USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

A teoría da multiplicación complexa e o soño de xuventude de Kronecker

Héctor Varela Rodríguez

Curso 2023/2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

A teoría da multiplicación complexa e o soño de xuventude de Kronecker

Héctor Varela Rodríguez

Setembro, 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: A teoría da multiplicación complexa e o soño de xuventude de Kronecker
Breve descrición do contido
Hilbert afirmou que "a teoría da multiplicación complexa non era tan só a parte máis fermosa das matemáticas, senón de toda a ciencia". O obxectivo deste traballo é entender en que se basea dita teoría e aprender algúns dos conceptos introdutorios, para logo comprender a relación co famoso soño de xuventude de Kronecker sobre extensións de Galois. Ao longo do traballo, iranse descubrindo diferentes obxectos matemáticos (curvas elípticas, funcións elípticas, extensións abelianas...) que se acabarán entrelazando entre eles de forma sorprendente, dando lugar a resultados que aínda hoxe seguen a abrir novas portas na investigación matemática.
Recomendacións
Ter cursado a materia de Ecuacións Alxébricas e ter interese por profundizar nela.
Outras observacións

Índice

Resumo

O soño de xuventude de Kronecker fai referencia ao problema de construír tódalas extensións abelianas dun corpo cuadrático imaxinario, estendendo así o teorema de Kronecker-Weber. Para o estudo desta cuestión, o instrumento central é unha certa clase de curvas elípticas, cunha estrutura aritmética especialmente rica denominada multiplicación complexa.

Neste traballo vaise explorar a relación entre estas dúas cuestións. Comezarase introducindo, por unha parte, as curvas elípticas, definindo nelas unha estrutura de grupo, centrando a atención nos puntos de orde finita; e doutra banda, as extensións de $\mathbb{Q}$, facendo fincapé naquelas cuxo grupo de Galois é abeliano, así coma nas xeradas por raíces da unidade ou puntos de curvas elípticas. Posteriormente, presentarase o concepto da multiplicación complexa e, finalmente, botando man tamén das representacións de grupos, aplicarase toda a teoría para estudar unha realización concreta do soño de xuventude de Kronecker, tomando como base o corpo cuadrático imaxinario $\mathbb{Q}(i)$.

Abstract

Kronecker's Jugendtraum is related to the problem of finding all abelian extensions of a quadratic imaginary field, therefore generalising the Kronecker-Weber theorem. To study this issue, the main tool is a certain class of elliptic curves, with a specially rich arithmetic structure, called complex multiplication.

In this work we will explore the connection between these two topics. We will start by introducing, on one side, the elliptic curves, defining over them a group structure, focusing on finite order points; and on the other, extensions of $\mathbb{Q}$, emphasising those with an abelian Galois group, as well as those generated by roots of unity or elliptic curve points. Afterwards, we will present the concept of complex multiplication and, finally, with the help from group representations, all the previous theory will be used to study a particular case of Kronecker's Jugendtraum, looking at the abelian extensions of $\mathbb{Q}(i)$.

Introdución

As curvas elípticas son conxuntos de puntos do plano proxectivo definidos por ecuacións de terceiro grao, é dicir, curvas cúbicas, que ademais son non singulares e presentan, cando menos, un punto. Entón, por que se emprega o adxectivo *elípticas* para describilas? A razón remóntase ao século XVIII, co estudo da lonxitude de arco das elipses. Na integral empregada para este cálculo, o integrando estaba composto pola raíz cadrada dun polinomio de grao 3 ou 4. Deste xeito, para determinar a lonxitude de arco da elipse, hai que integrar a función $y = \sqrt{f(x)}$, e o resultado virá dado en función da curva *elíptica* $y^2 = f(x)$.

O estudo destas curvas ten as súas raíces na teoría das ecuacións diofantianas, que comprende as solucións de ecuacións polinómicas en $\mathbb{Z}$ ou $\mathbb{Q}$. Entre os exemplos máis destacados atópase, por exemplo, a ecuación de Fermat:

$$x^n + y^n = z^n$$

para a cal, segundo o último teorema de Fermat, non existen solucións enteiras positivas para $n \geq 3$.

Outro exemplo destacado é a ecuación de Bachet, da forma

$$y^2 = x^3 + c, \;\; c \in \mathbb{Z}.$$

No 1621, este matemático francés descubriu unha propiedade moi interesante desta ecuación: existe unha fórmula da duplicación, mediante a cal, dada unha solución da ecuación nos números racionais, é posible xerar unha infinidade doutras, tamén en $\mathbb{Q}$. Para o caso das solucións en $\mathbb{Z}$, houbo que agardar ata 1908, cando Axel Thue probou que, para cada valor de c, existe tan só un número finito de solucións enteiras.

Máis en xeral, os exemplos anteriores responden a ecuacións diofantianas en dúas variables, da forma

$$f(x, y) = 0$$

sendo f un polinomio. O conxunto de solucións reais a unha ecuación deste tipo forman unha curva plana, denominada xeralmente *curva alxébrica*. E dentro del, resulta interesante determinar a existencia de solucións en $\mathbb{Z}$, en $\mathbb{Q}$ ou nunha extensión finita de $\mathbb{Q}$; de ser o caso, tamén interesa ter unha medida de cantas hai. Estas cuestións xa foron contestadas para ecuacións de graos 1 e 2. Para o caso das curvas elípticas, estas cuestións aínda non obtiveron unha resposta completa.

O estudo das curvas elípticas, entón, resulta interesante desde unha perspectiva alxébrica, pero tamén xeométrica. Non obstante, existe un terceiro campo co que gardan unha estreita relación: a teoría de números.

No estudo das extensións de $\mathbb{Q}$, aquelas que resultan máis interesantes son as abelianas, é dicir, aquelas cuxo grupo de Galois é abeliano. Máis en concreto, as extensións ciclotómicas, xeradas por raíces da unidade, posúen esta característica. Non só iso: o teorema de Kronecker-Weber garante que calquera extensión abeliana de $\mathbb{Q}$, necesariamente, estará contida nunha extensión ciclotómica.

Xa que se teñen estos resultados en $\mathbb{Q}$, semella tentador intentar estendelos a outros corpos diferentes, por exemplo, a extensións cuadráticas imaxinarias. Na situación de $\mathbb{Q}$, os xeradores das extensións abelianas son elementos da torsión da circunferencia, isto é, as raíces da unidade. Pois ben, agora, as curvas elípticas farán as veces da circunferencia; é dicir, a torsión de certas curvas elípticas xerará extensións abelianas dos corpos cuadráticos imaxinarios.

A construción das extensións abelianas dun corpo cuadrático imaxinario é o que xeralmente se coñece como *soño de xuventude de Kronecker*. Por suposto, pódese ir máis aló, e pensar nunha teoría xeral onde o corpo base $\mathbb{K}$ sexa arbitrario, obtendo unha xeneralización do teorema de Kronecker-Weber. Trátase dun problema aínda por resolver, incluído ademais no duodécimo lugar da lista de problemas de Hilbert.

Este traballo está estruturado en cinco capítulos, ao longo dos cales se explora a relación xa mencionada entre a álxebra, a xeometría e a teoría de números. O primeiro capítulo presenta as nocións básicas sobre curvas elípticas; inténtanse establecer analoxías e diferenzas co caso das curvas cónicas, constrúese unha estrutura de grupo coa suma de puntos e vese que está finitamente xerado, como recolle o teorema de Mordell. Ademais, proporciónase un xeito explícito de realizar a suma, e introdúcese a caracterización dos puntos de orde finita da curva.

No segundo capítulo trátanse as extensións abelianas de $\mathbb{Q}$, mencionando o teorema de Kronecker-Weber e o soño de xuventude de Kronecker. Tamén, dada unha extensión de Galois de $\mathbb{Q}$, determínase como actúa o seu grupo de Galois sobre os puntos dunha curva elíptica racional, así coma as extensións xeradas pola torsión de curvas elípticas.

O capítulo 3 é moi breve, e introduce a teoría de representacións de Galois, considerando matrices asociadas aos automorfismos do grupo de Galois dunha extensión actuando na torsión da curva elíptica. O grupo de Galois xogará un papel moi importante na teoría que se vai desenvolver. Do mesmo xeito que se fala dunha acción do grupo de Galois nos corpos ciclotómicos e na torsión da circunferencia, pódese considerar unha acción de Galois na torsión das curvas elípticas.

O obxectivo do capítulo 4 é presentar a teoría da multiplicación complexa. Tódalas curvas elípticas teñen a multiplicación por un enteiro arbitrario m como endomorfismo. Cando existen outros diferentes, ademais destes, falamos de curvas elípticas con multiplicación complexa. No caso de

corpos de característica cero, cúmprese que entón o anel de endomorfismos é unha orde no anel de enteiros dun corpo cuadrático imaxinario.

Por último, o capítulo 5 está adicado á aplicación dos contidos dos capítulos anteriores para estudar as extensións abelianas sobre $\mathbb{Q}(i)$, así como establecer a súa analoxía coas extensións ciclotómicas de $\mathbb{Q}$. Na liña do discutido no capítulo anterior, a curva $y^2 = x^3+x$ ten multiplicación complexa e o seu anel de endomorfismos é isomorfo aos enteiros gaussianos, $\mathbb{Z}[i]$. Neste caso, amosamos como as extensión obtidas ao adxuntar a $\mathbb{Q}(i)$ os puntos de torsión desa curva son abelianas. Non só iso: tamén se cumpre, aínda que a demostración é máis técnica e por iso se omite, que isto permite xerar tódalas extensións abelianas de $\mathbb{Q}(i)$.

Capítulo 1

Sobre curvas elípticas

1.1. Puntos racionais en curvas cónicas

Aínda que a intención é estudar os puntos racionais en curvas elípticas, comezarase un chanzo por debaixo, observando que sucede nas curvas cónicas, onde a caracterización destes puntos é máis sinxela e se ten completamente definida. Deste xeito, vanse intentar establecer analoxías entre os dous casos.

Definición 1.1. Sexa $P = (x, y) \in \mathbb{R}^2$. Dirase que P é un **punto racional** se $(x, y) \in \mathbb{Q}^2$.

Definición 1.2. Unha **recta racional** é unha ecuación de primeiro grao en dúas variables con coeficientes racionais.

Compróbase facilmente que toda recta que pasa por dous puntos racionais resulta ser unha recta racional. Da mesma maneira, dúas rectas racionais non paralelas intersecan nun punto racional.

Lémbrese que a ecuación xeral dunha cónica é

$$ax^2 + by^2 + cxy + dx + ey + f = 0. \tag{1.1}$$

De xeito análogo ás rectas, dirase que unha cónica é **racional** se os coeficientes da súa ecuación son racionais.

Díxose que a intersección de dúas rectas racionais, se existe, é un punto racional. Entón, a pregunta natural que cabe facer agora é se sucede o mesmo coa intersección entre unha cónica e unha recta. E a resposta é que, en xeral, non. En efecto, ao intentar despexar analiticamente as coordenadas dos puntos, obtense unha ecuación cuadrática con coeficientes racionais. E se as solucións obtidas son racionais, entón os puntos de intersección serán racionais. Non obstante, existe a posibilidade de que as solucións sexan números irracionais conxugados.

Agora ben, se un dos puntos é racional, entón o outro tamén, xa que a suma das solucións dunha

ecuación cuadrática nunha variable con coeficientes racionais, $ax^2 + bx + c = 0$, é $-b/a$. E é esta idea a que permite describir completamente os puntos racionais das curvas cónicas.

Supóñase unha cónica racional na que se sabe que existe un punto racional $\mathcal{O}$. Entón, tomando este punto como foco, pódese proxectar a cónica sobre unha recta racional arbitraria. Nótese que a proxección do punto $\mathcal{O}$ é realizada coa tanxente á cónica no punto $\mathcal{O}$.

A recta de proxección corta á recta racional nun punto de proxección Q e á cónica racional nun punto P:

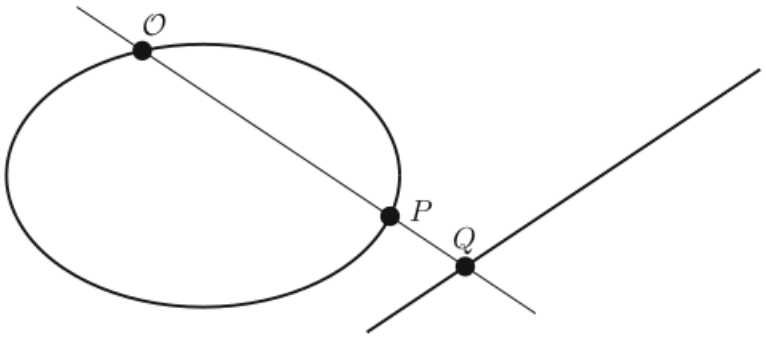


Figura 1.1: Proxección da cónica sobre unha recta racional. *Extraída de* [6].

Deste xeito, establécese unha bixección entre os puntos da recta racional e os da cónica, exceptuando o punto $\mathcal{O}'$ para o cal a recta que une $\mathcal{O}$ e $\mathcal{O}'$ resulta ser paralela á recta racional. Non obstante, ao enviar o punto $\mathcal{O}'$ ao punto do infinito da recta, este problema desaparece.

Tense que, se P é racional, entón Q tamén. En efecto, ao ser $\mathcal{O}$ e P racionais, a recta de proxección, que os une, é racional. Así, a súa intersección coa recta racional de partida, i.e., o punto Q, é racional. Reciprocamente, se Q é racional, o raio de proxección é racional, xa que une $\mathcal{O}$ con Q. Este raio corta á cónica nos puntos $\mathcal{O}$ e P. Logo, xa que $\mathcal{O}$ é racional, P tamén o será.

Hai que ter en conta que, neste razoamento, o que se fai é partir dunha cónica na que se supón que hai un punto racional, para a partir del determinar o resto de puntos racionais. Entón, cabe cuestionar o seguinte: é posible determinar se unha cónica posúe puntos racionais? A resposta é afirmativa, e aparece recollida no seguinte resultado:

Teorema 1.3 (Legendre)**.** *Considérese unha curva cónica de ecuación $aX^2 + bY^2 = cZ^2$, onde $a, b, c \in \mathbb{Z}$ cumpren ser non nulos, libres de cadrados (i.e., non existe ningún número primo p tal que p^2 sexa divisor de ningún deles) e coprimos dous a dous. Entón, a cónica ten un punto racional cando, e só cando, a, b e c posúen o mesmo signo e $-bc$, $-ac$ e $-ab$ son residuos cuadráticos de a, b e c, respectivamente.*

Obsérvese que toda cónica con coeficientes en $\mathbb{R}$ pode escribirse na forma do teorema, sen máis ca aplicar un cambio de coordenadas e facendo uso da xeometría proxectiva.

1.2. As curvas elípticas e o teorema de Mordell

Definición 1.4. Unha **curva cúbica** é unha ecuación polinómica de terceiro grao en dúas variables:

$$ax^3 + by^3 + cx^2y + dxy^2 + ex^2 + fy^2 + gxy + hx + iy + j = 0. \tag{1.2}$$

Dirase que a curva é **racional** se os seus coeficientes están en $\mathbb{Q}$.

Ao contrario do que sucede coas curvas cónicas, non se coñece ningún método que permita determinar, nun número finito de pasos, a existencia de puntos racionais nunha curva cúbica. É dicir, non existe ningún resultado coñecido análogo ao **Teorema de Legendre**. Así, dentro do conxunto de curvas cúbicas, vanse estudar, en particular, as seguintes:

Definición 1.5. Unha **curva elíptica** é unha cúbica proxectiva que cumpre, ademais, ser non singular e posuír, cando menos, un punto sobre o corpo no que está definida.

Aínda que se ten definido unha curva elíptica no plano proxectivo, é posible traballar nun modelo afín, escollendo unha referencia tal que a recta do infinito conteña un único punto da curva.

Observación 1.6. Do mesmo xeito que non existe un análogo para o teorema de Legendre nas curvas cúbicas, ao considerar curvas elípticas, non se pode empregar a técnica da proxección sobre unha recta racional, pois en xeral, a intersección dunha recta e unha curva cúbica está composta de 3 puntos; polo tanto, se un deles é racional, os outros dous poderían continuar sendo irracionais.

