f^{-1}(v)$, de modo que tenemos la igualdad de divisores*

$$f^{-1}(v) = \sum_{i=0}^{m_v - 1} \mu_{v,i} \Theta_{v,i}$$

para todo $v \in C$. A este sistema de numeración se le añade, naturalmente, la componente identidad $\Theta_{v,0}$ junto a su multiplicidad $\mu_{v,0} = 1$.

Una de las tareas más importantes al lidiar con superficies elípticas es poder comprender la estructura de sus fibras singulares. Para tal fin, se introduce la siguiente clasificación.

Definición 3.3.7 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Sea $v \in C$ y sea $F_v := f^{-1}(v)$. Entonces:*

- *Decimos que F_v es* de tipo I_0 *si $m_v = 1$ y F_v es no singular (de donde $g(F_v) = 1$).*
- *Decimos que F_v es* de tipo I_1 *si $m_v = 1$ y F_v es una curva racional con un nodo.*
- *Decimos que F_v es* de tipo I_2 *si $m_v = 2$, $\mu_{v,1} = 1$ y las componentes $\Theta_{v,0}$ y $\Theta_{v,1}$ se intersectan en exactamente dos puntos, y de forma tranversal; de donde necesariamente $\langle \Theta_{v,0}, \Theta_{v,1} \rangle = 2$.*

- *Dado* $m \in \mathbb{N}_{\geq 3}$, *decimos que* F_v *es* de tipo I_m *si* $m_v = m$ *y la numeración de las componentes irreducibles de* F_v *en 3.3.6 puede tomarse de tal forma que, para todos los* $i, j \in [0, m-2] \cap \mathbb{N}_0$, *se tenga* $\mu_{v,i} = \mu_{v,m-1} = 1$, $\langle \Theta_{v,i}, \Theta_{v,i+1} \rangle = \langle \Theta_{v,m_v-1}, \Theta_{v,0} \rangle = 1$ *y, si* $i+1 < j$ *y* $(i,j) \neq (0, m_v - 1)$, $\langle \Theta_{v,i}, \Theta_{v,j} \rangle = 0$.

- *Decimos que* F_v *es* de tipo II *si* $m_v = 1$ *y* F_v *es una curva racional cuspidal.*

- *Dado* $b \in \mathbb{N}_0$, *decimos que* F_v *es* de tipo I_b^* *si* $m_v = b + 5$ *y la numeración de las componentes irreducibles de* F_v *en 3.3.6 puede tomarse de tal forma que, para todos los* $i, j \in [0, b+4] \cap \mathbb{N}_0$ *con* $i \leq j$, *se tenga*

$$\mu_{v,i} = \begin{cases} 1, & i \leq 3 \\ 2, & i > 3 \end{cases}, \quad \langle \Theta_{v,i}, \Theta_{v,j} \rangle = \begin{cases} 1, & (i,j) \in \{(0,4), (1,4), (2, b+4), (3, b+4)\}, \\ 1, & 5 \leq i+1 = j, \\ -2, & i = j, \\ 0, & \text{en todo otro caso.} \end{cases}$$

  Obsérvese que el caso $i = j$ *está dado a priori por el último ítem del Teorema 3.3.5.*

- *Decimos que* F_v *es* de tipo III *si* $m_v = 2$ *y* $\Theta_{v,0}$ *y* $\Theta_{v,1}$ *se intersectan en un solo punto y satisfacen* $\langle \Theta_{v,0}, \Theta_{v,1} \rangle = 2$.

- *Decimos que* F_v *es* de tipo IV *si* $m_v = 3$, $\mu_{v,i} = 1$ *para todo* $i \in \{1, 2\}$, *de tal forma que las tres componentes concurren en un único punto y el número de intersección entre dos distintas de ellas es igual a* 1.

- *Decimos que* F_v *es* de tipo II^* *si* $m_v = 9$ *y la numeración de las componentes irreducibles de* F_v *en 3.3.6 puede tomarse tal que* $\mu_{v,1} = \mu_{v,7} = 2$, $\mu_{v,2} = \mu_{v,5} = 4$, $\mu_{v,3} = 6$, $\mu_{v,4} = 5$, $\mu_{v,6} = \mu_{v,8} = 3$ *y tal que, si* $i, j \in [0, 8] \cap \mathbb{N}_0$ *con* $i \leq j$,

$$\langle \Theta_{v,i}, \Theta_{v,j} \rangle = \begin{cases} 1, & (i,j) \in \{(3,8), (0,7)\}, \\ 1, & 2 \leq i+1 = j \leq 7, \\ -2, & i = j, \\ 0, & \text{en todo otro caso.} \end{cases}$$

- *Decimos que* F_v *es* de tipo III^* *si* $m_v = 8$ *y la numeración de las componentes irreducibles de* F_v *en 3.3.6 puede tomarse tal que se cumpla* $\mu_{v,1} = \mu_{v,5} = \mu_{v,7} = 2$, $\mu_{v,2} = \mu_{v,4} = 3$, $\mu_{v,3} = 4$, $\mu_{v,6} = 1$ *y, dados* $i, j \in [0, 7] \cap \mathbb{N}_0$ *con* $i < j$,

$$\langle \Theta_{v,i}, \Theta_{v,j} \rangle = \begin{cases} 1, & (i,j) = (3,7), \\ 1, & i+1 = j \leq 6, \\ -2, & i = j, \\ 0, & \text{en todo otro caso.} \end{cases}$$

- *Decimos que* F_v *es* de tipo IV^* *si* $m_v = 7$ *y la numeración de las componentes irreducibles de* F_v *en 3.3.6 puede tomarse tal que se satisfaga* $\mu_{v,1} = \mu_{v,5} = 1$,

$\mu_{v,2} = \mu_{v,4} = \mu_{v,6} = 2$, $\mu_{v,3} = 3$ *y tal que, dados* $i, j \in [0,6] \cap \mathbb{N}_0$ *con* $i \leq j$,

$$\langle \Theta_{v,i}, \Theta_{v,j} \rangle = \begin{cases} 1, & (i,j) \in \{(0,6),(3,6)\} \\ 1, & 2 \leq i+1 = j \leq 5, \\ -2, & i = j, \\ 0, & \textit{en todo otro caso.} \end{cases}$$

Si $m_v > 1$, *decimos que* F_v *es* multiplicativa *si es de tipo* I_n *para algún* $n \in \mathbb{N}_{\geq 2}$. *En caso contrario, decimos que* F_v *es* aditiva.

En la Definición 3.3.7 se listan todos los posibles tipos de fibras singulares que puede tener una superficie elíptica. Utilizando la versión general del Algoritmo de Tate que hemos expuesto en 3.4 es posible derivar como corolario que, en efecto, la lista de posibilidades es completa.

Convención 3.3.8 *De aquí en adelante, siempre que trabajemos en las fibras reducibles de una superficie elíptica, consideraremos una numeración en 3.3.6 compatible con las relaciones en 3.3.7.*

Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Para cada $v \in C$ definimos un retículo T_v como el grupo libre de rango $m_v - 1$ generado por $\{\Theta_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}\}$, con el pairing $(\cdot,\cdot)$ dado por $(\Theta_{v,i}, \Theta_{v,j}) = -\langle \Theta_{v,i}, \Theta_{v,j} \rangle$, para todos los $i, j \in [1, m_v - 1] \cap \mathbb{N}$. El hecho de que estamos excluyendo la componente principal nos dice que todos estos grupos serán triviales, excepto para aquellos puntos de C que inducen f-fibras que son singulares y reducibles.

Sea $v \in C$ tal que $f^{-1}(v)$ es singular y reducible. En consecuencia, es posible separar en los casos reducibles ofrecidos en la Definición 3.3.7 y calcular la matriz de intersección de T_v respecto del pairing $(\cdot,\cdot) = -\langle \cdot,\cdot \rangle$. De hecho, las mismas son exactamente las encontradas en 3.3.7, cambiando los signos en el pairing, y añadiendo el resultado dado por el último ítem del Teorema 3.3.5. Si uno efectúa las correspondientes verificaciones, puede corroborar que, en cada caso, obtiene una matriz simétrica definida positiva, con lo cual el retículo T_v resulta ser un retículo definido positivo. En particular, las componentes irreducibles de $f^{-1}(v)$ distintas de la identidad son $\mathbb{Z}$-linealmente independientes bajo la relación de equivalencia algebraica (donde el pairing de intersección de S sigue estando definido) y generan un grupo isomorfo a T_v. Por último, calculando el determinante de T_v, que notamos $m_v^{(1)}$, vemos que el mismo iguala al número de componentes simples de $f^{-1}(v)$; es decir, $m_v^{(1)} := \det(T_v)$ es el número de componentes irreducibles de multiplicidad 1 de la f-fibra inducida por v. Esto incluye a la correspondiente componente identidad, la cual es siempre simple por el primer ítem del Teorema 3.3.5, de manera que $m_v^{(1)} \geq 1$ para todo $v \in C$.

Resumiremos estos resultados en una proposición para la cual utilizaremos una notación clásica en teoría de retículos. Recordemos que, dado un retículo M, notamos M^- al retículo cuyo grupo abeliano libre subyacente es el mismo que el de M, y la forma bilineal simétrica no degenerada asociada consiste en tomar el opuesto aditivo de la de M.

Proposición 3.3.9 *Sea* S *una* $\mathbb{C}$*-superficie proyectiva no singular y sea* C *una* $\mathbb{C}$*-curva proyectiva no singular. Sea* $f : S \to C$ *una fibración elíptica. Sea* $v \in C$ *tal que* $f^{-1}(v)$ *es singular y reducible. Entonces las componentes irreducibles de* $f^{-1}(v)$ *distintas de* $\Theta_{v,0}$ *son*

$\mathbb{Z}$-linealmente independientes en $\mathrm{NS}(S)$ *y generan un subgrupo de rango* $m_v - 1$ *que, con el pairing de intersección de* S*, tiene estructura de retículo y, como tal, es naturalmente isomorfo a* T_v^-*. Además,* $m_v^{(1)} := \det(T_v)$ *es el número de componentes irreducibles de multiplicidad* 1 *de* $f^{-1}(v)$*.*

Convención 3.3.10 *Sea* S *una* $\mathbb{C}$*-superficie proyectiva no singular y sea* C *una* $\mathbb{C}$*-curva proyectiva no singular. Sea* $f : S \to C$ *una fibración elíptica, y sea* $v \in C$ *tal que* $f^{-1}(v)$ *es irreducible. Definimos entonces* T_v *como el retículo de rango* 1 *y determinante unitario, de modo que podemos extender la definición* $m_v^{(1)} := \det(T_v)$*, y nuevamente esto coincide con la cantidad de componentes irreducibles de multiplicidad* 1 *de* $f^{-1}(v)$*.*

La Proposición 3.3.9 es la base para aplicar la teoría de retículos en nuestro estudio de las superficies elípticas, lo cual nos brindará muy poderosas herramientas en las aplicaciones y, en particular, en el problema que buscamos resolver.

Finalmente, enunciaremos un resultado que necesitaremos en la sección 3.5 y que concierne la característica topológica de Euler de las fibras singulares.

Lema 3.3.11 *Sea* S *una* $\mathbb{C}$*-superficie proyectiva no singular y sea* C *una* $\mathbb{C}$*-curva proyectiva no singular. Sea* $f : S \to C$ *una fibración elíptica. Dada una* f*-fibra* $\mathscr{F}$*, se tiene* $e(\mathscr{F}) \geq 0$*, con igualdad si y solo si* $\mathscr{F}$ *es no singular.*

Daremos una idea esquemática de cómo se demuestra el Lema 3.3.11 siguiendo [21], al cual el lector interesado en una demostración completa puede acceder.

Si $R \subseteq C$ es el conjunto de puntos cuyas f-fibras son singulares, es posible tomar una 1-forma racional ω_C en C sin ceros ni polos en R. Fijada ω_C, se define $\omega := f^*\omega_C$, la 1-forma racional en X inducida por ω_C vía la fibración f. Dado $P \in S$ y un sistema de coordenadas locales (x, y) en P (es decir, las curvas $y = 0$ y $x = 0$ se intersectan en P transversalmente), sabemos entonces que, en el correspondiente entorno de P, $\omega = g(h_1 dx + h_2 dy)$ para algún $g \in \mathrm{Frac}(\mathcal{O}_{S,P})$ y algunos $h_1, h_2 \in \mathcal{O}_{S,P}$ coprimos. Como g es único a menos de multiplicación por unidades en $\mathcal{O}_{S,P}$ y (h_1, h_2) es único a menos de una transformación lineal en $\mathrm{GL}_2(\mathcal{O}_{S,P})$, entonces $m_P(\omega) := \dim_{\mathbb{C}}\left(\frac{\mathcal{O}_{S,P}}{(h_1,h_2)}\right)$ está bien definido, como así también $(\omega) := \mathrm{div}(g) \in \mathrm{Div}(S)$, el divisor principal de S inducido por g. Definimos

$$\langle \omega \rangle := \sum_{P \in S} m_P(\omega) P.$$

Como f es no singular en $C \setminus R$, se tiene $m_P(\omega) = 0$ para todo $P \in S \setminus f^{-1}(R)$, y que $(\omega) = \sum_{v \in C} D_v$, donde, para cada $v \in C$, D_v es un divisor tal que su soporte (es decir, la unión de sus divisores primos) está contenido en $f^{-1}(v)$. Se define, para cada $v \in C$,

$$\Delta_v := \left[\sum_{P \in f^{-1}(v)} m_P(\omega) \right] - \langle D_v, D_v \rangle .$$

Es posible demostrar que $\Delta_v \geq 0$ para todo $v \in C$, y que la igualdad se da para aquellos $v \in C$ cuyas f-fibras son no singulares. De hecho, la no negatividad es consecuencia de que Δ_v es la suma de dos números no negativos, puesto que el pairing de intersección es negativo en las componentes irreducibles de alguna fibra fijada, como vimos en la Proposición 3.3.9. Ambos sumandos son nulos cuando $v \notin R$.

Más difícil de probar es el recíproco: que, dado $v \in R$, $\Delta_v > 0$. Esto se sigue de un análisis caso por caso de las posibles fibras singulares, que fueron explicitadas en la Definición 3.3.6. Finalmente, se muestra que $e\left(f^{-1}(s)\right) = \Delta_s$ para todo $s \in C$, nuevamente por un análisis caso por caso, lo cual prueba lo que buscamos.

3.4 Algoritmo de Tate

En esta sección expondremos el conocido *Algoritmo de Tate*, el cual tiene importantes aplicaciones en la teoría de superficies elípticas (en particular, en nuestro problema). Con él veremos no solamente que la lista de singularidades en la Definición 3.3.6 es completa, sino que además veremos cómo encontrarlas todas y clasificarlas.

Dada una curva elíptica sobre el cuerpo de fracciones de una curva proyectiva no singular y de discriminante con al menos una solución, es natural preguntarse si es posible encontrar y caracterizar las fibras singulares de una superficie elíptica que tenga a esta curva como fibra genérica. Este problema puede resolverse muy satisfactoriamente, y este es el objetivo de la presente sección y el algoritmo que lleva su nombre.

Los típicos materiales que suelen consultarse para una exposición rigurosa y completa de este algoritmo son [27, IV 9] y el trabajo original de Tate [30], como así también un trabajo de Michael Szydlo del año 2004 [29] extendiendo el algoritmo a cuerpos no perfectos.

En esta sección expondremos una versión extremadamente simplificada del mismo algoritmo que, en consecuencia, aplicará bajo muy restrictivas condiciones que, sin embargo, serán suficientes para nuestros propósitos. Dedicaremos algunos párrafos para ser específicos en esta consideración.

En general, para una teoría clásica sobre superficies elípticas bastaría exponer el algoritmo para caracterizar las fibras de una fibración elíptica sobre un cuerpo k algebraicamente cerrado (o, en caso de requerirlo, simplemente cuerpo perfecto). Si, además, se trabaja sobre característica distinta de 2, el algoritmo puede simplificarse considerablemente, dado que muchas transformaciones involucradas no son necesarias, y los casos en que se subdivide resultan ser menores. En nuestro caso, como trabajamos sobre $\mathbb{C}$, contamos con esta ventaja computacional. Así, podemos exponer el Algoritmo de Tate tal y como se expone para cuerpos perfectos de característica distinta de 2. Un desarrollo del algoritmo bajo estas suposiciones puede encontrarse en [25, 5.8].

Sin embargo, optaremos metodológicamente por hacer una simplificación adicional, y supondremos que la curva base sobre la que está definida la superficie elíptica es $C = \mathbb{P}^1(\mathbb{C})$. Haremos esta simplificación por tres motivos: en primer lugar, porque dicha simplificación permite exponer el algoritmo en términos de relaciones completamente elementales, sin involucrar conceptos técnicos provenientes del contexto de álgebra conmutativa en los anillos de valuación. En segundo lugar, porque es extremadamente sencillo generalizar esta exposición al caso general de una curva proyectiva no singular cualquiera, por medio de la correcta interpretación de las relaciones y su traducción al contexto general, respecto de lo cual diremos algunas palabras al finalizar esta sección. Y, en tercer lugar, porque no solamente nos interesará el algoritmo por su interés teórico (probar que la lista de singularidades dada en 3.3.6 es completa), sino también porque lo aplicaremos en un caso bien concreto en el último capítulo, y dicho caso concreto involucra una superficie elíptica cuya curva base es, precisamente, $\mathbb{P}^1(\mathbb{C})$. En definitiva, tenemos muy buenas razones para optar convenientemente por esta exposición del Algoritmo de Tate.

En nuestra versión simplificada, el Algoritmo de Tate se enfrenta con el siguiente

problema. Sea

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

$$a_1, a_2, a_3, a_4, a_6 \in \mathbb{C}(t)$$

una $\mathbb{C}(t)$-curva elíptica en forma de Weierstrass cuyo discriminante admite al menos una solución. Nos preguntamos por las fibras no singulares en el modelo de Kodaira-Néron de dicha curva elíptica, recordando que el cuerpo de fracciones de $\mathbb{P}^1(\mathbb{C})$ es $\mathbb{C}(t)$.

Como $\text{Frac}(\mathbb{C}[t]) = \mathbb{C}(t)$, entonces, por lo visto en 1.2, podemos tomar un cambio de variables admisible y suponer sin pérdida de generalidad que $a_i \in \mathbb{C}[t]$ para todo $i \in \{1, 2, 3, 4, 6\}$. Decimos entonces que E es una $\mathbb{C}(t)$-curva elíptica *integral*. Notamos $\Delta \in \mathbb{C}[t] \setminus \{0\}$ a su discriminante. Como el discriminante original admitía al menos una solución, entonces Δ tiene grado positivo.

Dado $\alpha \in \mathbb{C}$, definimos $E(\alpha)$ a la $\mathbb{C}$-cúbica en forma de Weierstrass

$$E(\alpha) : y^2z + a_1(\alpha)xyz + a_3(\alpha)yz^2 = x^3 + a_2(\alpha)x^2z + a_4(\alpha)xz^2 + a_6(\alpha)z^3.$$

Así, si α no es una de las finitas raíces de Δ, entonces $E(\alpha)$ es una $\mathbb{C}$-curva elíptica.

Como $\mathbb{C}$ tiene característica distinta de 2, podemos suponer, vía otro cambio admisible de variables, que $a_1 = a_3 = 0$; de forma que, en definitiva, tenemos

$$E : y^2z = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

$$a_1 = 0, a_3 = 0, a_2, a_4, a_6 \in \mathbb{C}[t],$$

$$\Delta = -432a_6^2 + 288a_2a_4a_6 + 16a_2^2a_4^2 - 64a_2^3a_6 - 64a_4^3 \in \mathbb{C}[t] \setminus \mathbb{C}.$$

Tomamos una fibración elíptica $f : S \to \mathbb{P}^1(\mathbb{C})$, donde S es una $\mathbb{C}$-superficie proyectiva, lo cual es posible por la Proposición 3.2.1. Nos preguntamos: dado $\alpha \in \mathbb{P}^1(\mathbb{C})$, ¿qué tipo de fibra es $f^{-1}(\alpha)$?

Lo primero que sabemos es que, si $\alpha \neq (1 : 0)$, entonces $\alpha \in \mathbb{C}$ y, si su fibra es singular, entonces $\Delta(\alpha) = 0$, pues de lo contrario no hay singularidad posible. En otras palabras, estamos en el caso de una fibra de tipo I_0. En consecuencia, solamente nos interesan las raíces de Δ y el punto en el infinito.

Supongamos que $\alpha \in \mathbb{C}$. Debemos seguir los siguientes pasos. Lo primero que hacemos es transformar E en otra curva elíptica "centrada en α", en el siguiente sentido: si $\alpha \neq (1 : 0)$, entonces cambiamos t por $t + \alpha$ en la forma general de E obteniendo así una nueva $\mathbb{C}(t)$-curva elíptica integral $\widetilde{E}$ cuyo discriminante se anula en 0 y, sabiendo que el único punto singular de una $\mathbb{C}$-cúbica en forma de Weierstrass con $a_1 = a_3 = 0$ es siempre de la forma $(x_0 : 0 : 1)$, donde x_0 es raíz múltiple de $X^3 + a_2X^2 + a_4X + a_6$ (léase [12, p. 60]), entonces, por medio de una traslación en x, hacemos que el punto singular de $\widetilde{E}(0) = E(\alpha)$ sea movido a $(0 : 0 : 1)$, de modo que obtenemos una $\mathbb{C}(t)$-curva elíptica integral E^α con discriminante de grado positivo que tiene una raíz en 0 y de modo que la cúbica $E^\alpha(0)$ tiene un punto singular en $(0 : 0 : 1)$, de tal forma que obtenemos

$$E^\alpha : y^2 = x^3 + a_2'x^2 + ta_4'x + ta_6',$$

donde $a_2', a_4', a_6' \in \mathbb{C}[t]$.

Una vez obtenida E^α, aplicamos el siguiente algoritmo. Aquí, Δ sigue significando el valor original con el que fue definido.

(1) Si $t \nmid a_2'$, la fibra es de tipo I_m, donde $m = \text{mult}_\alpha(\Delta)$.

(2) Si $t \mid a_2'$ y $t \nmid a_6'$, la fibra es de tipo II.

(3) Si $t \mid a_2'$, $t \mid a_6'$ y $t^2 \nmid 4a_2'a_6' - ta_4'^2$, la fibra es de tipo III.

(4) Si $t \mid a_2'$, $t \mid a_6'$, $t^2 \mid 4a_2'a_6' - ta_4'^2$ y $t^2 \nmid a_6'$, la fibra es de tipo IV.

(5) Si $t \mid a_2'$, $t \mid a_6'$, $t^2 \mid 4a_2'a_6' - ta_4'^2$ y $t^2 \mid a_6'$, definir el polinomio en $\mathbb{C}[t][T]$

$$P(t)(T) := T^3 + \frac{a_2'}{t}T^2 + \frac{a_4'}{t}T + \frac{a_6'}{t^2}$$

y su discriminante como polinomio en T

$$\text{disc}(P) = t^{-6}\left(-4ta_2'^3a_6' + t^2a_2'^2a_4'^2 - 4t^3a_4'^3 - 27t^2a_6'^2 + 18t^2a_2'a_4'a_6'\right) \in \mathbb{C}[t].$$

(5.1) Si $t \nmid \text{disc}(P)$, la fibra es de tipo I_0^*.

(5.2) Si $t \mid \text{disc}(P)$ entonces $P(0)(T) \in \mathbb{C}[T]$ tiene al menos una raíz múltiple. Si tiene una raíz simple y una raíz doble, la fibra es de tipo I_n^* con $n = \text{mult}_\alpha(\Delta) - 6$.

(5.3) Si $t \mid \text{disc}(P)$ y $P(0)(T)$ tiene una raíz triple, hacemos una traslación en x de modo que esa raíz triple sea $T = 0$. Esto inducirá una nueva curva elíptica en la forma

$$E : y^2z = x^3 + a_2''x^2z + a_4''xz^2 + a_6''z^3,$$

donde $t^2 \mid a_2''$, $t^3 \mid a_4''$ y $t^4 \mid a_6''$.

(5.4) Si $a_6'' \neq 0$, la fibra es de tipo IV^*.

(5.5) Si $a_6'' = 0$ y $t^4 \nmid a_4''$, la fibra es de tipo III^*.

(5.6) Si $a_6'' = 0$ y $t^4 \mid a_4''$, redefinir E^α como

$$y^2 = x^3 + \frac{a_2'}{t^2}x^2 + \frac{ta_4'}{t^4}x + \frac{ta_6'}{t^6},$$

redefinir Δ como su valor original multiplicado por t^{-12} y volver al Paso (1).

Ahora veamos cómo caracterizar la fibra en $\alpha = (1:0)$. En este caso, podemos definir E^α como sigue: cambiamos t por $\frac{1}{t}$ en la forma de E y, por medio de un cambio admisible de variables, obtenemos una $\mathbb{C}(t)$-curva elíptica integral con un nuevo discriminante. Usando esta nueva curva elíptica y este nuevo discriminante, procedemos a aplicar el algoritmo con estos nuevos datos para la fibra inducida por 0.

Para un ejemplo desarrollado y detallado de aplicación de este algoritmo, acceder a la sección 4.2.

La demostración de este algoritmo consiste en concretar los pasos de la demostración de la Proposición 3.2.1, analizando cuidadosamente las posibles fibras singulares surgidas en cada paso del proceso de desingularización de la superficie. El lector interesado en una demostración completa separando en cada uno de los numerosos casos que este proceso induce, puede acceder a las referencias citadas al principio. Aquí ofreceremos un ejemplo de algunos de los casos más sencillos, para ver cómo estas singularidades pueden clasificarse en términos de las relaciones de divisibilidad anteriormente expuestas.

En primer lugar, fijamos $\alpha \in \mathbb{C}$ y supongamos que ya hemos construido nuestra curva centrada en α, que hemos notado E^α. Para esto hemos debido cambiar t por $t + \alpha$, lo

cual significa que las raíces de los polinomios involucrados han sido trasladadas por α. En segundo lugar, hemos hecho una traslación en x, y sabemos que esta operación no genera cambio alguno sobre el discriminante (léase [12, p. 63]). Esto nos dice que el único cambio que sufrió el discriminante Δ cuando hemos centrado E en α ha sido que se cambió t por $t + \alpha$. Esto tiene una importante consecuencia conceptual: todo paso del Algoritmo de Tate que involucra la multiplicidad de α en Δ puede reescribirse en términos del exponente de t en la factorización del discriminante de E^α. Si Δ^α es el discriminante de E^α, entonces $\text{mult}_\alpha(\Delta)$ es igual al exponente de t en la factorización de Δ^α. Por supuesto, es mucho más conveniente la forma original de exponerlo a la hora de concretar el algoritmo, pero para el análisis teórico, es más útil esta segunda caracterización. Aplicando la fórmula para el discriminante, obtenemos

$$\Delta^\alpha = -432t^2a_6'^2 + 288t^2a_2'a_4'a_6' + 16t^2a_2'^2a_4'^2 - 64ta_2'^3a_6' - 64t^3a_4'^3.$$

Imagínese que estamos en el caso en que $t \mid a_2'$. Esto significa que, al especializar en $t = 0$, la curva singular en forma de Weierstrass $E^\alpha(0)$ obtenida es cuspidal y no nodal, puesto que la misma será de la forma $y^2 = x^3$.

Por otro lado, la existencia del sumando $-432t^2a_6'^2$ nos dice que $t^3 \mid \Delta^\alpha$ si y solo si $t \mid a_6'$. Aplicando el Criterio del Jacobiano, es posible ver que el punto $(0, 0)$, que es el punto singular de $E^\alpha(0)$, es una singularidad de la superficie (o, más específicamente, el punto $((0:1), (0:0:1))$ en la superficie correspondiente) si y solo si $t \mid a_6'$ (obsérvese que este argumento no funciona en característica 2, lo cual genera más casos a considerar y complejiza el algoritmo). Esto significa que si $t \nmid a_6'$, entonces el punto correspondiente es un punto no singular de la superficie, y la fibra que buscamos caracterizar resulta ser una fibra racional cuspidal, que es el Paso 2 de nuestro algoritmo.

Si, en cambio, $t \mid a_6'$, entonces estamos ante una singularidad de la superficie, y corresponde realizar un *blow-up*. Este *blow-up* puede producir:

- Una curva racional de grado 2, que intersecta la transformada estricta de la curva racional cuspidal tangencialmente en un solo punto.
- Dos rectas que intersectan en un punto a la transformada estricta de la curva racional cuspidal.
- Una recta doble.

Recordemos que, dado un *blow-up*, la transformada estricta de un subconjunto de la variedad original que contiene al punto sobre el que se aplicó el *blow-up* se define como la clausura de la preimagen por el *blow-up* de este subconjunto sin dicho punto.

En los primeros dos casos, se ha completado el proceso de desingularización y estamos en el caso de una fibra de tipo III en el primer caso, y de tipo IV en el segundo (Pasos 3 y 4 del algoritmo). En cuanto al tercer caso, el proceso de desingularización debe continuar, y es el que desencadena el resto de los pasos del algoritmo. Nuevamente: para una exposición completa y detallada, léanse las referencias citadas.

Finalicemos esta sección explicitando la forma natural de exponer el algoritmo para el caso general. Tal y como mencionamos, trabajar con la multiplicidad de $\alpha \in \mathbb{C}$ en Δ equivale a trabajar con el exponente de t en Δ^α. En general, dada una $\mathbb{C}$-curva proyectiva no singular C y una $\mathbb{C}(C)$-curva elíptica con discriminante Δ con al menos una solución, entonces, dado $v \in C$, "centralizar en v" se traduce como tomar un parámetro local t en

C y una valuación normalizada ν. Nos interesan aquellos $v \in C$ tales que $\nu(\Delta) > 0$, ya que estos valores son los que inducen fibras singulares. No podemos integralizar la curva como hacíamos en $\mathbb{C}(t)$, asegurándonos de que todos sus coeficientes estén en $\mathbb{C}[t]$, pero sí podemos integralizar localmente en v; es decir, tomar un cambio admisible de variables de modo que las $\nu-$valuaciones en los coeficientes de la curva elíptica sean todas no negativas. Esto significa que, a falta de una "integralización global", para cada v tal que su valuación inducida es positiva en Δ tendremos que aplicar una adecuada integralización local. Esta es la única dificultad adicional que acarrea el caso general. En cuanto al resto del algoritmo, el mismo se mantiene exactamente igual, haciendo las traducciones correspondientes en términos de la valuación y el nuevo cuerpo de coeficientes.

Obsérvese que, en el caso simplificado que hemos expuesto, nuestro parámetro local es $t - \alpha$ y la valuación normalizada es el grado como polinomio desarrollado en $t - \alpha$. Así, es posible evitar los desarrollos enrevesados que pueden eventualmente surgir al cambiar t por $t + \alpha$ tomando las derivadas evaluadas en α y considerando los Desarrollos de Taylor.

3.5 Retículo de Néron-Severi

Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Retomando las definiciones en 3.3, para cada $v \in C$ definimos un retículo T_v como el grupo libre de rango $m_v - 1$ generado por $\{\Theta_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}\}$, con el paring $(\cdot, \cdot)$ dado por $(\Theta_{v,i}, \Theta_{v,j}) = -\langle \Theta_{v,i}, \Theta_{v,j} \rangle$, para todos los $i, j \in [1, m_v - 1] \cap \mathbb{N}$. Así, si $\Sigma \subseteq C$ es el conjunto de puntos de C cuyas f-fibras son singulares y reducibles, entonces $T_v = 0$ si y solo si $v \notin \Sigma$.

Vimos que estos retículos pueden pensarse como un subgrupo de $\mathrm{NS}(S)$. Concretamente, vimos que la unión entre los generadores que hemos definido para T_v con $v \in \Sigma$ forman una base del grupo que inducen en $\mathrm{NS}(S)$. Más aún, tenemos el siguiente resultado (más fuerte).

Proposición 3.5.1 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Los elementos del conjunto de clases algebraicas $\{(O), F\} \cup \{\Theta_{v,i} : v \in \Sigma, i \in [1, m_v - 1] \cap \mathbb{N}\} \subseteq \mathrm{NS}(S)$ forman una $\mathbb{Z}$-base del subgrupo de $\mathrm{NS}(S)$ generado por (O) y por las componentes irreducibles de las f-fibras.*

Demostración. Como todas las fibras son algebraicamente equivalentes por el Lema A.3.9, es claro que nuestro candidato a $\mathbb{Z}$-base del subgrupo de $\mathrm{NS}(S)$ generado por (O) y por las componentes irreducibles de las f-fibras, en efecto, es un conjunto de generadores de dicho grupo. Lo único que requiere justificación adicional es la razón por la cual se excluye $\Theta_{v,0}$ del sistema de generadores, para todo $v \in \Sigma$. Esto es así porque, como $v \in \Sigma$ y todas las fibras son algebraicamente equivalentes, el primer ítem del Teorema 3.3.5 nos dice que

$$F \approx \Theta_{v,0} + \sum_{i=1}^{m_v - 1} \mu_{v,i} \Theta_{v,i},$$

de donde, pasando al cociente en $\mathrm{NS}(S)$, la relación se convierte en una igualdad y vemos que $\Theta_{v,0}$ puede ser excluido del sistema de generadores. En esencia, hemos usado que, para todo $v \in \Sigma$, $\Theta_{v,0} = f^{-1}(v) - \sum_{i=1}^{m_v - 1} \mu_{v,i} \Theta_{v,i}$ en $\mathrm{Div}(S)$.

Entonces solamente queda ver la $\mathbb{Z}$-independencia lineal.

Si $v \in \Sigma$, sabemos que $\langle F, \Theta_{v,i} \rangle = 0$ para todo $i \in [1, m_v - 1] \cap \mathbb{N}$, por el Lema A.3.1. Además, como la componente identidad no está siendo tomada en consideración, también vale $\langle (O), \Theta_{v,i} \rangle = 0$ para todo $i \in [1, m_v - 1] \cap \mathbb{N}$, por el primer ítem del Teorema 3.3.5.

Por otra parte, dados $v, w \in \Sigma$ tales que $v \neq w$, y dados $i, j \in \mathbb{N}$ tales que $i < m_v$ y $j < m_w$, se tiene $\langle \Theta_{v,i}, \Theta_{w,j} \rangle = 0$, pues si existiera $x \in \Theta_{v,i} \cap \Theta_{w,j} \subseteq f^{-1}(v) \cap f^{-1}(w)$, entonces se tendría $v = f(x) = w$, absurdo.

Así, $\operatorname{span}\{(O), F\}$ y los grupos $\operatorname{span}\{\Theta_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}\}$ para cada $v \in \Sigma$ son ortogonales dos a dos respecto del pairing de intersección de S. En consecuencia, basta calcular la matriz de intersección de cada uno de ellos y verificar que los determinantes sean no nulos en cada caso.

En cuanto al grupo generado por $\{(O), F\}$, la matriz de intersección está dada, en virtud del Corolario 3.3.3, el Lema A.3.1 y el Lema 3.1.2, por $\begin{pmatrix} -\chi(S) & 1 \\ 1 & 0 \end{pmatrix}$. El determinante es igual a -1, que es no nulo. En cuanto al resto de componentes ortogonales, ya vimos en 3.3.9 que las mismas forman retículos definidos negativos, con lo cual los determinantes de sus matrices de intersección son también no nulos. ■

Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. La Proposición 3.5.1 nos permite pensar a los grupos T_v con $v \in C$ como subgrupos de $\operatorname{NS}(S)$ con estructura de retículo dada por el pairing de intersección de S. Básicamente, hemos visto que en estos grupos no tenemos torsión. Esto vale en general para el grupo $\operatorname{NS}(S)$, y esto es el principal resultado de esta sección. Pero requeriremos hacer uso de la Proposición 3.5.1 y la Proposición 3.3.9 para poder hablar del grupo

$$\mathbb{Z}F \oplus \bigoplus_{v \in \Sigma} T_v^- \subseteq \operatorname{NS}(S) \tag{3.2}$$

como un grupo dotado de estructura de retículo a través del pairing de intersección de S, que lo hace, a su vez, semidefinido negativo, y definido negativo en el subgrupo $\bigoplus_{v \in \Sigma} T_v^- \subseteq \operatorname{NS}(S)$.

Antes de probar el resultado principal de la sección, requeriremos un lema.

Lema 3.5.2 *Sea (f, σ_0) una $\mathbb{C}$-superficie elíptica, y sea S su superficie subyacente. Entonces se tiene $e(S) > 0$.*

Demostración. Sea E la fibra genérica de S, y sea C la curva subyacente de nuestra superficie elíptica. Sea $R \subseteq C$ el conjunto de puntos cuyas f-fibras son singulares. Por la Proposición A.3.8 tenemos

$$e(S) = e(C)\, e(E) + \sum_{s \in R} \left(e\left(f^{-1}(s)\right) - e(E) \right).$$

Sin embargo, sabemos por el Lema 3.3.11 que $e(E) = 0$, puesto que la fibra genérica es no singular. Así, se tiene

$$e(S) = \sum_{s \in R} e\left(f^{-1}(s)\right) > 0,$$

donde en la última desigualdad hemos usado nuevamente el Lema 3.3.11 y la existencia de fibras singulares según nuestra Definición 3.1.1. ■

Teorema 3.5.3 *Sea (f, σ_0) una $\mathbb{C}$-superficie elíptica. Entonces el grupo de Néron-Severi de la superficie subyacente es libre de torsión.*

Demostración. Sea F la clase de equivalencia algebraica de las f-fibras, sea S la superficie subyacente, y sea C la curva subyacente. Sea $D \in \mathrm{NS}(S)$ y $m \in \mathbb{N}$ tal que $mD = 0$. Queremos ver que $D = 0 \in \mathrm{NS}(S)$. Como $mD = 0$ y la equivalencia algebraica implica la equivalencia numérica (léase A.2), entonces, dado cualquier $D' \in \mathrm{Div}(S)$, se tiene que $0 = \langle mD, D' \rangle = m \langle D, D' \rangle$ y por lo tanto $\langle D, D' \rangle = 0$. Así, $D \equiv 0$.

Por lo tanto, basta ver que la equivalencia numérica, que es implicada por la equivalencia algebraica, es de hecho idénticamente la equivalencia algebraica. Sea D un divisor de S tal que $D \equiv 0$. Entonces el número de intersección entre D y cualquier otro divisor de S es nulo. Aplicando el Teorema A.3.2, obtenemos

$$\chi(D) = \chi(\mathcal{O}_S) + \frac{\langle D, D - \omega_S \rangle}{2}$$

$$\dim_{\mathbb{C}} H^0(\mathcal{O}_S(D), S) - \dim_{\mathbb{C}} H^1(\mathcal{O}_S(D), S) + \dim_{\mathbb{C}} H^2(\mathcal{O}_S(D), S) = \chi(S) + \frac{0}{2}$$

$$\dim_{\mathbb{C}} H^0(\mathcal{O}_S(D), S) + \dim_{\mathbb{C}} H^2(\mathcal{O}_S(D), S) = \chi(S) + \dim_{\mathbb{C}} H^1(\mathcal{O}_S(D), S)$$

$$\dim_{\mathbb{C}} H^0(\mathcal{O}_S(D), S) + \dim_{\mathbb{C}} H^2(\mathcal{O}_S(D), S) \geq \chi(S). \tag{3.3}$$

Aplicando la fórmula de Noether A.3 tenemos $12\chi(S) = e(S) + \langle K_S, K_S \rangle = e(S)$, donde en la última igualdad hemos usado el Lema 3.3.1. En consecuencia, la expresión 3.3 se transforma en

$$\dim_{\mathbb{C}} H^0(\mathcal{O}_S(D), S) + \dim_{\mathbb{C}} H^2(\mathcal{O}_S(D), S) \geq \frac{e(S)}{12} > 0,$$

donde en la última desigualdad hemos usado el Lema 3.5.2. Así, alguno de los $\mathbb{C}$-espacios vectoriales $H^0(\mathcal{O}_S(D), S)$ y $H^2(\mathcal{O}_S(D), S)$ es no trivial.

Si $D \sim 0$, en particular $D \approx 0$ y no hay nada que probar. Supongamos, entonces, sin pérdida de generalidad, que $D \not\sim 0$. Entonces $H^0(\mathcal{O}_S(D), S)$ debe ser trivial, pues de lo contrario D sería linealmente equivalente a un divisor $\mathfrak{D} \geq 0$ efectivo, y como la equivalencia lineal implica la equivalencia numérica, se tendría $\mathfrak{D} \equiv D \equiv 0$, de donde $D \sim \mathfrak{D} \sim 0$ (pues todo divisor efectivo numéricamente equivalente a 0 es linealmente equivalente a 0), contrario a nuestras hipótesis. Así, $H^2(\mathcal{O}_S(D), S)$ debe ser no trivial. Por la **Dualidad de Serre** (léase [10, III, Corollary 7.7]) se tiene

$$H^2(\mathcal{O}_S(D), S) \cong H^0(\mathcal{O}_S(K_S - D), S),$$

por lo tanto existe un divisor efectivo $D' \geq 0$ tal que $D' \sim K_S - D$. Así, para cada divisor D'' de S, se tiene $\langle D', D'' \rangle = \langle K_S - D, D'' \rangle$.

Veamos que si Θ es una componente irreducible de una f-fibra, entonces $\langle D', \Theta \rangle = 0$. En efecto, es claro que $\langle D, \Theta \rangle = 0$, pues $D \equiv 0$. En cuanto a K_S, el Lema 3.3.1 nos dice que $\langle K_S, \Theta \rangle = \langle (2g(C) - 2 + \chi(S)) F, \Theta \rangle = 0$, donde en la última igualdad hemos usado el Lema A.3.1. Esto prueba que $\langle D', \Theta \rangle = 0$ si Θ es cualquier componente irreducible de una f-fibra. En particular, $\langle D', F \rangle = 0$, pues F es combinación lineal de componentes irreducibles de f-fibras.

Como D' es efectivo, es suma de múltiplos no negativos de subvariedades irreducibles de S de codimensión 1 (curvas de S) distintas dos a dos. Escribimos $D' = D_1 + D_2$, donde

D_1 es suma de múltiplos no negativos de componentes irreducibles de f-fibras, y D_2 es suma de múltiplos no negativos de otro tipo de curvas de S. Veamos que $D_2 = 0$. Si no lo fuera, sea C_2 uno de los sumandos no nulos (sin su multiplicidad) que aparecen en D_2. Tomando $x \in C_2$, la fibra inducida por $f(x)$ tiene intersección no vacía con C_2, pues contiene al punto x. De esta forma, $\langle F, C_2\rangle > 0$, ya que F y C_2 no comparten componentes en común (por definición de C_2) y tienen intersección no vacía. Como esto lo probamos cualquiera sea C_2 en los sumandos de D_2 sin su multiplicidad, entonces $\langle F, D_2\rangle > 0$, por ser suma de múltiplos positivos de números naturales. Por otra parte, ya hemos probado que $\langle F, D'\rangle = 0$, y sabemos por el Lema A.3.1 y la definición de D_1 que $\langle F, D_1\rangle = 0$, por lo tanto obtenemos

$$0 = \langle F, D'\rangle = \langle F, D_1 + D_2\rangle = \langle F, D_1\rangle + \langle F, D_2\rangle = \langle F, D_2\rangle > 0,$$

que es un absurdo que provino de suponer que $D_2 \neq 0$.

Entonces D' es suma de múltiplos no negativos de componetes irreducibles de f-fibras. El pairing de intersección restringido al subgrupo de $\mathrm{NS}(S)$ dado por 3.2 es semidefinido negativo, y es definido negativo en el subgrupo generado por las componentes irreducibles de las fibras reducibles, tal y como vimos en la Proposición 3.5.1. Bajando al cociente en $\mathrm{NS}(S)$, escribimos $D' = D'_1 + D'_2$, donde $D'_1 \in \mathbb{Z}F$ y $D'_2 \in \bigoplus_{v\in\Sigma} T_v \subseteq \mathrm{NS}(S)$. Entonces $D'_2 = D' - D'_1$ pertenece a un subgrupo donde el pairing de intersección es definido negativo. Además, se tiene

$$\langle D' - D'_1, D' - D'_1\rangle = \langle D', D'\rangle - 2\langle D', D_1\rangle + \langle D'_1, D'_1\rangle.$$

Es claro que $\langle D', D'_1\rangle = 0$, pues D'_1 es algebraicamente equivalente a un múltiplo entero de F y $\langle D', F\rangle = 0$. Además, el Lema A.3.1 muestra que $\langle D'_1, D'_1\rangle = 0$. De esta forma, $\langle D'_2, D'_2\rangle = \langle D', D'\rangle$. Pero, por otra parte, el hecho de que $\langle D, \Theta\rangle = 0$ si Θ es una componente irreducible de una f-fibra muestra que $\langle D', D'\rangle = 0$, pues podemos descomponer uno de los argumentos de dicho pairing como suma de múltiplos de componentes irreducibles de f-fibras, ya que D' pertenece al grupo 3.2.

Hemos probado que D'_2 tiene *self-intersection* igual a 0 y que pertenece a un subgrupo de $\mathrm{NS}(S)$ donde el pairing de intersección es definido negativo. En consecuencia, necesariamente debe ser $D'_2 = 0$. Así, $D' \sim K_S - D$ debe ser algebraicamente equivalente a un múltiplo de F. Por el Lema 3.3.1, lo mismo vale para K_S, de donde $D \approx mF$ para algún $m \in \mathbb{Z}$. Pero $D \equiv 0$, luego $0 = \langle D, (O)\rangle = m\langle F, (O)\rangle = m$, pues (O) y F se intersectan exactamente en un punto, y de forma transversal, por el Lema 3.1.2. Por lo tanto $D \approx 0$. ■

El Teorema 3.5.3 tiene la importante consecuencia de que el grupo de Néron-Severi de una superficie elíptica, junto con el pairing de intersección de su superficie subyacente S forma un retículo. Este retículo se conoce como *el retículo de Néron-Severi*. Más aún, el Teorema A.2.2 nos garantiza que es un retículo no degenerado de signatura $(1, \rho(S) - 1)$, donde S es la superficie subyacente de nuestra superficie elíptica.

3.6 Retículo Trivial

Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica y sea F la clase de equivalencia algebraica de las f-fibras. Por la Proposición 3.5.1, el retículo

$$\mathbb{Z}(O) \oplus \mathbb{Z}F \oplus \bigoplus_{v\in\Sigma} T_v^- \subseteq \mathrm{NS}(S)$$

es un subretículo de $\mathrm{NS}(S)$. Dicho subretículo recibe el nombre de *retículo trivial* de la superficie elíptica, y se nota $\mathrm{Triv}(S)$.

Como vimos en la demostración de la Proposición 3.5.1, la componente $\mathbb{Z}(O) \oplus \mathbb{Z}F$ tiene matriz de intersección $\begin{pmatrix} -\chi(S) & 1 \\ 1 & 0 \end{pmatrix}$. El polinomio característico de esta matriz es $X^2 + \chi(S) X - 1$, cuyas raíces son

$$\frac{-\chi(S) \pm \sqrt{\chi(S)^2 + 4}}{2},$$

y el Lema 3.5.2 permite probar, exactamente igual a como se hizo en la demostración del Teorema 3.5.3 por medio de la Fórmula de Noether, que $\chi(S) > 0$. Así, ambas raíces difieren en su signo, y por lo tanto la signatura resulta ser $(1,1)$. En cuanto a los componentes T_v^- para $v \in \Sigma$, sabemos que sus signaturas son $(0, m_v - 1)$, por lo visto en 3.3.9. En consecuencia, la signatura de $\mathrm{Triv}(S)$ resulta ser

$$\left(1, 1 + \sum_{v \in \Sigma} (m_v - 1)\right).$$

Resumimos nuestros resultados en la siguiente proposición.

Proposición 3.6.1 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica. Entonces el pairing de intersección de S hace de $\mathrm{Triv}(S)$ un retículo de signatura $\left(1, 1 + \sum_{v \in \Sigma} (m_v - 1)\right)$. En particular, se tiene que $\mathrm{Triv}(S)$ es un retículo de rango*

$$\mathrm{rg}(\mathrm{Triv}(S)) = 2 + \sum_{v \in \Sigma} (m_v - 1).$$

Consideramos el cociente entre el retículo de Néron-Severi y el retículo trivial, el cual tiene rango

$$\mathrm{rg}(\mathrm{NS}(S)) - \mathrm{rg}(\mathrm{Triv}(S)) = \rho(S) - \left[2 + \sum_{v \in \Sigma} (m_v - 1)\right]. \tag{3.4}$$

La importancia de este cociente radica en este importante resultado, cuya demostración postergaremos para la sección 3.7.

Teorema 3.6.2 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica, y sea E su fibra genérica. Entonces existe un isomorfismo natural de grupos abelianos*

$$E(\mathbb{C}(C)) \cong \frac{\mathrm{NS}(S)}{\mathrm{Triv}(S)}.$$

El Teorema 3.6.2 tiene importantísimas consecuencias de toda índole, sobre las cuales se puede escribir y desarrollar muchísimo material. Una importancia conceptual es que permite comenzar a hablar de hacer aritmética en superficies elípticas. En nuestro caso, dos resultados serán de nuestro interés.

La primera consecuencia será que podemos recuperar el **Teorema de Mordell** que teníamos únicamente para curvas elípticas, lo cual es la base para cualquier aritmética que busquemos hacer en superficies elípticas.

Corolario 3.6.3 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica, y sea E su fibra genérica. Entonces $E(\mathbb{C}(C))$ es un grupo abeliano finitamente generado.*

Demostración. $\mathrm{NS}(S)$ es finitamente generado (léase A.2), por lo tanto todos sus cocientes también lo son. Por el Teorema 3.6.2, $E(\mathbb{C}(C))$ es isomorfo a un cociente de $\mathrm{NS}(S)$. ■

La segunda consecuencia que nos interesará destacar es lo que se conoce como **Fórmula de Shioda-Tate**. La misma relaciona el rango de la fibra genérica de una superficie elíptica con el número de Picard de S y la estructura de sus fibras singulares reducibles.

Corolario 3.6.4 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica, y sea E su fibra genérica. Sea Σ el conjunto de puntos en C cuyas f-fibras son singulares y reducibles. Entonces*

$$\rho(S) = \mathrm{rg}(E(\mathbb{C}(C))) + 2 + \sum_{v \in \Sigma} (m_v - 1).$$

Demostración. Por el Teorema 3.6.2, la expresión 3.4 iguala a $\mathrm{rg}(E(\mathbb{C}(C)))$, y esto nos da la fórmula del enunciado. ■

3.7 Fibra genérica

En esta sección demostraremos el Teorema 3.6.2. A lo largo de toda esta sección, fijamos una $\mathbb{C}$-superficie proyectiva no singular S, una $\mathbb{C}$-curva proyectiva no singular C y una fibración elíptica $f : S \to C$. Sea E su fibra genérica.

El grupo $\mathrm{Div}(C)$ de divisores de C admite al subgrupo $\mathrm{Div}_a(C)$ de divisores de grado cero, que a su vez admite el subgrupo $\mathrm{Div}_\ell(C)$ de divisores principales. Con base en estas notaciones, recordemos que $\mathrm{Pic}(C) := \mathrm{Div}(C) / \mathrm{Div}_\ell(C)$, $\mathrm{Pic}^0(C) := \mathrm{Div}_a(C) / \mathrm{Div}_\ell(C)$ y, además,

$$\mathrm{Div}(C) / \mathrm{Div}_a(C) \cong \mathbb{Z}.$$

Recordemos que $\mathrm{Pic}^0(S)$ es el subgrupo de divisores de S algebraicamente equivalentes a 0 módulo equivalencia lineal.

Sea $\mathcal{S}$ el esquema subyacente de S, y sea $\mathcal{C}$ el de C. Entonces $\mathcal{S}$ contiene a la fibra genérica de la superficie elíptica, lo cual se sigue trivialmente de aplicar el funtor *fully faithful* natural entre variedades sobre $\mathbb{C}$ y esquemas sobre $\mathbb{C}$ a la fibración elíptica (ver [10, p. 78]), obteniendo un morfismo de esquemas $\mathcal{F} : \mathcal{S} \to \mathcal{C}$, y tomar la fibra del punto genérico de C.