Non obstante, se se coñecen dous puntos racionais da curva, en xeral é posible achar un terceiro, sen máis ca trazar a recta que une eses dous puntos. Esta recta, que se sabe racional, cortará á cúbica nun terceiro punto. Alxebricamente, quérese resolver unha ecuación cúbica con coeficientes racionais, da que dúas solucións se saben racionais. Entón, necesariamente, a terceira tamén o ten que ser.

Así, dados dous puntos P e Q, ao trazar a recta que os une, denotarase por $P*Q$ o terceiro punto de intersección coa cúbica. Incluso se só se ten un punto racional P, pode xerarse outro, sen máis ca trazar a tanxente á cúbica en P (i.e., a recta que pasa por P e P). O mesmo argumento xustifica que $P * P$ é racional. A construción xeométrica aparece ilustrada na Figura 1.2.

Esta idea de obter máis puntos a partir duns poucos aparece recollida no seguinte resultado:

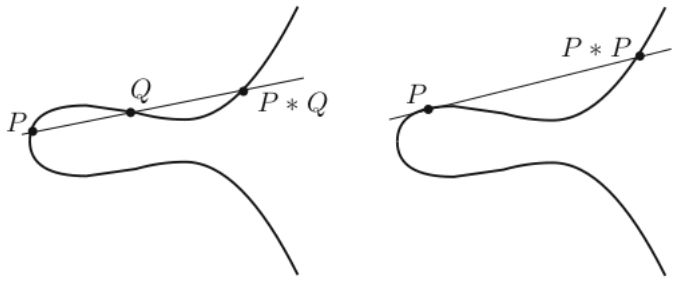


Figura 1.2: Composición de puntos racionais nunha curva elíptica. *Extraída de* [6].

Teorema 1.7 (Mordell)**.** *Sexa C unha curva cúbica racional e non singular. Entón, existe un conxunto finito de puntos racionais tal que tódolos demais puntos racionais se poden obter debuxando rectas e tomando intersecciónes de xeito continuo.*

O teorema anterior, que aparece enunciado en termos xeométricos, vaise reformular dun xeito máis alxébrico. Para iso, empregarase o **Teorema de Bézout**, que se enuncia a continuación:

Teorema 1.8 (Bézout)**.** *Sexan dúas curvas C_1 e C_2, sendo C_1 de grao m e C_2 de grao n. Entón, C_1 e C_2 intersecan en mn puntos.*

Demostración. Pódese consultar en [6]. □

A partir deste teorema, obtense o seguinte:

Corolario 1.9. *Sexan C, C_1 e C_2 curvas cúbicas. Supóñase que C pasa por 8 dos 9 puntos de intersección de C_1 e C_2. Entón, C tamén pasa polo noveno punto de intersección.*

Demostración. Para determinar unha curva cúbica, hai que dar os 10 coeficientes da súa ecuación alxébrica, (1.2). Multiplicalos por unha constante distinta de cero non cambia a curva descrita; así, o conxunto de tódalas curvas cúbicas posibles ten "dimensión 9".

Facer que a cúbica pase por un punto impón unha restrición linear nos coeficientes do polinomio. Logo, o conxunto de cúbicas que pasan por un punto ten "dimensión 8". Cada vez que se engada un novo punto polo que deba pasar, imponse unha nova condición linear sobre os coeficientes, reducindo nunha dimensión o conxunto de cúbicas desexado (sempre que a condición obtida sexa linearmente independente das anteriores).

En particular, a familia de cúbicas que pasan por 8 dos 9 puntos de $C_1 \cap C_2$, $P_1, \dots, P_8$, ten "dimensión 1".

Sexan $F_1(x, y) = 0$ e $F_2(x, y) = 0$ as respectivas ecuacións de C_1 e C_2. Para cada par de escalares $\lambda_1, \lambda_2 \in \mathbb{R}$, a curva $\lambda_1 F_1 + \lambda_2 F_2$ é unha cúbica que pasa por $P_1, \dots, P_8$. Como só existe unha familia de cúbicas que pase por eses puntos, o conxunto

$$\{\lambda_1 F_1 + \lambda_2 F_2 \mid \lambda_1, \lambda_2 \in \mathbb{R}\}$$

ten que ser tal familia. En particular, $C \equiv \lambda_1 F_1 + \lambda_2 F_2 = 0$, para unha certa combinación de λ_1 e λ_2.

Como $P_9 \in C_1 \cap C_2$, $F_1(x, y)$ e $F_2(x, y)$ anúlanse nese punto, logo $\lambda_1 F_1 + \lambda_2 F_2$ tamén. Así, $P_9 \in C$. □

Observación 1.10. No que segue, o punto racional da curva elíptica será denotado por $\mathcal{O}$.

A priori, a operación de composición definida sobre os puntos racionais, $P*Q$, non lle proporciona ningunha estrutura alxébrica ao conxunto. Agora ben, tendo o punto $\mathcal{O}$ fixado, pódese construír un grupo no conxunto de puntos racionais, de xeito que $\mathcal{O}$ sexa o elemento neutro. A operación do grupo é a seguinte:

Definición 1.11. Sexan P e Q dous puntos racionais dunha curva elíptica. Defínese a **suma dos puntos** P e Q como o terceiro punto de intersección da curva e a recta que une $\mathcal{O}$ con $P*Q$:

$$P + Q = \mathcal{O} * (P * Q)$$

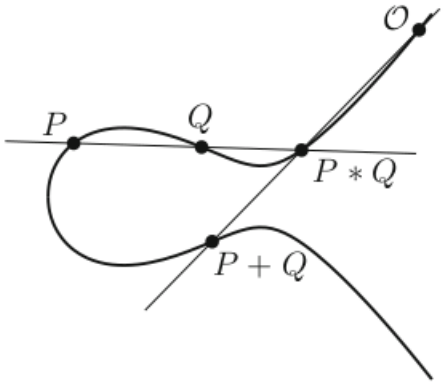


Figura 1.3: Visualización da suma de puntos nunha curva elíptica. *Extraída de* [6].

Proposición 1.12. $(C, \mathcal{O}, +)$ *é un grupo abeliano.*

Demostración. Hai que probar varios puntos:

1. Conmutatividade

$$P + Q = Q + P.$$

Esta propiedade é trivial, porque a recta que pasa por P e Q é a mesma cá que pasa por Q e P, logo $P * Q = Q * P$.

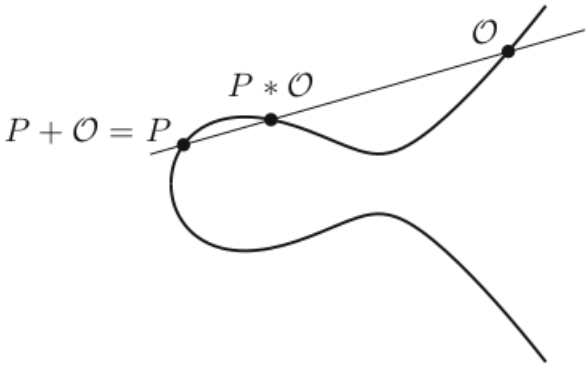


Figura 1.4: Elemento neutro da suma de puntos. *Extraída de* [6].

2. O elemento neutro é $\mathcal{O}$

$$P + \mathcal{O} = P.$$

É inmediato tamén: o terceiro punto da recta que une P e $\mathcal{O}$ é $P * \mathcal{O}$; logo, o terceiro punto de intersección da recta que pasa por $\mathcal{O}$ e $P * \mathcal{O}$ é P. Véxase a Figura 1.4.

3. Existe outro punto racional na cúbica tal que operado con P resulta no elemento neutro, $\mathcal{O}$. Este punto será denotado por $-P$:

$$P + (-P) = \mathcal{O}.$$

Para obtelo, séguese o seguinte procedemento:

   a) Debúxase a tanxente á cúbica en $\mathcal{O}$, que corta á cúbica en $S = \mathcal{O} * \mathcal{O}$ (lémbrese que supón a curva suponse non singular).

   b) Dado un punto P, trázase a recta que pasa por P e S. O terceiro punto de intersección é o inverso buscado:

$$-P = P * S.$$

En efecto, para determinar $P + (-P)$, áchase primeiro $P * (-P) = S$. Agora, únese S con $\mathcal{O}$ e tómase $S * \mathcal{O}$; pero esta recta é a tanxente á cúbica en $\mathcal{O}$, logo $S * \mathcal{O} = \mathcal{O}$:

$$P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * S = \mathcal{O}.$$

4. Asociatividade

$$(P + Q) + R = P + (Q + R).$$

Para achar $P + Q$, tómase $P * Q$ e a continuación, únese con $\mathcal{O}$ e áchase o terceiro punto de intersección, $P + Q = \mathcal{O} * (P * Q)$. A continuación, para sumar $P + Q$ con R, hai que construír $(P + Q) * R$, unilo con $\mathcal{O}$, e tomar a terceira intersección.

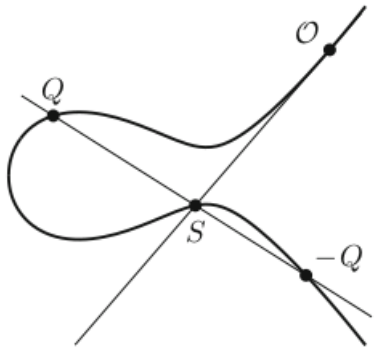


Figura 1.5: O inverso dun punto na curva elíptica. *Extraída de* [6].

Para achar $Q+R$, tómase $Q*R$, tómase $Q*R$, únese con $\mathcal{O}$ e escóllese o terceiro punto de intersección, $Q+R=\mathcal{O}*(Q*R)$. Despois, para sumar P e $Q+R$, constrúese $P*(Q+R)$, únese con $\mathcal{O}$, e tómase a terceira intersección.

Observando as operacións anteriores, é fácil decatarse de que, para demostrar a asociatividade, abonda probar que

$$(P+Q)*R=P*(Q+R).$$

Os puntos

$$\begin{array}{cccc} \mathcal{O}, & P, & P*Q, & Q*R, \\ Q, & R, & P+Q, & Q+R \end{array}$$

están situados nalgunha das rectas empregadas para a construción dos puntos $(P+Q)*R$ e $P*(Q+R)$.

Considérense as rectas que unen $P+Q$ con R e P con $Q+R$, respectivamente. É a súa intersección un punto da cúbica? En caso afirmativo, terase demostrado que $(P+Q)*R=P*(Q+R)$.

Téñense 9 puntos: os 8 anteriores e a intersección anterior. Doutra banda, tamén se teñen dúas cúbicas (dexeneradas) que pasan polos 9 puntos, xa que unha recta posúe unha ecuación linear, polo que se se teñen 3 ecuacións lineares e se multiplican, obtense unha ecuación cúbica. O conxunto de solucións a esa ecuación cúbica é a unión das 3 liñas.

Considérese C_1 a unión das 3 liñas descontinuas, e C_2 a unión das 3 liñas continuas, como se ve na Figura 1.6. Por construción, tanto C_1 coma C_2 pasan polos 9 puntos. E doutra banda, a curva C pasa polos 8 puntos enumerados anteriormente; logo, aplicando o **Corolario 1.9**, garántese que C pasa tamén pola intersección das curvas anteriores, quedando probado que $(P+Q)*R=P*(Q+R)$. □

Observación 1.13. A estrutura de grupo anterior non depende do punto $\mathcal{O}$ fixado.

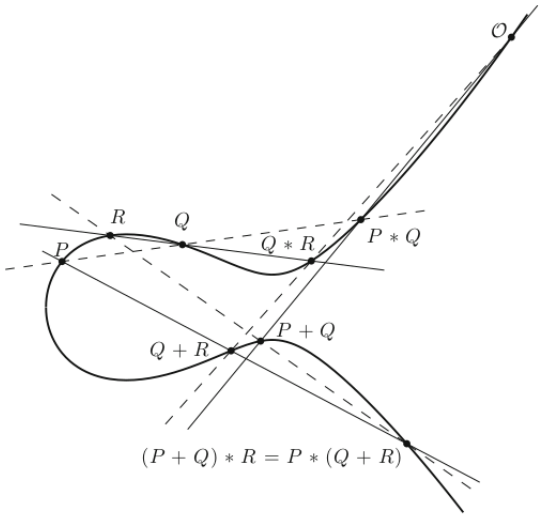


Figura 1.6: Demostración xeométrica da asociatividade da suma de puntos. *Extraída de* [6].

Ao ter definida esta lei de grupo na curva cúbica, pódese reformular o **Teorema de Mordell** como segue:

Teorema 1.14 (Mordell)**.** *O conxunto de puntos racionais dunha curva elíptica está finitamente xerado.*

Demostración. Pódese consultar en [6]. □

1.3. Fórmulas explícitas para a lei de grupo

Mordell probou o seu teorema dando fórmulas explícitas para a lei de adición. Para obter as fórmulas o máis sinxelas posible, pódese facer unha serie de transformacións lineares, resultando así nunha ecuación máis simplificada. En concreto, sempre que a característica do corpo $\mathbb{K}$ sobre o que se define a curva sexa distinta de 2 ou de 3 (no noso caso non vai haber problema porque se traballa nun corpo de característica 0), calquera curva elíptica pode ser expresada en **forma normal de Weierstrass**:

$$y^2 = x^3 + ax + b = f(x) \tag{1.3}$$

onde $a, b \in \mathbb{K}$.

Empregando coordenadas proxectivas, a forma normal de Weierstrass pode escribirse de xeito homoxéneo:

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{1.4}$$

Considérese a recta do infinito, $Z = 0$. Substituíndo na ecuación anterior, obtense $X^3 = 0$; isto

é, a curva elíptica corta á recta $Z = 0$ nun único punto, aínda que con multiplicidade tripla. É dicir: a curva elíptica ten un único punto no infinito; en concreto, aquel no que as rectas verticais (da forma $x = cte$) se cortan.
Ademais, este punto é un punto de inflexión da curva, no cal a recta tanxente é, precisamente, $Z = 0$, que a corta con multiplicidade 3. Máis aínda: este punto é non singular, o cal se pode comprobar facilmente estudando as derivadas parciais.

Así, para unha curva elíptica en forma normal de Weierstrass, existe un punto no infinito, e é non singular. De agora en diante, será denotado por $\mathcal{O}$. **Este punto considérase como racional**, e será tomado como o elemento neutro do grupo de puntos racionais.

Unha curva elíptica en forma normal de Weierstrass é simétrica respecto do eixo de abscisas. Deste xeito, é fácil decatarse de que $P * Q$ e $P + Q$ son simétricos respecto do eixo X. En particular, tendo en conta que o elemento neutro é o punto do infinito, o oposto dun punto P é a súa reflexión na curva elíptica respecto do eixo de abscisas. En coordenadas, se $P = (x, y)$, entón $-P = (x, -y)$ (sempre e cando $P \neq \mathcal{O}$).

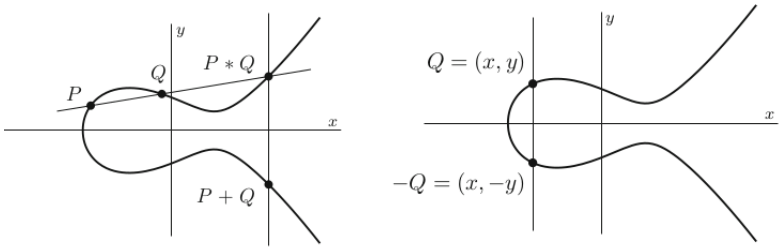


Figura 1.7: Operacións da lei de grupo en forma normal de Weierstrass. *Extraída de* [6].

Considérense dous puntos distintos $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ da curva elíptica. Facendo uso da forma normal de Weierstrass, pódense dar fórmulas explícitas para a suma P_1+P_2 en coordenadas. En particular, facendo $P_1 * P_2 = (x_3, y_3)$, sábese que $P_1 + P_2 = (x_3, -y_3)$.

Considérase a ecuación da recta que une P_1 e P_2, $y = mx + n$. Entón, é posible determinar a pendente e a ordenada na orixe a partir das coordenadas dos puntos:

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \qquad n = y_1 - mx_1 = y_2 - mx_2. \tag{1.5}$$

Por construción, a recta corta á cúbica en P_1 e P_2. Como obter o terceiro punto de intersección, $P_1 * P_2$?