Para cada $D \in \mathrm{Div}(S)$, escribimos $D = D_1 + D_2$, donde D_1 está generado por componentes irreducibles de f-fibras, y D_2 está generado por otro tipo de curvas en S. Mirando E como subesquema de $\mathcal{S}$, el mismo es disjunto de D_1, pues D_1 sigue siendo cerrado cuando se mira en $\mathcal{S}$ (es decir, la transformación funtorial considerada no lo altera), puesto que cada una de las finitas componentes irreducibles de D_1 está, por definición, contenida en alguna f-fibra, donde f es constante (compárese con el argumento análogo dado en la demostración de la Proposición 3.1.4). Así, ninguno de los puntos de las componentes irreducibles que aparecen en la expansión de D_1 puede tener al punto genérico de C como imagen por $\mathcal{F}$, y por lo tanto tienen intersección vacía con E incluso al considerarlos como subesquemas de $\mathcal{S}$.

Por otro lado, cada componente irreducible Y de D_2 se transforma funtorialmente en un divisor $\mathcal{Y}$ de $\mathcal{S}$ el cual, dentro de $\mathcal{S}$, nos permite definir $Y_\eta := \mathcal{Y} \cap E$. Es sabido que, en esta situación, se tiene que $f(Y) = C$, de donde $Y_\eta \neq \emptyset$, y que la clausura de cada punto en esta intersección es precisamente $\mathcal{Y}$ (léase [15, p. 349]). En particular, $\mathcal{Y}$ es la clausura de Y_η. Esto demuestra que sus grados como subesquemas de $\mathcal{S}$ coinciden, y es claro que Y_η resulta ser un divisor $\mathbb{C}(C)$-racional de E cuyo grado es $\langle Y, F\rangle$, donde F es, como siempre, la clase de equivalencia algebraica de las f-fibras. Definiendo L como el conjunto de componentes irreducibles en la expansión de D_2, y llamando $\alpha_Y \in \mathbb{Z} \setminus \{0\}$ a la multiplicidad de Y en dicha expansión para cada $Y \in L$, se tiene

$$D_2 = \sum_{Y \in L} \alpha_Y Y.$$

Definimos $D_E := \sum_{Y \in L} \alpha_Y Y_\eta$, que es un divisor $\mathbb{C}(C)$-racional de E cuyo grado es $\langle D, F\rangle$. Así, D_E consiste en la restricción del divisor D a E, visto este último como subesquema de $\mathcal{S}$, puesto que, como vimos anteriormente, dicha restricción elimina todas las componentes irreducibles de f-fibras.

Lema 3.7.1 *Sea $D \in \operatorname{Div}(S)$. Si $D_E \sim_E 0$, entonces $D \sim_S D'$ para algún $D' \in \operatorname{Div}(S)$ generado por componentes irreducibles de f-fibras.*

Demostración. Como $D_E \sim_E 0$, existe un divisor $\mathbb{C}(C)$-racional de $E(\mathbb{C}(C))$ que es principal y linealmente equivalente a D_E. Sea $h \in \mathbb{C}(C)(E)$ tal que $D_E = \operatorname{div}(h)$, el divisor principal inducido por h. Por medio de la fibración f, y del hecho de que E es la fibra genérica de dicha fibración, sabemos que $\mathbb{C}(S)$ está naturalmente identificado con $\mathbb{C}(C)(E)$; es decir, el $\mathbb{C}$-*function field* de S se identifica con el $\mathbb{C}(C)$-*function field* de E por medio de la restricción, de tal forma que existe $g \in \mathbb{C}(S)$ tal que $\operatorname{div}(g)_E = \operatorname{div}(h)$. Tomamos $D' = D - \operatorname{div}(g)$, el cual satisface, por definición, que $D'_E = 0$. De esto se sigue que D' está generado exclusivamente por componentes irreducibles de f-fibras, ya que, como $D'_E = 0$, el resto de componentes no figuran en su expansión. Finalmente, obtenemos directamente la relación $D \sim_S D - \operatorname{div}(g) = D'$. ■

Definimos $\theta : \operatorname{Div}(S) \to \operatorname{Pic}(E)$ que a cada $D \in \operatorname{Div}(S)$ le asigna la clase de equivalencia lineal en E de D_E. El Lema 3.7.1 nos dice que $\ker(\theta)$ está incluido en el conjunto de divisores cuyas clases de equivalencia lineal están generadas por componentes irreducibles de f-fibras.

Por el conocido **Teorema de Abel** (ver [18, Proposition 4.10] y sus subsecuentes generalizaciones), sabemos que la función $\gamma : E(\mathbb{C}(C)) \to \operatorname{Pic}^0(E(\mathbb{C}(C)))$ que a cada $P \in E(\mathbb{C}(C))$ le asigna la clase del divisor $P - O$, donde $O = (0:1:0)$, es un isomorfismo de grupos. Definimos $\Psi : \operatorname{Div}(S) \to E(\mathbb{C}(C))$ como

$$\Psi(D) = \gamma^{-1}(D_E - \langle D, F\rangle O)$$

para cada $D \in \operatorname{Div}(S)$, el cual está bien definido porque $\deg(D_E) = \langle D, F\rangle$, y por lo tanto $D_E - \langle D, F\rangle O \in \operatorname{Pic}^0(E(\mathbb{C}(C)))$. Esta definición implica que, si $D \in \operatorname{Div}(S)$, entonces $D_E - \langle D, F\rangle O \sim_E \Psi(D) - O$. Esta relación es la clave en el siguiente resultado.

Lema 3.7.2 *Sea $D \in \operatorname{Div}(S)$. Sea $P = \Psi(D) \in E(\mathbb{C}(C))$. Sea $\Sigma \subseteq C$ el conjunto de puntos de C cuyas f-fibras son singulares y reducibles. Entonces existen únicos $n, d \in \mathbb{Z}$ y $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Z}$ tales que*

$$D \approx (P) + (d-1)(O) + nF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i}.$$

Más aún, $d = \langle D, F \rangle$ y $n = \langle D, (O) \rangle - \langle (P), (O) \rangle + \chi(S)(\langle D, F \rangle - 1)$.

Además, fijamos $v \in \Sigma$ y definimos $A_v \in \mathbb{Z}^{(m_v-1)\times(m_v-1)}$ como $(A_v)_{ij} = \langle \Theta_{v,i}, \Theta_{v,j} \rangle$. Definimos $b_v \in \mathbb{Z}^{m_v - 1}$ como el vector en cuya i-ésima coordenada tiene el valor $b_{v,i}$ para cada $i \in [1, m_v - 1] \cap \mathbb{N}$, y definimos $S_v \in \mathbb{Z}^{m_v - 1}$ como el vector en cuya i-ésima coordenada tiene el valor $\langle \Theta_{v,i}, D - (P) \rangle$ para cada $i \in [1, m_v - 1] \cap \mathbb{N}$. Entonces A_v es inversible y $b_v = A_v^{-1} S_v$.

Demostración. Sea $D' = D - (P) - (d-1)(O)$, donde $d = \langle D, F \rangle$. Aplicando θ obtenemos $D'_E = D_E - (P)_E - (d-1)(O)_E = D_E - P - (d-1)O$, donde en la última igualdad hemos usado que, si $Q \in E(\mathbb{C}(C))$, entonces $(Q)_E = Q$, lo cual se sigue de la demostración de la Proposición 3.1.4, en virtud de la cual (Q) es la restricción a S de la clausura de $\mathcal{Q}$ de Q en $\mathcal{S}$, y satisface $\mathcal{Q} \cap E = \{Q\}$ transversalmente.

La relación $D_E - \langle D, F \rangle O \sim_E \Psi(D) - O$ nos dice que $D_E - dO = P - O$ en $\operatorname{Pic}(E)$, de donde $D'_E = D_E - P - (d-1)O = dO - O - (d-1)O = 0$. Por el Lema 3.7.1, D' es linealmente equivalente a un divisor generado por componentes irreducibles de f-fibras. Tomando equivalencia algebraica, obtenemos

$$D - (P) - (d-1)(O) = D' \approx nF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i}$$

para algún $n \in \mathbb{Z}$ y algunos $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Z}$. Aquí hemos usado que, en el grupo de Néron-Severi, el grupo de divisores generado por las componentes irreducibles de las f-fibras está dado por 3.2. Por otra parte, escribiendo

$$D - (P) = (d-1)(O) + nF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i} \in \operatorname{NS}(S),$$

vemos por la Proposición 3.5.1 que tenemos la unicidad buscada.

Calculemos los valores explícitos. Ya sabemos que $d = \langle D, F \rangle$.

Por el Corolario 3.3.3, $\langle (O), (O) \rangle = -\chi(S)$. Por el Lema 3.1.2, $\langle (O), F \rangle = 1$. Por el primer ítem del Teorema 3.3.5, dado $v \in \Sigma$, para todo $i \in [1, m_v - 1] \cap \mathbb{N}$ se tiene $\langle (O), \Theta_{v,i} \rangle = 0$. En consecuencia,

$$\langle D - (P), (O) \rangle = -\chi(S)(d-1) + n,$$

de donde $n = \langle D, (O) \rangle - \langle (P), (O) \rangle + \chi(S)(\langle D, F \rangle - 1)$.

Finalmente, fijamos $v \in \Sigma$. Usando que dos componentes irreducibles de f-fibras distintas son ortogonales, usando nuevamente el primer ítem del Teorema 3.3.5 y aplicando el Lema A.3.1, obtenemos, fijando $i \in [1, m_v - 1] \cap \mathbb{N}$,

$$\langle \Theta_{v,i}, D - (P) \rangle = 0 + 0 + \sum_{j=1}^{m_v - 1} \langle \Theta_{v,i}, \Theta_{v,j} \rangle b_{v,j},$$

de donde, usando que A_v es, por la Proposición 3.3.9, inversible, puesto que es la matriz de intersección de un retículo definido negativo, obtenemos la última igualdad buscada. ■

Observación 3.7.3 *Si $Q \in E(\mathbb{C}(C))$, entonces*

$$\Psi((Q)) = \gamma^{-1}((Q)_E - \langle (Q), F\rangle O) = \gamma^{-1}(Q - O) = \gamma^{-1}(\gamma(Q)) = Q,$$

donde hemos escrito $\langle (Q), F\rangle = 1$ en razón del Lema 3.1.2.

La observación 3.7.3 nos dice que Ψ es un morfismo sobreyectivo.

Definimos $\mathrm{N}_{\mathbb{Q}}(S) := \mathrm{NS}(S) \otimes \mathbb{Q}$. Por el Teorema 3.5.3, esta tensorización no elimina elementos de $\mathrm{NS}(S)$ y solamente consiste en ampliar los coeficientes de las expansiones al cuerpo de los números racionales. Similarmente, definimos $\mathrm{Tr}_{\mathbb{Q}}(S) := \mathrm{Triv}(S) \otimes \mathbb{Q}$. En estos grupos, el pairing de intersección se extiende naturalmente.

Lema 3.7.4 *Para cada $P \in E(\mathbb{C}(C))$ existe un único $\beta(P) \in \mathrm{N}_{\mathbb{Q}}(S)$ tal que se cumplen simultáneamente:*

- $\beta(P) \equiv (P) \pmod{\mathrm{Tr}_{\mathbb{Q}}(S)}$,
- $\beta(P) \perp \mathrm{Triv}(S)$.

Más aún, si $\Sigma \subseteq C$ el conjunto de puntos cuyas f-fibras son singulares y reducibles, entonces existen únicos $n, d \in \mathbb{Q}$ y $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Q}$ tales que

$$\beta(P) = (P) + d(O) + nF + \sum_{v\in\Sigma}\sum_{i=1}^{m_v-1} b_{v,i}\Theta_{v,i} \in \mathrm{N}_{\mathbb{Q}}(S),$$

donde $d = -1$ y $n = -\chi(S) - \langle (P), (O)\rangle$.

Además, fijamos $v \in \Sigma$ y definimos $A_v \in \mathbb{Z}^{(m_v-1)\times(m_v-1)}$ como $(A_v)_{ij} = \langle \Theta_{v,i}, \Theta_{v,j}\rangle$. Definimos $b_v \in \mathbb{Q}^{m_v-1}$ como el vector en cuya i-ésima coordenada tiene el valor $b_{v,i}$ para cada $i \in [1, m_v - 1] \cap \mathbb{N}$, y definimos $R_v \in \mathbb{Z}^{m_v-1}$ como el vector en cuya i-ésima coordenada tiene el valor $-\langle \Theta_{v,i}, (P)\rangle$ para cada $i \in [1, m_v - 1] \cap \mathbb{N}$. Entonces A_v es inversible y $b_v = A_v^{-1}R_v$.

Demostración. Sea $D_P \in \mathrm{N}_{\mathbb{Q}}(S)$. Entonces $D_P \equiv (P) \pmod{\mathrm{Tr}_{\mathbb{Q}}(S)}$ si y solo si existen $n, d \in \mathbb{Q}$ y $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Q}$ tales que

$$D_P = (P) + d(O) + nF + \sum_{v\in\Sigma}\sum_{i=1}^{m_v-1} b_{v,i}\Theta_{v,i} \in \mathrm{N}_{\mathbb{Q}}(S),$$

donde, además, dicha representación es única por la Proposición 3.5.1 (se sigue trivialmente de pasar restando (P) y limpiar denominadores).

En tal caso, $\langle D_P, F\rangle = 0$ si y solo si $0 = 1 + d + 0 + 0$, por los Lemas 3.1.2 y A.3.1. Así, $\langle D_P, F\rangle = 0$ si y solo si $d = -1$.

Además, $\langle D_P, (O)\rangle = 0$ si y solo si $0 = \langle (P), (O)\rangle - d\chi(S) + n + 0$, donde hemos usado el Corolario 3.3.3, el Lema 3.1.2 y el primer ítem del Teorema 3.3.5. En consecuencia, $\langle D_P, (O)\rangle = 0$ si y solo si $n = d\chi(S) - \langle (P), (O)\rangle$.

Ahora, fijando $v \in \Sigma$ y $i \in [1, m_v - 1] \cap \mathbb{N}$ y recordando que dos componentes irreducibles de f-fibras distintas son ortogonales, se tiene $\langle \Theta_{v,i}, D_P \rangle = 0$ si y solo si

$$0 = \langle \Theta_{v,i}, (P) \rangle + 0 + 0 + \sum_{j=1}^{m_v - 1} \langle \Theta_{v,i}, \Theta_{v,j} \rangle b_{v,j}$$

$$\sum_{j=1}^{m_v - 1} \langle \Theta_{v,i}, \Theta_{v,j} \rangle b_{v,j} = - \langle \Theta_{v,i}, (P) \rangle ,$$

donde hemos aplicado el primer ítem del Teorema 3.3.5 y el Lema A.3.1.

Juntando todas las condiciones y usando que, por la Proposición 3.3.9, la matriz A_v es inversible para todo $v \in \Sigma$, obtenemos lo que queríamos demostrar. ■

Sabemos que $\mathrm{NS}(S)$, junto con el pairing de intersección, es un retículo. En él tenemos definido el subretículo $\mathrm{Triv}(S)$. Introduciremos un nuevo retículo asociado a nuestra superficie elíptica.

Definición 3.7.5 *Definimos* $\mathscr{L}(S) := \left(\mathrm{Triv}(S)^{\perp}\right)^{-}$ *y lo denominamos* el retículo esencial *de la superficie elíptica considerada. En otras palabras, el retículo esencial es el complemento ortogonal del retículo trivial en el retículo de Néron-Severi, pero con el pairing aditivamente opuesto al pairing de intersección de* S.

El Lema 3.7.4 nos dice que tenemos una función $\beta : E(\mathbb{C}(C)) \to \mathrm{N}_{\mathbb{Q}}(S)$ bien definida. Veamos que es un morfismo de grupos.

Lema 3.7.6 $\beta : E(\mathbb{C}(C)) \to \mathrm{N}_{\mathbb{Q}}(S)$ *es un morfismo de grupos.*

Demostración. En esta demostración notaremos con el símbolo $\odot$ a la operación de grupo en $E(\mathbb{C}(C))$, para que la misma no se confunda con la suma en los grupos de divisores y sus grupos asociados.

Sean $P, Q \in E(\mathbb{C}(C))$. Existen $n \in \mathbb{Q}$ y $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Q}$ tales que

$$\beta(P) + \beta(Q) - (P \odot Q) = (P) + (Q) - 2(O) - (P \odot Q) + nF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i} \in \mathrm{N}_{\mathbb{Q}}(S) ,$$

por el Lema 3.7.4. Esta expresión para $\beta(P) + \beta(Q) - (P \odot Q)$ puede reescribirse como

$$\beta(P) + \beta(Q) - (P \odot Q) = \tag{3.5}$$

$$= (P) - (O) + (Q) - (O) - [(P \odot Q) - (O)] - (O) + nF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i} \in \mathrm{N}_{\mathbb{Q}}(S) .$$

Definimos $\widetilde{D} := (P) - (O) + (Q) - (O) - [(P \odot Q) - (O)] \in \mathrm{Div}(S)$. Aplicando θ obtenemos $\widetilde{D}_E = P - O + Q - O - [P \odot Q - O] = \gamma(P) + \gamma(Q) - \gamma(P \odot Q) = 0 \in \mathrm{Pic}(E)$. Por el Lema 3.7.1, $\widetilde{D}$ es linealmente equivalente en S a un divisor generado por componentes irreducibles de f-fibras. Como la equivalencia lineal implica la equivalencia algebraica, podemos volver a la expresión 3.5 y, módulo $\mathrm{Tr}_{\mathbb{Q}}(S)$, se anula el divisor $\widetilde{D}$, y el resto

de expresiones también se anulan trivialmente. De esta forma, hemos demostrado que $\beta(P) + \beta(Q) \equiv (P \odot Q) \pmod{\mathrm{Tr}_{\mathbb{Q}}(S)}$. Como $\beta(P) \perp \mathrm{Triv}(S)$ y $\beta(Q) \perp \mathrm{Triv}(S)$, entonces $[\beta(P) + \beta(Q)] \perp \mathrm{Triv}(S)$. Por la unicidad del Lema 3.7.4, se tiene entonces que

$$\beta(P \odot Q) = \beta(P) + \beta(Q),$$

y por lo tanto β es un morfismo de grupos. ■

Este morfismo tiene una relación importante con $\mathscr{L}(S)$, que haremos explícita a continuación. Recordando que, para cada $v \in \Sigma$, donde $\Sigma \subseteq C$ es el conjunto de las f-fibras singulares y reducibles, se tiene que $m_v^{(1)}$ es el número de componentes irreducibles simples de $f^{-1}(v)$, y que, por la Proposición 3.3.9, es a su vez el determinante de la matriz del retículo T_v, definimos $m(S) \in \mathbb{N}$ como el mínimo común múltiplo entre los elementos del conjunto $\left\{m_v^{(1)} : v \in \Sigma\right\}$. Entonces se tiene $m(S)\,\mathrm{Im}(\beta) \subseteq \mathscr{L}(S)$, por la segunda condición del Lema 3.7.4 y el hecho de que $m(S)\,\beta(P) \in \mathrm{NS}(S)$ para todo $P \in E(\mathbb{C}(C))$ (es decir, los coeficientes de su expansión son enteros), por el siguiente sencillo lema de álgebra lineal.

Lema 3.7.7 *Sea $n \in \mathbb{N}$ y sea $A \in \mathbb{Z}^{n\times n}$. Sea $x \in \mathbb{Z}^n$. Supongamos que $\det(A) \neq 0$, y definimos $b := A^{-1}x \in \mathbb{Q}^n$. Entonces $\det(A)\,b \in \mathbb{Z}^n$.*

Demostración. Escribimos $Ab = x$. Como $x \in \mathbb{Z}^n$, la Regla de Cramer nos dice que, para todo $i \in [1,n] \cap \mathbb{N}$, se tiene $b_i = \frac{a_i}{\det(A)}$, donde $a_i \in \mathbb{Z}$. Por consiguiente $\det(A)\,b_i \in \mathbb{Z}$ para todo $i \in [1,n] \cap \mathbb{N}$, como queríamos. ■

Definimos el conjunto $E^0(\mathbb{C}(C)) \subseteq E(\mathbb{C}(C))$ de los $P \in E(\mathbb{C}(C))$ tales que, para todo $v \in \Sigma$, $(P) \cap \Theta_{v,0} \neq \emptyset$. Es posible demostrar que $E^0(\mathbb{C}(C))$ es un subgrupo de $E(\mathbb{C}(C))$ y que $m(S)\,E(\mathbb{C}(C)) \subseteq E^0(\mathbb{C}(C))$. Como la demostración de este hecho se aleja del alcance de los argumentos que aquí estamos exponiendo (en tanto requiere la utilización de resultados geométricos más generales), la postergaremos para el final de la sección. Pero requeriremos tener este resultado presente para lo que sigue.

El próximo paso es probar que Ψ baja al grupo de Néron-Severi; en otras palabras, que los divisores algebraicamente equivalentes a 0 están en el núcleo de Ψ. Para esto, requeriremos el siguiente lema.

Lema 3.7.8 *El morfismo inducido $f^* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(S)$ es un isomorfismo.*

Demostración. La existencia de una sección σ nos dice que, como $f \circ \sigma$ es identitaria, $\sigma^* \circ f^*$ también lo es, de donde f^* es inyectiva. Falta ver que f^* es sobreyectiva.

Sea $D \in \mathrm{Div}(S)$ tal que $D \approx 0$. Queremos ver que su clase de equivalencia lineal está en la imagen de f^*.

Como $D \approx 0$, el grado de D_E es $\langle D, F\rangle = 0$, y por lo tanto existe $P \in E(\mathbb{C}(C))$ tal que $\gamma(P) = D_E$; es decir, $D_E \sim_E P - O$. Definimos $D' := D - (P) + (O)$. Aplicando θ, obtenemos $D'_E = D_E - (P)_E + (O)_E = D_E - (P - O) = 0 \in \mathrm{Pic}(E)$. Por el Lema 3.7.1, D' está generado en $\mathrm{Pic}(S)$ por componentes irreducibles de f-fibras. Esto es, existen $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Z}$, $m \in \mathbb{N}_0$ y un conjunto finito $\{v_i : i \in [1,m] \cap \mathbb{N}\} \subseteq C$ tales que

$$D - (P) + (O) \sim_S \sum_{i=1}^{m} a_i f^{-1}(v_i) + \sum_{v\in\Sigma} \sum_{i=1}^{m_v - 1} b_{v,i}\Theta_{v,i} \tag{3.6}$$

para algunos enteros $\{a_i : i \in [1,m] \cap \mathbb{N}\} \subseteq \mathbb{Z}$, donde $\Sigma \subseteq C$ el conjunto de puntos de C cuyas f-fibras son singulares y reducibles. Hemos excluido a $\Theta_{v,0}$ de la expansión para todo $v \in \Sigma$ puesto que, dado $v \in \Sigma$, $\Theta_{v,0} = f^{-1}(v) - \sum_{i=1}^{m_v-1} \mu_{v,i}\Theta_{v,i}$ en $\operatorname{Div}(S)$.

Si $P \in E^0(\mathbb{C}(C))$, fijamos $v \in \Sigma$ y $i \in [1, m_v - 1] \cap \mathbb{N}$. Sabemos, por la hipótesis sobre P y por el primer ítem del Teorema 3.3.5, que $\langle \Theta_{v,i}, (P) \rangle = \langle \Theta_{v,i}, (O) \rangle = 0$. Además, por el Lema A.3.1, $\left\langle \Theta_{v,i}, f^{-1}(v_j) \right\rangle = 0$ para todo $j \in [1,m] \cap \mathbb{N}$. Por consiguiente, tomando el número de intersección con $\Theta_{v,i}$ en la expresión 3.6, usando la nulidad algebraica de D y el hecho de que dos componentes irreducibles de f-fibras distintas son ortogonales, obtenemos

$$0 - 0 + 0 = 0 + \sum_{j=1}^{m_v-1} \langle \Theta_{v,i}, \Theta_{v,j} \rangle b_{v,j},$$

de donde $b_{v,j} = 0$ para todo $j \in [1, m_v - 1] \cap \mathbb{N}$, ya que la matriz en $\mathbb{Q}^{(m_v-1)\times(m_v-1)}$ en cuya entrada (i,j) tiene el valor $\langle \Theta_{v,i}, \Theta_{v,j} \rangle$ es inversible, por la Proposición 3.3.9. Como esto lo probamos para todo $v \in \Sigma$, entonces la expresión 3.6 se simplifica a

$$D - (P) + (O) \sim_S \sum_{i=1}^{m} a_i f^{-1}(v_i) = f^*\left(\sum_{i=1}^{m} a_i v_i\right). \tag{3.7}$$

Por el Lema 3.1.2,

$$\left\langle \sum_{i=1}^{m} a_i f^{-1}(v_i), (P) - (O) \right\rangle = \sum_{i=1}^{m} a_i - \sum_{i=1}^{m} a_i = 0,$$

luego, tomando número de intersección con $(P) - (O)$ en 3.7 obtenemos

$$\langle D, (P) \rangle - \langle D, (O) \rangle - \langle (P), (P) \rangle + \langle (P), (O) \rangle + \langle (O), (P) \rangle - \langle (O), (O) \rangle = 0$$

$$-2(-\chi(S)) + 2\langle (P), (O) \rangle = 0$$

$$\langle (P), (O) \rangle = -\chi(S),$$

donde hemos usado la nulidad algebraica de D y el Corolario 3.3.3. El Lema 3.5.2 permite probar, exactamente igual a como se hizo en la demostración del Teorema 3.5.3 por medio de la Fórmula de Noether, que $\chi(S) > 0$; por lo tanto $\langle (P), (O) \rangle < 0$. Si fuera $P \neq O$, entonces la Proposición 3.1.4 nos diría que $(P) \neq (O)$ y, por lo tanto, $\langle (P), (O) \rangle \geq 0$ (releer la última parte de 3.3.2), lo cual contradice la igualdad recién encontrada. Así, $P = O$ y la expresión 3.7 nos dice que $D \in \operatorname{Im}(f^*)$.

Esto lo probamos si $P \in E^0(\mathbb{C}(C))$. En general, $m(S)P \in E^0(\mathbb{C}(C))$. Definimos $\overline{D} := (m(S)P) - (O) - m(S)((P) - (O)) \in \operatorname{Div}(S)$. Entonces

$$\theta\left(\overline{D}\right) = (m(S)P)_E - (O)_E - m(S)((P)_E - (O)_E) =$$

$$= \gamma(m(S)P) - m(S)\gamma(P) = 0 \in \operatorname{Pic}(E),$$

de donde el Lema 3.7.1 nos dice que, multiplicando 3.6 por $m(S)$, obtenemos

$$m(S)D - (m(S)P) + (O) \sim_S \sum_{i=1}^{m'} a'_i f^{-1}(w_i) + \sum_{v\in\Sigma} \sum_{i=1}^{m_v-1} b'_{v,i}\Theta_{v,i}$$

para algún entero no negativo $m' \in \mathbb{N}_0$, algún conjunto finito $\{w_i : i \in [1, m'] \cap \mathbb{N}\} \subseteq C$ y algunos enteros $\{a'_i : i \in [1, m'] \cap \mathbb{N}\} \subseteq \mathbb{Z}$ y $\left\{b'_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\right\} \subseteq \mathbb{Z}$. Ahora podemos repetir el argumento con $P' := m(S) P \in E^0(\mathbb{C}(C))$, el cual demuestra que $m(S) D \sim f^*\left(\sum_{i=1}^{m'} a'_i w_i\right)$. Luego, identificando $\mathrm{Pic}^0(C)$ con un subgrupo de $\mathrm{Pic}^0(S)$ vía f^*, hemos probado que $m(S)\,\mathrm{Pic}^0(S) \subseteq \mathrm{Pic}^0(C) \subseteq \mathrm{Pic}^0(S)$. Es sabido que, en esta situación, se tiene entonces por cuestiones de dimensión la igualdad $\mathrm{Pic}^0(C) = \mathrm{Pic}(S)$ (léase [26, p. 12] o [19, p. 67]); lo cual, deshaciendo la identificación vía f^*, nos dice que f^* es sobreyectiva. ■

Usando este resultado, podremos probar que Ψ se anula sobre los divisores algebraicamente nulos. En efecto, si $D \in \mathrm{Div}(S)$ y $D \approx 0$, el Lema 3.7.8 nos dice que $D \sim_S f^*(B)$ para algún $B \in \mathrm{Pic}^0(C)$. Escribiendo B como combinación $\mathbb{Z}$-lineal de puntos de C y distribuyendo f^*, obtenemos que D es linealmente equivalente a una combinación $\mathbb{Z}$-lineal de f-fibras, con lo cual $D_E \sim_E 0$, y por lo tanto, teniendo en cuenta que $\langle D, F\rangle = 0$ pues $D \approx 0$, se tiene $\Psi(D) = \gamma^{-1}(D_E - \langle D, F\rangle O) = \gamma^{-1}(0) = O$. En consecuencia, Ψ induce naturalmente un morfismo sobreyectivo $\overline{\Psi} : \mathrm{NS}(S) \to E(\mathbb{C}(C))$ (la sobreyectividad está dada por la Observación 3.7.3).

Por el Lema 3.7.2 tenemos que, dado $D \in \mathrm{NS}(S)$,

$$D = \left(\overline{\Psi}(D)\right) + (d-1)(O) + nF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i},$$

donde los coeficientes se definen como en el referenciado lema. Así, si $D \in \ker\left(\overline{\Psi}\right)$, entonces $\left(\overline{\Psi}(D)\right) = (O)$ y $D \in \mathrm{Triv}(S)$. Recíprocamente, dado $D \in \mathrm{Triv}(S)$, $D = n(O) + \mathscr{D}$ para algún $n \in \mathbb{Z}$, donde $\mathscr{D} \in \mathrm{NS}(S)$ está generado por componentes irreducibles de f-fibras. En consecuencia

$$\overline{\Psi}(D) = \gamma^{-1}(nO + \mathscr{D}_E - \langle n(O) + \mathscr{D}, F\rangle O) =$$
$$= \gamma^{-1}(nO - n\langle (O), F\rangle O) = \gamma^{-1}(nO - nO) = O.$$

En la segunda igualdad hemos usado que $\mathscr{D}_E = 0$ (por estar generado por componentes irreducibles de f-fibras) y que $\langle \mathscr{D}, F\rangle = 0$ por el Lema A.3.1. En la tercera igualdad hemos usado que $\langle (O), F\rangle = 1$ por el Lema 3.1.2.

En definitiva, $\overline{\Psi} : \mathrm{NS}(S) \to E(\mathbb{C}(C))$ es un morfismo de grupos sobreyectivo tal que $\ker\left(\overline{\Psi}\right) = \mathrm{Triv}(S)$. Así, finalmente, tenemos un isomorfismo natural

$$\frac{\mathrm{NS}(S)}{\mathrm{Triv}(S)} \cong E(\mathbb{C}(C)),$$

lo cual prueba el Teorema 3.6.2.

Mencionemos una importante consecuencia conceptual de esta demostración. Obsérvese que hemos usado notaciones no ambiguas para los puntos P de $E(\mathbb{C}(C))$ y para las curvas (P) que son la imagen de sus secciones inducidas en la superficie elíptica. Dados $P, Q \in E(\mathbb{C}(C))$, tenemos la suma $P + Q$ según la operación en E, y tenemos la suma de divisores $(P) + (Q)$ en $\mathrm{Div}(S)$. Que $(P) + (Q) \neq (P + Q)$ debería estar claro en virtud del Lema 3.1.2, ya que si tomamos el número de intersección con cualquier f-fibra, la expresión de la izquierda nos da $1 + 1 = 2$, mientras que la expresión de la derecha nos da 1. Esto, además, nos dice que son distintos incluso si no distinguimos por equivalencia

algebraica. Sin embargo, la demostración que hemos expuesto en esta sección permite describir naturalmente el cociente de $\mathrm{Div}(S)$ donde estos dos elementos se identifican.

Sea $\varphi : E(\mathbb{C}(C)) \to \frac{\mathrm{NS}(S)}{\mathrm{Triv}(S)}$ que a cada $P \in E(\mathbb{C}(C))$ le asigna $(P) \mod \mathrm{Triv}(S)$. Ya vimos que $\overline{\Psi} : \mathrm{NS}(S) \to E(\mathbb{C}(C))$ induce un isomorfismo $\psi : \frac{\mathrm{NS}(S)}{\mathrm{Triv}(S)} \to E(\mathbb{C}(C))$. Por la Observación 3.7.3, se tiene

$$\psi(\varphi(P)) = \Psi((P)) = P.$$

Por otra parte, aplicando la definición de φ y el Lema 3.7.2, se tiene

$$\varphi(\psi(D)) = (\Psi(D)) \mod \mathrm{Triv}(S) = D,$$

de donde $\varphi = \psi^{-1}$ y por lo tanto φ es un morfismo de grupos. En definitiva, hemos demostrado que $(P+Q) = (P) + (Q)$ si cocientamos por los divisores algebraicamente nulos y aquellos generados por (O) y las componentes irreducibles de las f-fibras.

Por último, veamos que podemos derivar directamente una fórmula para el rango del retículo esencial $\mathscr{L}(S)$. Como el grupo $\mathscr{L}(S)$ es el complemento ortogonal de $\mathrm{Triv}(S)$, entonces su rango es igual a

$$\mathrm{rg}(\mathscr{L}(S)) = \mathrm{rg}(\mathrm{NS}(S)) - \mathrm{rg}(\mathrm{Triv}(S)) = \rho(S) - \left[2 + \sum_{v \in \Sigma} (m_v - 1)\right],$$

donde hemos usado la Proposición 3.6.1.

Veamos, finalmente, que $E^0(\mathbb{C}(C))$ es un subrupo de $E(\mathbb{C}(C))$ y que, además, se tiene la inclusión $m(S)\, E(\mathbb{C}(C)) \subseteq E^0(\mathbb{C}(C))$. Para esto, debemos traer a colación un resultado general de la *Teoría de Néron*, que enunciaremos con mucha menor generalidad aquí para adecuarlo al contexto de superficies elípticas. En general, la construcción del modelo de Kodaira-Néron que expusimos en 3.2 viene dada con la propiedad de que las operaciones de grupo en la fibra genérica de una superficie elíptica conmutan con la especialización en una fibra no singular; es decir, si $v \in C$ es tal que $f^{-1}(v)$ es no singular, entonces tenemos que $(P+Q)_v = P_v + Q_v$, donde la primera suma es la operación genérica, y la segunda suma es una operación especializada. Aquí, para cada $X \in E(\mathbb{C}(C))$, llamamos X_v a su especialización en $f^{-1}(v)$.

Lo que se puede probar por medio de la Teoría de Néron es que esta conmutatividad de la operación puede extenderse también al *smooth locus* de las fibras singulares. Concretamente: si $v \in C$ es tal que $F_v := f^{-1}(v)$ es singular, llamamos $F_v^{\#}$ al *smooth locus* de F_v; es decir, al grupo algebraico que resulta de eliminar las componentes irreducibles múltiples y también los nodos, que están dados por intersecciones entre componentes irreducibles. La Teoría de Néron nos dice que aquí también tenemos la extensión de la operación genérica y su conmutatividad con la especialización (consultar [4]) y, definiendo $F_{v,0}^{\#} := \Theta_{v,0} \cap F_v^{\#}$, entonces $F_{v,0}^{\#}$ es un subgrupo (normal) de $F_v^{\#}$ de forma que $G(F_v) := F_v^{\#}/F_{v,0}^{\#}$ es un grupo finito con tantos elementos como componentes irreducibles simples tenga F_v; en otras palabras, el orden de $G(F_v)$ es $m_v^{(1)}$ (aquí entra en juego nuestra Convención 3.3.10). La razón de esto último es que $G(F_v)$ resulta ser, de hecho, naturalmente isomorfo al *grupo discriminante* del retículo T_v.

Recuérdese que, en general, dado un retículo $(L, \langle\cdot,\cdot\rangle)$, tenemos definido el *retículo dual* L^* como aquellos elementos x de $L \otimes \mathbb{Q}$ tales que $\langle x, y\rangle \in \mathbb{Z}$ para todo $y \in L$, donde se

usa la extensión natural de $\langle\cdot,\cdot\rangle$ a $L\otimes\mathbb{Q}=L^*$. Así, se tiene $L\subseteq L^*$ y definimos *el grupo discriminante de* L como el cociente L^*/L, que resulta ser un grupo finito de orden $|\det(L)|$ (léase [25, p. 13]).

Dicho todo esto, hagamos algunas observaciones. En primer lugar, recuérdese que, dado $P\in E(\mathbb{C}(C))$, entonces (P) se define como la restricción a S de la clausura de P en $\mathcal{S}$, tal y como vimos en la demostración de la Proposición 3.1.4. Dado $v\in C$, de esto y el hecho de que $P_v\in S$ se sigue que $P_v\in(P)$. Además, por definición, $P_v\in F_v$. Pero el Lema 3.1.2 nos dice que no puede haber más de un solo punto en $F_v\cap(P)$, y por lo tanto se tiene necesariamente que $F_v\cap(P)=\{P_v\}$.

En segundo lugar, es natural preguntarse, inspirados en el párrafo anterior, si, dados $v\in C$ y $P\in E(\mathbb{C}(C))$, $F_v^{\#}\cap(P)=\{P_v\}$ o, equivalentemente, si al restringirnos al *smooth locus* de $F_v^{\#}$, es posible perder el punto P_v. La respuesta es que no. En efecto, como la intersección entre (P) y F_v se da de forma transversal en P_v, entonces P_v no puede pertenecer a una componente irreducible múltiple de F_v. Aquí estamos usando exactamente el mismo razonamiento por el que vale el primer ítem del Teorema 3.3.5. Lo único que falta probar es que P_v no es un punto de intersección entre dos componentes irreducibles distintas de F_v, pero esto es trivial puesto que, si P_v estuviera en más de una componente irreducible de F_v, la intersección $F_v\cap(P)$ no sería transversal en P_v y estaríamos violando el Lema 3.1.2.

Así, si $P\in E^0(\mathbb{C}(C))$ y $v\in C$, entonces $P_v\in F_v^{\#}\cap\Theta_{v,0}=F_{v,0}^{\#}$, y por lo tanto $(P)\cap F_{v,0}^{\#}=\{P_v\}$. Veamos un recíproco: supongamos que $P\in E(\mathbb{C}(C))$ y $(P)\cap F_{v,0}^{\#}=\{P_v\}$ para todo $v\in C$. Entonces, fijando $v\in C$, resulta que P_v, que es el único punto de intersección entre (P) y F_v, pertenece a $\Theta_{v,0}$, y como esto vale cualquiera sea $v\in C$, se sigue entonces que $P\in E^0(\mathbb{C}(C))$.

Hemos demostrado que, si $P\in E(\mathbb{C}(C))$, entonces $(P)\cap F_{v,0}^{\#}=\{P_v\}$ para todo $v\in C$ si y solo si $P\in E^0(\mathbb{C}(C))$. Veamos entonces por qué $E^0(\mathbb{C}(C))$ es un subrupo de $E(\mathbb{C}(C))$. Por definición (primer ítem del Teorema 3.3.5), $O\in E^0(\mathbb{C}(C))$. Sean $P,Q\in E^0(\mathbb{C}(C))$ y veamos que $P-Q\in E^0(\mathbb{C}(C))$. Fijamos $v\in C$. Buscamos probar que $(P-Q)\cap F_{v,0}^{\#}=\{(P-Q)_v\}$. Para esto, basta ver que $(P-Q)_v\in(P-Q)\cap F_{v,0}^{\#}$, puesto que $(P-Q)\cap F_{v,0}^{\#}$ no puede tener más de un elemento, por toda nuestra discusión anterior. Es claro que $(P-Q)_v\in(P-Q)$, pues ya vimos, en general, que si $X\in E(\mathbb{C}(C))$, entonces $X_v\in(X)$. Por otra parte, usando el citado resultado de la Teoría de Néron, se tiene que $(P-Q)_v=P_v-Q_v$. Y como $F_{v,0}^{\#}$ es un subgrupo de $F_v^{\#}$, se sigue que $P_v-Q_v\in F_{v,0}^{\#}$, ya que $P_v,Q_v\in F_{v,0}^{\#}$ pues $P,Q\in E^0(\mathbb{C}(C))$.

Veamos ahora que $m(S)E(\mathbb{C}(C))\subseteq E^0(\mathbb{C}(C))$. Sea $P\in E(\mathbb{C}(C))$ y sea $v\in C$. Sabemos entonces que $P_v\in F_v^{\#}$. Como $F_v^{\#}/F_{v,0}^{\#}$ es un grupo finito cuyo orden es exactamente $|\det(T_v)|=m_v^{(1)}$, entonces el Teorema de Lagrange nos dice que $m_v^{(1)}P_v\in F_{v,0}^{\#}$. Por definición se tiene que $m_v^{(1)}\mid m(S)$, y por lo tanto $m(S)P_v\in F_{v,0}^{\#}$. Usando nuevamente el resultado tomado de la Teoría de Néron, se tiene que $(m(S)P)_v\in F_{v,0}^{\#}$. Como $(m(S)P)\cap F_{v,0}^{\#}$ no puede tener más de un elemento, concluimos que $(m(S)P)\cap F_{v,0}^{\#}=\{(m(S)P)_v\}$. Como esto lo probamos cualquiera sea $v\in C$, esto demuestra que $m(S)P\in E^0(\mathbb{C}(C))$, como queríamos.

A modo de comentario, obsérvese que, si $P\in E(\mathbb{C}(C))$, entonces $P\in E^0(\mathbb{C}(C))$ si y solo si, para todo $v\in C$, la única componente de $f^{-1}(v)$ que intersecta a (P) es $\Theta_{v,0}$, lo cual equivale a que $(P)\cap\Theta_{v,i}$ para todo $v\in C$ y todo $i\in[1,m_v-1]\cap\mathbb{N}$, que

equivale a $\langle (P), \Theta_{v,i} \rangle = 0$ para todo $v \in C$ y todo $i \in [1, m_v - 1] \cap \mathbb{N}$, y por el Lema 3.7.4 esto equivale a $\beta(P) = (P) - (O) - (\chi(S) + \langle (P), (O) \rangle) F$. Más aún, la unicidad dada por el Lema 3.7.4 nos dice que, si $P \in E(\mathbb{C}(C))$, entonces $P \in E^0(\mathbb{C}(C))$ si y solo si $\beta(P) = (P) + a(O) + bF$ para algunos $a, b \in \mathbb{Q}$.

3.8 Torsión genérica

La Fórmula de Shioda-Tate dada por el Corolario 3.6.4 nos da información sobre la parte libre de la fibra genérica de una fibración elíptica. El objetivo de esta sección es brindar información sobre su grupo de torsión. Para esto, retomaremos todas las definiciones que hemos estipulado en la sección 3.7. En particular, analizaremos con mayor profundidad el morfismo de grupos $\beta : E(\mathbb{C}(C)) \to \mathrm{N}_{\mathbb{Q}}(S)$.

Antes de esto, requeriremos un lema adicional, que es algo que hemos demostrado implícitamente en los argumentos desarrollados en 3.7.

Lema 3.8.1 *Sean $D, D' \in \mathrm{Div}(S)$ tales que $D \approx D'$. Entonces $\theta(D) = \theta(D')$.*

Demostración. Sea $D'' := D - D'$. Como θ es un morfismo de grupos, lo que buscamos demostrar equivale a ver que $\theta(D'') = 0$. En efecto, como $D'' \approx 0$, entonces el Lema 3.7.8 nos dice que $D'' \sim_S f^*(B)$ para algún $B \in \mathrm{Pic}^0(C)$. Escribiendo B como combinación $\mathbb{Z}$-lineal de puntos de C y distribuyendo f^*, obtenemos que D'' es linealmente equivalente a una combinación $\mathbb{Z}$-lineal de f-fibras, con lo cual ${D''}_E \sim_E 0$; es decir, $\theta(D'') = 0$. ■

Para caracterizar los puntos de torsión genérica, veremos que $\ker(\beta) = E(\mathbb{C}(C))_{\mathrm{tors}}$. Dado $P \in E(\mathbb{C}(C))$, se tiene, por el Lema 3.7.4, que $\beta(P) = 0$ si y solo si $(P) - (O)$ es algebraicamente equivalente a una $\mathbb{Q}$-combinación lineal de componentes irreducibles de f-fibras. Equivalentemente, $\beta(P) = 0$ si y solo si existe $m \in \mathbb{N}$ tal que $m[(P) - (O)]$ es algebraicamente equivalente a un elemento del grupo 3.2.

Supongamos que $\beta(P) = 0$. Entonces, por el párrafo anterior, existe $m \in \mathbb{N}$ tal que $m[(P) - (O)]$ es algebraicamente equivalente a un elemento del grupo 3.2. Aplicando el Lema 3.8.1, podemos aplicar θ en esta relación y obtenemos

$$0 = \theta(m[(P) - (O)]) = m(P - O) = m\gamma(P) = \gamma(mP),$$

y como $\gamma : E(\mathbb{C}(C)) \to \mathrm{Pic}^0(E(\mathbb{C}(C)))$ es un isomorfismo, entonces $mP = O$ en $E(\mathbb{C}(C))$, y por lo tanto $P \in E(\mathbb{C}(C))_{\mathrm{tors}}$. Recíprocamente, si $P \in E(\mathbb{C}(C))_{\mathrm{tors}}$, entonces existe $m \in \mathbb{N}$ tal que $mP = O$ en $E(\mathbb{C}(C))$. En consecuencia, definiendo $D \in \mathrm{NS}(S)$ como $D = (P) - (O)$, el Lema 3.1.2 nos dice que $\langle D, F \rangle = 1 - 1 = 0$, y por lo tanto, usando la buena definición de θ módulo equivalencia algebraica dada por el Lema 3.8.1, se tiene

$$\overline{\Psi}(D) = \gamma^{-1}(D_E - \langle D, F \rangle O) = \gamma^{-1}(D_E) = \gamma^{-1}(P - O) = \gamma^{-1}(\gamma(P)) = P,$$

y por lo tanto $\overline{\Psi}(mD) = mP = O$; es decir, $m[(P) - (O)] \in \ker(\overline{\Psi})$. Pero vimos en la sección 3.7 que $\ker(\overline{\Psi}) = \mathrm{Triv}(S)$, y por lo tanto $m[(P) - (O)] \in \mathrm{Triv}(S)$. Así, por el Lema 3.5.1, existen $a, b \in \mathbb{Z}$ y un conjunto $\{b_{v,i} : i \in [1, m_v - 1] \cap \mathbb{N}, v \in \Sigma\} \subseteq \mathbb{Z}$ tales que

$$m[(P) - (O)] = a(O) + bF + \sum_{v \in \Sigma} \sum_{i=1}^{m_v - 1} b_{v,i} \Theta_{v,i}.$$

Tomando número de intersección con F y aplicando el Lema 3.1.2 y el Lema A.3.1, obtenemos

$$m(1-1) = a + 0 + 0 = a,$$

de donde $a = 0$ y por lo tanto $m[(P) - (O)]$ es algebraicamente equivalente a un elemento del grupo 3.2. Pero ya vimos que esto implica que $P \in \ker(\beta)$. Esto concluye nuestra demostración de que $\ker(\beta) = E(\mathbb{C}(C))_{\text{tors}}$.

Retomando el Lema 3.7.4 y la relación $m(S)\beta(E(\mathbb{C}(C))) \subseteq \mathscr{L}(S) \subseteq \text{NS}(S)$, lo anterior permite derivar el siguiente corolario que caracteriza los puntos de torsión genérica.

Proposición 3.8.2 *Sea S una $\mathbb{C}$-superficie proyectiva no singular y sea C una $\mathbb{C}$-curva proyectiva no singular. Sea $f : S \to C$ una fibración elíptica, y sea E su fibra genérica. Dado $P \in E(\mathbb{C}(C))$, son equivalentes:*

- $P \in E(\mathbb{C}(C))_{\text{tors}}$.
- $(P) \in \text{Tr}_{\mathbb{Q}}(S)$.
- *Existe $m \in \mathbb{Z} \setminus \{0\}$ tal que $m(P) \in \text{Triv}(S)$.*

Más aún: dado $m \in \mathbb{Z}$, se tiene $mP = O \in E(\mathbb{C}(C))$ si y solo si $m(P) \in \text{Triv}(S)$. En tal caso, el orden de torsión de P divide a $m(S)$.

3.9 Superficies elípticas racionales

Las superficies elípticas en las que la superficie subyacente es racional[2] se llaman *superficies elípticas racionales*. Para nosotros, $k = \mathbb{C}$. Sea C la superficie subyacente. Sabemos entonces que $\mathbb{C}(C)/\mathbb{C}$ es una subextensión de cuerpos de $\mathbb{C}(S)/\mathbb{C}$ cuyo grado de trascendencia es igual a 1. Por el **Teorema de Lüroth** (ver [7, p. 246]), sabemos que C tiene género 0. Por el Lema A.3.4, C es isomorfa a $\mathbb{P}^1(\mathbb{C})$.

Así, la fibra genérica de una superficie elíptica racional es una curva elíptica sobre el cuerpo de funciones de $\mathbb{P}^1(\mathbb{C})$, que es $\mathbb{C}(t)$. El Corolario 3.6.3 nos dice que dicha curva elíptica es de rango finito.

Dado que nuestro problema principal involucra solamente una superficie elíptica de este tipo, diremos algunas cosas respecto de las mismas. La ventaja aritmética de una tal superficie elíptica es que conocemos muy bien su característica de Euler y su número de Picard (léase A.3).

Proposición 3.9.1 *Sea (f, σ_0) una $\mathbb{C}$-superficie elíptica racional y sea S su superficie subyacente. Entonces $\chi(S) = 1$ y $\rho(S) = 10$.*

Demostración. Aplicamos la fórmula A.2 para obtener $\chi(S) = 1 - q(S) + p_g(S)$. Sabemos que $q(\mathbb{P}^2(\mathbb{C})) = p_g(\mathbb{P}^2(\mathbb{C})) = 0$. Como S es birracionalmente equivalente a $\mathbb{P}^2(\mathbb{C})$ por hipótesis, entonces podemos aplicar el Lema A.3.6 para obtener $\chi(S) = 1$.

Usando la Fórmula de Noether A.3, obtenemos $12 = e(S) + \langle K_S, K_S \rangle = e(S)$, donde en la última igualdad hemos usado el Lema 3.3.1. Por consiguiente, por la definición de

[2] Recuérdese que, dado un cuerpo k algebraicamente cerrado, una k-superficie proyectiva no singular S se dice *racional* si es birracionalmente equivalente a $\mathbb{P}^2(k)$ o, equivalentemente, si su cuerpo de funciones $k(S)$ es una extensión puramente trascendente de k cuyo grado de trascendencia es 2.

$e(S)$, se tiene $12 = e(S) = b_0(S) - b_1(S) + b_2(S) - b_3(S) + b_4(S) = 2 - 2b_1(S) + b_2(S)$, donde en la última igualdad hemos usado la Dualidad de Poincaré (léase A.3). Aplicando el Lema A.3.5 y el hecho de que $q(S) = 0$, obtenemos $b_1(S) = 0$, de donde $b_2(S) = 10$.

Recordemos que, dados $i, n \in \mathbb{N}_0$ y un grupo abeliano M, se tiene $H^i(\mathbb{P}^n(\mathbb{C}), M) \cong M$ si i es par y $i \leq 2n$, y que si no se cumplen esas dos condiciones, entonces $H^i(\mathbb{P}^n(\mathbb{C}), M) = 0$. Esto aplica directamente con $M = \mathbb{R}$ para ver que $b_2(\mathbb{P}^2(\mathbb{C})) = 1$. Por otra parte, usando que $\rho(\mathbb{P}^2(\mathbb{C})) = 1$, se tiene entonces $\rho(\mathbb{P}^2(\mathbb{C})) = b_2(\mathbb{P}^2(\mathbb{C})) = 1$. En particular, $\lambda(\mathbb{P}^2(\mathbb{C})) = b_2(\mathbb{P}^2(\mathbb{C})) - \rho(\mathbb{P}^2(\mathbb{C})) = 0$.

Como S es birracionalmente equivalente a $\mathbb{P}^2(\mathbb{C})$, el Lema A.3.6 nos dice que

$$0 = \lambda(\mathbb{P}^2(\mathbb{C})) = \lambda(S) = b_2(S) - \rho(S) = 10 - \rho(S),$$

de donde $\rho(S) = 10$. ■

A modo de comentario, el hecho de que valga $\rho(S) = 10$ en 3.9.1 puede justificarse de un modo más intuitivo, como se hace en [24, 8.8], usando el hecho de que una superficie elíptica racional es isomorfa a una superficie que se obtiene de $\mathbb{P}^2(\mathbb{C})$ haciendo nueve *blow-ups* sucesivos. Como $\rho(\mathbb{P}^2(\mathbb{C})) = 1$ y cada *blow-up* incrementa en 1 el valor del número de Picard (ver [25, p. 67] o [2, p. 12]), obtenemos nuevamente la Proposición 3.9.1.