Substituíndo a ecuación da recta na forma normal de Weierstrass, (1.3):

$$(mx+n)^2 = x^3+ax+b \iff m^2x^2+2mnx+n^2 = x^3+ax+b \iff x^3-m^2x^2+(a-2mn)x+b-n^2 = 0.$$

Esta é unha ecuación cúbica na variable x, e as raíces x_1, x_2 e x_3 corresponden ás abscisas dos

tres puntos de intersección. Así:

$$x^3 - m^2x^2 + (a - 2mn)x + b - n^2 = (x - x_1)(x - x_2)(x - x_3).$$

Desenvolvendo o produto, e igualando coeficientes, obtense:

$$x_3 = m^2 - x_1 - x_2 \qquad \Longrightarrow \qquad y_3 = mx_3 + n. \tag{1.6}$$

Supóñase agora que se dispón dun único punto $P_0 = (x_0, y_0)$ e se quere calcular $P_0 + P_0 = 2P_0$. Para achar a recta que une P_0 con P_0 non se pode utilizar a ecuación explícita da recta neste caso, porque a fórmula da pendente é inservible neste caso. Agora ben, o que si se sabe é que esta recta é tanxente á curva en P_0. Así, derivando implicitamente a ecuación $y^2 = f(x)$ en P_0, obtense:

$$m = \frac{dy}{dx}\Big|_{P_0} = \frac{f'(x_0)}{2y_0}.$$

e máis en xeral, para un punto (x, y):

$$m = \frac{f'(x)}{2y}.$$

Substituíndo a expresión de m no cálculo de x_3:

$$x_3 = \left(\frac{f'(x)}{2y}\right)^2 - 2x.$$

Se agora se substitúen as expresións de $f'(x)$ e y^2, facendo os cálculos, chégase á **fórmula da duplicación** para x_3:

$$x_3 = \frac{x^4 - 14ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}. \tag{1.7}$$

No caso da coordenada y_3, é posible derivar unha fórmula análoga para o seu cálculo.

1.4. A m-torsión das curvas elípticas

Agora que se ten definido un grupo sobre a curva elíptica, interesa estudar aqueles elementos de orde finita. Defínese así:

Definición 1.15. Sexa C unha curva elíptica. Considérese un punto racional $P \in C$. Dirase que P é un **punto de torsión** se existe un número natural $m \geq 1$ tal que $mP = \mathcal{O}$. En particular, dirase que P é un **punto de m-torsión**.

Observación 1.16. O punto $\mathcal{O}$, ao ser o elemento neutro da suma de puntos, é un punto de m-torsión $\forall\, m \in \mathbb{N}, m > 0$.

Considérese unha curva elíptica en forma normal de Weierstrass. Para caracterizar os puntos de m-torsión, pódese comezar estudando casos concretos de ordes baixas. Por exemplo:

- Para estudar os puntos de 2-torsión, i.e., aqueles puntos tales que $2P = \mathcal{O}$, é fácil decatarse de que este problema é equivalente a determinar que puntos satisfán a ecuación $P = -P$, con $P \neq \mathcal{O}$. Sendo $P = (x, y)$, terase que $-P = (x, -y)$; logo, os puntos que cumpren esta condición son aqueles tales que $y = 0$, i.e.,

$$P_1 = (\alpha_1, 0) \qquad P_2 = (\alpha_2, 0) \qquad P_3 = (\alpha_3, 0)$$

  onde $\alpha_1, \alpha_2, \alpha_3$ son as raíces (a priori, complexas) do polinomio $f(x)$. Obsérvese que, sendo a curva elíptica, en particular é non singular, logo garántese que os tres puntos serán diferentes.

- No caso dos puntos de 3-torsión, pódese aplicar unha técnica análoga: no canto de considerar $3P = \mathcal{O}$, tómese $2P = -P$. Así, un punto de orde 3 satisfai $x(2P) = x(-P) = x(P)$. Reciprocamente, se P cumpre $x(2P) = x(P)$, entón $2P = \pm P$, i.e., $P = \mathcal{O}$, o cal está excluído por hipótese. Deste xeito, os puntos de orde 3 están determinados pola ecuación $x(2P) = x(P)$.

O desenvolvemento das ideas anteriores conduce ao seguinte resultado:

Proposición 1.17. *Sexa C unha curva elíptica en forma normal de Weierstrass. Considérese un punto $P = (x, y) \in C, P \neq O$. Entón, verifícase:*

1. *P é de orde 2 $\iff y = 0$.*
2. *A curva C posúe exactamente 4 puntos con orde divisor de 2. Ademais, estes puntos forman un grupo isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
3. *P é de orde 3 $\iff x$ é raíz de $\psi_3(x) = 3x^4 + 18ax^2 + 12bx - a^2$.*
4. *A curva C posúe exactamente 9 puntos con orde divisor de 3. Ademais, estes puntos forman un grupo isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Demostración. Pódese atopar en [6]. □

Observación 1.18. Estes resultados son válidos sempre que se permitan coordenadas complexas para os puntos. Agora ben, hai que recordar que se ten definido o grupo dos puntos *racionais* da curva elíptica. Pero agora estanse aceptando coordenadas complexas. Entón, é natural preguntarse se esta operación lle proporciona estrutura de grupo tamén a outros conxuntos de puntos da curva máis extensos, de xeito que o conxunto dos puntos racionais sexa un subgrupo. E a resposta é afirmativa, pois cómpre ter en conta que a suma de puntos foi definida dun xeito puramente xeométrico.

A ecuación da curva elíptica permite definir varios conxuntos de puntos:

$$C(\mathbb{Q}) = \{(x, y) \in C \mid x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\},$$

$$C(\mathbb{R}) = \{(x, y) \in C \mid x, y \in \mathbb{R}\} \cup \{\mathcal{O}\},$$

$$C(\mathbb{C}) = \{(x, y) \in C \mid x, y \in \mathbb{C}\} \cup \{\mathcal{O}\}.$$

A lei de grupo que se definiu para os puntos racionais pode estenderse a estes conxuntos de puntos. Obsérvese que en todos eles se está introducindo o punto $\mathcal{O}$, que se establece como elemento neutro da suma.

En particular, tense unha cadea de grupos, $\{\mathcal{O}\} < C(\mathbb{Q}) < C(\mathbb{R}) < C(\mathbb{C})$. Así, para os casos anteriores:

- Se $m = 2$, tense que os puntos de $C(\mathbb{C})$ de orde 2 forman un grupo isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Entón, $C(\mathbb{Q})$ podería ser $\{\mathcal{O}\}$, $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- Se $m = 3$, tense que os puntos de orde 3 de $C(\mathbb{C})$ forman un grupo isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Entón, $C(\mathbb{Q})$ podería ser $\{\mathcal{O}\}$, $\mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Comezouse falando destes dous casos concretos. E que sucede, en xeral, para todo m? Vendo os resultados obtidos para $m = 2, 3$, semella lóxico pensar que isto se pode estender ás demais ordes finitas, de xeito que $C(\mathbb{C}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Pois ben, resulta que, efectivamente, sucede así, pero a demostración farase no capítulo seguinte, botando man das ferramentas que proporcionará a teoría de Galois.

É importante ter en conta que se pode definir a torsión sobre calquera corpo $\mathbb{K} \subset \mathbb{C}$. É dicir, pódense buscar puntos de torsión de calquera orde con coordenadas en calquera subcorpo de $\mathbb{C}$, de xeito que a lei de grupo é tamén extensible a $C(\mathbb{K})$, cumpríndose que $C(\mathbb{K}) < C(\mathbb{C})$.

En particular, ao poder traballar sempre coa forma normal de Weierstrass da curva elíptica, é posible realizar esta tarefa de maneira analítica, xa que se teñen descritas as coordenadas destes puntos. Se a curva elíptica é racional, estes puntos quedan determinados por polinomios con coeficientes racionais. Así, o corpo máis pequeno no que se atoparán as súas coordenadas é $\overline{\mathbb{Q}}$, a **clausura alxébrica** de $\mathbb{Q}$, i.e., o menor corpo formado por tódolos elementos alxébricos sobre $\mathbb{Q}$. Lémbrese que un elemento $\alpha \in \mathbb{C}$ é **alxébrico** sobre $\mathbb{Q}$ se existe algún polinomio non nulo $f \in \mathbb{Q}[X]$ tal que $f(\alpha) = 0$.

Capítulo 2

Corpos de números

2.1. Conceptos básicos de teoría de corpos

Lémbranse aquí certas definicións elementais da teoría de corpos:

Definición 2.1. Sexan $\mathbb{E}$ e $\mathbb{K}$ corpos. Dirase que $\mathbb{E}$ é unha **extensión** de $\mathbb{K}$, e denotarase $\mathbb{E} \mid \mathbb{K}$ ou $\mathbb{E} : \mathbb{K}$, se $\mathbb{K}$ é un subcorpo de $\mathbb{E}$.

Definición 2.2. Sexa $\mathbb{E} : \mathbb{K}$ unha extensión de corpos. Defínese o **grao da extensión**, denotado por $[\mathbb{E} : \mathbb{K}]$, como a dimensión de $\mathbb{E}$ como $\mathbb{K}$-espazo vectorial. Se a dimensión é finita, dirase que a extensión é **finita**.

No que resta do capítulo, traballarase con extensións nas cales $\mathbb{Q}$ será o corpo base, i.e., da forma $\mathbb{K} : \mathbb{Q}$. En particular, introdúcese:

Definición 2.3. Sexa $\mathbb{K} : \mathbb{Q}$ unha extensión de corpos. Dirase que $\mathbb{K}$ é un **corpo de números**, ou un **corpo numérico**, se a extensión é finita.

Para profundizar nos corpos numéricos, convén estudar o conxunto de homomorfismos da forma $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$. En particular, tense que o cardinal deste conxunto é, exactamente, o grao da extensión $\mathbb{K} : \mathbb{Q}$.
Dentro deste conxunto, existen homomorfismos tales que $\sigma_{\restriction_{\mathbb{K}}} = \mathrm{id}_{\mathbb{K}}$, i.e., automorfismos de $\mathbb{K}$. Estes automorfismos, coa composición usual de aplicacións, forman un grupo, denominado o **grupo de Galois da extensión**, que se denotará por $\mathrm{Gal}(\mathbb{K} : \mathbb{Q})$. Cando $|\mathrm{Gal}(\mathbb{K} : \mathbb{Q})| = [\mathbb{K} : \mathbb{Q}]$, dirase que esta é unha **extensión de Galois**.

Observación 2.4. Para construír un corpo numérico de Galois sobre $\mathbb{Q}$, abonda tomar un polinomio $f \in \mathbb{Q}[X]$ e considerar a súa factorización sobre $\mathbb{C}$, $f = c(X - \alpha_1) \cdot \cdots \cdot (X - \alpha_n)$. O seu corpo de escisión sobre $\mathbb{Q}$, $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, cumpre ser unha extensión finita de Galois. Reciprocamente, todo corpo numérico de Galois sobre $\mathbb{Q}$ resulta ser corpo de escisión dun polinomio $f \in \mathbb{Q}[X]$.

2.2. Extensións abelianas de $\mathbb{Q}$

Os grupos máis fáciles de estudar son os abelianos; por iso, resulta natural comezar co estudo daquelas extensións de Galois cuxo grupo de Galois sexa abeliano, i.e., as **extensións abelianas**.

Un exemplo moi sinxelo deste tipo de extensións son as extensións ciclotómicas xeradas por raíces primitivas da unidade. Cómpre definir a continuación estes dous conceptos:

Definición 2.5. Sexa $\mathbb{K} : \mathbb{Q}$ unha extensión de corpos. Dirase que a extensión é **ciclotómica** se $\mathbb{K} = \mathbb{Q}(\zeta)$, onde ζ é unha raíz m-ésima da unidade.

Definición 2.6. Sexa ζ unha raíz m-ésima da unidade. Dirase que ζ é unha raíz **primitiva m-ésima** se m é o menor enteiro positivo para o cal $\zeta^m = 1$.

Como xa se adiantou, tense:

Proposición 2.7. *O grupo de Galois dunha extensión ciclotómica é abeliano. Máis en particular, se ζ é unha raíz m-ésima primitiva da unidade, entón existe un isomorfismo de grupos*

$$t : \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$$

que está determinado por $\sigma(\zeta) = \zeta^{t(\sigma)}$.

Demostración. Sexa ζ unha raíz m-ésima primitiva da unidade, e considérese a extensión ciclotómica $\mathbb{Q}(\zeta) : \mathbb{Q}$. Cúmprese que tódalas potencias de ζ están contidas en $\mathbb{Q}(\zeta)$.

Sendo ζ raíz primitiva, m é o menor enteiro positivo para o cal $\zeta^m = 1$. Así, en particular, as demais raíces m-ésimas da unidade están tamén contidas en $\mathbb{Q}(\zeta)$. Entón, tense garantido que $\mathbb{Q}(\zeta)$ é o corpo de escisión do polinomio $X^m - 1$, e polo tanto, $\mathbb{Q}(\zeta) : \mathbb{Q}$ é unha extensión de Galois.

Un automorfismo $\sigma : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$ queda determinado de xeito único pola imaxe de ζ, $\sigma(\zeta)$, que tamén será unha raíz primitiva, xa que os homomorfismos de grupos preservan as ordes dos elementos. Ademais, cada raíz primitiva m-ésima da unidade é unha potencia de ζ; en concreto, é da forma ζ^t, onde t é coprimo con m. Así, obtense unha aplicación inxectiva entre conxuntos

$$t : \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$$

que queda completamente determinada da seguinte maneira:

$$\sigma(\zeta) = \zeta^{t(\sigma)} \quad \forall\, \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}).$$

Hai que demostrar agora que t é un homomorfismo de grupos. Dados $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$, tense:

$$\zeta^{t(\sigma\tau)} = \sigma\tau(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{t(\tau)}) = \sigma(\zeta)^{t(\tau)} = (\zeta^{t(\sigma)})^{t(\tau)} = \zeta^{t(\sigma)t(\tau)}.$$

Así, $t(\sigma\tau) \equiv t(\sigma)t(\tau) \pmod{m}$, e cúmprese que t é un monomorfismo (xa se demostrou o seu carácter inxectivo).

O primeiro teorema de isomorfía de grupos garante que

$$\frac{\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})}{\ker t} \simeq \mathrm{Im}\, t$$

e sendo t un monomorfismo, $\ker t = \{\mathrm{id}_{\mathbb{Q}(\zeta)}\}$; en particular, $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \simeq \mathrm{Im}\, t$, o que garante que $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ é un grupo abeliano.