Teniendo esta propiedad, requeriremos también de un criterio para decidir cuándo una superficie elíptica que construiremos especialmente es o no racional. Para esto, supongamos que tenemos una $\mathbb{C}(t)$-curva elíptica E tal que sus coeficientes están en $\mathbb{C}[t]$, lo cual siempre puede lograrse vía un adecuado cambio admisible de variables, tal y como vimos en 1.2, puesto que $\mathrm{Frac}(\mathbb{C}[t]) = \mathbb{C}(t)$. Supongamos, además, que su discriminante $\Delta \in \mathbb{C}[t]$ tiene grado positivo. En la Proposición 3.2.1 vimos un proceso para obtener una $\mathbb{C}$-superficie proyectiva no singular S y una fibración elíptica $f : S \to \mathbb{P}^1(\mathbb{C})$ cuya fibra genérica es E.

Ahora impondremos una nueva condición sobre E. Supóngase que E viene dada en la forma de Weierstrass usual,

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$
$$a_1, a_2, a_3, a_4, a_6 \in \mathbb{C}[t].$$

Supongamos que existe $\alpha \in \mathbb{C}$ que es raíz de a_i de multiplicidad mayor o igual que i, para todo $i \in \{1, 2, 3, 4, 6\}$. Si aplicamos el cambio admisible de variables inducido por $\begin{pmatrix} u^2 & 0 & 0 \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, donde $u := t - \alpha$, entonces, para cada $i \in \{1, 2, 3, 4, 6\}$, el coeficiente a_i queda multiplicado por $(t - \alpha)^{-i}$, lo cual implica que la multiplicidad de α como raíz de a_i se vio reducida en i unidades. Repitiendo este procedimiento suficientes veces, resulta que existe $i \in \{1, 2, 3, 4, 6\}$ tal que la multiplicidad de α como raíz de a_i es menor que i. Ahora podemos repetir el proceso con algún otro $\beta \in \mathbb{C}$ que es raíz de a_i de multiplicidad mayor o igual que i, para todo $i \in \{1, 2, 3, 4, 6\}$, y seguir repitiendo con nuevos valores hasta que no haya ninguno de ellos.

Este proceso debe terminar eventualmente, dado que el hecho de que no valen las identidades $a_i = 0$ para todo $i \in \{1, 2, 3, 4, 6\}$ (o de lo contrario tendríamos una cúbica singular $y^2z = x^3$) nos dice que el conjunto de raíces comunes a todos los coeficientes de E es un conjunto finito y las multiplicidades de cada una de ellas en cada coeficiente no son todas infinitas. Además, dicho conjunto puede verse reducido al aplicar los cambios admisibles de variable anteriormente estipulados, pero nunca ampliado.

Sea $d := \min\{n \in \mathbb{N} : \forall i \in \{1,2,3,4,6\}\,(\deg(a_i) \leq ni)\}$. Para cada $i \in \{1,2,3,4,6\}$, homogeneizamos a_i en $\mathcal{O}_{\mathbb{P}^1}(di)$ y deshomogeneizamos en $t = 1$. Si ahora aplicamos nuevamente el proceso de reducción con $s = 0$ y volvemos nuevamente a la expresión en función de t, entonces esta es la *minimalización* para $t = \infty = (1:0)$. Equivalentemente, minimalizar ∞ puede realizarse por medio del reemplazo de t por $\frac{1}{t}$, la aplicación del cambio admisible de variables inducido por $\begin{pmatrix} u^2 & 0 & 0 \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ con $u := t^{-d}$, y minimalizar 0 (de ser necesario), para luego volver a cambiar t por $\frac{1}{t}$ y aplicar el mismo cambio admisible de variables.

En consecuencia, supondremos que E es una $\mathbb{C}(t)$-curva elíptica E en forma de Weierstrass tal que sus coeficientes están en $\mathbb{C}[t]$, su discriminante Δ es de grado positivo, y tal que no existe ninguna raíz común a a_1, a_2, a_3, a_4, a_6 tal que su multiplicidad como raíz de a_i sea mayor o igual que i, para todo $i \in \{1,2,3,4,6\}$. Además, supondremos que tenemos la minimalidad en ∞. Cuando se cumplen todas estas condiciones (salvo quizá la hipótesis sobre Δ), decimos entonces que E es $\mathbb{C}[t]$-*minimal*. Cuando se cumplen todas estas condiciones salvo quizá la hipótesis sobre Δ y la minimalidad en ∞, decimos que E es $\mathbb{C}[t]$-*minimal en* $\mathbb{C}$.

Es natural inferir algunas condiciones bajo las cuales la $\mathbb{C}[t]$-minimalidad en $\mathbb{C}$ se alcanza. Por ejemplo, si para algún $i \in \{1,2,3,4,6\}$ se cumple que $\deg(a_i) < i$, entonces la curva elíptica es $\mathbb{C}[t]$-minimal en $\mathbb{C}$. Por otra parte, si $\deg(a_i) \leq i$ para algún $i \in \{1,2,3,4,6\}$, y además a_i tiene más de una raíz, entonces también tenemos $\mathbb{C}[t]$-minimalidad en $\mathbb{C}$.

Trabajando sobre las 2-formas diferenciales de S, es posible demostrar que, si $d = 1$, entonces S es racional (léase [25, 5.13]). Esto nos ofrece un sencillo criterio para saber si una superficie elíptica construida en virtud del proceso anteriormente mencionado es o no racional. Esencialmente, los pasos de la demostración pueden esquematizarse como sigue: es posible demostrar que $K_S = (d-2)F_\infty$, donde F es la f-fibra inducida por ∞, y $p_g(S) = d - 1$; esto último como consecuencia de la posibilidad de encontrar una base afín de $H^0(S, K_S)$. Así, si $d = 1$, se tiene que $p_g(S) = 0$ y que $-K_S = F_\infty > 0$ es efectivo. Esto último permite ver que todos los plurigéneros de S se anulan; en particular, $P_2(S) = 0$. Aplicando la Proposición A.3.7, obtenemos lo que queremos.

Capítulo 4

Solución del problema principal

Estamos, finalmente, en posición de encarar nuestro problema principal. A lo largo de todo este capítulo, fijamos $a \in \mathbb{Q}$ tal que $|a| < 1$, y notamos E_a a la $\mathbb{C}(t)$-curva elíptica en forma de Weierstrass

$$E_a : y^2 z = x^3 + t\left[(1+a)^2 t + 4(a-3)\right] x^2 z + 32(1-a)\, t^2 x z^2.$$

Asimismo, notaremos $P_{a,t} := \left(8t : 8(1+a)\, t^2 : 1\right)$. Nuestro objetivo es probar que, para todos salvo finitos valores de $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$, la $\mathbb{Q}$-curva elíptica que consiste en especializar E_a en este valor de t es de rango positivo.

Más generalmente, probaremos que el grupo $E_a(\mathbb{C}(t))$ tiene rango 1 y que $P_{a,t}$ es un punto sin torsión, y veremos cómo usar este resultado para probar que, para todos salvo finitos valores de $t \in \mathbb{Q}$, se tiene que la $\mathbb{Q}$-curva elíptica que consiste en especializar E_a en este valor de t tiene rango al menos 1. Este resultado, más fuerte, implica lo que buscamos demostrar y finaliza la demostración que dejamos inconclusa en el Capítulo 2.

4.1 Verificación de definiciones

En esta sección nos dispondremos a verificar que E_a induce una superficie elíptica y que, de hecho, la misma es una superficie elíptica racional.

Sabemos que E_a es una $\mathbb{C}(t)$-curva elíptica cuyos coeficientes están en $\mathbb{C}[t]$. Veamos que E_a es, de hecho, $\mathbb{C}[t]$-minimal. En efecto, si definimos $a_1 := 0$, $a_3 := 0$, $a_6 := 0$, $a_2 := t\left[(1+a)^2 t + 4(a-3)\right]$ y $a_4 := 32(1-a)\, t^2$, entonces

$$E_a : y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3,$$

donde $\deg(a_i) \leq i$ para $i \in \{1,2,3,4,6\}$, con igualdad si y solo si $i = 2$. En particular, $d := \min\{n \in \mathbb{N} : \forall i \in \{1,2,3,4,6\}\,(\deg(a_i) \leq ni)\} = 1$. Pero a_2 tiene dos raíces distintas, pues una de ellas es 0, y la otra es $\frac{4(3-a)}{(1+a)^2}$, la cual está bien definida pues $1 + a > 0$ al ser $|a| < 1$, y además es no nula pues, por la misma razón, $a \neq 3$. En consecuencia, tenemos minimalidad en todos los puntos de $\mathbb{C}$. Para ver si tenemos minimalidad en ∞, homogeneizamos cada coeficiente en el grado correspondiente y tomamos $t = 1$, lo cual nos da

$$y^2 z = x^3 + \left[(1+a)^2 + 4(a-3)\, s\right] x^2 z + 32(1-a)\, s^4 x z^2,$$

que cumple que las desigualdades estrictas $\deg(\widetilde{a_i}) < i$ para $i \in \{1,2,3,4,6\}$, donde $\widetilde{a_i}$ es la expresión de la homogeneización de a_i en $\mathcal{O}_{\mathbb{P}^1}(i)$ deshomogeneizada en $t = 1$. Así, tenemos también la minimalidad en ∞. Por lo tanto E_a es $\mathbb{C}[t]$-minimal.

Calculemos el discriminante Δ de E_a. Tenemos que

$$\begin{aligned}
b_2 &:= a_1^2 + 4a_2 = 4a_2 = 4t\left[(1+a)^2 t + 4(a-3)\right],\\
b_4 &:= 2a_4 + a_1a_3 = 2a_4 = 2\cdot 32(1-a)t^2 = 64(1-a)t^2,\\
b_6 &:= a_3^2 + 4a_6 = 0,\\
b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = -a_4^2 = -1024(1-a)^2t^4.
\end{aligned}$$

Así,

$$\begin{aligned}
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = -b_2^2b_8 - 8b_4^3\\
&= -16t^2\left[(1+a)^2t + 4(a-3)\right]^2\left[-1024(1-a)^2t^4\right] - 2097152(1-a)^3t^6\\
&= 16384(1-a)^2t^6\left[(1+a)^4t^2 + 8(1+a)^2(a-3) + 16(a-3)^2\right] - 2097152(1-a)^3t^6\\
&= 16384(1-a)^2t^6\left[(1+a)^4t^2 + 8(1+a)^2(a-3) + 16(a-3)^2 - 128(1-a)\right]\\
&= 2^{14}(1-a)^2t^6\left[(1+a)^4t^2 + 8(1+a)^2(a-3) + 16(1+a)^2\right]\\
&= 2^{14}\left(1-a^2\right)^2t^6\left[(1+a)^2t^2 + 8(a-3)t + 16\right].
\end{aligned}$$

Como $|a| < 1$, entonces $a^2 \neq 1$ y $1 + a > 0$. Por consiguiente, Δ es un polinomio de grado positivo.

En definitiva, E_a es una $\mathbb{C}(t)$-curva elíptica que es $\mathbb{C}[t]$-minimal y su discriminante es un polinomio de grado positivo en t. Por la Proposición 3.2.1, sabemos que existe una $\mathbb{C}$-superficie proyectiva no singular S y una fibración elíptica $f : S \to \mathbb{P}^1(\mathbb{C})$ cuya fibra genérica es E_a. Más aún, como $d = 1$, entonces lo discutido al final de la sección 3.9 implica que S es racional.

4.2 Singularidades

En la sección 4.1 vimos que E_a es una $\mathbb{C}(t)$-superficie elíptica cuyo discriminante es

$$\Delta = 2^{14}\left(1-a^2\right)^2t^6\left[(1+a)^2t^2 + 8(a-3)t + 16\right].$$

Asimismo, vimos cómo asociar una superficie elíptica a E_a. En esta sección aplicaremos el *Algoritmo de Tate*, tal y como fue expuesto en 3.4, para encontrar y clasificar las fibras singulares de esta superficie elíptica.

En primer lugar, calculemos las raíces de Δ. Está claro que 0 es una de ellas, y que el resto debemos buscarlas en las raíces de

$$(1+a)^2t^2 + 8(a-3)t + 16 \in \mathbb{C}[t],$$

las cuales están dadas por

$$\sigma_\pm = \frac{-8(a-3) \pm \sqrt{[8(a-3)]^2 - 4(1+a)^2\cdot 16}}{2(1+a)^2} = \frac{4(3-a) \pm 8\sqrt{2(1-a)}}{(1+a)^2}.$$

En consecuencia, nos interesa analizar las fibras dadas por $t \in \{0, \sigma_+, \sigma_-, \infty\}$.

Comenzaremos con σ_+ y σ_-. Sea $\sigma \in \{\sigma_+, \sigma_-\}$. Antes que nada, observemos que $\sigma \neq 0$. Si fuera $\sigma = 0$, entonces $4(3-a) \pm 8\sqrt{2(1-a)} = 0$, es decir, $3 - a = \mp 2\sqrt{2-2a}$. Elevando al cuadrado obtenemos $9 - 6a + a^2 = 4(2-2a)$, que se reduce a $0 = a^2 + 2a + 1 = (a+1)^2$. En consecuencia se tiene $a = -1$, lo cual es absurdo pues $|a| < 1$.

Como primera medida, debemos reemplazar t por $t + \sigma$ en E_a y posteriormente evaluar en 0 para obtener una $\mathbb{C}$-cúbica en forma de Weierstrass singular (que es $E_a(\sigma)$), a la cual le debemos aplicar una traslación en x para que su punto singular sea $(0:0:1)$. Se tiene que

$$E_a(\sigma) : y^2 z = x^3 + \sigma\left[(1+a)^2\sigma + 4(a-3)\right] x^2 z + 32(1-a)\sigma^2 x z^2$$

Buscamos la raíz múltiple de $X^3 + \sigma\left[(1+a)^2\sigma + 4(a-3)\right] X^2 + 32(1-a)\sigma^2 X$. Obsérvese que su derivada es $3X^2 + 2\sigma\left[(1+a)^2\sigma + 4(a-3)\right] X + 32(1-a)\sigma^2$, que no tiene a 0 como raíz puesto que $32(1-a)\sigma^2 \neq 0$, ya que $\sigma \neq 0$ y $a \neq 1$ pues $|a| < 1$. Por lo tanto, buscamos raíces comunes de los polinomios

$$P_\sigma := X^2 + \sigma\left[(1+a)^2\sigma + 4(a-3)\right] X + 32(1-a)\sigma^2,$$
$$Q_\sigma := 3X^2 + 2\sigma\left[(1+a)^2\sigma + 4(a-3)\right] X + 32(1-a)\sigma^2.$$

La raíz común entre P_σ y Q_σ es también raíz de

$$\begin{aligned} 3P_\sigma - Q_\sigma &= \sigma\left[(1+a)^2\sigma + 4(a-3)\right] X + 64(1-a)\sigma^2 \\ &= \sigma\left[\pm 8\sqrt{2(1-a)}\right] X + 64(1-a)\sigma^2. \end{aligned}$$

Así, la raíz común x_σ entre P_σ y Q_σ satisface

$$\begin{aligned} \pm\sqrt{2}\sqrt{1-a}\, x_\sigma &= -8(1-a)\sigma \\ \pm\sqrt{2}\, x_\sigma &= -8\sigma\sqrt{1-a} \\ x_\sigma &= \mp 4\sigma\sqrt{2-2a}. \end{aligned}$$

Cambiando x por $x + \sigma$ en la ecuación de E_a, obtenemos (afinizando)

$$y^2 = (x + x_\sigma)^3 + t\left[(1+a)^2 t + 4(a-3)\right](x + x_\sigma)^2 + 32(1-a)t^2(x + x_\sigma), \tag{4.1}$$

de donde el coeficiente de x^2 en 4.1 nos queda

$$3x_\sigma + t\left[(1+a)^2 t + 4(a-3)\right].$$

Para obtener la curva E_a^σ, según la notación introducida en 3.4, deberíamos reemplazar t por $t + \sigma$ en 4.1. Si hacemos eso, el coeficiente de x^2 nos quedará igual a

$$3x_\sigma + (t+\sigma)\left[(1+a)^2(t+\sigma) + 4(a-3)\right].$$

En consecuencia, para completar el Paso 1 del Algoritmo de Tate, debemos verificar si t divide o no a esta expresión o, equivalentemente, ver si la misma se anula o no en 0. Evaluando en 0, obtenemos

$$3x_\sigma + \sigma\left[(1+a)^2\sigma + 4(a-3)\right] = \mp 12\sigma\sqrt{2-2a} + \sigma\left[\pm 8\sqrt{2(1-a)}\right].$$

Si esto fuese nulo, entonces, usando que $\sigma \neq 0$, se tendría

$$\begin{aligned} 12\sqrt{2-2a} &= 8\sqrt{2-2a} \\ 3\sqrt{1-a} &= 2\sqrt{1-a}, \end{aligned}$$

de donde $\sqrt{1-a} = 0$ y por lo tanto $a = 1$, lo cual es absurdo pues $|a| < 1$. El absurdo provino de suponer que t divide al coeficiente de x^2 en E_a^σ, por lo tanto dicha divisibilidad no tiene lugar. Esto significa que el Algoritmo de Tate para σ finaliza en su Paso 1, dando como resultado que la fibra inducida por σ es de tipo $I_{\mathrm{mult}_\sigma(\Delta)} = I_1$, ya que σ_+ y σ_- aparecen en la factorización de Δ únicamente como raíces del factor cuadrático $(1+a)^2 t^2 + 8(a-3)t + 16$, el cual no tiene raíces dobles puesto que su discriminante es $512(1-a) \neq 0$, pues $a \neq 1$ ya que $|a| < 1$. En definitiva, las fibras inducidas por σ_+ y σ_- son ambas de tipo I_1.

Veamos ahora la fibra que induce 0. Cambiar t por $t+0$ es no hacer ningún cambio. Además, obsérvese que $E_a(0) : y^2 z = x^3$, con lo cual su punto singular ya es $(0:0:1)$. En consecuencia, no es necesario hacer una traslación en x y podemos comenzar el algoritmo directamente, y tenemos $E_a^0 = E_a$, de donde $a_2' = t\left[(1+a)^2 t + 4(a-3)\right]$, $a_4' = 32(1-a)t$ y $a_6' = 0$. De esta forma, se tiene $t \mid a_2'$, $t^2 \mid a_6'$ y, usando que $t \mid a_4'$, obtenemos también $t^2 \mid 4a_2'a_6' - ta_4'^2$. En consecuencia, estamos en el Paso 5 del Algoritmo de Tate, con lo cual debemos construir el polinomio en $\mathbb{C}[t][T]$

$$P(t)(T) := T^3 + \frac{a_2'}{t}T^2 + \frac{a_4'}{t} + \frac{a_6'}{t^2} = T^3 + \left[(1+a)^2 t + 4(a-3)\right]T^2 + 32(1-a)T$$

y su discriminante como polinomio en T

$$\begin{aligned} &t^{-6}\left(-4ta_2'^3a_6' + t^2a_2'^2a_4'^2 - 4t^3a_4'^3 - 27t^2a_6'^2 + 18t^2a_2'a_4'a_6'\right) = t^{-6}\left(t^2a_2'^2a_4'^2 - 4t^3a_4'^3\right) \\ &= t^{-6}\left(t^6\left[(1+a)^2 t + 4(a-3)\right]^2\left[32(1-a)t\right]^2 - 4t^6\left[32(1-a)t\right]^3\right) \\ &= \left[(1+a)^2 t + 4(a-3)\right]^2\left[32(1-a)t\right]^2 - 4\left[32(1-a)t\right]^3 \in \mathbb{C}[t]. \end{aligned}$$

Como t divide a este discriminante, estamos en el Paso 5.2, con lo cual debemos analizar la raíz múltiple de $P(0)(T) = T^3 + 4(a-3)T^2 + 32(1-a)T$. Esta raíz múltiple no es triple, pues 0 es raíz de este polinomio mónico, lo cual nos dice que si hubiese una raíz triple, esta necesariamente debería ser 0 y el polinomio sería igual a T^3; lo cual no es cierto, por ejemplo, porque su coeficiente lineal es no nulo al ser $a \neq 1$ pues $|a| < 1$. Se sigue que $P(0)(T)$ tiene una raíz doble y una raíz simple, pues tiene grado 3 y sabemos que su discriminante es nulo. Es decir, hemos terminado el Algoritmo de Tate en el Paso 5.2, concluyendo que la 0-fibra es de tipo $I^*_{\mathrm{mult}_0(\Delta)-6} = I^*_{6-6} = I^*_0$.

Por último, caractericemos la ∞-fibra. Para esto, cambiamos t por $\frac{1}{t}$ en E_a, obteniendo

$$y^2 z = x^3 + \frac{1}{t}\left[(1+a)^2\frac{1}{t} + 4(a-3)\right]x^2 z + 32(1-a)\frac{1}{t^2}xz^2.$$

Ahora, procedemos a tomar un cambio admisible de variables para integralizar esta curva. Sabemos que el cambio de variables inducido por $\begin{pmatrix} u^2 & 0 & 0 \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ con $u \in \mathbb{C}(t)^\times$ multiplica

el coeficiente de x^2 por u^{-2}, y el coeficiente de x por u^{-4}. En consecuencia, tomando $u = t^{-1}$, obtenemos

$$\widetilde{E}_a : y^2 z = x^3 + \left[(1+a)^2 + 4(a-3)t\right] x^2 z + 32(1-a)t^2 x z^2.$$

Procedemos a tomar esta nueva curva elíptica como curva base, y caracterizar su 0-fibra. En este caso tenemos una $\mathbb{C}(t)$-curva elíptica en la forma

$$y^2 z + A_1 xy + A_3 y = x^3 + A_2 x^2 z + A_4 x + A_6,$$

donde $A_1 = A_3 = A_6 = 0$, $A_2 = (1+a)^2 + 4(a-3)t$ y $A_4 = 32(1-a)t^2$. En consecuencia,

$$\begin{aligned}
B_2 &:= A_1^2 + 4A_2 = 4A_2 = 4\left[(1+a)^2 + 4(a-3)t\right], \\
B_4 &:= 2A_4 + A_1 A_3 = 2A_4 = 64(1-a)t^2, \\
B_6 &:= A_3^2 + 4A_6 = 0, \\
B_8 &:= A_1^2 A_6 + 4A_2 A_6 - A_1 A_3 A_4 + A_2 A_3^2 - A_4^2 = -A_4^2 = -1024(1-a)^2 t^4.
\end{aligned}$$

Así, su discriminante $\widetilde{\Delta}$ está dado por

$$\begin{aligned}
\widetilde{\Delta} &= -B_2^2 B_8 - 8B_4^3 - 27B_6^2 + 9B_2 B_4 B_6 = -B_2^2 B_8 - 8B_4^3 \\
&= -16\left[(1+a)^2 + 4(a-3)t\right]^2 \left[-1024(1-a)^2 t^4\right] - 2097152(1-a)^3 t^6 \\
&= 16384\left[(1+a)^4 + 8(1+a)^2(a-3)t + 16(a-3)^2 t^2\right](1-a)^2 t^4 - 2097152(1-a)^3 t^6.
\end{aligned}$$

Lo que nos importará es que 0 es raíz de multiplicidad 4 de $\widetilde{\Delta}$. En efecto, es claro que $\widetilde{\Delta}$ es divisible por t^4. Además, evaluando en 0 el polinomio $\frac{\widetilde{\Delta}}{t^4}$, obtenemos

$$16384(1+a)^4(1-a)^2 \neq 0,$$

donde en la última desigualdad hemos usado que $a \neq \pm 1$ pues $|a| < 1$.

Debemos caracterizar la 0-fibra respecto de esta nueva $\mathbb{C}(t)$-curva elíptica $\widetilde{E}_a$ en 0. Nuevamente, cambiar t por $t+0$ es no hacer cambio alguno, y como, afinizando,

$$\widetilde{E}_a(0) : y^2 = x^3 + (1+a)^2 x^2,$$

entonces tampoco es necesario hacer una traslación en x, pues el punto singular de $\widetilde{E}_a(0)$ ya es $(0:0:1)$. Es decir, $E_a^\infty = \widetilde{E}_a^0 = \widetilde{E}_a$. Obsérvese que t no divide al coeficiente de x^2 de $\widetilde{E}_a$, con lo cual el Algoritmo de Tate finaliza en el Paso 1 y nos dice que la ∞-fibra es de tipo $I_{\mathrm{mult}_0(\widetilde{\Delta})} = I_4$.

Hemos encontrado todas las fibras singulares y las hemos clasificado. Tenemos un total de cuatro fibras singulares, dos de las cuales son de tipo I_1, una es de tipo I_0^* y una es de tipo I_4. Recordando las definiciones dadas en 3.3.7, vemos que, de nuestras cuatro fibras singulares, solamente dos son reducibles: la de tipo I_0^*, que tiene exactamente $0+5=5$ componentes irreducibles, y la de tipo I_4, que tiene exactamente 4 componentes irreducibles.

4.3 Cómputo del rango

En esta sección calcularemos el rango de E_a como $\mathbb{C}(t)$-curva elíptica.

En 4.1 vimos que E_a tiene naturalmente asociada una superficie elíptica racional. En consecuencia, aplicamos la Proposición 3.9.1 para afirmar que la superficie subyacente tiene número de Picard igual a 10.

Por otra parte, en 4.2 vimos que hay solamente dos fibras de la superficie elíptica que son singulares y reducibles. Una de ellas tiene exactamente 5 componentes irreducibles, y la otra tiene exactamente 4 componentes irreducibles.

Aplicando esta información en la fórmula de Shioda-Tate dada por el Corolario 3.6.4, obtenemos

$$10 = \operatorname{rg}\left(E_a\left(\mathbb{C}(t)\right)\right) + 2 + (5-1) + (4-1),$$

de donde $\operatorname{rg}\left(E_a\left(\mathbb{C}(t)\right)\right) = 1$.

4.4 Grupo de torsión

En esta sección hallaremos $E_a\left(\mathbb{C}(t)\right)_{\text{tors}}$.

Comenzaremos buscando los puntos de orden 2.

Dado $P \in E_a\left(\mathbb{C}(t)\right)$, sabemos que P tiene orden 2 si y solo si $(0:1:0) \neq P = -P$. Así, aplicando la expresión 1.3, vemos que P tiene orden 2 si y solo si admite una forma afinizada $(Q,0)$ con $Q \in \mathbb{C}(t)$ tal que

$$0 = Q^3 + t\left[(1+a)^2 t + 4(a-3)\right] Q^2 + 32(1-a)\, t^2 Q.$$

En consecuencia, si $\overline{\mathbb{C}(t)}$ es una clausura algebraica de $\mathbb{C}(t)$, los puntos de orden 2 de $E_a\left(\mathbb{C}(t)\right)$ son un subconjunto de los puntos de orden 2 de $E_a\left(\overline{\mathbb{C}(t)}\right)$, y estos últimos están dados en la forma afinizada $(\alpha, 0)$, donde $\alpha \in \overline{\mathbb{C}(t)}$ es una raíz de

$$X^3 + t\left[(1+a)^2 t + 4(a-3)\right] X^2 + 32(1-a)\, t^2 X \in \mathbb{C}(t)[X]. \tag{4.2}$$

En consecuencia, hallar todos los puntos de orden 2 de $E_a\left(\mathbb{C}(t)\right)$ equivale a hallar las raíces de 4.2 y quedarnos solamente con aquellas que pertenezcan a $\mathbb{C}(t)$. Es claro que $0 \in \mathbb{C}(t)$ es una de esas raíces, con lo cual $(0,0)$ es uno de los puntos de orden 2 del grupo $E_a\left(\mathbb{C}(t)\right)$. El resto de los puntos debemos buscarlos, pues, en las raíces de

$$X^2 + t\left[(1+a)^2 t + 4(a-3)\right] X + 32(1-a)\, t^2 \in \mathbb{C}(t)[X]. \tag{4.3}$$

Afirmamos que ninguna de las raíces de 4.3 pertenece a $\mathbb{C}(t)$. Para esto, usando que 4.3 es un polinomio cuadrático, basta ver que su discriminante

$$\left(t\left[(1+a)^2 t + 4(a-3)\right]\right)^2 - 4\left[32(1-a)\, t^2\right] \tag{4.4}$$

no es un cuadrado en $\mathbb{C}(t)$. Como 4.4 es claramente divisible por t^2, que es un cuadrado en $\mathbb{C}(t)$, entonces ver que 4.4 no es un cuadrado en $\mathbb{C}(t)$ equivale a ver que

$$\left[(1+a)^2 t + 4(a-3)\right]^2 - 4\left[32(1-a)\right]$$
$$= (1+a)^4 t^2 + 8(1+a)^2 (a-3)\, t + 16(a-3)^2 - 128(1-a) \in \mathbb{C}[t] \tag{4.5}$$

no es un cuadrado en $\mathbb{C}(t)$.

Lema 4.4.1 *Sea R un dominio de factorización única, sea $r \in R$ y $\alpha \in \mathrm{Frac}(R)$ tales que $\alpha^n = r$ para algún $n \in \mathbb{N}$. Entonces $\alpha \in R$.*

Demostración. Como $\alpha \in \mathrm{Frac}(R)$, escribimos $\alpha = \frac{u}{v}$ con $u, v \in R$ y $v \neq 0$. Como R es un dominio de factorización única, podemos suponer que u y v son coprimos sin pérdida de generalidad. Así, la expresión $\alpha^n = r$ se reescribe como $u^n = rv^n$. Si existiera un factor irreducible π de v, entonces, como $r \in R$, se tiene $\pi \mid rv^n = u^n$ en R, y como π es irreducible, entonces $\pi \mid u$. Esto contradice que u y v son coprimos.

El absurdo provino de suponer que v admite factores irreducibles. En consecuencia v debe ser una unidad en R, y por lo tanto $\alpha = \frac{u}{v} \in R$. ■

Como $\mathbb{C}[t]$ es un dominio de factorización única y $\mathrm{Frac}(\mathbb{C}[t]) = \mathbb{C}(t)$, entonces, por el Lema 4.4.1, ver que 4.5 no es un cuadrado en $\mathbb{C}(t)$ equivale a ver que 4.5 no es un cuadrado en $\mathbb{C}[t]$. Esto, a su vez, usando que 4.5 es un polinomio cuadrático en $\mathbb{C}[t]$, equivale a ver que su discriminante

$$\begin{aligned}
&\left[8(1+a)^2(a-3)\right]^2 - 4(1+a)^4\left[16(a-3)^2 - 128(1-a)\right] \\
&= (1+a)^4\left[64(a-3)^2 - 64(a-3)^2 + 512(1-a)\right] \\
&= 512(1+a)^4(1-a)
\end{aligned}$$

es no nulo. Pero esto es trivialmente verdadero, pues $|a| < 1$; en particular, $a \neq \pm 1$. Concluimos que $(0:0:1)$ es el único punto de orden 2 del grupo $E_a(\mathbb{C}(t))$.

Vimos en la sección 4.1 que E_a tiene naturalmente asociada una superficie elíptica racional. Aplicamos la Proposición 3.9.1 para afirmar que su número de Euler, que notamos χ, es igual a 1. Sabemos, por la sección 4.3, que el rango de $E_a(\mathbb{C}(t))$ es igual a 1. En consecuencia, los únicos valores de $s \in \mathbb{R}$ tales que $\mathrm{rg}(E_a(\mathbb{C}(t))) \leq s\chi - 2$ son aquellos $s \in \mathbb{R}$ tales que $s \geq 3$. Usando esto, podemos consultar la tabla expuesta en [20, p. 264], que expone las posibilidades para el grupo de torsión de las superficies elípticas cuyas curvas base tienen género nulo (como lo es nuestro caso, pues nuestra curva base es $\mathbb{P}^1(\mathbb{C})$) en función de parámetros como la característica de Euler y el rango de la fibra genérica. Haciendo esto, vemos que $E_a(\mathbb{C}(t))_{\mathrm{tors}}$ puede ser isomorfo solamente a alguno de estos grupos:

$$\{0\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Como $(0:0:1)$ es un punto de torsión, excluimos $\{0\}$ de la lista de posibilidades. Como, además, tiene orden 2, también podemos excluir $\mathbb{Z}/3\mathbb{Z}$ (pues de lo contrario $2 \mid 3$). Adicionalmente, como $(0:0:1)$ es el único punto de orden 2, excluimos también $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Así, las únicas posibilidades para $E_a(\mathbb{C}(t))_{\mathrm{tors}}$ son $\mathbb{Z}/2\mathbb{Z}$ y $\mathbb{Z}/4\mathbb{Z}$.

Finalmente, excluyamos la última posibilidad. Para esto, requeriremos un lema, cuya demostración es una aplicación directa de los resultados de la sección 1.3.

Lema 4.4.2 *Sea $\mathbb{K}$ un cuerpo perfecto y sea*

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$
$$a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$$

una $\mathbb{K}$-curva elíptica. Sea $P \in E(\mathbb{K})$ tal que $P \neq (0:1:0) \neq 2P$. Entonces, escribiendo $P = (x_0 : y_0 : 1)$ con $x_0, y_0 \in \mathbb{K}$, se tiene $2P = (x_1 : y_1 : 1)$ con $x_1, y_1 \in K$ y

$$x_1 = \frac{x_0^4 - b_4x_0^2 - 2b_6x_0 - b_8}{4x_0^3 + b_2x_0^2 + 2b_4x_0 + b_6}.$$

Supongamos que $E_a(\mathbb{C}(t))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}$. Tomando un generador $P \in E_a(\mathbb{C}(t))$ de $E_a(\mathbb{C}(t))_{\text{tors}}$, se tiene que P tiene orden 4, y por lo tanto $2P$ tiene orden 2. Como $(0:0:1)$ es el único punto de orden 2, entonces $2P = (0:0:1)$. Más aún, como $P \neq (0:1:0)$ pues P tiene orden 4, entonces existen $x_0, y_0 \in \mathbb{C}(t)$ tales que $P = (x_0 : y_0 : 1)$. Usando que $2P = (0:0:1)$, el Lema 4.4.2 nos dice que

$$\frac{x_0^4 - b_4 x_0^2 - 2b_6 x_0 - b_8}{4x_0^3 + b_2 x_0^2 + 2b_4 x_0 + b_6} = 0, \tag{4.6}$$

donde $a_1 = a_3 = a_6 = 0$, $a_2 = t\left[(1+a)^2 t + 4(a-3)\right]$, $a_4 = 32(1-a)t^2$ y, por lo visto en la sección 4.1,

$$\begin{aligned} b_2 &= 4t\left[(1+a)^2 t + 4(a-3)\right], \\ b_4 &= 64(1-a)t^2, \\ b_6 &= 0, \\ b_8 &= -1024(1-a)^2 t^4. \end{aligned}$$

Eliminando el denominador de la expresión 4.6, obtenemos

$$0 = x_0^4 - b_4 x_0^2 - 2b_6 x_0 - b_8 = x_0^4 - 64(1-a)t^2 x_0^2 + 1024(1-a)^2 t^4 = \left[x_0^2 - 32t^2(1-a)\right]^2,$$

de donde $x_0^2 - 32t^2(1-a) = 0$; es decir, $x_0^2 = 32t^2(1-a)$.

Como $|a| < 1$, entonces $1 - a > 0$. Sea $k := \sqrt{\frac{1-a}{2}} > 0$. Entonces $a = 1 - 2k^2$, luego

$$x_0^2 = 32t^2(1-a) = 32t^2\left(2k^2\right) = (8kt)^2,$$

de donde $x_0 = \pm 8kt$. Sustituyendo $x = x_0 = \pm 8kt$, $y = y_0$, $z = 1$ y $a = 1 - 2k^2$ en la ecuación de E_a, obtenemos

$$\begin{aligned} y_0^2 &= (\pm 8kt)^3 + t\left[\left(1 + 1 - 2k^2\right)^2 t + 4\left(1 - 2k^2 - 3\right)\right](\pm 8kt)^2 + 32\left(2k^2\right)t^2(\pm 8kt) \\ &= 2(\pm 8kt)^3 + t\left[\left(2 - 2k^2\right)^2 t - 4\left(2 + 2k^2\right)\right] \cdot 64k^2t^2 \\ &= \pm 1024k^3t^3 + 64k^2t^3\left[4\left(1 - k^2\right)^2 t - 8\left(1 + k^2\right)\right] \\ &= 256k^2t^3\left[\pm 4k + \left(1 - k^2\right)^2 t - 2\left(1 + k^2\right)\right] \in \mathbb{C}[t]. \end{aligned}$$

Definiendo $P_1 := 256k^2t^3 \in \mathbb{C}[t]$ y $P_2 := \pm 4k + \left(1 - k^2\right)^2 t - 2\left(1 + k^2\right) \in \mathbb{C}[t]$, veamos que P_1 y P_2 son coprimos en $\mathbb{C}[t]$. Como $k \in \mathbb{R}_{>0}$, el único factor mónico irreducible que divide a P_1 es t. Así, debemos ver que $t \nmid P_2$. Si lo dividiera, se tendría $\pm 4k - 2\left(1 + k^2\right) = 0$; es decir, $0 = k^2 \mp 2k + 1 = (k \mp 1)^2$, de donde $|k| = 1$, y como $k > 0$, $1 = k = \sqrt{\frac{1-a}{2}}$, y por lo tanto $a = -1$, absurdo pues $|a| < 1$.

Lema 4.4.3 *Sea R un dominio de factorización única tal que, para toda unidad μ de R, existe $\eta \in R$ tal que $\eta^2 = \mu$. Entonces, dados $r, s \in R \setminus \{0\}$ coprimos y $\alpha \in \text{Frac}(R)$ tales que $rs = \alpha^2$, se sigue que r y s son cuadrados en R.*

Demostración. Para ver que un elemento x de R es un cuadrado perfecto, basta ver que los exponentes de cada uno de sus factores irreducibles en su factorización única en irreducibles son pares. En efecto, esto probará que dicho elemento es un múltiplo unitario de un cuadrado perfecto, y como toda unidad es un cuadrado en R por hipótesis, se sigue que x será, de hecho, un cuadrado en R.

Por el Lema 4.4.1 se tiene que $\alpha \in R$; luego admite una factorización única en irreducibles. En consecuencia, α^2 admite una factorización única en irreducibles en la cual todos sus exponentes son pares. Si r es unidad, no hay nada que probar, pues en tal caso es un cuadrado por hipótesis y los exponentes de s en su factorización única en irreducibles coinciden con los de α^2, que son todos pares, y entonces podemos aplicar lo expuesto en el párrafo anterior. Supongamos entonces que r no es una unidad y sea π uno de sus factores irreducibles. Por hipótesis, π no figura en la factorización única en irreducibles de s, por lo tanto, el exponente de π en la factorización única en irreducibles de r coincide con el de α^2, que es par. Así, hemos probado que todos los factores irreducibles de r figuran con exponente par en la factorización única en irreducibles de r. Por lo visto en el primer párrafo, esto implica que $r = c^2$ para algún $c \in R$. Pero entonces $c^2 \mid \alpha^2$ en R, de donde $c \mid \alpha$ en R, luego $\frac{\alpha}{c} \in R$ y $s = \left(\frac{\alpha}{c}\right)^2$. ■

Es claro que el dominio de factorización única $\mathbb{C}[t]$ satisface las hipótesis del Lema 4.4.3, pues su grupo de unidades es el cuerpo $\mathbb{C}$, que es algebraicamente cerrado. Así, aplicando dicho lema con $R = \mathbb{C}[t]$, $r = P_1$, $s = P_2$ y $\alpha = y_0$, obtenemos que P_1 es un cuadrado en $\mathbb{C}[t]$, lo cual es imposible puesto que el grado de P_1 es impar.

El absurdo provino de suponer que $E_a(\mathbb{C}(t))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}$. Por consiguiente, la única posibilidad es que $E_a(\mathbb{C}(t))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$, y que dicho grupo esté generado por el único elemento de orden 2, que es $(0:0:1)$.

4.5 Punto sin torsión genérica

En esta sección probaremos que $P_{a,t}$ es un punto sin torsión en $E_a(\mathbb{C}(t))$ y haremos algunas observaciones importantes de este hecho. Lo que más nos importará es que habremos encontrado un punto en $E_a(\mathbb{Q}(t))$ que no tiene torsión en el grupo $E_a(\mathbb{C}(t))$.

Esto se sigue trivialmente de lo visto en 4.4. Allí vimos que el grupo de torsión es

$$E_a(\mathbb{C}(t))_{\text{tors}} = \mathbb{Z}(0:0:1) = \{(0:1:0),(0:0:1)\} \cong \mathbb{Z}/2\mathbb{Z},$$

al cual $P_{a,t}$ no pertenece.

Obsérvese que, como $P_{a,t}$ es un punto de $E_a(\mathbb{Q}(t))$, que es un subgrupo de $E_a(\mathbb{C}(t))$ (léase A.1), entonces el hecho de que $P_{a,t}$ no tenga torsión en $E_a(\mathbb{C}(t))$ implica trivialmente que tampoco la tiene en $E_a(\mathbb{Q}(t))$.

Sin embargo, ha de tenerse la siguiente precaución: esto no significa que, dado $t_0 \in \mathbb{Q}$ distinto de las raíces de Δ, el punto $\left(8t_0 : 8(1+a)t_0^2 : 1\right)$ sea un punto sin torsión en la $\mathbb{Q}$-curva elíptica

$$E_a : y^2z = x^3 + t_0\left[(1+a)^2 t_0 + 4(a-3)\right]x^2z + 32(1-a)t_0^2xz^2.$$

En efecto, el hecho de que los puntos de la forma $mP_{a,t} \in E_a(\mathbb{Q}(t))$ con $m \in \mathbb{Z}$ sean genéricamente distintos dos a dos como expresiones racionales en t no implica que esto

siga valiendo cuando especializamos en un valor particular de $t \in \mathbb{Q}$. En consecuencia, el problema sigue sin resolverse.

En la siguiente sección veremos que existe un resultado teórico que permite sortear esta dificultad.

4.6 Solución

Para terminar de resolver el problema, nos valdremos de un resultado conocido como el *Teorema de Especialización de Silverman*, el cual no enunciaremos en su mayor generalidad, sino en una versión débil que será la que utilizaremos. El resultado general puede encontrarse demostrado en [27, p. 271]. Dada E una $\mathbb{C}(t)$-curva elíptica con coeficientes en $\mathbb{C}[t]$ cuyo discriminante es un polinomio de grado positivo en t, y dado $t_0 \in \mathbb{C}$ tal que el discriminante de E no se anula en t_0 (lo cual se cumple para todos salvo finitos valores de $\mathbb{C}$, por la hipótesis sobre el discriminante), tenemos naturalmente definida una función *especialización en* t_0, que consiste en definir $\sigma_{t_0} : E(\mathbb{C}(t)) \to E(t_0)(\mathbb{C})$ que a cada $P \in E(\mathbb{C}(t))$ le asigna $P(t_0) \in E(t_0)(\mathbb{C})$. La buena definición de σ_{t_0} se sigue de que la evaluación en t_0 es un morfismo de anillos, y el hecho de que σ_{t_0} sea un morfismo de grupos se sigue también de esta propiedad de la evaluación en t_0 y la estructura de las fórmulas de la operación de grupo, expuestas en 1.3.

Lema 4.6.1 *Sea E una $\mathbb{C}(t)$-curva elíptica. Para todos salvo finitos $t_0 \in \mathbb{Q}$, el morfismo σ_{t_0} es inyectivo.*

Aplicando el Lema 4.6.1 obtenemos que, para todos salvo finitos $t_0 \in \mathbb{Q}$, el morfismo $\sigma_{t_0} : E_a(\mathbb{C}(t)) \to E_a(t_0)(\mathbb{C})$ es inyectivo. En particular, como $iP_{a,t} \neq jP_{a,t}$ si $i, j \in \mathbb{Z}$ y $i \neq j$, entonces esta desigualdad también vale al aplicar σ_{t_0}, lo cual nos muestra que $P_{a,t}(t_0) \in E_a(t_0)(\mathbb{C})$ es un punto sin torsión. Ahora, usando que $P_{a,t}(t_0)$ está, de hecho, en $E_a(t_0)(\mathbb{Q})$ y que la operación en las curvas elípticas es cerrada en subcuerpos por lo visto en A.1, se sigue entonces que para todos salvo finitos $t_0 \in \mathbb{Q}$, la $\mathbb{Q}$-curva elíptica

$$y^2 z = x^3 + t_0\left[(1+a)^2 t_0 + 4(a-3)\right] x^2 z + 32(1-a)\, t_0^2 x z^2$$

admite una solución sin torsión dada por $\left(8t_0 : 8(1+a)\, t_0^2 : 1\right)$. Por la Proposición 2.2.2 y la discusión de la sección 2.3, esto resuelve nuestro problema principal.

4.7 Resultados adicionales

Habiendo resuelto nuestro problema, expondremos a modo de comentario algunos resultados adicionales que Matilde Lalín y Xinchun Ma pudieron demostrar en [13]. En esta sección, todas las tablas mostradas están tomadas de este paper.

Un primer resultado importante que Lalín y Ma consiguieron demostrar es que el rango de $E_a(\mathbb{C}(t))$ no solamente es igual a 1, sino que $P_{a,t} = \left(8t : 8(1+a)t^2 : 1\right)$ es generador del mismo. Esto, junto con la determinación del grupo de torsión, logra tener perfectamente caracterizada la $\mathbb{C}(t)$-curva elíptica que ofrece tantos resultados geométricos.

Recordando que a era, en nuestro modelo, el coseno de uno de los ángulos de nuestro triángulo (que habíamos notado como θ), el caso $a = 0$ permite analizar qué sucede con pares de un triángulo rectángulo entero y un ω-paralelogramo entero, ambos con la misma área y el mismo perímetro, y $a = t\sin(\omega)$. Así, trabajando con $E_{0,t}$ (la cual es no singular para $t \neq 0$), lograron recuperar el resultado obtenido por Yong Zhang en el año 2016 mencionado en la introducción. Observaron que $P_{0,t}$ es de orden finito solamente para los valores $t \in \left\{\frac{1}{2}, \frac{2}{3}, 1\right\}$, y analizaron cada una de esas excepciones, proporcionando una tabla con la información de estos puntos de incertidumbre.

t	ω	$E_{0,t}(\mathbb{Q})$	generators	solutions
$\frac{1}{2}$	$\frac{\pi}{6}$	$\mathbb{Z}/6\mathbb{Z}$	$\langle(2,1)\rangle$, $P_{0,\frac{1}{2}} = 2(2,1)$	none
$\frac{2}{3}$	$\sin^{-1}(2/3)$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\langle P_{0,\frac{2}{3}}, (0,0)\rangle$	$(4,0)$, $\left(\frac{32}{9}, 0\right)$ $p = q = x$, $y = \frac{4}{3}x$
1	$\frac{\pi}{2}$	$\mathbb{Z}/6\mathbb{Z}$	$\langle P_{0,1}\rangle$	none

Debe aclararse que, en todas las tablas, *none* en la parte de soluciones significa que solamente hay soluciones degeneradas, las cuales no son de nuestro interés.

En esta última tabla, el caso $t = 1$ es particularmente interesante, en tanto el mismo recupera el primer resultado de Richard Guy de 1995.

En el caso en que $a = \frac{1}{2}$ es el caso en que $\theta = \frac{\pi}{3}$. Resulta que $E_{\frac{1}{2},t}$ es no singular exactamente en los puntos $t \notin \left\{0, \frac{8}{9}, 8\right\}$. Dado un t distinto de 0, $\frac{8}{9}$ y 8, el punto $P_{\frac{1}{2},t}$ tiene orden infinito para los $t \notin \left\{-1, \frac{1}{2}, \frac{4}{5}, 1, 2\right\}$. Por supuesto, los casos $t = -1$ y $t = 2$ son irrelevantes para el problema geométrico. Para el resto de los casos, Lalín y Ma proporcionando una tabla pertinente.

t	ω	$E_{\frac{1}{2},t}(\mathbb{Q})$	generators	solutions
$\frac{1}{2}$	$\sin^{-1}(\sqrt{3}/4)$	$\mathbb{Z}/6\mathbb{Z}$	$\langle\left(1, \frac{3}{4}\right)\rangle$, $P_{\frac{1}{2},\frac{1}{2}} = 2\left(1, \frac{3}{4}\right)$	none
$\frac{4}{5}$	$\sin^{-1}(2\sqrt{3}/5)$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\langle P_{\frac{1}{2},\frac{4}{5}}, (0,0)\rangle$	$(4,0)$, $\left(\frac{64}{25}, 0\right)$ $p = q = x$, $y = \frac{8}{5}x$
1	$\frac{\pi}{3}$	$\mathbb{Z}/8\mathbb{Z}$	$\langle P_{\frac{1}{2},1}\rangle$	$(4, \pm 2)$ $p = x = y$, $q = p/2$

También consideraron el caso $a = -\frac{1}{2}$, en el cual $\theta = \frac{2\pi}{3}$. Aquí, $E_{-\frac{1}{2},t}$ es no singular

para los $t \neq 0$. Y, dado $t \neq 0$, $P_{-\frac{1}{2},t}$ es de orden infinito para $t \notin \left\{\frac{1}{2}, \frac{4}{7}, \frac{2}{3}\right\}$, y en estos casos excepcionales ofrecieron, también, información resumida sobre cada situación. El caso llamativo fue $t = \frac{4}{7}$ en el cual, si bien $P_{-\frac{1}{2},\frac{4}{7}}$ es un punto de torsión de $E_{-\frac{1}{2},\frac{4}{7}}$, lograron encontrar un punto sin torsión y, por lo tanto, el razonamiento del Capítulo 2 aplica para garantizar la existencia de infinitas soluciones.

t	ω	$E_{-\frac{1}{2},t}(\mathbb{Q})$	generators (if torsion) or point of infinite order (if positive rank)	solutions
$\frac{1}{2}$	$\sin^{-1}(\sqrt{3}/4)$	$\mathbb{Z}/6\mathbb{Z}$	$\langle(3, \frac{3}{4})\rangle$, $P_{-\frac{1}{2},\frac{1}{2}} = 2\left(3, \frac{3}{4}\right)$	none
$\frac{4}{7}$	$\sin^{-1}(2\sqrt{3}/7)$	$\mathrm{rk}(E_{-\frac{1}{2},\frac{4}{7}}(\mathbb{Q})) > 0$	$\left(\frac{12}{7}, \frac{144}{49}\right)$	$3\left(\frac{12}{7}, \frac{144}{49}\right)$ infinitely many
$\frac{2}{3}$	$\sin^{-1}(1/\sqrt{3})$	$\mathbb{Z}/6\mathbb{Z}$	$\langle P_{-\frac{1}{2},\frac{2}{3}}\rangle$	none

La motivación para mirar los casos $a \in \left\{0, \frac{1}{2}, -\frac{1}{2}\right\}$ radica en que inducen los ángulos $\frac{\pi}{2}$, $\frac{\pi}{3}$ y $\frac{2\pi}{3}$, los cuales son los únicos ángulos que son múltiplos racionales de π y cuyos cosenos son racionales.

Es interesante, por otro lado, analizar el caso $t = 1$, en el que $\sin(\theta) = \sin(\omega)$; es decir, $\theta \in \{\omega, \pi - \omega\}$. Encontraron que $E_{a,1}$ nunca es singular para $|a| < 1$, y que $P_{a,1}$ es un punto sin torsión de $E_{a,1}$ exactamente cuando $a \notin \left\{0, \frac{1}{2}, \frac{2}{3}\right\}$, y, como antes, es posible resumir los resultados obtenidos en cada caso.

a	ω	$E_{a,1}(\mathbb{Q})$	generators	solutions
0	$\frac{\pi}{2}$	$\mathbb{Z}/6\mathbb{Z}$	$\langle P_{0,1}\rangle$	none
$\frac{1}{2}$	$\frac{\pi}{3}$	$\mathbb{Z}/8\mathbb{Z}$	$\langle P_{\frac{1}{2},1}\rangle$	$(4, \pm 2)$ $p = x = y$, $q = p/2$
$\frac{2}{3}$	$\sin^{-1}(\sqrt{5}/3)$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\langle P_{\frac{2}{3},1}, (0,0)\rangle$	$(3,0)$, $\left(\frac{32}{9}, 0\right)$ $y = \frac{8}{9}x$, $p = q = \frac{2}{3}x$ $\left(4, \pm\frac{4}{3}\right)$, $\left(\frac{8}{3}, \pm\frac{8}{9}\right)$ $y = \frac{4}{3}x$, $p = x$, $q = \frac{2}{3}p$

Lalín y Ma analizaron más casos; como, por ejemplo, el caso dado por la relación $t = 2a$, que conduce a $\sin(\omega) = \sin(2\theta)$, y también consideraron otro tipo de situaciones. En cualquier caso, está claro que este trabajo permite ofrecer una gran variedad de resultados aritméticos geométricos muy particulares.