Doutra banda, lémbrese que o grao da extensión $\mathbb{Q}(\zeta) : \mathbb{Q}$ é $\phi(m)$, sendo ϕ a función de Euler. En efecto, tense que o polinomio irreducible de ζ sobre $\mathbb{Q}$, $\mathrm{Irr}(\zeta, \mathbb{Q})$, é Φ_m, onde Φ_m é o polinomio ciclotómico de orde m, cuxo grao é, precisamente, $\phi(m)$. Deste xeito, e sabendo que a extensión é de Galois, $|\,\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})| = \phi(m)$, logo $|\,\mathrm{Im}\, t| = \phi(m)$. Agora ben, $\mathrm{Im}\, t < (\mathbb{Z}/m\mathbb{Z})^*$, e polo tanto, xa que posúen a mesma orde, $\mathrm{Im}\, t = (\mathbb{Z}/m\mathbb{Z})^*$, quedando probado que t é un isomorfismo de grupos. □

Considérese agora unha subextensión dun corpo ciclotómico, $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{Q}(\zeta)$. Segundo o teorema fundamental da teoría de Galois, cúmprese que a extensión $\mathbb{F} : \mathbb{Q}$ é de Galois cando, e só cando, $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{F})$ é un subgrupo normal de $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$. Agora ben, acábase de demostrar na proposición anterior que o grupo de Galois de $\mathbb{Q}(\zeta) : \mathbb{Q}$ é abeliano; entón, todo subgrupo seu será normal, e en particular $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{F})$. Así, a extensión $\mathbb{F} : \mathbb{Q}$ é de Galois, cumprídose ademais que

$$\frac{\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{F})} \simeq \mathrm{Gal}(\mathbb{F} : \mathbb{Q}).$$

É dicir, todo subcorpo dun corpo ciclotómico é unha extensión abeliana de Galois sobre $\mathbb{Q}$. E sorprendentemente, o recíproco tamén resulta ser certo:

Teorema 2.8 (Kronecker-Weber)**.** *Sexa $\mathbb{F}$ un corpo numérico de Galois sobre $\mathbb{Q}$. Supóñase que $\mathrm{Gal}(\mathbb{F} : \mathbb{Q})$ é abeliano. Entón, existe unha extensión ciclotómica $\mathbb{Q}(\zeta) : \mathbb{Q}$ tal que $\mathbb{F} \subset \mathbb{Q}(\zeta)$. É dicir, as extensións de Galois abelianas sobre $\mathbb{Q}$ son, precisamente, os subcorpos dos corpos ciclotómicos.*

Este teorema pode ser presentado doutro xeito facendo uso da análise complexa. Considérese a función exponencial:

$$f(z) = e^{2\pi i z}$$

e en particular a súa expansión en serie de Taylor:

$$f(z) = \sum_{k=0}^{\infty} \frac{(2\pi i z)^k}{k!}.$$

Esta función, en particular, é enteira en $\mathbb{C}$, i.e., holomorfa en todo punto do plano complexo. Se agora se avalía nos puntos da forma $z = 1/n$, obtense:

$$f\left(\frac{1}{n}\right) = e^{2\pi i/n} = \sum_{k=0}^{\infty} \frac{(2\pi i)^k}{n^k k!}.$$

É dicir, tense unha serie converxente a un certo número, que resulta ser raíz do polinomio $X^n - 1 \in \mathbb{Q}[X]$. Ademais, a extensión de $\mathbb{Q}$ xerada por $f(1/n)$ é de Galois, e posúe un grupo de Galois abeliano. E non só iso: calquera extensión abeliana de Galois sobre $\mathbb{Q}$ está contida nunha destas extensións.

Así, as extensións abelianas de $\mathbb{Q}$ poden describirse en termos de certos valores da función holomorfa $f(z) = e^{2\pi iz}$. Máis aínda, segundo a **Proposición 2.7**, cúmprese:

$$\sigma\left(f\left(\frac{1}{n}\right)\right) = f\left(\frac{t(\sigma)}{n}\right)$$

i.e., pódese describir como actúa cada automorfismo σ sobre $\zeta = f(1/n)$ en termos de f e t.

Toda a teoría que se desenvolveu neste capítulo xira en torno a extensións nas cales o corpo base é $\mathbb{Q}$. Entón, xorde de maneira natural a pregunta de se é posible estender estes resultados a outras extensións, nas cales o corpo base $\mathbb{F}$ varíe. E esta mesma pregunta fora xa formulada por Leopold Kronecker en 1880, nunha carta a Richard Dedekind. Kronecker chamoulle a este problema o seu **soño de xuventude** (*Jugendtraum*, en alemán).

En particular, Kronecker esperaba atopar unha función holomorfa $f(z)$ tal que, para calquera extensión de Galois abeliana $\mathbb{K} : \mathbb{F}$, existen certos valores $f(a_1), \dots, f(a_n)$ tales que o corpo $\mathbb{F}(f(a_1), \dots, f(a_n))$ xerado por estes valores é unha extensión de Galois abeliana, cumpríndose que $\mathbb{K}$ é subcorpo seu. Tamén desexaba que, para cada elemento σ do grupo de Galois de $\mathbb{F}(f(a_1), \dots, f(a_n)) : \mathbb{F}$, $\sigma(f(a_i))$ puidese ser descrito en termos de $f(z)$, para algún valor concreto de z, e a_i. Kronecker e os seus contemporáneos conseguiron estender esta teoría aos corpos cuadráticos, pero o problema segue aberto para o caso dun corpo numérico arbitrario.

2.3. Puntos alxébricos nas curvas elípticas

Considérese C unha curva elíptica racional en forma normal de Weierstrass, dada pola ecuación (1.3). No capítulo anterior definíronse os conxuntos de puntos $C(\mathbb{Q}), C(\mathbb{R})$ e $C(\mathbb{C})$; en particular, estudouse a estrutura dos conxuntos de puntos de ordes 2 e 3 en $C(\mathbb{C})$. Agora ben, como xa se adiantara, se $\mathbb{K} \subset \mathbb{C}$ é un subcorpo dos complexos, pódese considerar tamén o conxunto de puntos con coordenadas en $\mathbb{K}$,

$$C(\mathbb{K}) = \{(x, y) \in C \mid x, y \in \mathbb{K}\} \cup \{\mathcal{O}\}$$

onde $\mathcal{O}$ é o punto do infinito, considerado como o elemento neutro da lei de grupo.

É fácil decatarse, a partir das fórmulas da lei de adición en C, de que $C(\mathbb{K})$ é pechado coa suma de puntos, polo que é un subgrupo de $\mathbb{C}$.

Considérese $\mathbb{K}:\mathbb{Q}$ unha extensión de Galois. Entón, dados $P=(x,y)\in C(\mathbb{K})$ e $\sigma\in \mathrm{Gal}(\mathbb{K}:\mathbb{Q})$, defínese unha nova aplicación:

$$\sigma : P\in C \longmapsto \sigma(P) := \begin{cases} (\sigma(x),\sigma(y)) & \text{se } P\neq\mathcal{O} \\ \mathcal{O} & \text{se } P=\mathcal{O} \end{cases}$$

Esta aplicación resulta ser un endomorfismo de $C(\mathbb{K})$:

Proposición 2.9. *Sexa C unha curva elíptica racional. Considérese $\mathbb{K}:\mathbb{Q}$ unha extensión de Galois. Entón, verifícase:*

1. *O conxunto $C(\mathbb{K})$ é un subgrupo de $C(\mathbb{C})$.*
2. *$\sigma(P)\in C(\mathbb{K})\ \ \forall\, P\in C(\mathbb{K})$.*
3. *Para cada $P\in C(\mathbb{K})$ e cada $\sigma,\tau\in\mathrm{Gal}(\mathbb{K}:\mathbb{Q})$,*

   $$(\sigma\tau)(P)=\sigma(\tau(P)).$$

   Ademais, o elemento neutro $\mathrm{id}\in\mathrm{Gal}(\mathbb{K}:\mathbb{Q})$ actúa trivialmente, i.e., $\mathrm{id}(P)=P$.
4. *Para cada $P,Q\in C(\mathbb{K})$ e cada $\sigma\in\mathrm{Gal}(\mathbb{K}:\mathbb{Q})$,*

   $$\sigma(P+Q)=\sigma(P)+\sigma(Q) \qquad\qquad \sigma(-P)=-\sigma(P).$$

   En particular, $\sigma(nP)=n\cdot\sigma(P)\ \ \forall\, n\in\mathbb{Z}$.
5. *Se $P\in C(\mathbb{K})$ é un punto de orde n, entón, $\sigma(P)$ tamén é de orde n, $\ \forall\,\sigma\in\mathrm{Gal}(\mathbb{K}:\mathbb{Q})$.*

Demostración. 1. Dados $P_1,P_2\in C(\mathbb{K})$, as súas coordenadas están en $\mathbb{K}$. Observando as fórmulas explícitas para a lei de grupo, é inmediato ver que $P_1\pm P_2$ ten coordenadas en $\mathbb{K}$. Así, $C(\mathbb{K})$ é pechado para a suma, logo é un subgrupo de $C(\mathbb{C})$.

2. Dado $P=(x,y)\in C(\mathbb{K})$, sábese que $\sigma(x),\sigma(y)\in\mathbb{K}$. Así, só resta comprobar que $\sigma(P)\in C$. Xa que $\sigma\in\mathrm{Gal}(\mathbb{K}:\mathbb{Q})$:

$$\begin{aligned} P=(x,y)\in C(\mathbb{K}) &\overset{(1.3)}{\Longrightarrow} y^2-x^3-ax-b=0 \\ &\Longrightarrow \sigma(y^2-x^3-ax-b)=0 \\ &\Longrightarrow \sigma(y)^2=\sigma(x)^3+\sigma(a)\sigma(x)+\sigma(b) \\ &\Longrightarrow \sigma(y)^2=\sigma(x)^3+a\sigma(x)+b \\ &\Longrightarrow \sigma(P)\in C. \end{aligned}$$

3. $(\sigma\tau)(P) = ((\sigma\tau)(x), (\sigma\tau)(y)) = (\sigma(\tau(P)), \sigma(\tau(P))) = \sigma(\tau(P))$.

   Ademais, $\mathrm{id}(P) = (\mathrm{id}_{\mathbb{K}}(x), \mathrm{id}_{\mathbb{K}}(y)) = (x, y) = P$.

4. Sexa $\sigma \in \mathrm{Gal}(\mathbb{K} : \mathbb{Q})$ e $P = (x, y) \in C(\mathbb{K})$. Considerando a forma normal de Weierstrass de C, tense que $-P = (x, -y)$. Así:

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

   Sexa agora outro punto $Q \in C(\mathbb{K})$. Distinguiranse os seguintes casos para calcular $\sigma(P+Q)$:

   a) $P \neq \pm Q$

   Fágase $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P+Q = (x_3, y_3)$. Lembrando as fórmulas explícitas para a suma de puntos, (1.5) e (1.6), tense:

$$\sigma(x_3) = \sigma(m^2 - x_1 - x_2) = \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}\right)^2 - \sigma(x_1) - \sigma(x_2)$$

$$\sigma(y_3) = \sigma(mx_3 + n) = \sigma(m(x_3 - x_1) + y_1) = \frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}(\sigma(x_3) - \sigma(x_1)) + \sigma(y_1).$$

   Obsérvase que as coordenadas de $\sigma(P + Q)$ se poden obter aplicando as fórmulas da lei de grupo a $\sigma(P) + \sigma(Q)$. Así, efectivamente, $\sigma(P + Q) = \sigma(P) + \sigma(Q)$.

   b) $P = Q$

   Para esta situación, hai que botar man da fórmula da duplicación, (1.7). Mediante un razoamento análogo ao caso anterior, aplicando σ sobre as coordenadas de $2P$, obtense:

$$\sigma(x_3) = \sigma\left(\frac{(x_1)^4 - 14a(x_1)^2 - 8bx_1 + a^2}{4(x_1)^3 + 4ax_1 + 4b}\right) = \frac{\sigma(x_1)^4 - 14a\sigma(x_1)^2 - 8b\sigma(x_1) + a^2}{4\sigma(x_1)^3 + 4a\sigma(x_1) + 4b}.$$

   É dicir, a abscisa de $\sigma(x_3)$ pódese obter aplicando a fórmula da duplicación sobre a abscisa de $\sigma(P)$. Procedendo do mesmo xeito coa ordenada, tense o resultado.

   c) $P = -Q$

   Este caso é inmediato, pois:

$$\sigma(P + Q) = \sigma(P - P) = \sigma(\mathcal{O}) = \mathcal{O}$$
$$\sigma(P) + \sigma(Q) = \sigma(P) + \sigma(-P) = \sigma(P) - \sigma(P) = \mathcal{O}.$$

   Finalmente, para probar que $\sigma(nP) = n\sigma(P)\ \forall\ n \in \mathbb{Z}$, pódese facer un razoamento indutivo no caso $n \geq 1$, e unha vez probado isto, aplicar a propiedade $\sigma(-P) = -\sigma(P)$ para garantir que tamén se cumpre para os enteiros negativos. O caso $n = 0$ é trivial.

5. Considérese P un punto de orde n, i.e., $nP = \mathcal{O}$. Denótese por m a orde de $\sigma(P)$. Botando man do apartado anterior, tense que:

$$\mathcal{O} = \sigma(nP) = n\sigma(P) \implies m|n.$$

Reciprocamente, sendo σ un automorfismo, e sabendo que $m\sigma(P) = \mathcal{O}$, chégase a que:

$$\mathcal{O} = \sigma^{-1}(\mathcal{O}) = \sigma^{-1}(m\sigma(P)) = m\sigma^{-1}(\sigma(P)) = mP \implies n|m.$$

Xuntando os dous resultados, conclúese que $m = n$. □

No apartado anterior, definiuse un corpo ciclotómico como o corpo de escisión sobre $\mathbb{Q}$ dun polinomio $X^n - 1$. Para intentar evidenciar a analoxía coas curvas elípticas, vaise reformular esta condición do seguinte xeito.

Considérese o grupo multiplicativo dos complexos non nulos, $(\mathbb{C}^*, \cdot)$. Para cada $n \in \mathbb{Z}$, a m-ésima potencia proporciona un endomorfismo de $\mathbb{C}^*$:

$$\lambda_m : z \in \mathbb{C}^* \longmapsto \lambda_m(z) := z^m.$$

O núcleo deste endomorfismo, $\ker \lambda_m$, é o conxunto de raíces m-ésimas da unidade. Así, un corpo ciclotómico é xerado sobre $\mathbb{Q}$ polos elementos do núcleo dun certo endomorfismo λ_m.

Sexa agora o grupo aditivo dos puntos con coordenadas complexas dunha curva elíptica C, $(C(\mathbb{C}), +)$. Pódese definir un endomorfismo análogo ao anterior, consistente na multiplicación m-ésima de puntos:

$$\lambda_m : P \in C(\mathbb{C}) \longmapsto \lambda_m(P) := mP.$$

O núcleo de λ_m é un subgrupo de $C(\mathbb{C})$, que se denotará por

$$C[m] = \ker \lambda_m = \{P \in \mathbb{C} \mid mP = \mathcal{O}\}.$$

Obsérvese que este conxunto é, precisamente, a m-torsión da curva elíptica C.

Proposición 2.10. *$C[m]$ é suma directa de dous grupos cíclicos de orde m:*

$$C[m] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Demostración. Dados dous complexos $\omega_1, \omega_2 \in \mathbb{C}$, pódese considerar o retículo que xeran, i.e., o conxunto de tódalas súas combinacións lineares con coeficientes enteiros:

$$L = \{m_1\omega_1 + m_2\omega_2 \mid m_1, m_2 \in \mathbb{Z}\}.$$

É posible construír un isomorfismo de grupos entre $C(\mathbb{C})$ e $\mathbb{C}/L$, tal e como se recolle en [6]. Deste xeito, os puntos de $C[m]$ pódense caracterizar como segue:

$$z \in C[m] \iff mz \in L.$$

Esta descrición proporciona un isomorfismo de grupos, que se define a continuación:

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} &\longrightarrow C[m] \subset \mathbb{C}/L \\ (a_1, a_2) &\longmapsto \frac{a_1}{m}\omega_1 + \frac{a_2}{m}\omega_2 \end{aligned}$$

o que completa a proba. □

Como se acaba de comprobar, as extensións ciclotómicas están xeradas polos elementos do núcleo do endomorfismo da m-ésima potencia. Analogamente, quérense considerar as extensións xeradas polos puntos en $C[m]$. En particular, pódese estudar o corpo xerado polas coordenadas destes puntos:

Proposición 2.11. *Sexa C unha curva elíptica racional dada pola ecuación de Weierstrass* (1.3)*. Cúmprese:*

1. *Sexa $P = (x, y) \in C[m]$ un punto con orde divisor de m. Entón, x e y son alxébricos sobre $\mathbb{Q}$, i.e., son raíces dun polinomio non nulo de $\mathbb{Q}[X]$.*

2. *Sexa o conxunto de puntos de $C(\mathbb{C})$ con orde divisor de m,*

$$C[m] = \{(x_1, y_1), \dots, (x_n, y_n), \mathcal{O}\}$$

*onde $n = m^2 - 1$, segundo a **Proposición 2.10**. Considérese o corpo xerado polas coordenadas de tódolos puntos de $C[m]$,*

$$\mathbb{K} = \mathbb{Q}(x_1, y_1, \dots, x_n, y_n).$$

Entón, $\mathbb{K} : \mathbb{Q}$ é unha extensión de Galois.

Demostración. Sexa $\sigma : \mathbb{K} \longrightarrow \mathbb{C}$ un homomorfismo de corpos. Para demostrar que $\mathbb{K} : \mathbb{Q}$ é unha extensión de Galois, hai que comprobar que $\sigma(\mathbb{K}) = \mathbb{K}$.