Pero el trabajo de Lalín y Ma no se reduce únicamente a mostrar algunos de estos casos particulares. Un resultado muy interesante que lograron probar es el siguiente: sabemos, por la Sección 4.4, que $(0:0:1)$ es un punto de orden 2 en la $\mathbb{C}(t)$-curva elíptica E_a. En consecuencia, dado $t_0 \in \mathbb{Q}$ tal que $E(t_0)$ es no singular, resulta que $E_a(t_0)$ será una $\mathbb{Q}$-curva elíptica con un punto de torsión de orden 2. En vistas al Teorema 1.2.4, eso significa que su grupo de torsión solamente puede ser de la forma $\mathbb{Z}/2n\mathbb{Z}$ con $n \in \{1,2,3,4,5,6\}$, o bien de la forma $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ con $n \in \{1,2,3,4\}$. Dada esta situación, es natural preguntarse

cuáles de estos grupos de torsión se realizan para alguna elección particular de $a, t \in \mathbb{Q}$. La respuesta es que todos los posibles grupos de torsión son realizados.

(a,t)	$E_{a,t}(\mathbb{Q})_{\text{tor}}$	torsion generators	$\text{rk}(E_{a,t}(\mathbb{Q}))$
$\left(0, \frac{1}{3}\right)$	$\mathbb{Z}/2\mathbb{Z}$	$\langle (0,0) \rangle$	> 0
$\left(\frac{47}{72}, 1\right)$	$\mathbb{Z}/4\mathbb{Z}$	$\langle \left(\frac{10}{3}, \frac{35}{108}\right) \rangle$	> 0
$\left(\frac{1}{4}, \frac{2}{9}\right)$	$\mathbb{Z}/10\mathbb{Z}$	$\langle P_{\frac{1}{4},\frac{2}{9}} + (0,0) \rangle$	0
$\left(\frac{7}{8}, \frac{4}{3}\right)$	$\mathbb{Z}/12\mathbb{Z}$	$\langle P_{\frac{7}{8},\frac{4}{3}} \rangle$	0
$\left(\frac{11}{21}, \frac{7}{8}\right)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\langle (3,0), (0,0) \rangle$	> 0
$\left(\frac{17}{18}, 3\right)$	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\langle P_{\frac{17}{18},3}, \left(-\frac{9}{4}, 0\right) \rangle$	0

Veamos ahora el más fuerte de los resultados alcanzados por Lalín y Ma en [13]. Concretamente, se nos plantea el mismo problema con una restricción adicional. En todo nuestro trabajo, nunca se impusieron condiciones de tipo aritmético sobre ω. Es posible preguntarse si esta infinidad de soluciones al problema principal es alcanzada si, además, buscamos soluciones con $\cos(\omega) \in \mathbb{Q}$. El tratamiento de este problema sigue las mismas líneas, pero converge a un lugar distinto.

Usando geometría euclídea elemental, se ve que la condición $\cos(\omega) \in \mathbb{Q}$ equivale a $\sin(w) = \tau \sin\left(\frac{\omega}{2} + \tau\right)$ para algún $\tau \in \mathbb{Q}$. Por medio de un adecuado cambio de variables siguiendo los mismos procedimientos que en nuestro problema principal, Lalín y Ma demostraron lo siguiente: Sean $a, \tau \in \mathbb{Q}$ tales que $|a| < 1$, $0 < \tau$, $a\tau < 1$ y $2a\tau < \tau^2 + 1$. Entonces, si la $\mathbb{Q}$-curva elíptica

$$F_{a,\tau} : Y^2 = X^3 + \tau(1 - a\tau)\left[2(a-3)\left(\tau^2 - 2a\tau + 1\right) + (1+a)^2 \tau(1 - a\tau)\right] X^2 +$$

$$+ 8(1-a)\tau^2(1-a\tau)^2\left(\tau^2 - 2a\tau + 1\right)^2 X$$

admite infinitas soluciones en $F_{a,\tau}(\mathbb{Q})$ cumpliendo las condiciones

$$2(1-a)\tau(1-a\tau)\left(\tau^2 - 2a\tau + 1\right) < X < 4\tau(1-a\tau)\left(\tau^2 - 2a\tau + 1\right),$$

$$|Y| < (1+a)\tau(1-a\tau)X,$$

entonces existen infinitos pares de un triángulo θ-entero y un ω-paralelogramo entero tales que $\cos(\theta) = a$ y $\sin(w) = \tau \sin\left(\frac{\omega}{2} + \tau\right)$ y tales que ambas figuras tienen la misma área y el mismo perímetro, sin distinción por semejanza.

Hecho esto, sería natural preguntarse si es posible repetir el procedimiento usado para $E_{a,t}$. La respuesta es que no, puesto que la superficie elíptica que inducimos no resulta racional, y por lo tanto no tenemos a nuestra disposición las ventajas de una tal superficie elíptica. Existe una forma de dar una clasificación de las superficies elípticas, una de cuyas

clases es la clase de superficies elípticas racionales, y otra a la que pertenece $F_{a,\tau}$, conocidas como superficies elípticas K3, que aquí no hemos tratado. Lalín y Ma, tomando el camino de trabajar directamente en $F_a(\mathbb{Q}(\tau))$ sin pasar antes por $F_a(\mathbb{C}(\tau))$, y aplicando exactamente el mismo método usado en B, consiguieron probar que el punto (afinizado)

$$Q_{a,\tau} := \left(4\tau(1-a\tau)\left(\tau^2-2a\tau+1\right), 4(1+a)\tau^2(1-a\tau)^2\left(\tau^2-2a\tau+1\right)\right)$$

es un punto sin torsión en la $\mathbb{Q}(\tau)$-curva elíptica F_a, y que para todos salvo finitos $\tau \in \mathbb{Q}$, el punto evaluado en τ es un punto sin torsión de la $\mathbb{Q}$-curva elíptica $F_a(\tau)$. Con esto ya es suficiente para dar una respuesta afirmativa a nuestro problema principal con el requisito adicional de que $\cos(\omega) \in \mathbb{Q}$.

Si uno intenta trabajar sobre el rango de $F_a(\mathbb{C}(\tau))$, puede realizar el Algoritmo de Tate, y una primera dificultad se encuentra en la necesidad de discriminar entre los casos $a \neq 0$ y $a = 0$. En el primer caso, el análisis de singularidades revela la existencia de dos fibras de tipo I_0^* (5 componentes irreducibles) y dos fibras de tipo I_4 (4 componentes irreducibles), mientras que el resto de las fibras son o bien no singulares, o bien singulares pero irreducibles. La teoría general de superficies elípticas K3 permite dar una cota universal para su número de Picard, la cual está dada por 20 (léase [24, 13.1]). Usando esto y la fórmula de Shioda-Tate, el rango de $F_a(\mathbb{C}(\tau))$ puede acotarse superiormente por 4. Repitiendo para $a = 0$, se obtiene la misma cota. Además, probaron que si el rango es 1, entonces $Q_{a,\tau}$ es un generador de la parte libre de $F_a(\mathbb{C}(\tau))$.

También consideraron la $\mathbb{Q}(a,\tau)$-curva elíptica F, cuyo rango pudieron demostrar que es igual a 1 y que su parte libre está generada por $Q_{a,\tau}$.

Finalmente, consideraron la $\mathbb{Q}(\tau)$-curva elíptica $F_{\frac{1}{2}}(\mathbb{Q}(\tau))$ y probaron que es de rango 1 y su parte libre está generada por $Q_{\frac{1}{2},\tau}$. Este último resultado expuesto dejó dos problemas abiertos. Cuando Lalín y Ma intentaron probar el mismo resultado para $F_0(\mathbb{Q}(\tau))$ y $F_{-\frac{1}{2}}(\mathbb{Q}(\tau))$, solamente lograron acotar superiormente el rango por 2. Queda, entonces, la pregunta abierta: ¿cuáles son los rangos de $F_0(\mathbb{Q}(\tau))$ y $F_{-\frac{1}{2}}(\mathbb{Q}(\tau))$?

Apéndice A

Geometría Algebraica

El objetivo de este apéndice es tener disponible una serie de resultados provenientes de la Geometría Algebraica para su pertinente referencia. Si bien en esta tesis suponemos al lector familiarizado con las nociones básicas de Geometría Algebraica, con este apéndice pretendemos ofrecer una vía rápida de consulta y referencia a diversos resultados que serán centrales en contextos específicos del trabajo de tesis. En consecuencia, rara vez nos detendremos en sus demostraciones, con la particular excepción de la primera sección.

A.1 Operación en cúbicas

Nos dispondremos a probar que la operación $C\left(\overline{\mathbb{K}}\right) \times C\left(\overline{\mathbb{K}}\right) \to C\left(\overline{\mathbb{K}}\right)$ que hemos definido en 1.1 como $(P, Q) \mapsto PQ$ puede restringirse y correstringirse a $C(\mathbb{K}) \times C(\mathbb{K}) \to C(\mathbb{K})$. Para eso, requeriremos algunos resultados previos.

En general, dado un cuerpo k y una cúbica proyectiva plana no singular C sobre k, podemos tomar una clausura algebraica $\overline{k}$ de k y usar la operación definida en 1.1 para la cúbica C pensada con sus coeficientes en $\overline{k}$, de tal forma que tenemos la operación $C\left(\overline{k}\right) \times C\left(\overline{k}\right) \to C\left(\overline{k}\right)$ que aplica $(P, Q) \mapsto PQ$. El objetivo de esta sección es probar que si $P, Q \in C(k)$, entonces $PQ \in C(k)$. A lo largo de esta sección, dada una cúbica proyectiva plana no singular sobre cualquier cuerpo k, por *la operación en* C nos referiremos a la operación definida en $C\left(\overline{k}\right) \times C\left(\overline{k}\right) \to C\left(\overline{k}\right)$, como antes.

Recordemos que, dado un cuerpo k y dos curvas planas afines F y G en $k[x, y]$, entonces, para cada $P \in k^2$, la *multiplicidad de intersección de* F *y* G *en* P se define como la dimensión del $\overline{k}$-espacio vectorial

$$\frac{\mathcal{O}_P\left(\overline{k}^2\right)}{(F, G)},$$

donde $\mathcal{O}_P\left(\overline{k}^2\right) \subseteq \overline{k}(x, y)$ es el anillo local de P en $\overline{k}^2$ de las funciones racionales sobre $\overline{k}^2$ definidas en P, $\overline{k}$ es una clausura algebraica de k y (F, G) es el ideal de $\mathcal{O}_P\left(\overline{k}^2\right)$ generado por F y G. En el caso de curvas proyectivas planas, la multiplicidad de intersección entre dos curvas sobre un punto se define como la multiplicidad de intersección de las curvas afinizadas sobre el punto afinizado, por medio de una afinización adecuada. Para más detalles, léase [8, pp. 53-54].

Sea K una extensión galoisiana de k, y sea $n \in \mathbb{N}$. Sea $\sigma \in \mathrm{Gal}(K/k)$. Dado un polinomio $H \in K[x_1, \cdots, x_n]$, tenemos definido como $\sigma(H)$ al polinomio que se obtiene de

H reemplazando sus coeficientes por su transformación vía σ. Esto define un isomorfismo de anillos $\sigma : K[x_1, \cdots, x_n] \to K[x_1, \cdots, x_n]$ que se extiende naturalmente a un isomorfismo de cuerpos $\sigma : K(x_1, \cdots, x_n) \to K(x_1, \cdots, x_n)$ por medio de la propiedad universal del cuerpo de fracciones.

Dado un polinomio $H \in K[x_1, \cdots, x_n]$, se tiene $\sigma(H(P)) = \sigma(H)(\sigma(P))$ para todo $P \in K^n$, donde $\sigma(P)$ consiste en reemplazar las coordenadas de P por su transformación vía σ. Más aún, como $\sigma : K \to K$ es biyectiva, tenemos una función bien definida $\mathbb{P}^n(K) \to \mathbb{P}^n(K)$ definida análogamente.

Para probar lo que deseamos, requeriremos un lema previo.

Lema A.1.1 *Sea k un cuerpo y sea K una extensión de cuerpos finita y galoisiana de nuestro cuerpo k. Sea $\sigma \in \mathrm{Gal}(K/k)$ y sean $F, G \in k[x, y]$. Entonces, para todo $P \in K^2$, se tiene $I(P, F \cap G) = I(\sigma(P), \sigma(F) \cap \sigma(G))$.*

Demostración. Sea $\overline{k}$ una extensión de K a una clausura algebraica de k. Tomamos una extensión de σ a $\overline{k} \to \overline{k}$, que notamos $\widehat{\sigma}$.

Fijamos $P \in K^2$. El isomorfismo de anillos $\widehat{\sigma} : \overline{k}(x, y) \to \overline{k}(x, y)$ induce naturalmente un morfismo de anillos

$$S : \mathcal{O}_P\left(\overline{k}^2\right) \to \frac{\mathcal{O}_{\sigma(P)}\left(\overline{k}^2\right)}{(\sigma(F), \sigma(G))}$$

por medio de la restricción y correstricción, seguida de la composición con la proyección al cociente. Es claro que la restricción y correstricción es válida, pues, si $b \in \overline{k}[x, y]$ y $b(P) \neq 0$, entonces

$$0 \neq \widehat{\sigma}(b(P)) = \widehat{\sigma}(b)(\sigma(P)).$$

Esto implica, además, usando que $\widehat{\sigma} : \overline{k} \to \overline{k}$ es biyectiva, que esta restricción y correstricción define una biyección. En particular, S es sobreyectiva.

Veamos que $\ker(S) = (F, G)$. Observemos que F y G están en $\ker(S)$, pues, como los coeficientes de F están en K, $\widehat{\sigma}(F) = \sigma(F)$. Análogamente, $\widehat{\sigma}(G) = \sigma(G)$. Como ambos elementos se anulan al proyectar al cociente $\dfrac{\mathcal{O}_{\sigma(P)}\left(\overline{k}^2\right)}{(\sigma(F), \sigma(G))}$, se sigue que $(F, G) \subseteq \ker(S)$. Recíprocamente, sea $H \in \mathcal{O}_P\left(\overline{k}^2\right)$ tal que $S(H) = 0$. Entonces existen $a, b \in \mathcal{O}_{\sigma(P)}\left(\overline{k}^2\right)$ tales que $\widehat{\sigma}(H) = a\sigma(F) + b\sigma(G)$. Como $\widehat{\sigma} : \mathcal{O}_P\left(\overline{k}^2\right) \to \mathcal{O}_{\sigma(P)}\left(\overline{k}^2\right)$ es biyectiva, existen $a', b' \in \mathcal{O}_P\left(\overline{k}^2\right)$ tales que $a = \widehat{\sigma}(a')$ y $b = \widehat{\sigma}(b')$. Así, la igualdad $\widehat{\sigma}(H) = a\sigma(F) + b\sigma(G)$ se reescribe como $\widehat{\sigma}(H) = \widehat{\sigma}(a'F + b'G)$, de donde $H = a'F + b'G$ y por lo tanto $H \in (F, G)$, lo cual prueba la otra inclusión que buscábamos. Así, S induce un isomorfismo de anillos

$$\frac{\mathcal{O}_P\left(\overline{k}^2\right)}{(F, G)} \cong \frac{\mathcal{O}_{\sigma(P)}\left(\overline{k}^2\right)}{(\sigma(F), \sigma(G))}$$

que es, además, una transformación $\widehat{\sigma}$-lineal, con lo cual ambos $\overline{k}$-espacios vectoriales tienen la misma dimensión. Esto prueba lo que queríamos. ■

Sea k un cuerpo, sea K una extensión finita y galoisiana de k y sea $n \in \mathbb{N}$. Fijando $\sigma \in \mathrm{Gal}(K/k)$, el isomorfismo de anillos inducido $\sigma : K[x_1, \cdots, x_n] \to K[x_1, \cdots, x_n]$

satisface, para cada $i \in [1,n] \cap \mathbb{N}$, que, cualquiera sea $F \in K[x_1, \cdots, x_n]$,

$$\sigma\left(\frac{\partial F}{\partial x_i}\right) = \frac{\partial \sigma(F)}{\partial x_i}.$$

En efecto, por la aditividad de la derivación basta verlo para monomios $\lambda \prod_{j=1}^{n} x_j^{i_j}$, donde $\lambda \in K$ y $i_j \in \mathbb{N}_0$ para todo $j \in [1,n] \cap \mathbb{N}$, y en este caso la identidad es trivialmente válida.

Es claro entonces que σ preserva la propiedad de no singularidad. En efecto, dado $F \in k[x_1, \cdots, x_n]$, se tiene que un punto P (afín o proyectivo) es un punto singular de F si y solo si P se anula en F y en $\frac{\partial F}{\partial x_i}$ para todo $i \in [1,n] \cap \mathbb{N}$, lo cual ocurre si y solo si $\sigma(P)$ se anula en $\sigma(F)$ y en $\sigma\left(\frac{\partial F}{\partial x_i}\right)$ para todo $i \in [1,n] \cap \mathbb{N}$, lo cual equivale a que $\sigma(P)$ se anule en $\sigma(F)$ y en $\frac{\partial \sigma(F)}{\partial x_i}$ para todo $i \in [1,n] \cap \mathbb{N}$, lo cual ocurre si y solo si $\sigma(P)$ es un punto singular de $\sigma(F)$.

Sean F y G dos curvas planas proyectivas sin componentes comunes. El Lema A.1.1 implica que, si los puntos de $F \cap G$ (que, en principio, están en $\mathbb{P}^2\left(\overline{k}\right)$, fijada una clausura algebraica $\overline{k}$ de k que contiene a K) están en $\mathbb{P}^2(K)$, entonces

$$\sigma(F) \bullet \sigma(G) = \sum_{P \in \mathbb{P}^2(K)} I(P, F \cap G)\, \sigma(P), \tag{A.1}$$

con lo cual, en particular, tenemos el siguiente lema:

Lema A.1.2 *Sea k un cuerpo y sea K una extensión finita y galoisiana de k. Sea C una cúbica plana proyectiva no singular sobre K y sean $P, Q, R \in C(K)$ tales que $PQ = R$ en la operación de C. Entonces, para todo $\sigma \in \mathrm{Gal}(K/k)$, se tiene $\sigma(P)\,\sigma(Q) = \sigma(R)$ en la operación de $\sigma(C)$.*

Demostración. Aplicando A.1 usando que $C \bullet L = P+Q+R$, donde L es la recta por P y Q si $P \neq Q$, y la recta tangente a C en P si $P = Q$, tenemos $\sigma(C) \bullet \sigma(L) = \sigma(P)+\sigma(Q)+\sigma(R)$, de donde $\sigma(P)\,\sigma(Q) = \sigma(R)$ en la operación de $\sigma(C)$. ■

Ahora estamos en condiciones de probar el resultado principal de esta sección.

Proposición A.1.3 *Sea k un cuerpo perfecto y sea C una cúbica proyectiva plana con coeficientes en k. Sean $P, Q \in C(k)$. Entonces, según la operación en C, $PQ \in C(k)$.*

Demostración. Sabemos que $R := PQ$ tiene una representación con coordenadas proyectivas en una clausura algebraica $\overline{k}$ de k. Fijamos esa representación y tomamos la extensión de k generada por dichas coordenadas. Esta es una extensión finita que puede extenderse una extensión K de tal forma que K/k es normal y finita. Al ser finita, es algebraica, y al ser k perfecto, K/k es galoisiana. Como $R = PQ \in C(K)$, el Lema A.1.2 nos dice que $\sigma(P)\,\sigma(Q) = \sigma(R)$ en la operación de $\sigma(C)$. Pero como C tiene coeficientes en k, se sigue que $\sigma(C) = C$, y como P y Q tienen coordenadas en k, entonces $PQ = \sigma(R)$ en la operación de C, de donde $R = \sigma(R)$. Entonces R es fijado por $\mathrm{Gal}(K/k)$, de donde la Teoría de Galois nos dice que $R \in C(k)$. ■

A.2 El grupo de Néron-Severi

En esta sección consideraremos superficies proyectivas sobre $\mathbb{C}$. Si bien lo que aquí expondremos puede generalizarse a cuerpos en general, las particularidades del caso complejo permiten ofrecer una exposición más sencilla que involucra menos carga conceptual, y dado que en esta tesis analizamos una $\mathbb{C}$-superficie elíptica, no necesitamos más.

Fijamos una superficie proyectiva no singular compleja S y notamos $\mathrm{Pic}(S)$ a su *grupo de Picard*, es decir, el grupo de divisores módulo equivalencia lineal.

Si $\mathcal{O}_S$ es el haz estructural de S y $\mathcal{O}_S^*$ es el haz de elementos multiplicativamente inversibles de $\mathcal{O}_S$, entonces sabemos que $\mathrm{Pic}(S)$ es isomorfo al primer grupo de cohomología $H^1(S, \mathcal{O}_S^*)$ (léase [10, p. 143]). Sea $\varphi : \mathrm{Pic}(S) \to H^1(S, \mathcal{O}_S^*)$ el correspondiente isomorfismo.

Por otra parte, la función exponencial $x \mapsto e^{2\pi i x}$ induce una secuencia exacta corta de grupos abelianos

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{C} \xrightarrow{f} \mathbb{C}^\times \longrightarrow 0$$

que induce, a su vez, una secuencia exacta corta de haces de S

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_S \xrightarrow{f} \mathcal{O}_S^* \longrightarrow 0$$

que, a su vez, induce una secuencia exacta larga en los grupos de cohomología a la cual se le puede agregar el morfismo φ para generar el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^1(S,\mathbb{Z}) & \longrightarrow & H^1(S,\mathcal{O}_S) & \longrightarrow & H^1(S,\mathcal{O}_S^*) & \xrightarrow{\delta} & H^2(S,\mathbb{Z}) & \longrightarrow & \cdots \\ & & & & & & \uparrow{\scriptstyle \varphi} & \nearrow{\scriptstyle c_1} & & & \\ & & & & & & \mathrm{Pic}(S) & & & & \end{array}$$

donde $\delta : H^1(S, \mathcal{O}_S^*) \to H^2(S, \mathbb{Z})$ es el morfismo de conexión dado por el *Lema de la Serpiente*, y $c_1 := \delta \circ \varphi$ recibe el nombre de *primer morfismo de Chern de S*. Este morfismo es el que define el objeto de estudio de esta sección.

Definición A.2.1 *Sea S una $\mathbb{C}$-superficie proyectiva no singular. Definimos el* grupo de Néron-Severi *de S como la imagen del primer morfismo de Chern de S, y lo notamos* $\mathrm{NS}(S)$.

Que el grupo de Néron-Severi de una $\mathbb{C}$-superficie proyectiva no singular S es finitamente generado se sigue del hecho de que es un subrupo de $H^2(S, \mathbb{Z})$. Su rango, que notamos $\rho(S)$, se conoce como *el número de Picard de S*. Por otra parte, si c_1 es el primer morfismo de Chern, su núcleo resulta isomorfo al cociente $\mathrm{Pic}^0(S) := H^1(S, \mathcal{O}_S)/H^1(S, \mathbb{Z})$. Su dimensión, que llamamos *la irregularidad de S*, la notamos $q(S)$.

El grupo de Néron-Severi es naturalmente isomorfo a un cociente del grupo de Picard de S. Es posible demostrar que el *pairing de intersección de S* $\langle \cdot, \cdot \rangle : \mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}$ (léase [10, V 1]) es compatible con la relación de equivalencia inducida por dicho cociente (esta relación recibe el nombre de *equivalencia algebraica*). Podemos eliminar la torsión del grupo de Néron-Severi de S mediante la tensorización $\mathrm{N}_{\mathbb{R}}(S) := \mathrm{NS}(S) \otimes \mathbb{R}$, que no solamente es un $\mathbb{R}$-espacio vectorial de dimensión $\rho(S)$ sino que, junto con su forma bilineal simétrica inducida por el pairing de intersección de S mediante la extensión lineal a $\mathrm{N}_{\mathbb{R}}(S)$, se rige bajo el resultado estructural conocido como **Teorema del índice de Hodge**, que enunciamos a continuación.

Teorema A.2.2 *Sea S una superficie proyectiva compleja. Entonces la forma bilineal simétrica $\mathrm{N}_{\mathbb{R}}(S) \times \mathrm{N}_{\mathbb{R}}(S) \to \mathbb{R}$ inducida por el pairing de intersección de S es no degenerada y de signatura $(1, \rho(S) - 1)$.*

Así, definiendo $\mathrm{Num}(S) := \mathrm{NS}(S) / \mathrm{NS}(S)_{\mathrm{tors}}$, este grupo libre finitamente generado adquiere estructura de retículo por medio de la forma bilineal simétrica no degenerada que hereda de $\mathrm{N}_{\mathbb{R}}(S)$. Esta observación será crucial en el contenido de la tesis. Por lo pronto, señálese que este cociente induce una nueva relación de equivalencia en los divisores de S (trivialmente implicada por la relación de equivalencia algebraica, por definición) que denominamos *equivalencia numérica*.

Entonces tenemos tres relaciones de equivalencia en los divisores de una $\mathbb{C}$-superficie proyectiva no singular S: equivalencia numérica, equivalencia algebraica y equivalencia lineal, cada una implicada por la siguiente. Recordemos que la notación para dos divisores D y D' de S que son linealmente equivalentes es $D \sim D'$, y que dicha relación se da exactamente cuando la diferencia entre ambos es un divisor principal.

La equivalencia numérica es, explícitamente, la relación entre dos divisores D y D' (notada $D \equiv D'$) que se da exactamente cuando $\langle D, C \rangle = \langle D', C \rangle$ para todas las curvas $C \subseteq S$. En cuanto a la equivalencia algebraica, requeriremos un poco más de espacio para definirla.

Decimos que un divisor D de S es *efectivo* (y lo notamos $D \geq 0$) si todas las coordenadas en su expansión en el grupo libre de divisores de S son no negativas.