A aplicación σ queda completamente determinada polas imaxes dos distintos x_i e y_i. Por hipótese, $P_i \in C[m]\ \forall\, i \in \{1, \dots, n\}$, e a **Proposición 2.9** garante que $\sigma(P_i) \in C[m]$. É dicir, $\sigma(P_i) = P_j$, con i e j podendo ser iguais. Sendo isto certo para todo $i \in \{1, \dots, n\}$, garántese que $\sigma(\mathbb{K}) = \mathbb{K}$. Así, tense que $\mathbb{K} : \mathbb{Q}$ é unha extensión de Galois, deixando demostrado o segundo punto.

Pódese reformular o que se fixo no parágrafo anterior do seguinte xeito: cada homomorfismo de corpos $\sigma : \mathbb{K} \longrightarrow \mathbb{C}$ queda determinado por unha permutación dos puntos $P_1, \dots, P_n$. En particular, isto significa que o conxunto de tales homomorfismos é finito; noutras palabras, $\mathbb{K} : \mathbb{Q}$ é unha extensión finita, e polo tanto, alxébrica. Así, tódolos x_i e y_i son alxébricos sobre $\mathbb{Q}$, quedando probado o primeiro punto. □

Observación 2.12. En xeral, o grupo de Galois da extensión anterior non é abeliano.

2.4. Un exemplo: o grupo da circunferencia

Para repasar os conceptos que se viron ata agora, considérese o seguinte exemplo. Na circunferencia $\mathbb{S}^1$ pódese definir un grupo coa seguinte operación:

$$\mathbb{S}^1 \times \mathbb{S}^1 \longrightarrow \mathbb{S}^1$$
$$(\alpha, \beta) \rightsquigarrow \alpha + \beta \mod 2\pi$$

onde os puntos de orde finita son as raíces da unidade. En efecto, a $m-$torsión está composta polos puntos da forma:

$$m\alpha = 2k\pi \iff \alpha = \frac{2k\pi}{m} \quad 0 \leq k < m$$

e compoñen un subgrupo cíclico de orde m.

A continuación, pódese considerar, para cada raíz da unidade, a extensión xerada polas súas coordenadas, i.e.,

$$\mathbb{Q}(\cos(2k\pi/m),\ \text{sen}(2k\pi/m)) \qquad 0 \leq k < m.$$

Obsérvese que tódolos ángulos considerados son múltiplos de $2\pi/m$. En particular, a fórmula de De Moivre permite expresar o seno e o coseno de calquera múltiplo dun ángulo en función do seno e o coseno deste. Polo tanto, tense:

$$\cos(2k\pi/m),\ \text{sen}(2k\pi/m) \ \in\ \mathbb{Q}(\cos(2\pi/m),\ \text{sen}(2\pi/m))$$

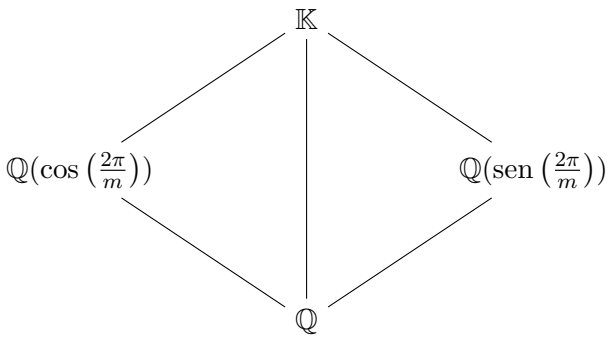
é dicir, a extensión xerada polas coordenadas de $2\pi/m$ contén as coordenadas das demais raíces m-ésimas da unidade.

En consecuencia, considerando a extensión das coordenadas dos puntos da m-torsión, $\mathbb{K}$, mencionada na **Proposición 2.11**, tense

$$\mathbb{K} = \mathbb{Q}(\cos(2\pi/m),\ \text{sen}(2\pi/m))$$

e sábese que é unha extensión de Galois sobre $\mathbb{Q}$.

Tense así o seguinte diagrama:

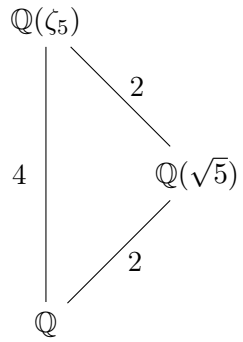


Estudaranse un pouco máis polo miúdo as extensións intermedias do seno e o coseno, intentando relacionalas coa extensión ciclotomica $\mathbb{Q}(\zeta_m)$, onde $\zeta_m = e^{\frac{2\pi i}{m}}$. Para iso, comezarase dando un par de exemplos concretos, a partir dos cales se establecerá unha xeneralización para calquera valor de m.

Cando $m = 5$, segundo se viu na **Proposición 2.7**, o grao da extensión $\mathbb{Q}(\zeta_5) : \mathbb{Q}$ é 4. Necesariamente, $\cos(2\pi/5) \in \mathbb{Q}(\zeta_5)$, xa que

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\zeta_5 + \zeta_5^{-1}}{2} = \frac{1+\sqrt{5}}{4}.$$

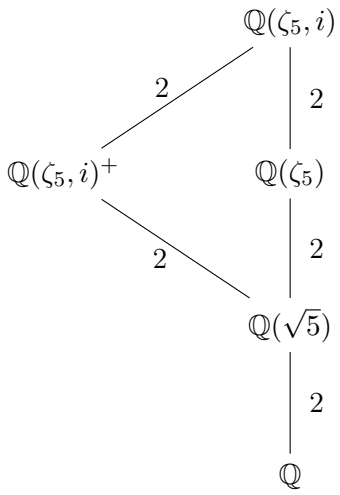
Máis aínda: está na maior subextensión contida en $\mathbb{R}$, que será denotada por $\mathbb{Q}(\zeta_5)^+$. Neste caso, tal extensión resulta ser $\mathbb{Q}(\sqrt{5})$, obtendo a torre de corpos



Doutra banda,

$$\operatorname{sen}\left(\frac{2\pi}{5}\right) = \frac{\zeta_5 - \zeta_5^{-1}}{2i}$$

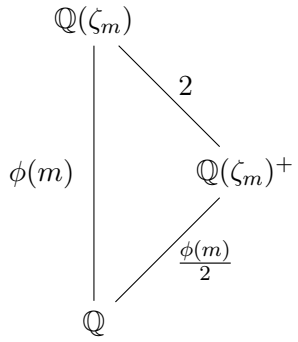
polo que se garante que $\operatorname{sen}(2\pi/5) \in \mathbb{Q}(\zeta_5, i)$. De xeito análogo, sábese que ten que estar na maior subextensión contida en $\mathbb{R}$, $\mathbb{Q}(\zeta_5, i)^+$. De feito, sendo $\operatorname{Irr}(\operatorname{sen}(2\pi/5), \mathbb{Q}) = X^4 - \frac{5}{4}X^2 + \frac{5}{16}$, tense que pertence a unha extensión de $\mathbb{Q}$ de grao 4, aínda que neste caso é diferente de $\mathbb{Q}(\zeta_5)$. A torre de corpos neste caso é a seguinte:



Analogamente, no caso $m = 6$ sucede algo semellante. Aquí, de novo segundo a **Proposición 2.7**, $[\mathbb{Q}(\zeta_6) : \mathbb{Q}] = 2$, xa que $(\mathbb{Z}/6\mathbb{Z})^* = \{[1], [5]\}$.

Vólvese cumprir que $\cos(2\pi/6) \in \mathbb{Q}(\zeta_6)^+$ e $\operatorname{sen}(2\pi/6) \in \mathbb{Q}(\zeta_6, i)^+$, aínda que neste caso, $\mathbb{Q}(\zeta_6)^+ = \mathbb{Q}$ e $\mathbb{Q}(\zeta_6, i)^+$ ten grao 2, sendo diferente de $\mathbb{Q}(\zeta_6)$.

Que sucede entón no caso xeral? Sexa ζ_m unha raíz primitiva da unidade, e considérese o corpo ciclotómico $\mathbb{Q}(\zeta_m)$. O seu grupo de Galois é isomorfo a $(\mathbb{Z}/m\mathbb{Z})^*$. Lémbrese que as unidades de $\mathbb{Z}/m\mathbb{Z}$ son aqueles x tales que $\operatorname{mcd}(x, m) = 1$. Entón, $|\operatorname{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q})| = \phi(m)$, onde ϕ é a función de Euler. Tense así a torre de corpos:



Facendo agora $X = \zeta_m$, tense:

$$\cos(2\pi/m) = \frac{1}{2}\left(X + \frac{1}{X}\right) \iff X^2 - 2\cos(2\pi/m)X + 1 = 0$$

e polo tanto:

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\cos(2\pi/m))] = 2.$$

Como $\cos(2\pi/m) \in \mathbb{Q}(\zeta_m)^+$, e o grao da extensión $\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)^+$ é 2, tense que $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\cos(2\pi/m))$.

Por outra parte, de xeito completamente análogo aos exemplos anteriores, tense garantido que $\operatorname{sen}(2\pi/m) \in \mathbb{Q}(\zeta_m, i)$.

Cúmprese que $i \in \mathbb{Q}(\zeta_m) \iff m$ é múltiplo de 4. En efecto:

($\Longrightarrow$) Supóñase que $i \in \mathbb{Q}(\zeta_m)$. Entón, para certo $0 \leq k < m$,

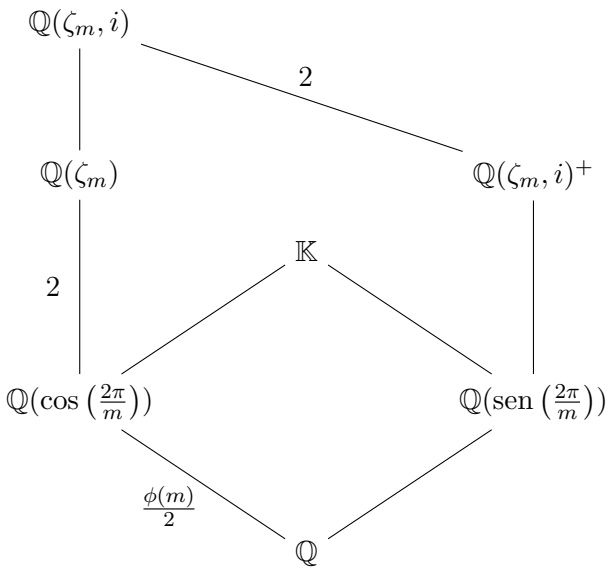
$$\left.\begin{array}{l} \cos\left(\frac{2k\pi}{m}\right) = 0 \\ \operatorname{sen}\left(\frac{2k\pi}{m}\right) = 1 \end{array}\right\} \implies \frac{2k\pi}{m} = \frac{\pi}{2} \iff m = 4k.$$

($\Longleftarrow$) Reciprocamente, supóñase que $m = 4k$ para certo $k \in \mathbb{Z}$. Entón:

$$\zeta_m^m = 1 \iff (\zeta_m^k)^4 = 1.$$

Logo ζ_m^k é raíz cuarta da unidade, e así, garántese que $i \in \mathbb{Q}(\zeta_m)$.

En calquera caso, xeralmente tense o seguinte diagrama:



Considerando $\mathbb{S}^1$ como un subgrupo de $\mathbb{C}$, os puntos de m-torsión resultan ser as raíces m-ésimas da unidade, que están definidas sobre o corpo $\mathbb{Q}(\zeta_m)$. Como actúa o grupo de Galois sobre elas?

Lembrando a **Proposición 2.7**, tense un isomorfismo de grupos

$$t : \text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*.$$

Así, dado $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q})$, a súa acción sobre o conxunto de raíces m-ésimas da unidade $\{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}$ vén determinada polo número $t(\sigma)$. Coñecendo o valor de $\zeta_m^{t(\sigma)}$, é posible determinar a imaxe de calquera potencia de ζ_m.

E cal é a relación deste exemplo coas curvas elípticas?

Lémbrese a m-torsión das curvas elípticas, $C[m]$. Tomando as coordenadas destes puntos, pódese considerar a extensión que xeran sobre $\mathbb{Q}$, recollida na **Proposición 2.11**. No seguinte capítulo, estudarase como actúa o grupo de Galois desta extensión sobre $C[m]$, permitindo dar unha representación do mesmo, de xeito análogo á que se ten dado para as extensións ciclotómicas.

Capítulo 3

Representacións de Galois

A m-torsión dunha curva elíptica C, $C[m]$, tense definida como o conxunto de puntos con orde un divisor de m:

$$C[m] = \{\mathcal{O}, (x_1, y_1), \dots, (x_n, y_n)\}.$$

No capítulo anterior introduciuse a extensión de $\mathbb{Q}$ xerada polas coordenadas dos puntos de $C[m]$, $\mathbb{Q}(x_1, y_1, \dots, x_n, y_n)$.

Definición 3.1. O corpo anterior, que será denotado por $\mathbb{Q}(C[m])$, recibe o nome de **corpo de definición de** $C[m]$ **sobre** $\mathbb{Q}$:

$$\mathbb{Q}(C[m]) = \mathbb{Q}(x_1, y_1, \dots, x_n, y_n).$$

Observación 3.2. Se se cambia o corpo base $\mathbb{F}$, empregarase igualmente a notación $\mathbb{F}(C[m])$.

Tense demostrado, na **Proposición 2.11**, que este corpo é unha extensión de Galois sobre $\mathbb{Q}$. En particular, isto implica

$$[\mathbb{Q}(C[m]) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q})|.$$

Como describir o grupo de Galois desta extensión?

Sexa $\sigma \in \operatorname{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q})$, e considérese $P \in C[m]$. Segundo a **Proposición 2.9**, σ define un endomorfismo de $C(\mathbb{Q}(C[m]))$ (é dicir, o conxunto de puntos da curva con coordenadas en $\mathbb{Q}(C[m])$) tal que preserva as ordes dos puntos; en particular, tense que $\sigma(P) \in C[m]$.

É dicir, cada $\sigma \in \operatorname{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q})$ induce unha permutación dos elementos de $C[m]$. Non obstante, esta permutación non é completamente arbitraria. En efecto, non é máis cá restrición do endomorfismo anterior a este grupo, que como se probou na **Proposición 2.10**, é isomorfo a $(\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$. En particular, $C[m]$ está xerado por dous puntos P_1 e P_2, proporcionando a seguinte descrición:

$$C[m] = \{a_1P_1 + a_2P_2 \mid a_1, a_2 \in \mathbb{Z}/m\mathbb{Z}\}.$$

Considérese h un endormorfismo arbitrario de $C[m]$. Entón, tense que cumprir

$$h(a_1P_1 + a_2P_2) = a_1h(P_1) + a_2h(P_2).$$

É dicir, a imaxe de calquera endomorfismo de $C[m]$ queda completamente determinada pola imaxe dunha base súa. Reciprocamente, dados $Q_1, Q_2 \in C[m]$, pódese definir un endomorfismo

$$a_1P_1 + a_2P_2 \mapsto a_1Q_1 + a_2Q_2.$$

En consecuencia, h queda definido a través de $h(P_1)$ e $h(P_2)$. Máis aínda, $h(P_1), h(P_2) \in C[m]$, logo poden escribirse como combinacións lineares de P_1 e P_2:

$$h(P_1) = \alpha_h P_1 + \gamma_h P_2 \tag{3.1}$$
$$h(P_2) = \beta_h P_1 + \delta_h P_2 \tag{3.2}$$

onde os coeficientes $\alpha_h, \beta_h, \gamma_h, \delta_h \in \mathbb{Z}/m\mathbb{Z}$ dependen unicamente do endomorfismo h.

As relacións anteriores poden escribirse en notación matricial do seguinte xeito:

$$\begin{bmatrix} h(P_1) & h(P_2) \end{bmatrix} = \begin{bmatrix} P_1 & P_2 \end{bmatrix} \begin{bmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{bmatrix}.$$

En particular, tense que a cada endormorfismo $h : C[m] \longrightarrow C[m]$ se lle pode asignar unha matriz cadrada $A \in \mathcal{M}_2(\mathbb{Z}/m\mathbb{Z})$.

Sexa agora $g : C[m] \longrightarrow C[m]$ outro endomorfismo de $C[m]$. Entón, é posible considerar a composición $g \circ h$. Cal é a matriz de coeficientes para este novo endomorfismo?

$$\begin{bmatrix} (g \circ h)(P_1) & (g \circ h)(P_2) \end{bmatrix} = \begin{bmatrix} P_1 & P_2 \end{bmatrix} \begin{bmatrix} \alpha_{g\circ h} & \beta_{g\circ h} \\ \gamma_{g\circ h} & \delta_{g\circ h} \end{bmatrix}.$$

Facendo o cálculo, obtense o seguinte:

$$\begin{aligned} \alpha_{g\circ h}P_1 + \gamma_{g\circ h}P_2 &= (g \circ h)(P_1) = g(h(P_1)) \\ &= g(\alpha_h P_1 + \gamma_h P_2) \\ &= \alpha_h g(P_1) + \gamma_h g(P_2) \\ &= \alpha_h(\alpha_g P_1 + \gamma_g P_2) + \gamma_h(\beta_g P_1 + \delta_g P_2) \\ &= (\alpha_g\alpha_h + \beta_g\gamma_h)P_1 + (\gamma_g\alpha_h + \delta_g\gamma_h)P_2. \end{aligned}$$

En resumo, chégase a que

$$\alpha_{g\circ h} = \alpha_g\alpha_h + \beta_g\gamma_h \tag{3.3}$$
$$\gamma_{g\circ h} = \gamma_g\alpha_h + \delta_g\gamma_h. \tag{3.4}$$

Mediante un razoamento análogo para $(g \circ h)(P_2)$, obtense que:

$$\beta_{g\circ h} = \alpha_g\beta_h + \beta_g\delta_h \tag{3.5}$$

$$\delta_{g\circ h} = \gamma_g\beta_h + \delta_g\delta_h. \tag{3.6}$$

Polo tanto,

$$\begin{bmatrix}(g\circ h)(P_1) & (g\circ h)(P_2)\end{bmatrix} = \begin{bmatrix}P_1 & P_2\end{bmatrix}\begin{bmatrix}\alpha_g\alpha_h + \beta_g\gamma_h & \alpha_g\beta_h + \beta_g\delta_h \\ \gamma_g\alpha_h + \delta_g\gamma_h & \gamma_g\beta_h + \delta_g\delta_h\end{bmatrix}$$

é dicir, a matriz da composición resulta ser o produto das matrices dos dous endomorfismos:

$$\begin{bmatrix}\alpha_{g\circ h} & \beta_{g\circ h} \\ \gamma_{g\circ h} & \delta_{g\circ h}\end{bmatrix} = \begin{bmatrix}\alpha_g & \beta_g \\ \gamma_g & \delta_g\end{bmatrix}\begin{bmatrix}\alpha_h & \beta_h \\ \gamma_h & \delta_h\end{bmatrix}.$$

Ata este momento estívose falando de endomorfismos arbitrarios de $C[m]$. E pódese ver que se estableceron analoxías coa álxebra linear: existe unha bixección entre endomorfismos e matrices cadradas, e a matriz da composición correspóndese co produto das respectivas matrices. Entón, é natural pensar se existen máis semellanzas; por exemplo, que sucede cos isomorfismos? Existe unha matriz inversa?

Sexa así h un isomorfismo, e $g = h^{-1}$ o seu inverso. En particular, cúmprese que $g \circ h = \mathrm{id}_{C[m]}$, e como se acaba de ver, isto implica, matricialmente:

$$\begin{bmatrix}1 & 0 \\ 0 & 1\end{bmatrix} = \begin{bmatrix}\alpha_{h^{-1}} & \beta_{h^{-1}} \\ \gamma_{h^{-1}} & \delta_{h^{-1}}\end{bmatrix}\begin{bmatrix}\alpha_h & \beta_h \\ \gamma_h & \delta_h\end{bmatrix}$$

isto é, a matriz de h é, efectivamente, inversible. E reciprocamente, cada matriz inversible, con coeficientes en $\mathbb{Z}/m\mathbb{Z}$, proporciona un automorfismo de $C[m]$.

Definición 3.3. O **grupo linear xeral**, denotado por $\mathrm{GL}_n(R)$, é o grupo de matrices inversibles de orde $n \in \mathbb{Z}^+$ con coeficientes nun certo anel R coa operación de multiplicación:

$$\mathrm{GL}_n(R) = \{A \in \mathcal{M}_n(R) \mid \det(A) \in R^*\}.$$

Cómpre recordar o seguinte resultado:

Lema 3.4. *Sexan R un anel, $n \in \mathbb{Z}^+$ e $A \in \mathcal{M}_n(R)$. Verifícase:*

$$A \in \mathrm{GL}_n(R) \iff \det(A) \in R^*.$$

Demostración. ($\Longrightarrow$) Supóñase que existe a matriz A^{-1}, de tal xeito que $AA^{-1} = I_n$. Entón, aplicando as propiedades dos determinantes, obtense:

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(A)\det(A)^{-1} \implies \det(A) \in R^*.$$

($\Longleftarrow$) A proba que aquí se dá só é válida para o caso $n = 2$. Aínda que a proba do caso xeral non é complexa, no que resta do capítulo só se vai traballar con matrices de orde 2, e ademais, esta proba dá unha forma explícita de obter a matriz inversa.

Supóñase así $A \in \mathcal{M}_2(R)$, asociada a un certo isomorfismo h, tal que $\Delta = \det(A) \in R^*$. A partir das ecuacións (3.3), (3.4), (3.5) e (3.6), obtéñense dous sistemas de dúas ecuacións lineares con dúas incógnitas:

$$\begin{cases} \alpha_h\alpha_{h^{-1}} + \gamma_h\beta_{h^{-1}} = 1 \\ \beta_h\alpha_{h^{-1}} + \delta_h\beta_{h^{-1}} = 0 \end{cases} \qquad \begin{cases} \alpha_h\gamma_{h^{-1}} + \gamma_h\delta_{h^{-1}} = 0 \\ \beta_h\gamma_{h^{-1}} + \delta_h\delta_{h^{-1}} = 1 \end{cases}$$

onde os coeficientes da matriz A, α_h, β_h, γ_h, δ_h, son coñecidos, sendo as incógnitas os coeficientes da matriz A^{-1}, asociada ao isomorfismo h^{-1}.

Resolvendo os sistemas anteriores, aplicando por exemplo o método de redución, chégase a que, efectivamente, A posúe matriz inversa, e pode calcularse como segue:

$$A^{-1} = \begin{bmatrix} \delta_h/\Delta & -\beta_h/\Delta \\ -\gamma_h/\Delta & \alpha_h/\Delta \end{bmatrix}.$$

□

Retomando agora o corpo de definición de $C[m]$ sobre $\mathbb{Q}$, $Q(C[m])$, considérese de novo o seu grupo de Galois. Cada elemento σ é un automorfismo deste corpo, que á súa vez induce un automorfismo no conxunto de puntos de C con coordenadas en $\mathbb{Q}(C[m])$,

$$\sigma : C(\mathbb{Q}(C[m])) \longrightarrow C(\mathbb{Q}(C[m])).$$

Tense probado que a m-torsión da curva é un subgurpo de $C(\mathbb{Q}(C[m]))$; logo, a restrición de σ a $C[m]$ tamén é un automorfismo de grupos. Entón, como se viu neste capítulo, a σ pódeselle asignar unha matriz $A_\sigma \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Esquematicamente, tense o seguinte:

$$\begin{array}{ccccc} \mathrm{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q}) & \longrightarrow & \mathrm{Aut}(C[m]) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma & \longmapsto & \sigma & \longmapsto & A_\sigma \end{array}$$

É dicir, tense unha aplicación:

$$\begin{aligned} \rho_m : \mathrm{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q}) &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\longmapsto A_\sigma \end{aligned}$$

con $A_\sigma = \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix}$. Lémbrese que os seus coeficientes quedan determinados polas fórmulas

$$\begin{aligned} \sigma(P_1) &= \alpha_\sigma P_1 + \gamma_\sigma P_2 \\ \sigma(P_2) &= \beta_\sigma P_1 + \delta_\sigma P_2. \end{aligned}$$

Como se demostrou anteriormente, a matriz da composición de endomorfismos de $C[m]$ pódese calcular como o produto das respectivas matrices de cada endomorfismo. Así, cúmprese:

$$\rho_m(\sigma\tau) = \rho_m(\sigma)\rho_m(\tau) \quad \forall\, \sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q}).$$

É dicir, ρ_m é un homomorfismo do grupo de Galois da extensión $\mathbb{Q}(C[m]) : \mathbb{Q}$, máis abstracto e descoñecido, ao grupo linear xeral $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, moito máis estudado e do que se coñece a súa estrutura concreta. Así, o que se ten é unha **representación** deste grupo. Ao tratarse dun grupo de Galois, en particular dirase que esta é unha **representación de Galois**.

Todo o desenvolvemento que se ten feito ata agora aparece recollido no seguinte teorema:

Teorema 3.5 (Representacións de Galois)**.** *Sexa C unha curva elíptica racional en forma normal de Weierstrass. Considérese $n \in \mathbb{Z}, n \geq 2$. Fíxense P_1 e P_2 dous xeradores da m-torsión da curva, $C[m]$. Entón, a aplicación*

$$\begin{aligned} \rho_m : \mathrm{Gal}(\mathbb{Q}(C[m]) : \mathbb{Q}) &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\longmapsto A_\sigma \end{aligned}$$

é un monomorfismo de grupos.

Demostración. O único que resta por probar é o carácter inxectivo de ρ_m. Sabendo xa que é un homomorfismo, verase que o seu núcleo é o conxunto formado polo automorfismo identidade.

Considérese así $\sigma \in \ker \rho_m$, e véxase que $\sigma = \mathrm{id}_{\mathbb{Q}(C[m])}$. En particular, cúmprese que

$$\rho_m(\sigma) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Polo tanto, aplicando as ecuacións (3.1) e (3.2), tense:

$$\left.\begin{aligned} \sigma(P_1) &= P_1 \\ \sigma(P_2) &= P_2 \end{aligned}\right\} \implies \sigma(P) = P \ \ \forall\, P \in C[m].$$

Lémbrese que, se $P = (x, y)$, por definición, $\sigma(P) = \sigma(x, y) = (\sigma(x), \sigma(y))$, i.e., σ fixa as coordenadas dos puntos de $C[m]$. En particular, xa que $\mathbb{Q}(C[m]) = \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n)$, σ fixa os xeradores da extensión, e polo tanto, o corpo enteiro. Logo, necesariamente, $\sigma = \mathrm{id}_{\mathbb{Q}(C[m])}$, e efectivamente, ρ_m é un monomorfismo. □

Obsérvese que se ten unha analoxía coas extensións ciclotómicas: sexa $\zeta \in \mathbb{C}^*$ un xerador do grupo de raíces m-ésimas da unidade. Segundo a **Proposición 2.7**, tense un isomorfismo

$$t : \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \longrightarrow \mathrm{GL}_1(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^*$$

determinado pola relación $\sigma(\zeta) = \zeta^{t(\sigma)}$. Dise neste caso que t é unha **representación ciclotómica m-ésima de $\mathbb{Q}$**. Ademais, xa que é un isomorfismo, en particular sábese que

$$\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*.$$

No caso das representacións de Galois, o homomorfismo ρ_m non é sobrexectivo en xeral. Porén, xa que se busca construír extensións abelianas de $\mathbb{Q}$, isto non é un problema; ao contrario, $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ non é abeliano para $n \geq 2$; logo, de ser ρ_m un isomorfismo, a extensión xa non posúe un grupo de Galois abeliano. Para a maioría das curvas elípticas, sempre existen valores de m para os cales a representación de Galois ρ_m é sobrexectiva. Non obstante, e xa que interesa estudar extensións de $\mathbb{Q}$ abelianas, a atención vai centrarse naquelas curvas para as cales ρ_m nunca é un isomorfismo: as curvas con *multiplicación complexa*.

Capítulo 4

A multiplicación complexa

Dada unha curva elíptica C, sábese que o conxunto dos seus puntos con coordenadas complexas, $C(\mathbb{C})$, forma un grupo abeliano coa suma de puntos. Como tal, para cada $m \in \mathbb{Z}$, é posible definir un endomorfismo, a *multiplicación por* m,

$$\begin{aligned} \lambda_m : C(\mathbb{C}) &\longrightarrow C(\mathbb{C}) \\ P &\longmapsto mP \end{aligned}$$

tal que $\ker \lambda_m = C[m]$.

Tense visto, no primeiro capítulo, que escribindo a curva C en forma normal de Weierstrass, (1.3), é posible dar fórmulas explícitas para a lei de grupo, (1.6) e (1.7); ademais, estas fórmulas veñen dadas por funcións racionais, i.e., cocientes de polinomios.

Definición 4.1. Sexan C_1, C_2 dúas curvas elípticas entre as cales se establece unha aplicación $\phi : C_1 \longrightarrow C_2$. Dirase que ϕ é un **morfismo de curvas** se vén dada por funcións racionais.

Definición 4.2. Sexa $\phi : C_1 \longrightarrow C_2$ un morfismo de curvas elípticas. Dirase que ϕ é un **homomorfismo de grupos** se ϕ respecta a estrutura de grupo das curvas. En particular, cando $C_1 = C_2$, dáselle o nome de **endomorfismo**.

En particular, para cada $m \in \mathbb{Z}$, a multiplicación por m é un endomorfismo de C. Agora ben, cómpre preguntarse: *existen outros endomorfismos*?

Definición 4.3. Sexa C unha curva elíptica. Dise que C posúe **multiplicación complexa** se admite outros endomorfismos distintos da multiplicación por m.

A continuación introdúcense un par de exemplos de curvas que posúen esta propiedade:

1. A curva $y^2 = x^3 + x$ admite o seguinte endomorfismo:

$$(x, y) \longmapsto (-x, iy)$$

2. Para cada $a \in \mathbb{Q}$, a curva $y^2 = x^3 + a$ posúe o endomorfismo

$$(x, y) \longmapsto (\zeta x, y)$$

onde $\zeta = \frac{1}{2}(-1 + \sqrt{3}i)$ é raíz cúbica da unidade.

4.1. Por que multiplicación complexa?

O grupo $C(\mathbb{C})$ é isomorfo a $\mathbb{C}/L$, con L un retículo. Lémbrese que L é da forma

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a_1\omega_1 + a_2\omega_2 \mid a_1, a_2 \in \mathbb{Z}\}$$

onde ω_1, ω_2 son dous complexos $\mathbb{R}$-linearmente independentes.

Como se recolle en [5], a cada endomorfismo dunha curva elíptica $\phi : C(\mathbb{C}) \longrightarrow C(\mathbb{C})$ pódeselle asignar unha función holomorfa

$$f : \mathbb{C}/L \longrightarrow \mathbb{C}/L.$$

Sendo f holomorfa, en particular en $z = 0$, admite un desenvolvemento en series de potencias

$$f(z) = \sum_{k=0}^{\infty} c_k z^k$$

nunha veciñanza dese punto. Doutra banda, f tamén ten que ser un homomorfismo; logo, debe verificar:

$$f(z_1 + z_2) = f(z_1) + f(z_2) \quad \forall\, z_1, z_2 \text{ nunha veciñanza de } 0.$$

Porén, cómpre ter en conta que a igualdade anterior se dá no cociente $\mathbb{C}/L$. En termos de $\mathbb{C}$, a igualdade anterior equivale a que

$$f(z_1 + z_2) - f(z_1) - f(z_2) \in L \quad \forall\, z_1, z_2 \text{ nunha veciñanza de } 0.$$

Fixados z_1, z_2 de xeito arbitrario dentro dunha veciñanza do 0, considérese a función

$$\begin{aligned} g : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto g(z) := f(z_1 + z_2) - f(z_1) - f(z_2). \end{aligned}$$

Cúmprese que g é holomorfa, e ademais, $g(\mathbb{C}) \subset L$. Ao ser L un retículo, en particular é un conxunto discreto, e polo tanto non contén abertos non baleiros. Doutra banda, o teorema da aplicación aberta garante que a imaxe dun aberto a través dunha función holomorfa non constante é tamén aberta. Pero $\mathbb{C}$ é un aberto, e non obstante, $g(\mathbb{C})$ non pode ser aberto, ao ser non baleiro. Así, necesariamente, g é unha función constante, e verifícase:

$$f(z_1 + z_2) + c_0 = f(z_1) + f(z_2) \quad \forall\, z_1, z_2 \text{ nunha veciñanza de } 0$$

onde $c_0 \in L$. Obsérvese que, sen importar o valor de c_0, pasando ao cociente tense sempre o mesmo homomorfismo. Así, pódese tomar, sen perda de xeneralidade, $c_0 = 0$.

Recapitulando: dada unha curva elíptica C, tómase ϕ un endomorfismo arbitrario seu. A ϕ pódeselle asociar unha función holomorfa $f : \mathbb{C}/L \longrightarrow \mathbb{C}/L$, que nunha veciñanza de $z = 0$ pode ser expresada como serie de potencias e, ademais, é un homomorfismo aditivo.

Ao impoñer todas estas condicións, non poden existir demasiadas funcións f que as cumpran. En efecto, verifícase o seguinte:

Proposición 4.4. *Sexa $f : \mathbb{C} \longrightarrow \mathbb{C}$ unha función holomorfa nunha veciñanza de $z = 0$, na cal tamén se cumpre que $f(z_1 + z_2) = f(z_1) + f(z_2)$. Entón, $f(z) = cz$, para certo $c \in \mathbb{C}$.*

Demostración. Considérese $z \in \mathbb{C}$ un punto arbitrario situado nunha veciñanza do 0. Estúdese que sucede coa derivada de f nese punto:

$$\begin{aligned} f'(z) &= \lim_{h\to 0} \frac{f(z+h) - f(z)}{h} \\ &\overset{(*)}{=} \lim_{h\to 0} \frac{f(z) + f(h) - f(z)}{h} \\ &= \lim_{h\to 0} \frac{f(h)}{h} \\ &\overset{(*)}{=} \lim_{h\to 0} \frac{f(h) - f(0)}{h} = f'(0). \end{aligned}$$

(*) Aquí aplicouse o feito de que f é un homomorfismo de grupos.

Ísto é, a derivada de f nunha veciñanza de 0 resulta ser constante. Así, tense que f é da forma

$$f(z) = c_0 + c_1 z.$$

Sendo f un homomorfismo aditivo, tomando $z_1 = z_2 = 0$, chégase a que $f(0) = 2f(0)$, logo $f(0) = 0$ e así, $c_0 = 0$, obtendo o resultado. □

Observación 4.5. Sexan $z_1, z_2 \in \mathbb{C}$ tales que $z_1 - z_2 \in L$. Entón, no cociente $\mathbb{C}/L$, tense que $f(z_1) = f(z_2)$, ou equivalentemente, $cz_1 = cz_2$; logo, en $\mathbb{C}$, cúmprese que $c(z_1 - z_2) \in L$.

É dicir, dada unha función da forma $f(z) = cz$ definida en $\mathbb{C}/L$, para un certo retículo L, cúmprese que $cL \subset L$.

A proposición anterior especifica a forma da función f, pero non responde á seguinte cuestión: cales son os posibles valores de c?

Se $c \in \mathbb{Z}$, entón correspóndese co endomorfismo multiplicación por c, λ_c. Pero, e que sucede se a curva elíptica admite multiplicación complexa?

Proposición 4.6. *Sexa C unha curva elíptica con multiplicación complexa, de xeito que existe unha función holomorfa*

$$\begin{aligned} f : \mathbb{C}/L &\longrightarrow \mathbb{C}/L \\ z &\longmapsto cz \mod L \end{aligned}$$

tal que $c \notin \mathbb{Z}$. Entón, cúmprese que $c \notin \mathbb{R}$.

Demostración. Supóñase, por redución ao absurdo, que $c \in \mathbb{R}$. Dados $z_1, z_2 \in \mathbb{C}$, tense que $f(z_1) - f(z_2) = c(z_1 - z_2)$. Doutra banda, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, onde ω_1, ω_2 son $\mathbb{R}$-linearmente independentes, i.e., dada unha combinación linear $r_1\omega_1 + r_2\omega_2 = 0$, con $r_1, r_2 \in \mathbb{R}$, tense que $r_1 = r_2 = 0$.

Como se apuntou na observación anterior, cúmprese que $cL \subset L$. En particular, $c\omega_1 \in L$, logo $c\omega_1 = A\omega_1 + B\omega_2$, con $A, B \in \mathbb{Z}$. Así:

$$\left.\begin{aligned} (A-c)\omega_1 + B\omega_2 = 0 \\ \omega_1, \omega_2 \ \mathbb{R}\text{-linearmente independentes} \end{aligned}\right\} \implies A - c = 0 = B.$$

Chégase deste xeito a que $A - c = 0 \iff A = c$. Non obstante, isto contradí a hipótese inicial $c \notin \mathbb{Z}$. Así, necesariamente, $c \in \mathbb{C} - \mathbb{R}$. □

E con esta última proposición, enténdese por que se fala de *multiplicación complexa*: cada endomorfismo dunha curva elíptica diferente da multiplicación por $m \in \mathbb{Z}$ está asociado a unha función holomorfa $f : \mathbb{C}/L \longrightarrow \mathbb{C}/L$ da forma $f(z) = cz \mod L$, con $c \notin \mathbb{R}$. Na seguinte sección, verase que, en particular, estes complexos forman parte dun corpo cuadrático imaxinario.

4.2. O anel de endomorfismos dunha curva elíptica

O conxunto de tódolos endomorfismos dunha curva elíptica C será denotado por $\mathrm{End}(C)$. Nel, defínense as seguintes operacións:

1. Suma de endomorfismos: dados $\phi_1, \phi_2 \in \mathrm{End}(C)$,

$$\begin{aligned} \phi_1 + \phi_2 : C(\mathbb{C}) &\longrightarrow C(\mathbb{C}) \\ P &\longmapsto (\phi_1 + \phi_2)(P) := \phi_1(P) + \phi_2(P) \end{aligned}$$

   Lémbrese que os endomorfismos veñen dados por funcións racionais; así, a suma tamén o será, e polo tanto o conxunto é pechado respecto da suma. É trivial que se respectan as propiedades conmutativa e asociativa, que existe un elemento neutro (o endomorfismo nulo) e todo elemento posúe oposto.

2. Composición de endomorfismos: dados $\phi_1, \phi_2 \in \mathrm{End}(C)$,

$$\begin{aligned} \phi_1\phi_2 : C(\mathbb{C}) &\longrightarrow C(\mathbb{C}) \\ P &\longmapsto (\phi_1\phi_2)(P) := \phi_1(\phi_2(P)) \end{aligned}$$

   É inmediato comprobar que esta aplicación vén dada por funcións racionais, polo que $\mathrm{End}(C)$ tamén é pechado respecto desta operación. De xeito análogo á suma, tense propiedade asociativa e elemento neutro (a identidade), ademais de ser distributiva respecto da adición. Con todo, non tódolos elementos posúen inverso.

Deste xeito, estas operacións proporciónanlle a $\mathrm{End}(C)$ estrutura de anel.

Definición 4.7. A terna formada polo conxunto $\mathrm{End}(C)$, xunto coas operacións de suma e composición anteriores, recibe o nome de **anel de endomorfismos** da curva elíptica C.

Agora ben, que estrutura presenta $\mathrm{End}(C)$? Pódense distinguir dous casos, en función de se C admite ou non multiplicación complexa.

Comécese polo segundo caso: entón, $\mathrm{End}(C) \simeq \mathbb{Z}$. En efecto, os únicos endomorfismos que posúe C son as multiplicacións por enteiros, $\{\lambda_m\}_{m\in\mathbb{Z}}$. A cada λ_m correspóndelle a función holomorfa $z \mapsto mz$ (en particular, o enteiro m). Ademais:

$$\begin{aligned} \lambda_m + \lambda_n &\longmapsto m + n \\ \lambda_m\lambda_n &\longmapsto mn \end{aligned}$$

e tense así un isomorfismo de aneis.

E se C admite multiplicación complexa?

Proposición 4.8. *Sexan C unha curva elíptica con multiplicación complexa e $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ un retículo tal que $C \simeq \mathbb{C}/L$. Considérese o seguinte subconxunto de $\mathbb{C}$:*

$$R_L = \{c \in \mathbb{C} \mid cL \subset L\}$$

Verifícanse as seguintes afirmacións:

1. *Para cada $c \in R_L$, con $c \notin \mathbb{Z}$, $[\mathbb{Q}(c) : \mathbb{Q}] = 2$.*
2. *R_L é un subanel do anel de enteiros do corpo $\mathbb{Q}(\kappa)$, $\mathcal{O}_{\mathbb{Q}(\kappa)}$, sendo $\kappa = \omega_1/\omega_2$.*

Demostración. Ao admitir C multiplicación complexa, para cada endomorfismo diferente da multiplicación por un enteiro, existe unha certa función holomorfa $f : z \in \mathbb{C}/L \longmapsto cz \mod L$, onde $c \notin \mathbb{Z}$. En particular, para ese valor de c, tense que $cL \subset L$. Así, sendo ω_1 e ω_2 os xeradores de L, pódese escribir:

$$\begin{cases} c\omega_1 = a_1\omega_1 + a_2\omega_2 \\ c\omega_2 = b_1\omega_1 + b_2\omega_2 \end{cases}$$

Dividindo agora por ω_2, e facendo $\kappa = \omega_1/\omega_2$:

$$\begin{cases} c\kappa = a_1\kappa + a_2 \\ c = b_1\kappa + b_2 \end{cases}$$

Á vista das ecuacións anteriores, cúmprese:

$$c^2 - (a_1 + b_2)c + a_1b_2 - a_2b_1 = 0$$

Facendo $A = -(a_1 + b_2)$ e $B = a_1b_2 - a_2b_1$, cúmprese que $X^2 + AX + B \in \mathbb{Z}[X]$, e que c é unha das raíces deste polinomio. Polo tanto, e sabendo que $c \notin \mathbb{R}$, como se demostrou na **Proposición 4.6**, pódese concluír que o polinomio é irreducible sobre $\mathbb{Z}[X]$, e en consecuencia tamén o é sobre $\mathbb{Q}[X]$.

Do razoamento anterior dedúcese que $\mathrm{Irr}(c, \mathbb{Q}) = X^2 + AX + B$, e así, $[\mathbb{Q}(c) : \mathbb{Q}] = 2$, quedando probado o primeiro punto. En particular, cada $c \in R_L$ xera unha extensión cuadrática imaxinaria de $\mathbb{Q}$.

Na igualdade $c = b_1\kappa + b_2$, obtida antes, sábese que $b_1 \neq 0$ e $\kappa \notin \mathbb{R}$. Entón, automaticamente, tense garantido que $\mathbb{Q}(c) = \mathbb{Q}(\kappa)$. E deste feito, sabendo que $X^2 + AX + B \in \mathbb{Z}[X]$, dedúcese que R_L é un subanel de $\mathcal{O}_{\mathbb{Q}(\kappa)}$, demostrando así o segundo punto. □

Observación 4.9. Cómpre lembrar que os subaneis de $\mathcal{O}_{\mathbb{Q}(\kappa)}$ son da forma $\mathbb{Z} + c\mathcal{O}_{\mathbb{Q}(\kappa)}$, onde o enteiro $c \geq 1$ é o chamado *condutor*.

Lémbrese que a cada endomorfismo de C se lle pode asignar unha función holomorfa, que como se demostrou na **Proposición 4.4** ten a forma $f(z) = cz$. Así, tense unha aplicación:

$$\begin{aligned} \Lambda : \mathrm{End}(C) &\longrightarrow R_L \\ \phi &\longmapsto c_\phi \end{aligned}$$

onde c_ϕ é o complexo tal que $\phi(z) = c_\phi z$.

Esta aplicación determina a estrutura de $\mathrm{End}(C)$:

Proposición 4.10. *A aplicación Λ é un isomorfismo de aneis.*

Demostración. En primeiro lugar, obsérvese que, por definición, a aplicación é inxectiva, pois a cada endomorfismo ϕ élle asignado o único complexo c_ϕ tal que $\phi(z) = c_\phi z$.

Para demostrar que é un homomorfismo de aneis, hai que comprobar que preserva as operacións. No caso da suma, dados $\phi, \psi \in \mathrm{End}(C)$, tense:

$$(\phi + \psi)(z) = \phi(z) + \psi(z) = c_\phi z + c_\psi z = (c_\phi + c_\psi)z.$$

É dicir, necesariamente, a partir da definición de Λ, á suma de dous endomorfismos seralle asignada a suma dos correspondentes números complexos. Polo tanto, $\Lambda(\phi + \psi) = \Lambda(\phi) + \Lambda(\psi)$.

Analogamente, para o caso da composición:

$$(\phi\psi)(z) = \phi(\psi(z)) = \phi(c_\psi z) = c_\phi c_\psi z = (c_\phi c_\psi)z.$$

A partir das igualdades anteriores, dedúcese que $\Lambda(\phi\psi) = \Lambda(\phi)\Lambda(\psi)$.

Só falta por probar o carácter sobrexectivo. Para iso, fíxese L un retículo do plano complexo. Entón, para cada $c \in R_L$, pódese definir a función $f : z \in \mathbb{C}/L \mapsto cz \mod L$, a cal é un endomorfismo de $\mathbb{C}/L$. Logo, en particular, a f pódeselle asociar un endomorfismo da curva elíptica C. Así, efectivamente, Λ é un isomorfismo entre $\mathrm{End}(C)$ e R_L. $\square$

En resumo, tense completamente determinada a estrutura alxébrica do anel de endomorfismos dunha curva elíptica C definida sobre o corpo dos números complexos:

- Se C non posúe multiplicación complexa, $\mathrm{End}(C) \simeq \mathbb{Z}$.
- Se C posúe multiplicación complexa, $\mathrm{End}(C)$ é isomorfo a un subanel do anel de enteiros dunha extensión cuadrática imaxinaria de $\mathbb{Q}$.

Capítulo 5

Extensións abelianas de $\mathbb{Q}(i)$

Ao longo deste traballo tense visto que nunha curva elíptica é posible definir unha operación de suma de puntos, que lle proporciona estrutura de grupo abeliano. Dentro deste grupo, dado un certo $m \in \mathbb{Z}$, pódese considerar a m-torsión, $C[m]$, o conxunto dos puntos de orde divisora de m. As coordenadas destes puntos xeran unha extensión de Galois sobre $\mathbb{Q}$, cuxo grupo de Galois admite unha representación como subgrupo de $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

En particular, interesa estudar aquelas curvas elípticas con multiplicación complexa, nas cales a representación de Galois non é sobrexectiva para ningún valor de m. Doutra banda, demostrouse que, para unha curva deste tipo, o seu anel de endomorfismos, $\mathrm{End}(C)$, é isomorfo a unha orde dun corpo cuadrático imaxinario. Neste caso, a situación máis simple ten lugar cando $\mathrm{End}(C) \simeq \mathbb{Z}[i]$. Este capítulo vai estar adicado ao estudo dun exemplo no que se dea esta situación.

En concreto, vanse estudar os corpos xerados polos puntos de orde finita da curva elíptica

$$C : y^2 = x^3 + x.$$

Como se viu no capítulo anterior, esta curva posúe multiplicación complexa; en particular, admite o endomorfismo

$$\begin{aligned} \phi : C &\longrightarrow C \\ (x, y) &\longmapsto (-x, iy). \end{aligned}$$

Sexa $\mathbb{K} : \mathbb{Q}$ unha extensión de Galois. Xa que ϕ é un endomorfismo de C, dado $P = (x, y) \in C(\mathbb{K})$, tense que $\phi(P) = (-x, iy) \in C(\mathbb{K})$. Agora ben, isto implica que $y, iy \in \mathbb{K}$, de onde se deduce que $i \in \mathbb{K}$. É dicir, calquera extensión de Galois xerada por puntos da curva C, necesariamente, conterá a unidade imaxinaria i.

Considérese $\sigma \in \mathrm{Gal}(\mathbb{K} : \mathbb{Q})$. Existen dous xeitos de obter un novo punto de $C(\mathbb{K})$:

1. A través do endomorfismo ϕ.
2. A través do automorfismo σ.

Quérese agora estudar se ϕ e σ conmutan, i.e.,

$$\sigma(\phi(P)) = \phi(\sigma(P)) \ \ \forall\, P \in C(\mathbb{K})?$$

Facendo os cálculos, obsérvase que :

$$\sigma(\phi(P)) = \sigma(-x, iy) = (\sigma(-x), \sigma(iy)) = (-\sigma(x), \sigma(i)\sigma(y))$$
$$\phi(\sigma(P)) = \phi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y))$$

Entón, a conmutatividade dáse sempre que $\sigma(i) = i$; noutras palabras, cando $\sigma \in \mathrm{Gal}(\mathbb{K} : \mathbb{Q}(i))$. Por esta razón, resulta máis conveniente empregar ϕ para estudar as extensións abelianas de $\mathbb{Q}(i)$, en vez das de $\mathbb{Q}$.

O teorema principal deste capítulo garante que os puntos de orde finita da curva C xeran extensións abelianas de $\mathbb{Q}(i)$:

Teorema 5.1. *Sexa C a curva elíptica dada pola ecuación*

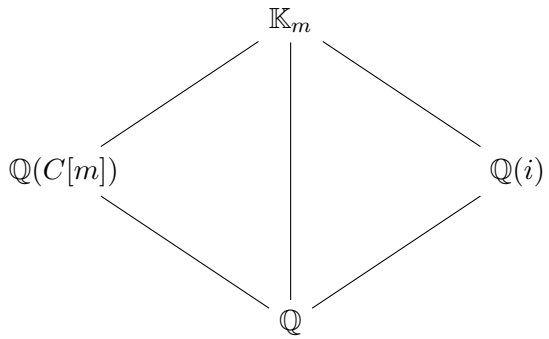
$$y^2 = x^3 + x.$$

Para cada enteiro $m \geq 1$, sexa

$$\mathbb{K}_m = \mathbb{Q}(i)(C[m])$$

o corpo xerado por i e as coordenadas dos puntos de $C[m]$. Entón, $\mathbb{K}_m : \mathbb{Q}(i)$ é unha extensión de Galois, e o seu grupo de Galois é abeliano.

Demostración (Teorema 5.1, parte 1). Tense o seguinte diagrama:



Dunha banda, xa se demostrara, na **Proposición 2.11**, que a extensión $\mathbb{Q}(C[m]) : \mathbb{Q}$ é de Galois. E por outra parte, tamén o é a extensión $\mathbb{Q}(i) : \mathbb{Q}$, pois $\mathbb{Q}(i)$ é o corpo de escisión do polinomio $X^2 + 1$. En consecuencia, $\mathbb{K}_m$ é de Galois sobre $\mathbb{Q}$, como composición dos corpos $\mathbb{Q}(i)$ e $\mathbb{Q}(C[m])$.

A parte interesante do teorema é probar que $\mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i))$ é abeliano. Lembrando a teoría de representacións vista no capítulo 3, fíxense P_1, P_2 dous xeradores de $C[m]$. Entón, tense un monomorfismo

$$\begin{aligned} \rho_m : \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i)) &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\longmapsto \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix} \end{aligned}$$

tal que

$$\begin{aligned} \sigma(P_1) &= \alpha_\sigma P_1 + \gamma_\sigma P_2 \\ \sigma(P_2) &= \beta_\sigma P_1 + \delta_\sigma P_2. \end{aligned}$$

Analogamente, ϕ induce un homomorfismo $\phi : C[m] \longrightarrow C[m]$. En efecto, dado $P \in C[m]$:

$$m\phi(P) = \phi(mP) = \phi(\mathcal{O}) = \mathcal{O}$$

logo $\phi(P) \in C[m]$. Polo tanto, existen coeficientes $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ de xeito que

$$\begin{aligned} \phi(P_1) &= aP_1 + cP_2 \\ \phi(P_2) &= bP_1 + dP_2. \end{aligned}$$

Así, a cada $\phi \in \mathrm{End}(C)$ pódeselle asignar unha matriz con coeficientes en $\mathbb{Z}/m\mathbb{Z}$:

$$\phi \longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Doutra banda, e este é un detalle fundamental na proba, viuse no inicio do capítulo que para cada $\sigma \in \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i))$ e cada $P \in C(\mathbb{K}_m)$, se verifica que $\sigma(\phi(P)) = \phi(\sigma(P))$. Tomando os casos particulares $P = P_1$ e $P = P_2$, obtense que as matrices para ϕ e σ conmutan:

$$\begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix}.$$

Para completar a demostración, son precisos os seguintes resultados:

1. Verase que a matriz de ϕ non é unha matriz escalar, i.e., un múltiplo da matriz identidade.
2. Dada unha matriz cadrada A de orde 2 non escalar, comprobarase que calquera par de matrices que conmutan con A tamén o fan entre elas.

Das afirmacións anteriores, dedúcese que $\mathrm{Im}\,\rho_m$ é un subgrupo abeliano de $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, e sendo ρ_m un monomorfismo, pódese concluír que $\mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i))$ é abeliano. A continuación, enunciaranse e demostraranse os resultados anteriores, e posteriormente, retomarase a proba do teorema. □

Lema 5.2. *Sexa A a matriz correspondente ao endomorfismo ϕ,*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Verifícanse as seguintes afirmacións:

1. $A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.
2. *Sexa p un factor primo de m. Entón, a redución de A módulo p non é unha matriz escalar. Equivalentemente, cando menos unha das 3 condicións seguintes é certa:*
   a) $b \not\equiv 0 \mod p$,
   b) $c \not\equiv 0 \mod p$,
   c) $a \not\equiv d \mod p$.

Demostración. 1. Para probar este punto, verase que $\det(A) \in (\mathbb{Z}/m\mathbb{Z})^*$. Dado un punto calquera $P = (x, y) \in C$, aplicando dúas veces ϕ sobre el, obtense:

$$\phi(\phi(P)) = \phi(-x, iy) = \phi(x, -y) = -P$$

onde a última igualdade se ten porque C está en forma normal de Weierstrass. Deste feito dedúcese que A satisfai a ecuación $A^2 = -I$, podendo escribir:

$$1 = \det(A^2) = \det(A)^2.$$

Logo, efectivamente, $\det(A) \in (\mathbb{Z}/m\mathbb{Z})^*$, e $A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

2. Razoando por redución ao absurdo, supóñase que existe p un factor primo de m e un certo $n \in \mathbb{Z}$ de xeito que

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} m & 0 \\ 0 & m \end{bmatrix} \mod p.$$

Isto, en particular, significa que o endomorfismo $\phi : C[p] \longrightarrow C[p]$ se corresponde coa multiplicación por m,

$$\phi(P) = mP \quad \forall\, P \in C[p].$$

Sexa $\tau : \mathbb{C} \longrightarrow \mathbb{C}$ a conxugación complexa. Esta aplicación pode interpretarse como un elemento de $\mathrm{Gal}(\mathbb{K}_m : \mathbb{Q})$, pois en particular deixa fixo $\mathbb{Q}$. Logo, segundo a **Proposición 2.9**, cúmprese que $m\tau(P) = \tau(mP)$. Doutra banda, xa que $\tau(i) = -i$, tense:

$$\tau(\phi(P)) = \tau(-x, iy) = (-\tau(x), -i\tau(y)) = -\phi(\tau(P)).$$

Isto é certo para $C(\mathbb{K}_m)$; en particular, para cada $P \in C[p]$:

$$m\tau(P) = \tau(mP) = \tau(\phi(P)) = -\phi(\tau(P)) = -m\tau(P).$$

Das igualdades anteriores extráese que $2m\tau(P) = \mathcal{O} \quad \forall\, P \in C[p]$. Agora ben, τ non é máis ca unha permutación dos elementos de $C[p]$. Así, verifícase que $2mP = \mathcal{O} \quad \forall\, P \in C[p]$.

Logo, existen dúas posibilidades para p:

a) $p \mid m$

b) $p = 2$

Se o primeiro caso fose certo, entón cumpriríase que $\phi(P) = \mathcal{O} \ \ \forall\, P \in C[p]$, o cal é absurdo, xa que se demostrou antes que $\phi(\phi(P)) = -P$. Entón, necesariamente, $p = 2$.

Agora, facendo uso da **Proposición 1.17**, vese que

$$C[2] = \{\mathcal{O}, (-i, 0), (0, 0), (i, 0)\}$$

e ademais, $C[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Logo, pódense escoller como xeradores de $C[2]$ os puntos $P_1 = (0, 0)$ e $P_2 = (i, 0)$. Aplicando o endomorfismo ϕ a estes puntos, tense:

$$\begin{aligned} \phi(P_1) &= (0, 0) = P_1 \\ \phi(P_2) &= (-i, 0) = P_1 + P_2 \end{aligned}$$

onde a última igualdade se obtén a partir das fórmulas (1.6). Deste xeito, a matriz asociada a ϕ é

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Agora ben, esta matriz non é escalar módulo ningún primo. Polo tanto, $p = 2$ é tamén un absurdo, quedando probado o resultado. □

Lema 5.3. *Sexa $A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ unha matriz non escalar módulo p, para cada p factor primo de m. Entón, verifícase que o conxunto*

$$\mathcal{H} = \{B \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \mid AB = BA\}$$

é un subgrupo abeliano de $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Noutras palabras, as matrices que conmutan con A tamén conmutan entre si.

Demostración (Lema 5.3, parte 1). En primeiro lugar, verase que efectivamente é un subgrupo. Considérense así $B, C \in \mathcal{H}$. Conmuta o produto BC con A?

$$A(BC) = (AB)C \overset{(*)}{=} (BA)C = B(AC) \overset{(*)}{=} B(CA) = (BC)A.$$

(*) Aquí aplicouse o feito de que $B, C \in \mathcal{H}$.

A anterior cadea de igualdades demostra que, efectivamente, $BC \in \mathcal{H}$. Doutra banda, para cada $B \in \mathcal{H}$, tense tamén que $B^{-1} \in \mathcal{H}$:

$$AB = BA \implies A = BAB^{-1} \implies B^{-1}A = AB^{-1}.$$

Así, $\mathcal{H}$ é un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Agora resta por probar que é abeliano. Para isto, en primeiro lugar, cómpre ter en conta que abonda reducirse ao caso $m = p^e$, onde p é un número primo e o expoñente e, un enteiro positivo. E para esta situación concreta, aplicaranse dous resultados que se mencionan a continuación. Aínda que non se inclúen as súas demostracións neste traballo, poden atoparse en [6]. □

Sublema 5.4. *Sexan p un número primo e $A \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ unha matriz non escalar módulo p. Entón, existe unha matriz de cambio de base $T \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ tal que A se converte na forma*

$$T^{-1}AT = \begin{bmatrix} 0 & * \\ 1 & * \end{bmatrix}.$$

Sublema 5.5. *Sexa $m \in \mathbb{Z}$. Considérese $A \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ unha matriz da forma:*

$$A = \begin{bmatrix} 0 & * \\ 1 & * \end{bmatrix}.$$

Entón, o conxunto

$$\{B \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \mid AB = BA\}$$

é un subgrupo abeliano de $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Tendo introducido estes sublemas auxiliares, retómase a proba do **Lema 5.3**:

Demostración (Lema 5.3, parte 2). Sexa $A \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ unha matriz non escalar módulo p. Segundo o **Sublema 5.4**, existe unha matriz de cambio de base T tal que

$$T^{-1}AT = \begin{bmatrix} 0 & * \\ 1 & * \end{bmatrix}.$$

Considérense dúas matrices $B, C \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ que conmutan con A, é dicir, $AB = BA$ e $AC = CA$, respectivamente. Destas igualdades dedúcense as seguintes:

$$(T^{-1}AT)(T^{-1}BT) = (T^{-1}BT)(T^{-1}AT),$$
$$(T^{-1}AT)(T^{-1}CT) = (T^{-1}CT)(T^{-1}AT).$$

Logo, o **Sublema 5.5** garante que as matrices $T^{-1}BT$ e $T^{-1}CT$ conmutan entre si:

$$(T^{-1}BT)(T^{-1}CT) = (T^{-1}CT)(T^{-1}BT).$$

Agora ben, operando na expresión anterior, chégase a que

$$BC = CB$$

completando así a proba do lema. □

Chegados a este punto, xa se teñen tódolos ingredientes precisos para rematar a proba do **Teorema 5.1**:

Demostración (Teorema 5.1, parte 2). Dunha banda, para cada $m \in \mathbb{Z}$ tense a representación de Galois

$$\rho_m : \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i)) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

e por outra, a matriz A asociada ao endomorfismo ϕ,

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Aplicando o **Lema 5.2**, sábese que A non é escalar módulo ningún dos factores primos de m.

Sexa agora $\sigma \in \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i))$. Tense visto que σ e ϕ conmutan na súa acción sobre $C[m]$; polo tanto, as súas matrices asociadas tamén o farán, i.e.,

$$A\rho_m(\sigma) = \rho_m(\sigma)A.$$

Deste xeito, e de acordo co **Lema 5.3**, as matrices do conxunto

$$\mathrm{Im}\,\rho_m = \{\rho_m(\sigma) \mid \sigma \in \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i))\}$$

conmutan entre si. Polo tanto, sendo ρ_m un homomorfismo de grupos, pódese escribir:

$$\rho_m(\sigma_1\sigma_2) = \rho_m(\sigma_1)\rho_m(\sigma_2) = \rho_m(\sigma_2)\rho_m(\sigma_1) = \rho_m(\sigma_2\sigma_1) \qquad \forall\, \sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i)).$$

Agora ben, segundo o **Teorema 3.5**, ρ_m é inxectivo; deste xeito, a igualdade anterior implica, necesariamente, que

$$\sigma_1\sigma_2 = \sigma_2\sigma_1 \qquad \forall\, \sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i)).$$

E con isto, queda garantido que $\mathrm{Gal}(\mathbb{K}_m : \mathbb{Q}(i))$ é abeliano, completando a proba do teorema. □

Lémbrese que, para o caso no cal se toma $\mathbb{Q}$ como corpo base, o **Teorema de Kronecker-Weber** caracteriza completamente as súas extensións abelianas: son as subextensións dos corpos ciclotómicos. Pois ben, existe un resultado análogo para $\mathbb{Q}(i)$:

Teorema 5.6. *Sexa a curva elíptica $C : y^2 = x^3 + x$. Considérese $\mathbb{F} : \mathbb{Q}(i)$ unha extensión de Galois finita. Supóñase que $\mathrm{Gal}(\mathbb{F} : \mathbb{Q}(i))$ é abeliano. Entón, existe un enteiro $m \geq 1$ tal que*

$$\mathbb{F} \subset \mathbb{K}_m = \mathbb{Q}(i)(C[m]).$$

É dicir, a torsión da curva elíptica C xera tódalas extensións abelianas de $\mathbb{Q}(i)$. E máis en xeral, para outros corpos cuadráticos imaxinarios, existirán curvas elípticas con multiplicación complexa que permiten xerar as súas extensións abelianas.

Bibliografía

[1] Cassels, J.W.S. (1991). *Lectures on Elliptic Curves*, Cambridge University Press.

[2] Lipman, J. (2007). *Rational Points on Conics, and Local-Global Relations in Number Theory.* `https://www.math.purdue.edu/~jlipman/LegendreTalk.pdf`. [Online] Consultado por última vez o 23 de febreiro de 2024.

[3] Milne, J.S. (2006). *Elliptic Curves*, BookSurge Publishers.

[4] Silverman, J.H. (1994). *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer.

[5] Silverman, J.H. (2009). *The Arithmetic of Elliptic Curves*, 2.ª edición, Graduate Texts in Mathematics, Springer.

[6] Silverman, J.H. e Tate, J.T. (2015). *Rational Points on Elliptic Curves*, 2.ª edición, Undergraduate Texts in Mathematics, Springer.

[7] Smith, B. (2008). *Mappings of elliptic curves.* `https://www.hyperelliptic.org/tanja/conf/summerschool08/slides/Maps.pdf`. [Online] Consultado por última vez o 24 de xuño de 2024.