Decimos que un divisor D de S es *algebraicamente equivalente a* 0 si existe un esquema conexo W y un divisor efectivo $\overline{D}$ en $S \times W$ tal que $\overline{D}$ es playo sobre W y $D = \overline{D}_{w_1} - \overline{D}_{w_2}$ para algún par $(w_1, w_2) \in W^2$, donde $\overline{D}_w$ es la fibra de $\overline{D}$ en w para todo $w \in W$. En tal caso, notamos $D \approx 0$. Decimos que dos divisores D_1 y D_2 de S son *algebraicamente equivalentes* si $D_1 - D_2 \approx 0$. Es posible demostrar que esta es una relación de equivalencia y que, de hecho, es la inducida por el núcleo del primer morfismo de Chern en $\mathrm{Pic}(S)$. De hecho, para cuerpos distintos de $\mathbb{C}$, esta es exactamente la definición del grupo de Néron-Severi: el grupo de Picard módulo equivalencia algebraica, lo cual está bien definido pues todo lo que es linealmente equivalente a cero, es algebraicamente equivalente a cero. Más aún, esto induce un isomorfismo natural con el grupo de divisores módulo equivalencia algebraica, que es también otra de las definiciones clásicas del grupo de Néron-Severi. Aunque, con estas definiciones, no es tan fácil probar que es un grupo finitamente generado.

A.3 Invariantes de superficies

Tenemos definido el grupo de divisores de una superficie S sobre un cuerpo k algebraicamente cerrado como el grupo libre generado por las curvas irreducibles en S; o, más formalmente, como el grupo libre generado por las subvariedades irreducibles de S de codimensión 1. En general, tenemos definido el concepto de *divisor de Weil* para todo esquema noetheriano, integral y separable que es *regular en codimensión* 1, es decir, tal que todos sus anillos locales de dimensión 1 son regulares. El grupo de divisores de Weil de un tal esquema se define como el grupo libre generado por sus *divisores primos*, entendidos como los subesquemas cerrados de codimensión 1.

Dada una superficie S proyectiva y no singular sobre un cuerpo algebraicamente cerrado k, sabemos que existe una biyección canónica entre $\mathrm{Pic}(S)$ y el grupo de haces inversibles (es decir, haces localmente libres de rango 1) en S a menos de isomorfismo, donde el haz estructural $\mathcal{O}_S$ es la identidad, la tensorización es la operación de grupos, y la inversión está dada por la dualización, es decir: dado un haz inversible $\mathcal{L}$ en S, podemos tomar el haz dual $\mathcal{L}^* := \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{L}, \mathcal{O}_S)$, cuya tensorización con $\mathcal{L}$ es naturalmente isomorfa a $\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{L}, \mathcal{L}) = \mathcal{O}_S$. La buena definición de esta estructura de grupo está dado por el siguiente argumento estándar: dados dos haces inversibles $\mathcal{L}$ y $\mathcal{M}$ en S, está claro que $\mathcal{L} \otimes \mathcal{M}$ es un haz inversible, pues ambos haces son localmente libres y de rango 1 y $\mathcal{O}_S \otimes \mathcal{O}_S \cong \mathcal{O}_S$. La existencia de la biyección aludida al principio del párrafo es una aplicación directa de la identificación entre *divisores de Weil* y *divisores de Cartier* (léase [10, pp. 141-142]) que se da bajo condiciones que son satisfechas por nuestra superficie S. Para cada divisor D de S, notamos $\mathcal{O}_S(D)$ al haz inversible correspondiente a la clase de equivalencia lineal de D.

Esta identificación nos permite redefinir el pairing de intersección de S a través de la *característica de Euler*. Recordemos que, dado un esquema X proyectivo sobre k de dimensión n, definimos la característica de Euler de $\mathscr{F}$, para todo haz coherente $\mathscr{F}$ en X, como

$$\chi(\mathscr{F}) := \sum_{i=0}^{n} (-1)^i \dim_k H^i(X, \mathscr{F}).$$

Así, podemos definir $\langle \cdot, \cdot \rangle : \mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}$ de la siguiente manera: dados dos haces inversibles $\mathcal{L}$ y $\mathcal{L}'$ en S, podemos tomar

$$\left\langle \mathcal{L}, \mathcal{L}' \right\rangle := \chi(\mathcal{O}_S) - \chi\left(\mathcal{L}^{-1}\right) - \chi\left(\mathcal{L}'^{-1}\right) + \chi\left(\mathcal{L}^{-1} \otimes \mathcal{L}'^{-1}\right).$$

Esta función resulta ser una forma bilineal simétrica tal que, si C y C' son curvas irreducibles distintas en S de grados c y c' respectivamente, entonces $\langle \mathcal{O}_S(C), \mathcal{O}_S(C') \rangle$ es igual al número de intersección entre ambas curvas vistas como curvas en S (léase [2, Theorem I.4]), que iguala a cc' cuando $S = \mathbb{P}^2(k)$ por el **Teorema de Bézout**. En efecto, recordemos que, dado $x \in C \cap C'$, la multiplicidad de intersección de C y C' en x se define como la dimensión del k-espacio vectorial $\dfrac{\mathcal{O}_{S,x}}{(C, C')}$, que coincide con la definición clásica que ofrecimos en A.1 en el caso en que $S = \mathbb{P}^2(k)$, y el número de intersección entre C y C' es la suma de estas multiplicidades para los puntos de $C \cap C'$ (ver [10, p. 360]).

Uno de los corolarios inmediatos clásicos, y del que hacemos un muy particular uso en la tesis, es el que permite cuantificar el número de *self-intersection* de las fibras de una fibración. Concretamente, se tiene lo siguiente.

Lema A.3.1 *Sea k un cuerpo algebraicamente cerrado, sea S una k-superficie proyectiva no singular y sea C una k-curva proyectiva no singular. Sea $f : S \to C$ una fibración; es decir, un morfismo sobreyectivo con fibras conexas. Entonces toda f-fibra F satisface $\langle F, F\rangle = \langle F, \Theta\rangle = 0 \geq \langle \Theta, \Theta\rangle$, con igualdad si y solo si $\Theta = F$, donde Θ es cualquier componente irreducible de F.*

La última parte del Lema A.3.1 es una parte de un resultado más general conocido como **Lema de Zariski**. Esa parte en concreto puede encontrarse demostrada en un contexto más general en [14, p. 61]. Para el Lema de Zariski completo, ver [1, p. 111]. La primera parte es un corolario inmediato del Lema A.3.9: Si $D \in \{F, \Theta\}$, entonces tomamos una fibra $F' \neq F$, y por lo tanto F y F' son disjuntas, por ser fibras distintas. En consecuencia $0 = \langle F', D\rangle = \langle F, D\rangle$, donde en la segunda igualdad hemos usado el Lema A.3.9 y que el pairing de intersección no distingue por equivalencia algebraica.

Naturalmente, esta forma bilineal se levanta a una forma bilineal simétrica en el grupo de divisores (que no distingue equivalencia lineal), y como, en general, para superficies proyectivas no singulares sobre cuerpos algebraicamente cerrados existe únicamente una forma bilineal simétrica en el grupo de divisores que cumple todas estas propiedades (ver [10, pp. 358-359]), entonces hemos encontrado una nueva forma de definir el pairing de intersección en S. Esta definición, junto con la Dualidad de Serre (ver [10, p. 244]), permite probar resultados como la siguiente fórmula de Riemann-Roch:

Teorema A.3.2 *Sea S una superficie proyectiva no singular sobre un cuerpo algebraicamente cerrado. Sea $\mathcal{L}$ un haz inversible en S. Entonces*

$$\chi(\mathcal{L}) = \chi(\mathcal{O}_S) + \frac{\langle \mathcal{L}, \mathcal{L} - \omega_S\rangle}{2}.$$

En el enunciado del Teorema A.3.2, hemos notado ω_S al haz canónico de S. Recordemos que dicho haz se define, en general, para una variedad no singular X de dimensión n sobre un cuerpo algebraicamente cerrado k, como el producto wedge

$$\omega_X := \bigwedge^n \Omega_{X/k},$$

donde $\Omega_{X/k}$ es el haz de diferenciales relativos de X sobre k, el cual resulta ser un haz inversible. El *género geométrico de X*, que notamos $p_g(X)$, se define como la dimensión del k-espacio vectorial dado por las secciones globales del haz ω_X, que notamos $\Gamma(X, \omega_X)$.

Así, si S es una superficie proyectiva no singular sobre un cuerpo algebraicamente cerrado, ω_S tiene naturalmente asociada una clase de equivalencia lineal de divisores que notamos K_S, y llamamos *la clase canónica de divisores de S*. Esta clase cumple con una fórmula de adjunción que expondremos a continuación, y que puede derivarse del Teorema A.3.2. Dada una curva $C \subseteq S$, tenemos definido el *género aritmético* de C como $p_a(C) := 1 - \chi(\mathcal{O}_C)$, que coincide con el género cuando la curva es no singular.

Teorema A.3.3 *Sea S una superficie proyectiva no singular sobre un cuerpo algebraicamente cerrado. Dada una curva $C \subseteq S$, se tiene*

$$2p_a(C) - 2 = \langle C, C\rangle + \langle C, K_S\rangle.$$

El género aritmético, además, ofrece un criterio de racionalidad que nos será particularmente útil.

Lema A.3.4 *Sea S una superficie proyectiva no singular sobre $\mathbb{C}$ y sea C una curva en S tal que $p_a(C) = 0$. Entonces C es no singular e isomorfa a $\mathbb{P}^1(\mathbb{C})$.*

Sea S una superficie proyectiva no singular sobre $\mathbb{C}$. Para cada $i \in \mathbb{N}_0$ definimos *el i-ésimo número de Betti de S* como $b_i(S) := \dim_{\mathbb{R}} H^i(S, \mathbb{R})$. Definimos la *característica de Euler-Poincaré topológica de S* como

$$e(S) := \sum_{i=0}^{4} (-1)^i b_i(S).$$

De hecho, es posible definir análogamente la característica de Euler-Poincaré topológica de una $\mathbb{C}$-variedad proyectiva no singular X como la suma alternada de sus números de Betti, tal y como hicimos para superficies. Más aún, si n es la dimensión de X, es sabido que $\dim_{\mathbb{R}} H^{2n}(X, \mathbb{R}) = 1$ y que, de hecho, para cada $i \in [0, 2n] \cap \mathbb{N}_0$ existe un pairing no degenerado $H^i(X, \mathbb{R}) \times H^{2n-i}(X, \mathbb{R}) \to H^{2n}(X, \mathbb{R})$ (conocido como *producto cup*). Este resultado, conocido como *Dualidad de Poincaré*, tiene el importante corolario de que, para todo $i \in [0, 2n] \cap \mathbb{N}_0$, se tiene $b_i(X) = b_{2n-i}(X)$, con valor 1 si $i = 0$.

Una relación entre la irregularidad y los números de Betti está dada en razón del siguiente lema.

Lema A.3.5 *Sea S una $\mathbb{C}$-superficie proyectiva no singular. Entonces $b_1(S) = 2q(S)$.*

Definimos, a su vez, la *característica de Euler de S* como la característica de Euler de su haz estructural; es decir, como $\chi(S) := \chi(\mathcal{O}_S)$. La Dualidad de Serre permite probar que

$$\chi(S) = 1 - q(S) + p_g(S). \tag{A.2}$$

Señálese, asimismo, la conocida *Fórmula de Noether* (ver [2, p. 8]), en virtud de la cual tenemos la igualdad

$$12\chi(S) = e(S) + \langle K_S, K_S \rangle. \tag{A.3}$$

Para cada $n \in \mathbb{N}_0$, definimos el *n-ésimo plurigénero de S* como

$$P_n(S) := \dim_{\mathbb{C}} H^n(S, nK_S).$$

Recordemos que tanto los plurigéneros como la irregularidad son cero si $S = \mathbb{P}^2(\mathbb{C})$.

Finalmente, definimos *el número de Lefschetz* de S como $\lambda(S) := b_2(S) - \rho(S)$. La importancia de estas constantes que hemos definido es que muchas de ellas son birracionalmente invariantes.

Lema A.3.6 *Sean S y S' dos $\mathbb{C}$-superficies proyectivas no singulares birracionalmente equivalentes. Entonces $q(S) = q(S')$, $\chi(S) = \chi(S')$, $p_g(S) = p_g(S')$, $\lambda(S) = \lambda(S')$ y $P_n(S) = P_n(S')$ para todo $n \in \mathbb{N}_0$.*

En el caso del espacio proyectivo, estas constantes están muy bien entendidas. A modo de ejemplo, se sabe que $q\left(\mathbb{P}^2(\mathbb{C})\right) = p_g\left(\mathbb{P}^2(\mathbb{C})\right) = 0$ y que $\rho\left(\mathbb{P}^2(\mathbb{C})\right) = 1$. Por otro lado, en función de ellas es posible establecer el siguiente criterio de racionalidad, conocido como **Criterio de Castelnuovo**.

Proposición A.3.7 *Sea S una $\mathbb{C}$-superficie proyectiva no singular. Entonces S es birracionalmente equivalente a $\mathbb{P}^2(\mathbb{C})$ si y solo si $q(S) = P_2(S) = 0$.*

Dado que en esta tesis estaremos trabajando con superficies que admiten un morfismo sobreyectivo a una curva, requeriremos también del siguiente resultado, que es un caso particular de [2, Lemma VI.4].

Proposición A.3.8 *Sea S una $\mathbb{C}$-superficie proyectiva no singular tal que existe un morfismo sobreyectivo $f : S \to C$, donde C es una $\mathbb{C}$-curva proyectiva no singular, de forma que f tiene fibras conexas y solamente finitas de ellas son singulares. Sea E la fibra genérica de f y sea $R \subseteq C$ el conjunto de puntos cuyas f-fibras son singulares. Entonces*

$$e(S) = e(C)\, e(E) + \sum_{s \in R} \left(e\left(f^{-1}(s)\right) - e(E) \right).$$

En el mismo contexto, podemos dar un argumento para probar el siguiente resultado.

Lema A.3.9 *Sea S una $\mathbb{C}$-superficie proyectiva no singular tal que existe un morfismo sobreyectivo $f : S \to C$, donde C es una $\mathbb{C}$-curva proyectiva no singular. Entonces todas las fibras son algebraicamente equivalentes.*

En esencia, se está usando que cualesquiera dos miembros de una familia algebraica de divisores son algebraicamente equivalentes. Léase también [25, p. 61].

Apéndice B

Solución alternativa

En este apéndice expondremos una solución alternativa de nuestro problema principal. Si bien la misma involucra menos conceptos, requiere de cómputos extremadamente enrevesados y, además, hace uso del **Teorema de Mazur** (nuestro Teorema 1.2.4), que es altamente sofisticado de demostrar. Por esta razón hemos decidido exponer esta solución alternativa como apéndice para todo aquel que desee conocer un argumento para dar solución al problema principal, sin tener que involucrarse en la teoría de superficies elípticas y los conceptos de geometría algebraica.

Por lo visto en el Capítulo 2, queremos ver que, fijado $a \in (-1,1) \cap \mathbb{Q}$, para todos salvo finitos $t \in \left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$, la $\mathbb{Q}$-cúbica en forma de Weierstrass

$$E_{a,t} : y^2 z = x^3 + t\left[(1+a)^2 t + 4(a-3)\right] x^2 z + 32(1-a)\, t^2 x z^2$$

es una curva elíptica y admite un punto sin torsión.

Fijado $t \in \mathbb{Q}$, sabemos que $P_{a,t} = \left(8t : 8(1+a)\, t^2 : 1\right)$ es solución de la $\mathbb{Q}$-cúbica expuesta, y que para todos salvo finitos valores de t, la misma es una curva elíptica, pues su discriminante es una expresión polinomial en t que, como tal, solamente se anula para finitos valores de t. Nuestro objetivo es ver que, para todos salvo finitos valores racionales de t para los cuales $E_{a,t}$ es una curva elíptica, la misma admite un punto sin torsión. Si demostramos esto, entonces habremos terminado, pues si hay solamente finitas excepciones en $\mathbb{Q}$, automáticamente habrá finitas excepciones en el subconjunto $\left(0, \frac{1}{\sqrt{1-a^2}}\right] \cap \mathbb{Q}$.

Sea $t \in \mathbb{Q}$ tal que $E_{a,t}$ es una curva elíptica. Es claro que $Q := (0:0:1)$ es también un punto solución de $E_{a,t}$. Aplicando repetidamente las fórmulas de 1.3, es posible ver las siguientes identidades, que expresamos de forma afinizada.

$$Q = (0,0)\,,$$

$$P_{a,t} = \left(8t, 8(1+a)\, t^2\right),$$
$$-P_{a,t} = \left(8t, -8(1+a)\, t^2\right),$$
$$P_{a,t} + Q = \left(4(1-a)\, t, -4\left(1-a^2\right) t\right),$$
$$-\left(P_{a,t} + Q\right) = \left(4(1-a)\, t, 4\left(1-a^2\right) t\right),$$
$$2P_{a,t} = \left(4, -4(a-3)\, t - 8\right),$$
$$-2P_{a,t} = \left(4, 4(a-3)\, t + 8\right),$$

$$2P_{a,t}+Q=\left(8\left(1-a\right)t^2,8\left(1-a\right)\left[\left(a-3\right)t+2\right]t^2\right),$$
$$-\left(2P_{a,t}+Q\right)=\left(8\left(1-a\right)t^2,-8\left(1-a\right)\left[\left(a-3\right)t+2\right]t^2\right),$$
$$3P_{a,t}=\left(\frac{8t\left[\left(a-1\right)t+1\right]^2}{\left(2t-1\right)^2},-\frac{8\left(a+1\right)t^2\left[\left(a-1\right)t+1\right]\left[2\left(a-1\right)t^2+\left(a-3\right)t+3\right]}{\left(2t-1\right)^3}\right),$$
$$-3P_{a,t}=\left(\frac{8t\left[\left(a-1\right)t+1\right]^2}{\left(2t-1\right)^2},\frac{8\left(a+1\right)t^2\left[\left(a-1\right)t+1\right]\left[2\left(a-1\right)t^2+\left(a-3\right)t+3\right]}{\left(2t-1\right)^3}\right),$$
$$3P_{a,t}+Q=\left(-\frac{4\left(a-1\right)t\left(2t-1\right)^2}{\left[\left(a-1\right)t+1\right]^2},-\frac{4\left(a^2-1\right)t^2\left(2t-1\right)\left[2\left(a-1\right)t^2+\left(a-3\right)t+3\right]}{\left[\left(a-1\right)t+1\right]^3}\right),$$
$$-\left(3P_{a,t}+Q\right)=\left(-\frac{4\left(a-1\right)t\left(2t-1\right)^2}{\left[\left(a-1\right)t+1\right]^2},\frac{4\left(a^2-1\right)t^2\left(2t-1\right)\left[2\left(a-1\right)t^2+\left(a-3\right)t+3\right]}{\left[\left(a-1\right)t+1\right]^3}\right),$$
$$4P_{a,t}=\left(\frac{4\left[2\left(a-1\right)t^2+1\right]^2}{\left[\left(a-3\right)t+2\right]^2},\frac{4\left[2\left(a-1\right)t^2+1\right]}{\left[\left(a-3\right)t+2\right]^3}S\left(t\right)\right),$$
$$-4P_{a,t}=\left(\frac{4\left[2\left(a-1\right)t^2+1\right]^2}{\left[\left(a-3\right)t+2\right]^2},-\frac{4\left[2\left(a-1\right)t^2+1\right]}{\left[\left(a-3\right)t+2\right]^3}S\left(t\right)\right),$$
$$4P_{a,t}+Q=\left(-\frac{8\left(a-1\right)t^2\left[\left(a-3\right)t+2\right]^2}{\left[2\left(a-1\right)t^2+1\right]^2},\frac{8\left(a-1\right)t^2\left[\left(a-3\right)t+2\right]}{\left[2\left(a-1\right)t^2+1\right]^3}S\left(t\right)\right),$$
$$-\left(4P_{a,t}+Q\right)=\left(-\frac{8\left(a-1\right)t^2\left[\left(a-3\right)t+2\right]^2}{\left[2\left(a-1\right)t^2+1\right]^2},-\frac{8\left(a-1\right)t^2\left[\left(a-3\right)t+2\right]}{\left[2\left(a-1\right)t^2+1\right]^3}S\left(t\right)\right),$$

donde

$$S\left(t\right):=2\left(a-1\right)\left(a^2-2a+5\right)t^4+8a^2\left(a-3\right)\left(a-1\right)t^3-\left(a^2-22a+25\right)t^2-4\left(a-3\right)t-2.$$

Estas expresiones inducen 17 puntos que, vistos como puntos en $\mathbb{Q}\left(t\right)\times\mathbb{Q}\left(t\right)$, son genéricamente distintos dos a dos. Si quisiésemos imponer que haya dos de estos puntos que coincidan, tendríamos que plantear un total de $\binom{17}{2}=136$ sistemas de dos ecuaciones (una por cada coordenada) polinomiales en t, y buscar $t\in\mathbb{Q}$ tal que al menos uno de estos sistemas sea satisfecho. Como los 17 puntos son genéricamente distintos, al menos una ecuación de cada sistema será polinomial en t y de grado positivo. Por consiguiente, cada sistema tendrá a lo sumo finitas soluciones racionales. Tomamos la unión, sobre cada sistema, de las soluciones racionales del mismo. Esto nos dará un número finito de valores de $t\in\mathbb{Q}$ para los cuales alguno de los 136 sistemas admite solución. Descartando estos finitos valores de t, y descartando también los finitos valores de t tales que el discriminante de $E_{a,t}$ se anula, obtenemos, para todo otro valor de t, que $E_{a,t}$ es una $\mathbb{Q}$-curva elíptica que admite 17 soluciones distintas dos a dos. Pero el Teorema 1.2.4 implica que una $\mathbb{Q}$-curva elíptica no puede tener más de 16 puntos de torsión. Así, hemos probado que para todos salvo finitos valores de t, $E_{a,t}$ es una $\mathbb{Q}$-curva elíptica de rango positivo.

Referencias

[1] Barth, Wolf P.; Hulek, Klaus; Peters, Chris A. M.; Van den Ven, Antonius, *Compact Complex Surfaces* (Second Enlarged Edition). Springer-Verlag Berlin Heidelberg, 2004.

[2] Beauville, Arnaud, *Complex Algebraic Surfaces* (Second Edition). London Mathematical Society Student Texts, vol. 34, Cambridge University Press, digital printing (2003).

[3] Bombieri, Enrico; Mumford, David, *Enrique's Classification of Surfaces in Char. p*, II. Complex Analysis and Algebraic Geometry. Iwanami Shoten Publishers, Cambridge University Press, 1977.

[4] Bosch, Siegfried; Lütkebohmert, Werner; Raynaud, Michel, *Néron Models*. Springer Verlag, Berlin (1990).

[5] Cai, Tianxin; Zhang, Yong, *A variety of Euler's conjecture* (2013).

[6] Chern, Shane, *Integral right triangle and rhombus pairs with a common area and a common perimeter*. Forum Geom. **16** (2016), 25-27. MR 3474530

[7] Coolidge, Julian Lowell, *A treatise on Algebraic Plane Curves*. New York, Dover Publications, 1959.

[8] Fulton, William, *ALGEBRAIC CURVES. An Introduction to Algebraic Geometry*. January 28, 2008.
http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[9] Hardy, G. H.; Wright, E. M.; Heath-Brown, D. R.; Silverman, J. H., *An Introduction to the Theory of Numbers* (6th edition). New York: Oxford University Press, 2008.

[10] Hartshorne, Robin, *Algebraic Geometry*. Graduate Texts in Mathematics, vol. 52. Springer, New York-Heidelberg, 1977.

[11] Ivorra Castillo, Carlos, *Curvas Elípticas*.
https://www.uv.es/ivorra/Libros/Elipticas.pdf

[12] Knapp, Anthony W., *Elliptic Curves*. Princeton University Press, Princeton, New Jersey, 1992.

[13] Lalín, Matilde; Ma, Xinchun, *θ-triangle and ω-parallelogram pairs with common area and common perimeter*. J. Number Theory **202** (2019), 1–26.

[14] Lang, Serge, *Introduction to Arakelov Theory*. Springer-Verlag, New York, 1988.

[15] Liu, Qing, *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics | 6. Oxford University Press, Oxford, 2006.

[16] Marcus, Daniel, *Number Fields*. Springer-Verlag: New York, 1977.

[17] Matsumura, Hideyuki, *Commutative Algebra* (Second Edition). Mathematics lecture note series, 56, 1980.

[18] Milne, J. S., *Elliptic Curves*, BookSurge Publishers, 2006.

[19] Miranda, Rick, *The basic theory of elliptic surfaces* (1989). Notes of lectures, Department of Mathematics, Colorado State University. Fort Collins, CO 80523, USA.

[20] Miranda, Rick; Persson, Ulf, *Torsion groups of elliptic surfaces*. Compositio Math. **72** (1989), no. 3, 249-267.

[21] Oguiso, Keiji, *An elementary proof of the topological Euler characteristic formula for an elliptic surface*. Commentarii Mathematici, Universitatis Sancti Pauli, Vol. 39, no. 1, 81–86 (1990).

[22] Procesi, Claudio, *LIE GROUPS. An Approach through Invariants and Representations*. USA, Springer, Universitext, 2007.

[23] Schinzel, Andrzej, *Triples of positive integers with the same sum and the same product*. Serdica Math J. **22** (1996), no. 4, 587-588. MR **1483607 (98g:**11033).

[24] Schütt, Matthias; Shioda, Tetsuji, *Elliptic Surfaces* (2010). https://arxiv.org/abs/0907.0298v3

[25] Schütt, Matthias; Shioda, Tetsuji, *Mordell-Weil Lattices*. Springer Nature, Singapore Pte Ltd., 2019.

[26] Shioda, Tetsuji, *On the Mordell-Weil Lattices*. Commentarii Mathematici Universitatis Sancti Pauli **39**, 211–240 (1990).

[27] Silverman, Joseph H., *Advanced Topics in the Arithmetic of Elliptic Curves* (Corrected second printing, 1999). New York, Springer-Verlag, Graduate Texts in Mathematics.

[28] Silverman, Joseph H.; Tate, John T., *Rational Points on Elliptic Curves* (Second Edition). Springer, Undergraduate Texts in Mathematics, 2015.

[29] Szydlo, Michael, *Elliptic fibers over non-perfect residue fields*. Journal of Number Theory, Volume 104, Issue 1, January 2004, Pages 75-99.

[30] Tate, John T., *Algorithm for determining the type of a singular fiber in an elliptic pencil*. SLN **476**, 33-52 (1975).

[31] Vakil, Ravi, *THE RISING SEA. Foundations of Algebraic Geometry*. Version of November 18, 2017. http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf