REPRESENTACIONES DE GALOIS

LUIS DIEULEFAIT, ARIEL PACETTI, AND FERNANDO RODRIGUEZ VILLEGAS

Índice

1. Teoría de Cuerpos

1.1. Generalidades. Recordemos la siguiente definición.

Date: 12 de marzo de 2019 (versión preliminar).

Estas notas corresponden al curso dictado por Ariel Pacetti, Fernando Rodríguez Villegas, y Luis Dieulefait en la escuela AGRA III, Aritmética, Grupos y Análisis, del 9 al 20 de Julio de 2018 en Córdoba, Argentina.

Definición 1.1. Un cuerpo es una terna $(K, +, *)$ dada por un conjunto K, y dos operaciones binarias

$$+, * : K \times K \mapsto K,$$

que satisfacen las siguientes propiedades:

- $(K, +)$ es un grupo abeliano (o sea la operación es asociativa, conmutativa, posee un neutro denotado 0 y todo elemento tiene inverso).
- $(K \setminus \{0\}, *)$ es un grupo abeliano.
- Vale la propiedad distributiva del producto sobre la suma, o sea

$$a * (b + c) = a * b + a * c,$$

para toda terna de elementos a, b, c en K.

Ejemplos 1.2.

1. El conjunto de números racionales con sus operaciones naturales es un cuerpo $(\mathbb{Q}, +, *)$. Lo mismo sucede con el conjunto de números reales $(\mathbb{R}, +, *)$ y de números complejos $(\mathbb{C}, +, *)$.
2. Otros cuerpos de gran utilidad son aquellos para los cuales el conjunto K es finito. Por ejemplo, si p es un número primo, y denotamos por $\mathbb{F}_p = \mathbb{Z}/p$ el conjunto de clases de equivalencia de números enteros módulo p (donde identificamos dos números enteros si su diferencia es divisible por p), entonces el conjunto $(\mathbb{F}_p, +, *)$ es un cuerpo con p elementos.

Un *morfismo de cuerpos* es simplemente un morfismo de anillos, o sea si K y L son cuerpos, un morfismo de cuerpos $\varphi : K \to L$ es una función que satisface:

- $\varphi(x + y) = \varphi(x) + \varphi(y)$ para todo par de elementos $x, y \in K$.
- $\varphi(x * y) = \varphi(x) * \varphi(y)$ para todo par de elementos $x, y \in K$.
- $\varphi(1) = 1$.

De manera usual, un *isomorfismo* de cuerpos, es un morfismo de cuerpos biyectivo (es fácil ver que todo morfismo de cuerpos es inyectivo).

Recordar que si K es un cuerpo, entonces el anillo de polinomios $K[x]$ posee un algoritmo de división; esto es dados dos polinomios $f(x), g(x) \in K[x]$, con $g(x)$ no nulo, existen únicos polinomios $q(x), r(x) \in K[x]$ con $r(x) = 0$ o de grado menor que el grado de $g(x)$ tales que

$$f(x) = g(x)q(x) + r(x).$$

Dicho algoritmo permite definir el máximo común divisor de polinomios de manera análoga a lo hecho para números enteros (imponiendo la condición de que el máximo común divisor es un polinomio mónico, para obtener unicidad), y demostrar que dados dos polinomios $f(x), g(x) \in K[x]$, alguno no nulo, el máximo común divisor entre ellos se escribe como combinación lineal de ambos, o sea: existen $r(x), s(x) \in K[x]$ tales que

$$\gcd(f(x), g(x)) = r(x)f(x) + s(x)g(x).$$

Proposición 1.3. *Sea K un cuerpo, y sea $p(x) \in K[x]$ un polinomio irreducible. Entonces el anillo $L = K[x]/(p(x))$ es un cuerpo.*

Demostración. Como estamos cocientando por un ideal (el generado por $p(x)$), el cociente tiene automáticamente una estructura de anillo. Lo que precisamos demostrar para obtener un cuerpo es que todo elemento no nulo tiene inverso multiplicativo. Sea así $\overline{f(x)}$ la clase de representantes de un elemento no nulo del cociente, y sea $f(x) \in K[x]$ algún polinomio en dicha clase. Como $\overline{f(x)}$ es no nulo, $p(x) \nmid f(x)$. Como $p(x)$ es irreducible, $\gcd(f(x), p(x)) = 1$, con lo cual existen $r(x), s(x) \in K[x]$ tales que

$$1 = r(x)f(x) + s(x)p(x). \tag{1.1}$$

Entonces en el cociente, la clase de $r(x)$ es un inverso multiplicativo de la clase de $f(x)$. □

Así obtenemos muchos ejemplos nuevos de cuerpos. Por ejemplo:

- Tomando $p(x) = x^2 + 1 \in \mathbb{Q}[x]$ obtenemos el cuerpo $\mathbb{Q}[x]/(x^2+1)$ que es isomorfo (como cuerpo) al cuerpo $\mathbb{Q}[i] = \{a + bi \ : \ a, b \in \mathbb{Q}\}$ (donde $i^2 = -1$).
- Tomando $p(x) = x^2 + 1$ en $\mathbb{F}_3[x]$ (verificar que es irreducible), obtenemos el cuerpo $\mathbb{F}_3[x]/(x^2+1)$, que denotamos $\mathbb{F}_9$. ¿Cuántos elementos tiene dicho cuerpo?
- Mas generalmente, si p es un número primo, y si $q(x) \in \mathbb{F}_p[x]$ es un polinomio irreducible de grado d, ¿ cuántos elementos tiene el cuerpo $\mathbb{F}_p[x]/(q(x))$?

Notar que si K y L son cuerpos y $K \subset L$, podemos pensar a L como un K-espacio vectorial. En particular tiene sentido mirar la dimensión de L como K-espacio vectorial y preguntarse si es finita o no.

Definición 1.4. Si K y L son cuerpos y $K \subset L$, decimos que L es una extensión de cuerpos de K. Definimos el *grado* de la extensión, y lo denotamos $[L : K]$, como la dimensión de L como K-espacio vectorial.

Ejercicio 1.5. Sea $p(x) \in K[x]$ un polinomio irreducible de grado d, y denotemos por $L = K[x]/(p(x))$. Calcular $[L : K]$.

Definición 1.6. Un cuerpo de números es un cuerpo K tal que $\mathbb{Q} \subset K$, y el grado de la extensión es finito.

El siguiente resultado vale en contextos muy generales, pero lo enunciamos solamente para el caso de cuerpos de números, que es en el que lo vamos a usar.

Teorema 1.7 (Teorema de elementos primitivos)**.** *Si K es un cuerpo de números, y $[K : \mathbb{Q}] = d$, entonces existe un polinomio $p(x) \in \mathbb{Q}[x]$ irreducible de grado d tal que K es isomorfo a $\mathbb{Q}[x]/(p(x))$.*

El elemento de K que se corresponde con la variable x bajo el isomorfismo se suele llamar un *elemento primitivo* de K.

1.2. Los números p-ádicos. Una referencia clásica sobre los números p-ádicos es el libro ([Kob84]). Existen otros cuerpos además de los mencionados anteriormente que juegan un rol preponderante en la teoría de números. Dichos cuerpos son los que se obtienen a partir de completar el cuerpo de números racionales con un valor absoluto (o sea son construcciones similares a la de los números reales). La diferencia, es que en lugar de utilizar el valor absoluto usual (llamado arquimediano), es preciso utilizar otros valores absolutos (los no-arquimedianos).

Fijemos un primo p. Definimos la valuación p-ádica como la función $v_p : \mathbb{Z} \setminus \{0\} \mapsto \mathbb{Z}$ dada por

$$v_p(a) = \text{máx}\{n \in \mathbb{N} \cup \{0\} \ : \ p^n \mid a\} \tag{1.2}$$

Así, $v_3(12) = 1$ y $v_3(10) = 0$. Extendemos la valuación a los racionales no nulos, por

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Definición 1.8. El valor absoluto p-ádico esta dado por:

$$\left|\frac{a}{b}\right|_p := \begin{cases} 0 & \text{si } \frac{a}{b} = 0, \\ p^{-v_p(\frac{a}{b})} & \text{en otro caso.} \end{cases}$$

Luego, por ejemplo $\left|\frac{2}{3}\right|_3 = 3$, y $\left|\frac{9}{7}\right|_3 = \frac{1}{9}$. Es fácil verificar las siguientes propiedades.

Proposición 1.9. *El valor absoluto p-ádico satisface las siguientes propiedades:*

1. $|a|_p = 0$ *si y sólo si* $a = 0$.

2. $|a \cdot b|_p = |a|_p \cdot |b|_p$.
3. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$. *Mas aún, si* $|a|_p$ *y* $|b|_p$ *son distintos, entonces vale la igualdad.*

La última propiedad de la Proposición se conoce como la propiedad *ultramétrica*. Dicha propiedad implica la desigualdad triangular (dejamos esto como ejercicio), pero es mucho mas fuerte. En particular, el valor absoluto p-ádico nos da una manera de medir que tan cerca están dos números racionales. Notar que esta forma de medir dista bastante de la forma usual, por ejemplo, los números p^n tienen valor absoluto p-ádico muy pequeño cuando n es grande ($|p^n|_p = \frac{1}{p^n}$). En particular, dos números enteros están cerca con el valor absoluto p-ádico si su diferencia es divisible por potencias grandes de p.

Observación 1.10. El valor absoluto tiene una propiedad muy importante, que es que el conjunto de valores que toma tiene como único punto de acumulación el cero. De la definición se puede ver fácilmente que

$$|\mathbb{Q}|_p = \{0\} \cup \{p^{\mathbb{Z}}\}.$$

Así por ejemplo, si $p = 2$, si un número tiene valor absoluto 2-ádico mayor que 1, automáticamente es mayor o igual que 2 (dado que en el intervalo $(1, 2)$ no hay ningún valor posible).

Definición 1.11. Definimos el *cuerpo de números p-ádicos* y lo denotamos $\mathbb{Q}_p$ al conjunto obtenido al completar el conjunto de números racionales $\mathbb{Q}$ con respecto al valor absoluto p-ádico. Dicho conjunto tiene una suma y un producto que lo hacen un cuerpo (ver Ejercicio 1.12).

Recordemos el proceso para completar un espacio métrico $\mathcal{B}$ con respecto a su valor absoluto $|\,.\,|$: consideramos sucesiones de Cauchy en $\mathcal{B}$ (con respecto al valor absoluto $|\,.\,|$), y definimos una relación de equivalencia, donde identificamos dos sucesiones $\{a_n\}$ y $\{b_n\}$ (y notamos $\{a_n\} \sim \{b_n\}$) si su diferencia $\{a_n - b_n\}$ tiende a cero. Luego la completación $\overline{\mathcal{B}}$ se define como el cociente del conjunto de sucesiones de Cauchy por la relación $\sim$.

Ejercicio 1.12. Probar que si $(\mathcal{B}, +, *)$ es un cuerpo con un valor absoluto, existe una forma natural de extender la suma y producto a la completación $\overline{\mathcal{B}}$, que hacen de $(\overline{\mathcal{B}}, +, *)$ un cuerpo.

A la vez, existe una manera natural de extender el valor absoluto $|\,.\,|$ a la completación $\overline{\mathcal{B}}$. En particular, $\mathbb{Q}_p$ también posee un valor absoluto p-ádico.

Ejercicio 1.13.
- Probar que si $(x_n) \subset \mathbb{Q}$ es una sucesión de Cauchy entonces $|x_n|_p$ es una sucesión de Cauchy. En particular existe $\lim_n |x_n|_p$.
- Probar que si $(x_n), (y_n) \subset \mathbb{Q}$ son sucesiones de Cauchy equivalentes, $\lim_n |x_n|_p = \lim_n |y_n|_p$.
- Deducir que si $x \in \mathbb{Q}_p$, podemos definir $|x|_p = \lim_n |x_n|_p$, donde (x_n) es cualquier sucesión de Cauchy que converge a él.
- Probar que el valor absoluto definido en elementos $x \in \mathbb{Q}$ coincide con el valor absoluto p-ádico.

Ejercicio 1.14. Demostrar las siguientes propiedades del valor absoluto:

1. El conjunto de valores que alcanza el valor absoluto de $\mathbb{Q}_p$ es el mismo que el de $\mathbb{Q}$, o sea $|\mathbb{Q}_p|_p = |\mathbb{Q}|_p = \{0\} \cup \{p^{\mathbb{Z}}\}$.
2. Probar que las bolas abiertas en $\mathbb{Q}_p$ son cerradas, y las bolas cerradas son abiertas; esto es: si $x_0 \in \mathbb{Q}_p$ y $r > 0$, la bola de centro x_0 y radio r es

$$B_r(x_0) = \{y \in \mathbb{Q}_p \ : \ |x_0 - y|_p < r\}.$$

Probar que dado $r > 0$, existe un número $r' > 0$ tal que $B_r(x_0) = \overline{B_{r'}(x_0)}$. A la vez, dado $r' > 0$, existe un $r > 0$ tal que $\overline{B_{r'}(x_0)} = B_r(x_0)$. Esto en particular implica que como espacio métrico, $\mathbb{Q}_p$ es totalmente disconexo.

Definición 1.15. El conjunto de los *enteros p-ádicos* se define como la bola cerrada de radio 1 centrada en cero, esto es $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \ : \ |x|_p \leq 1\}$.

Ejercicio 1.16. Probar que el conjunto $\mathbb{Z}_p$ es un anillo (sugerencia: usar la propiedad de que el valor absoluto p-ádico es una ultramétrica, ver Proposición 1.9). A la vez, probar que $\mathbb{Z} \subset \mathbb{Z}_p$, y $\mathbb{Z}_p$ es la clausura topológica de $\mathbb{Z}$.

Existe una manera de entender los enteros p-ádicos, mediante la expansión en base p. Recordar que todo número natural $N \in \mathbb{N}$ se puede expresar de forma única como

$$N = a_0 + a_1 p + \ldots + a_r p^r, \tag{1.3}$$

donde $0 \leq a_i < p$, para $i = 0, 1, \ldots r$ (esta es la expresión en base p de N). A la vez, si N_1, N_2 son dos números naturales tales que $v_p(N_1 - N_2) \geq t$, entonces los primeros $t+1$ términos de la expresión en base p de N_1 y N_2 coinciden.

Ejercicio 1.17. Probar que si $\{b_n\}$ es una sucesión de Cauchy para el valor absoluto p-ádico (donde cada b_n es un número natural), existen únicos $(a_n)_{n\geq 0}$ con $0 \leq a_n < p$ tales que la sucesión $\{b_n\}$ converge a la serie

$$\sum_{n\geq 0} a_n p^n \in \mathbb{Q}_p. \tag{1.4}$$

Esto sugiere que considerar sucesiones de Cauchy para el valor absoluto p-ádico de números naturales es equivalente a considerar series como en (1.4). Si comenzamos con sucesiones de Cauchy para el valor absoluto p-ádico de números enteros, es fácil ver que también podemos asociarles una tal serie. Luego resta entender que sucede al considerar sucesiones de números racionales.

Ejercicio 1.18. Probar que si $x \in \mathbb{Q}_p$, entonces podemos representar el número x de manera única como una serie de la forma

$$\sum_{i\geq N_0} a_i p^i,$$

donde $0 \leq a_i < p$ y $N_0 \in \mathbb{Z}$. A la vez, probar que $\mathbb{Z}_p$ se puede caracterizar como aquellas series que no poseen términos no nulos con índices negativos, o sea si $i < 0$ entonces $a_i = 0$.

Observación 1.19. Esta manera de describir los números p-ádicos es muy útil para entender propiedades de los mismos, pero poco eficiente para operar. No entraremos en detalles de los problemas computacionales que aparecen naturalmente al trabajar con los números p-ádicos (ver por ejemplo [Kob84]).

1.3. Teoría de Galois en extensiones finitas. El propósito del presente curso (y sus notas) no es dar un exposición exhaustiva sobre teoría de Galois, pero precisamos repasar algunas propiedades importantes de la misma (para mas detalles, ver por ejemplo los libros [Rot98], [Ste15] o [Cox12]).

Si K es un cuerpo, posee un neutro para el producto que denotamos por 1. Tenemos un morfismo natural de anillos de $\psi : \mathbb{Z} \mapsto K$, dado por mandar $1 \to 1$. El núcleo de ψ es un ideal $\mathfrak{a}$ de $\mathbb{Z}$ y obtenemos una inclusión

$$\psi : \mathbb{Z}/\mathfrak{a} \hookrightarrow K,$$

con lo cual $\mathbb{Z}/\mathfrak{a}$ debe ser un dominio íntegro, y por lo tanto $\mathfrak{a}$ es un ideal primo. Existen dos tipos de ideales primos en $\mathbb{Z}$:

- $\mathfrak{a} = \{0\}$,
- $\mathfrak{a} = p\mathbb{Z}$, donde p es un número primo.

Decimos que el cuerpo K tiene *característica cero* si ψ es inyectiva, y decimos que K tiene *característica* p si el núcleo de ψ es el ideal $p\mathbb{Z}$.

Ejemplos 1.20.
1. El cuerpo de números racionales $\mathbb{Q}$ tiene característica 0. Lo mismo sucede con el cuerpo $\mathbb{R}$ de números reales.
2. El cuerpo finito $\mathbb{F}_p$ tiene característica p.

En este curso solamente consideraremos cuerpos K que tengan característica 0 o que sean finitos, con lo cual de ahora en más nos vamos a restringir a dichos cuerpos.

Definición 1.21. Sean $K \subset L$ cuerpos. Decimos que $\alpha \in L$ es *algebraico* sobre K si existe un polinomio mónico $p(x) \in K[x]$ tal que $p(\alpha) = 0$. Decimos que la extensión L/K es *algebraica* si todos los elementos de L son algebraicos sobre K.

Ejemplos 1.22. Consideremos la extensión $\mathbb{Q} \subset \mathbb{R}$.
1. El elemento $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, dado que es raíz del polinomio $x^2 - 2 \in \mathbb{Q}[x]$.
2. El número π es irracional, o sea no es raíz de ningún polinomio $p(x) \in \mathbb{Q}[x]$. Luego $\mathbb{R}/\mathbb{Q}$ no es una extensión algebraica (buscar información en wikipedia).

Ejercicio 1.23. Probar que si $[L : K] < \infty$, entonces la extensión L/K es algebraica.

Consideremos en $\mathbb{Q}[x]$ el polinomio $p(x) = x^2 - 2$. Claramente dicho polinomio es irreducible (dado que si no lo fuera se podría escribir como producto de dos polinomios de grado 1, y en particular tendría una raíz racional, que claramente no tiene). Nos podemos preguntar cual es el menor cuerpo en el cual dicho polinomio se vuelve reducible. La Proposición 1.3 nos dice que el cociente $L := \mathbb{Q}[t]/(t^2 - 2)$ es un cuerpo. Notar que el polinomio $x^2 - 2$ tiene una raíz en dicho cuerpo, dado que $t^2 = 2$, o sea

$$x^2 - 2 = (x - t)(x + t).$$

Además, $[L : \mathbb{Q}] = 2$, con lo cual cualquier cuerpo que tenga una raíz de $p(x)$ "contiene" a L (en el sentido de que si K es un cuerpo donde $p(x)$ posee una raíz, entonces existe un morfismo inyectivo de cuerpos de L en K).

Proposición 1.24. *Si $p(x) \in K[x]$, existe un único cuerpo L (salvo isomorfismos) que satisface las siguientes dos propiedades:*
- *el polinomio $p(x)$ tiene todas sus raíces en L,*
- *si M es un cuerpo tal que $p(x)$ tiene todas sus raíces en M, entonces existe un morfismo de cuerpos de L en M.*

Al cuerpo L se lo llama el cuerpo de descomposición de $p(x)$.

Demostración. La demostración es constructiva, y se hace mediante un proceso inductivo agregando de a una raíz siguiendo el procedimiento del ejemplo anterior. Ver por ejemplo el Teorema 48 de [Rot98]. □

Definición 1.25. Sea L/K una extensión algebraica, y K de característica 0 o finito. La extensión L/K se dice *Galois* si todo polinomio irreducible en $K[x]$ que posee una raíz en L tienen todas sus raíces en L.

Si L/K es una extensión algebraica, definimos el conjunto de automorfismos de L sobre K como

$$\mathrm{Aut}_K(L) = \{\psi : L \to L \text{ morfismo de cuerpos tal que } \psi(k) = k \, \forall k \in K\}.$$

O sea son los morfismos del cuerpo L en sí mismo que al restringirlos a K dan la identidad.

Hay una caracterización alternativa de extensiones Galois en términos del grupo $\mathrm{Aut}_K(L)$: una extensión L/K finita es Galois si y sólo si $[L:K] = \#\,\mathrm{Aut}_K(L)$. Con esta caracterización, no es difícil ver que el cuerpo de descomposición de un polinomio $p(x) \in K[x]$ siempre es una extensión Galois de K (ver por ejemplo la demostración del Teorema 56 en [Rot98]).

Ejemplo 1.26. Toda extensión L/K cuadrática (o sea $[L:K] = 2$) es claramente Galois.

Existe otra construcción muy importante que es la de agregar no las raíces de un polinomio irreducible de K, sino agregar todas las raíces de todos los polinomios irreducibles de K.

Definición 1.27. Una clausura algebraica de K es una extensión algebraica L/K que satisface la propiedad de que todo polinomio $p(x) \in K[x]$ posee todas sus raíces en L, o sea $p(x)$ se factoriza como producto de polinomios de grado 1 en $L[x]$.

Teorema 1.28. *Todo cuerpo K posee una clausura algebraica que denotamos por $\overline{K}$. Dicha clausura algebraica es única salvo isomorfismos.*

Así por ejemplo, la clausura algebraica de $\mathbb{C}$ es $\mathbb{C}$, mientras que la clausura algebraica de $\mathbb{R}$ es $\mathbb{C}$. La clausura algebraica de $\mathbb{Q}$ la podemos pensar como los números algebraicos de $\mathbb{C}$, o sea $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \ : \ \alpha \text{ es algebraico sobre } \mathbb{Q}\}$. Notar que $\overline{\mathbb{Q}}$ es mucho mas chico que $\mathbb{C}$. Es fácil ver que $\overline{\mathbb{Q}}$ es numerable, mientras que $\mathbb{C}$ claramente no lo es.

Si la extensión L/K es Galois, denotamos por $\mathrm{Gal}(L/K)$ al grupo $\mathrm{Aut}_K(L)$. El principal resultado de la teoría de Galois es el siguiente.

Teorema 1.29 (Galois)**.** *Si L/K es una extensión Galois y finita, entonces:*

1. $\#\,\mathrm{Gal}(L/K) = [L:K]$.
2. *Existe una biyección entre los siguientes conjuntos:*
   $\{$*Subextensiones N con $K \subset N \subset L$*$\}$ *y el conjunto de subgrupos de* $\mathrm{Gal}(L/K)$*, o sea* $\{H : H < \mathrm{Gal}(L/K)\}$*. La biyección esta dada por:*

$$N \ \to \ \mathrm{Aut}_N(L) \subset \mathrm{Gal}(L/K) \tag{1.5}$$

$$\{\alpha \in L \ : \ \sigma(\alpha) = \alpha\,,\ \forall \sigma \in H\} \ \leftarrow \ H \tag{1.6}$$

   Al conjunto $\{\alpha \in L \ : \ \sigma(\alpha) = \alpha\,,\ \forall \sigma \in H\}$ se lo denota L^H.
3. *Si $K \subset N \subset L$, entonces la extensión N/K es Galois si y sólo si el grupo* $\mathrm{Gal}(L/N)$ *es un subgrupo normal de* $\mathrm{Gal}(L/K)$*. En tal caso,* $\mathrm{Gal}(N/K) \simeq \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/N)$.

Ejemplos 1.30.

1. Consideremos el cuerpo $K := \mathbb{Q}(\sqrt{2})$, que corresponde al cuerpo de descomposición del polinomio irreducible $x^2 - 2$ en $\mathbb{Q}[x]$. La extensión $K/\mathbb{Q}$ es Galois (por ser de grado 2, o por ser K un cuerpo de descomposición), y el grupo $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ tiene orden 2. El elemento no trivial corresponde a la involución $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$, donde $a, b \in \mathbb{Q}$.
2. Consideremos K el cuerpo de descomposición del polinomio $x^3 - 2$. En términos de radicales, $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ (recordar que las raíces cúbicas de la unidad son $\xi_3 = \frac{-1+\sqrt{-3}}{2}$ y su conjugado). En particular $[K:\mathbb{Q}] = 6$ (>por qué?). El grupo $\mathrm{Gal}(K/\mathbb{Q})$ tiene orden 6, y está generado por los morfismos:
   - $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(\sqrt{-3}) = -\sqrt{-3}$,
   - $\sigma(\sqrt[3]{2}) = \xi_3\sqrt[3]{2}$, $\sigma(\sqrt{-3}) = \sqrt{-3}$.

   El morfismo τ tiene orden 2 mientras que σ tiene orden 3. Es fácil verificar que $\sigma\tau \neq \tau\sigma$, con lo cual $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3$.

Por último, queremos mencionar la estructura que tienen los grupos de Galois de cuerpos finitos. Si K es un cuerpo de característica p, entonces $\mathbb{F}_p \subset K$. En particular, existe un morfismo llamado de *Frobenius*, y denotado σ_p dado por

$$\sigma_p(x) = x^p.$$

Ejercicio 1.31. Probar que si K tiene característica p (en particular cualquier múltiplo de p es cero en K), entonces el morfismo de Frobenius es un morfismo de cuerpos, o sea $(a+b)^p = a^p + b^p$ y $(ab)^p = a^p b^p$.

Teorema 1.32. *Si K es un cuerpo finito de p^d elementos, entonces* $\mathrm{Gal}(K/\mathbb{F}_p)$ *es cíclico de orden d. Más aún,* $\mathrm{Gal}(K/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$.

2. Representaciones de Artin

2.1. Introducción a las representaciones de Artin. Sea $K/\mathbb{Q}$ una extensión finita de Galois. Vamos a estudiar las representaciones

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}(V)$$

donde V es un espacio vectorial de dimensión finita sobre $\mathbb{C}$. Veremos cómo Artin le asocia a ρ una serie de Dirichlet $L(\rho, s)$ que extiende simultáneamente la definición de la función zeta de Riemann $\zeta(s)$ y de las series $L(\chi, s)$ donde χ es un carácter de Dirichlet. Estas *L-series de Artin* $L(\rho, s)$ codifican mucha de la aritmética del cuerpo de números K.

2.2. Representaciones lineales de grupos finitos. Empezamos considerando sólo un grupo finito G (que luego será $\mathrm{Gal}(K/\mathbb{Q})$) dejando de lado la extensión $K/\mathbb{Q}$. Una *representación* de G es un homomorfismo

$$\rho : G \to \mathrm{GL}(V)$$

donde V es un espacio vectorial de dimensión finita sobre $\mathbb{C}$. En otras palabras, G actúa en V por medio de transformación lineales. También hablaremos de la representación V, usando la notación $g \cdot v$ (o simplemente gv) para $g \in G$ y $v \in V$ en vez de $\rho(g)(v)$, cuando la representación ρ en cuestión es clara del contexto.

Sea $n := \dim V$. Si elegimos una base de V tenemos que $\mathrm{GL}(V)$ es isomorfo al grupo lineal $\mathrm{GL}_n(\mathbb{C})$ de matrices $n \times n$ complejas inversibles. Nos interesan las representaciones sólo módulo isomorfismo, por definición la clase de isomorfía de ρ es la clase módulo conjugación del homomorfismo resultante

$$\rho : G \to \mathrm{GL}_n(\mathbb{C}),$$

que abusando la notación seguimos llamando ρ si no lleva a confusión, independientemente de la base elegida. Pasaremos de una versión de ρ a otra según convenga.

En lo que sigue damos un resumen breve de las propiedades principales de las representaciones de grupos finitos que necesitamos. Las demostraciones se pueden encontrar en cualquier libro introductorio (como [FH91]).

Definición 2.1. i) Una subrepresentación de V es un subespacio $U \subseteq V$ que es estable por multiplicación por G via ρ. Es decir, para todo $u \in U$ y para todo $g \in G$ vale que

$$\rho(g)u \in U.$$

ii) La representación ρ es irreducible si y sólo si sus únicas subrepresentaciones son $\{0\}$ y V.

Teorema 2.2. *Toda representación de G es suma directa de representaciones irreducibles.*

Demostración. La idea de la demostración es probar que si $U \subseteq V$ es una subrepresentación entonces existe otra subrepresentación U' tal que

$$V = U \oplus U'.$$

Sabemos que existe siempre un tal subespacio vectorial U' (un complemento de U). Lo que necesitamos probar es que se puede elegir U' tal que también sea estable por multiplicación por G vía ρ.

Una forma útil de mostrar esto es probando que existe un producto Hermitiano $(\cdot,\cdot)$ no degenerado en V para el cual $\rho(g)$ es una isometría. En efecto, dado este producto basta tomar $U' = U^{\perp}$. Para conseguir un tal producto Hermitiano empezamos con un producto Hermitiano positivo cualquiera $(\cdot,\cdot)_0$ y definimos

$$(u, v) := \sum_{g\in G}(gu, gv)_0$$

como el promedio de $(\cdot,\cdot)_0$ sobre G. □

Vale la pena notar que este resultado fundamental es falso en situaciones mas generales. Por ejemplo,

1) si el grupo G es infinito:

$$\begin{array}{rccc} \rho & : \mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ & 1 & \longmapsto & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array}$$

tiene como única subrepresentación de dimensión 1 el subespacio generado por el vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$;

2) si la característica del cuerpo divide al orden del grupo:

$$\begin{array}{rccc} \rho & : \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_p) \\ & 1 & \mapsto & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array}$$

también tiene como única subrepresentación de dimensión 1 el subespacio generado por el vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Una observación importante sobre nuestras representaciones ρ es la siguiente.

Proposición 2.3. *Sea $g \in G$ y $A := \rho(g) \in \mathrm{GL}_n(\mathbb{C})$. Entonces*

1) A es diagonalizable;

2) los autovalores de A son raíces de la unidad de orden dividiendo $|G|$.

Definición 2.4. Dada una representación ρ definimos su *carácter* $\chi : G \to \mathbb{C}$ como la función

$$\chi(g) := \mathrm{Tr}(\rho(g)).$$

Es claro que χ sólo depende de la clase de isomorfía de ρ. De hecho, tenemos el siguiente resultado fundamental.

Teorema 2.5. *El carácter χ determina unívocamente la clase de isomorfía de ρ; mas precisamente, dos representaciones ρ, ρ' son isomorfas si y sólo si sus respectivos caracteres χ, χ' son iguales.*

Veamos algunas de las propiedades básicas del carácter de una representación.

Proposición 2.6. *Sea*

$$\rho : G \to \mathrm{GL}(V)$$

una representación, χ su carácter y $n := \dim V$ su dimensión. Para todo $g \in G$ tenemos

1. χ *es constante en clases de conjugación de* G*;*
2. $\chi(g)$ *es un entero algebraico (esto es* $\chi(g)$ *es raíz de un polinomio mónico con coeficientes enteros);*
3. $|\chi(g)| \leq n$*;*
4. *la igualdad vale en 3. si y sólo si* $\rho(g)$ *es la identidad;*
5. $\chi(1) = n$*.*

2.3. Representaciones de permutación de grupos finitos. Una forma natural en que la que ocurre un grupo es por medio de permutaciones de un conjunto finito; por ejemplo, caso central a estas notas, el grupo de Galois de un polinomio actúa como permutación de sus raíces.

Sea G un grupo finito y X un conjunto finito donde G actúa por medio de permutaciones; i.e., tenemos $G \hookrightarrow S(X)$. Llamamos esto una *representación de permutación* de G y le asociamos una representación lineal ρ como sigue. Sea $V = \{\varphi : X \to \mathbb{C}\}$ el espacio vectorial de funciones en X a valores complejos. Definimos para $x \in X$

$$\rho(g)\varphi(x) := \varphi(g^{-1}x).$$

Es fácil verificar que tenemos efectivamente una representación de G

$$\rho : G \to \mathrm{GL}(V)$$

de dimensión $\dim(V) = \#X$. (Aquí es crucial que la definición usa g^{-1} en el argumento de φ para que se satisfaga que $\rho(g_1g_2) = \rho(g_1)\rho(g_2)$ y no $\rho(g_1g_2) = \rho(g_2)\rho(g_1)$.) Resulta también sencillo verificar que el carácter χ asociado a ρ está dado por el número de puntos fijos de g:

$$\chi(g) = \#\{x \in X \mid gx = x\}.$$

En particular, el carácter toma valores enteros no negativos.

Notemos que el subespacio de V de las funciones constantes es una subrepresentación de ρ de dimensión uno. Por lo tanto, una representación lineal que proviene de una de permutación no es nunca irreducible si su dimensión es mayor que uno.

Ejemplo 2.7. Tomemos como ejemplo $G = S_n$ actuando en $\{1, \ldots, n\}$ en forma natural. Obtenemos una representación lineal de dimensión n. Concretamente, $\sigma \in S_n$ actúa en $\mathbb{C}^n$ por medio de la correspondiente matriz de permutación $A = (a_{i,j})$ donde

$$a_{i,j} = \begin{cases} 1, & \sigma^{-1}(i) = j \\ 0, & \sigma^{-1}(i) \neq j \end{cases},$$

ya que en la base canónica $e_1, \ldots, e_n$ de $V_0 := \mathbb{C}^n$ (pensando el vector e_i como la función definida por $e_i(j) = \delta_{i,j}$ para $j = 1, \ldots, n$) tenemos

$$\sigma e_i = e_{\sigma(i)}.$$

Las matrices de permutación son aquellas que tienen un solo elemento no nulo igual a 1 en cada fila y columna.

Explícitamente, tomemos por ejemplo $n = 5$ y $\sigma = (235) \in S_5$. Entonces si $v = (a, b, c, d, e)$ tenemos

$$\sigma v = ae_1 + be_3 + ce_5 + de_4 + ee_2 = (a, e, b, d, c)$$

y la matriz de permutación correspondiente es

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Para $n > 1$ la representación se descompone en la suma directa no trivial de representaciones

$$V_0 = U \oplus V$$

donde $U := \langle (1, 1, \ldots, 1) \rangle$ y

$$V := \{(x_1, \ldots, x_n) \,|\, x_1 + \cdots + x_n = 0\}.$$

Llamamos a V la *representación estándar* de S_n.

Teorema 2.8. *La representación estándar de S_n es irreducible.*

Ejemplo 2.9. Si $H < G$ es un subgrupo, G actúa en las coclases G/H a izquierda por multiplicación: $g \cdot xH := (gx)H$. Obtenemos entonces una representación de permutación y por lo tanto una representación lineal correspondiente de dimensión $[G : H]$. Si tomamos $H = \{1\}$ el subgrupo trivial la representación correspondiente se conoce como la *representación regular* ρ_{reg} de G. Su dimensión es $|G|$ y su carácter asociado es la función

$$\chi_{\text{reg}}(g) = \begin{cases} |G|, & g = 1 \\ 0, & g \neq 1 \end{cases}.$$

En la representación de permutación asociada a un subgrupo $H \leqslant G$, el grupo G actúa transitivamente (podemos pasar de una coclase xH a la coclase H multiplicando a izquierda por x^{-1}). Recíprocamente, toda acción transitiva de G en un conjunto finito X da lugar a una representación de permutación isomorfa a G/H donde H es el estabilizador de un punto cualquiera de X.

Por otro lado, toda acción de G en un conjunto finito X determina una partición de X en órbitas. En cada órbita G actúa transitivamente. Concluimos que las representaciones lineales de G que provienen de una representación de permutación son suma directa de aquellas asociadas a subgrupos.

Digamos que dos representaciones de permutación de un grupo G son *equivalentes* si existe una biyección equivariante entre los respectivos conjuntos donde G actúa. En ese caso las representaciones lineales correspondientes son isomorfas. Veremos más adelante §4.3 que la recíproca no es cierta. Existen representaciones de permutación no equivalentes que dan lugar a representaciones lineales isomorfas. Este fenómeno esta relacionado con el problema de *can you hear the shape of a drum?* de variedades Riemannianas. En nuestro contexto da lugar a cuerpos de números no isomorfos con la misma función zeta.

En general clasificar representaciones de permutación módulo equivalencia es bien difícil mientras que clasificar representaciones lineales módulo isomorfismo es mucho más accesible, como vemos en la sección siguiente.

2.4. Tabla de caracteres. En el espacio vectorial de funciones $\phi : G \longrightarrow \mathbb{C}$ definimos el producto Hermitiano

$$(\phi, \psi) := \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}.$$

Sea $\mathcal{C}$ el subespacio vectorial de todas las funciones $G \longrightarrow \mathbb{C}$ que son constante en clases de conjugación con el mismo producto Hermitiano. Una tal función se llama una *función de clase*. Como vimos (Proposición(2.6) i) el carácter χ de una representación de G es un elemento de $\mathcal{C}$.

Teorema 2.10. *El conjunto de caracteres de representaciones irreducibles de G es una base ortonormal de $\mathcal{C}$.*

Corolario 2.11. 1. *El número de representaciones irreducibles de G no isomorfas entre sí es igual al número de clases de conjugación de G.*

2. *Sea $U_1, \dots, U_r$ una lista de todas las representaciones irreducibles de G no isomorfas entre sí. Denotemos por χ_i el carácter de U_i. Sea V una representación arbitraria de G de carácter χ. Entonces, V admite una descomposición en suma directa*

$$V \simeq U_1^{m_1} \oplus \cdots \oplus U_r^{m_r},$$

con enteros no negativos $m_1, \dots, m_r$ si y sólo si

$$\chi = m_1\chi_1 + \cdots m_r\chi_r.$$

El entero m_i se llama la *multiplicidad* de U_i en V; notemos que

$$m_i = (\chi, \chi_i).$$

Deducimos que toda la información necesaria para descomponer representaciones de un grupo finito G en suma de irreducibles está contenida en la *tabla de caracteres* de G. Ésta consiste en una matriz $r \times r$ con los valores $\chi_i(c_j)$, donde $c_1, \dots, c_r$ son representantes de las clases de conjugación de G. Conviene también listar el número de elementos de cada clase de conjugación para facilitar el cálculo del producto interno.

Veamos un ejemplo. Tomemos $G = S_4$. Su tabla de caracteres es la siguiente.

	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
	1	6	8	6	3
U	1	1	1	1	1
U'	1	−1	1	−1	1
V	3	1	0	−1	−1
V'	3	−1	0	1	−1
W	2	0	−1	0	2

La tabla se puede calcular usando alguno de los varios programas existentes (por ejemplo MAGMA o GAP). También se puede calcular a mano sin gran dificultad. Aquí elegimos tomar la tabla como dada y entender las representaciones irreducibles de S_4 a partir de ella.

La primer fila da los representantes $c_1, \dots, c_5$ de las clases de conjugación. En general para S_n las clases de conjugación están naturalmente indexadas por la descomposición en ciclos. La segunda fila tiene el número de elementos de la clase correspondiente (1 elemento trivial, 6 transposiciones, 8 triciclos, etc.).

Cada fila de la tabla corresponde al carácter de una representación irreducible de S_4. En general es bastante mas fácil dar el carácter de una representación irreducible que describir explícitamente la representación misma. Quizás parezca paradójico pero no es inusual obtener el carácter de una representación primero y solo luego construir trabajosamente la representación. Nos encontramos algo artificialmente en tal situación pero es un caso sencillo.

Las dos primeras representaciones U, U' son la representación trivial (donde $\rho(g) = 1$ para todo $g \in G$) y la representación signo respectivamente (donde $\rho(\sigma) = \epsilon(\sigma)$ es el signo de la permutación σ). La representación V es la representación estándar de S_4 ya mencionada y $V' = V \otimes U'$ es su producto tensorial con la representación signo (esto es $\rho_{V'}(\sigma) = \epsilon(\sigma)\rho_V(\sigma)$).

Nos queda entender la última representación W. Notemos que su carácter χ_W esta completamente determinado por el resto de la tabla. En efecto, χ_W es ortogonal a todas las otras filas (una condición que determina un espacio vectorial de dimensión 1 en $\mathcal{C}$), tiene norma $(\chi_W, \chi_W) = 1$ y $\chi_W(1) = \dim W$.

El grupo S_4 tiene un subgrupo normal $A \trianglelefteq S_4$ de orden 4, el famoso *Vierergruppe* de Klein. Consiste de la identidad y todos los productos de dos transposiciones disjuntas

$$A := \{1, (12)(34), (13)(24), (14)(23)\}.$$

El cociente S_4/A es isomorfo a S_3. Componiendo el homomorfismo correspondiente $S_4 \longrightarrow S_3$ con la representación estándar de S_3 obtenemos una representación ρ de dimensión 2 de S_4. Como la representación estándar de S_3 es irreducible (Teorema 2.8) ρ también lo es.

Más directamente, S_4 actúa por conjugación en el conjunto $\{(12)(34), (13)(24), (14)(23)\}$ y un cálculo simple muestra que la correspondiente representación es isomorfa a $U \oplus W$.

3. Aritmética en extensiones

3.1. Factorización en primos. Sea $K/\mathbb{Q}$ una extensión finita de grado n y $\mathcal{O}_K$ su anillo de enteros, esto es el conjunto formado por todos los enteros algebraicos en K (que se puede ver es un anillo). Un número primo p genera un ideal primo de $\mathbb{Z}$ que se factoriza en $\mathcal{O}_k$ de la siguiente forma,

$$p\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}, \tag{3.1}$$

donde $\mathcal{P}_i$ son primos distintos de $\mathcal{O}_K$ y e_i son enteros positivos. La factorización es única salvo reordenamiento. Definimos los enteros positivos $f_1, \ldots, f_r$ tal que

$$|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}, \qquad i = 1, \ldots, r.$$

Se tiene entonces que

$$e_1 f_1 + \cdots e_r f_r = n.$$

De hecho, salvo para un número finito de excepciones los exponentes e_i son siempre igual a uno. Tales primos p para los que algún $e_i > 1$ se llaman *ramificados* en $K/\mathbb{Q}$.

Teorema 3.1. *(Dedekind) Sea $h \in \mathbb{Z}[x]$ un polinomio mónico irreducible tal que $K \simeq \mathbb{Q}[x]/(h)$. Sea Δ el discriminante de h y $p \nmid \Delta$ un primo. Entonces p es no ramificado en $K/\mathbb{Q}$ y si*

$$h \equiv h_1 \cdots h_r \text{ mód } p,$$

es la factorización de h en $\mathbb{Z}/p\mathbb{Z}[x]$ en producto de irreducibles distintos se tiene que ordenando los factores apropiadamente el grado de h_i es f_i.

En general, Δ es divisible por más primos que los ramificados en K y para estos primos el teorema deja sin poder calcular los f_i. Para buena parte de nuestra discusión esto no es un gran inconveniente.

3.2. Automorfismo de Frobenius. Sea $L/\mathbb{Q}$ una extensión finita de Galois de grado n, $\mathcal{O}_L$ su anillo de enteros y $G := \mathrm{Gal}(L/\mathbb{Q})$. Tomemos un primo p y $\mathcal{P}$ un primo de L en la factorización de p en $\mathcal{O}_L$. El *grupo de descomposición* $D_\mathcal{P}$ de $\mathcal{P}$ es el subgrupo de G de elementos que fijan $\mathcal{P}$. Tenemos un morfismo de reducción natural

$$\phi : D_\mathcal{P} \to \mathrm{Gal}(k_\mathcal{P}/k), \tag{3.2}$$

donde $k_\mathcal{P} := \mathcal{O}_L/\mathcal{P}$ y $k := \mathbb{Z}/p\mathbb{Z}$. Este morfismo ϕ es siempre sobreyectivo, su núcleo $I_\mathcal{P}$ se conoce como el *grupo de inercia* de $\mathcal{P}$. Si el primo p es no ramificado en $L/\mathbb{Q}$ el grupo de inercia es trivial y ϕ es un isomorfismo.

El grupo de Galois $\mathrm{Gal}(k_\mathcal{P}/k)$ es cíclico generado por el automorfismo $\sigma_p : x \mapsto x^p$ (ver Teorema 1.32). En el caso de que p sea no ramificado existe entonces un único automorfismo $\mathrm{Frob}_\mathcal{P} \in D_\mathcal{P}$, el *automorfismo de Frobenius* asociado a $\mathcal{P}$, tal que $\phi(\mathrm{Frob}_\mathcal{P}) = \sigma_p$.

Si p es no ramificado y tomamos otro primo $\mathcal{P}'$ en la factorización de p obtenemos un automorfismo $\mathrm{Frob}_{\mathcal{P}'}$ conjugado a $\mathrm{Frob}_\mathcal{P}$. Esto resulta del hecho que el grupo de Galois G actúa transitivamente en los primos de L que dividen a p. En definitiva tenemos que dado un primo p no ramificado en $L/\mathbb{Q}$ existe una clase de conjugación de G asociada bien definida Frob_p: la clase de conjugación de $\mathrm{Frob}_\mathcal{P}$ para cualquier primo $\mathcal{P}$ de L que divide a p.

Tomemos ahora una extensión finita arbitraria $K/\mathbb{Q}$ y sea $L/\mathbb{Q}$ su clausura Galoisiana (esto es la menor extensión de Galois que contiene a K). Un primo p no ramificado en K sera también no ramificado en L. La factorización de p en $\mathcal{O}_K$ determina una *partición* de $n := [K : \mathbb{Q}]$: $\tau_p := [f_1, f_2, \ldots, f_r]$ donde $f_1 \geq f_2 \geq \cdots f_r$. Basta reordenar los números f_i de mayor a menor. Llamaremos a τ_p *tipo* de factorización de p en K.

Sea $h \in \mathbb{Q}[x]$ un polinomio irreducible tal que $K = \mathbb{Q}(\theta)$ con $\theta \in K$ una raíz de h. El grupo de Galois $G = \mathrm{Gal}(L/\mathbb{Q})$ actúa en las raíces de h lo que nos da un homomorfismo $\iota : G \to S_n$.

Teorema 3.2. *Con la notación anterior, tenemos que la partición de n dada por la descomposición en ciclos de $\iota(\mathrm{Frob}_p)$ es τ_p.*

Combinando este resultado con el Teorema 3.1 nos da una forma práctica de conocer la descomposición en ciclos de los automorfismos de Frobenius como permutación de las raíces de h. Observemos que esto *no* es lo mismo que la clase de conjugación en G. En efecto al pasar de G a S_n vía ι dos elementos de G pueden ser conjugados en S_n si ser conjugados en G. De todas formas este resultado es sumamente útil.

3.3. Un ejemplo. Teorema de Chebotarev. Tomemos $h = x^4 + x + 1$ y $K := \mathbb{Q}(\theta)$ con $\theta \in \mathbb{C}$ una raíz cualquiera de h. Como su discriminante 229 es primo tenemos que $\mathrm{disc}(K) = 229$. Esta es la lista de τ_p para los primos $p \leq 50$.

p	τ_p
2	[4]
3	[3, 1]
5	[3, 1]
7	[4]
11	[3, 1]
13	[4]
17	[3, 1]
19	[3, 1]
23	[2, 1, 1]
29	[2, 1, 1]
31	[4]
37	[2, 2]
41	[4]
43	[3, 1]
47	[2, 1, 1]

Vemos que aparecieron todos las posibles particiones de 4 excepto por $[1, 1, 1, 1]$. De hecho tenemos el siguiente resultado de Chebotarev. (En lo que sigue ignoramos tácitamente los primos ramificados o en general que dividan al discriminante del polinomio en cuestión).

Teorema 3.3. *Sea C una clase de conjugación de G. Entonces*

$$\lim_{x\to\infty} \frac{\#\{p \leq x \mid \mathrm{Frob}_p = C\}}{\#\{p \leq x\}} = \frac{\#C}{|G|}. \tag{3.3}$$

Corolario 3.4. *Sea τ una partición de n correspondiente a la descomposición de ciclos de $\iota(\sigma)$ para un $\sigma \in G$. Entonces existen infinitos primos p tales que $\tau = \tau_p$.*

En nuestro ejemplo se puede verificar que $G = S_4$ (de hecho, dada la lista de τ_p que obtuvimos necesariamente $G = S_4$). Entonces de acuerdo al corolario toda partición de 4 es de la forma τ_p para infinitos primos p. Es típico que la clase $[1, 1, \ldots, 1]$ que corresponde a $\sigma = 1$ (o alternativamente a primos p donde h se factoriza en n factores lineales módulo p) requiera primos p más bien grandes (ver [RS94]). En nuestro caso el primer primo tal

que $\tau_p = [1,1,1,1]$ es $p = 193$ aunque la proporción de tales primos con $p \leq x$ para x muy grande es aproximadamente $1/24$.

Para una partición τ de n sea

$$\delta(\tau, x) := \frac{\#\{p \leq x \mid \tau_p = \tau\}}{\#\{p \leq x\}}.$$

En la Figura 1 damos una lista de $d(x) := 24\delta([1,1,1,1], x)$ para varios valores de x. El Teorema 3.3 de Chebotarev garantiza que $\lim_{x\to\infty} d(x) = 1$.

k	$d(500k)$
1	0.252631579
2	0.428571429
3	0.702928870
4	0.633663366
5	0.719346049
6	0.837209302
7	0.785276074
8	0.872727273
9	0.944262295
10	0.932735426

k	$d(10^4k)$
1	0.937347437
2	0.933687003
3	0.902311248
4	0.896502498
5	0.921098773
6	0.911342249
7	0.934390771
8	0.958530050
9	0.980603696
10	0.988323603

k	$d(10^6k)$
1	0.989069785
2	0.994594885
3	0.995682975
4	0.995867856
5	0.997770528
6	0.994533110
7	0.998170558
8	0.996455944
9	0.996705334
10	0.996071197

FIGURA 1. Valores de $24\delta([1,1,1,1], x)$

Como vemos la convergencia en (3.3) no es particularmente rápida; es importante tener buenas cotas para el error

$$\frac{\#\{p \leq x \mid \mathrm{Frob}_p = C\}}{\#\{p \leq x\}} - \frac{\#C}{|G|}$$

y esto está ligado a la hipótesis de Riemann generalizada. Ver [SL96] para una historia del Teorema de Chebotarev y [LO77] para una demostración con una cota para el error.

Desde otro punto de vista, el tipo de factorización τ_p codifica el número de raíces que tiene el polinomio en los cuerpos $\mathbb{F}_q$ con q una potencia de p. (Éste es el punto de vista adoptado en [RV07].) Más precisamente, sea

$$N(q) := \#\{\theta \in \mathbb{F}_q \mid f(\theta) = 0\}.$$

Entonces, es claro que

$$N(p^r) = \sum_{d|r} m_d$$

donde m_d es el número de partes de τ_p iguales a d. Ver [Ser12] para una discusión general sobre cómo varía el número de puntos de una variedad algebraica sobre un cuerpo finito.

4. Series L de Artin

Ahora combinamos las representaciones de grupos finitos de la sección 2.2 con la aritmética de la sección 3 para definir las series L de Artin. Estas series generalizan simultáneamente la función ζ de un cuerpo de números y las series $L(\chi, s)$ asociadas a un carácter de Dirichlet.

Supongamos que $L/\mathbb{Q}$ es una extensión finita de Galois con $G := \mathrm{Gal}(L/\mathbb{Q})$ y que

$$\rho: \quad G \to GL(V)$$

es una representación compleja de G. Siguiendo a Artin vamos a definir una serie de Dirichlet, es decir una serie de la forma

$$L(\rho, s) = \sum_{n\geq 1} a_n n^{-s}, \qquad \Re(s) \gg 0, \tag{4.1}$$

asociada a esta situación.

Esta serie se define a partir de un producto de Euler de la forma de

$$L(\rho, s) = \prod_p L_p(\rho, p^{-s})^{-1}, \tag{4.2}$$

donde p recorre todos los números primos y $L_p(\rho, T)$ son polinomios de grado acotado. Llamamos a $L_p(\rho, T)$ el *factor de Euler* en p.

4.1. Factores de Euler. Si p es un primo no ramificado de $L/\mathbb{Q}$ definimos el factor de Euler asociado de la siguiente manera

$$L_p(\rho, T) := \det\left(1 - \rho(\mathrm{Frob}_p)T\right).$$

Hay algo de abuso de notación aquí ya que Frob_p no es un elemento de G si no una clase de conjugación. Pero basta tomar cualquier representante de esta clase para calcular el determinante. El resultado no dependerá de esta elección. Lo mismo sucede en lo que sigue al tomar la traza $\mathrm{Tr}(\rho(\mathrm{Frob}_p))$, por ejemplo. No insistiremos con el tema.

Tenemos que

$$L_p(\rho, T) = 1 - a_p\, T + \cdots$$

y por lo tanto

$$L_p(\rho, T)^{-1} = 1 + a_p\, T + \cdots$$

Vemos entonces que la traza de $\rho(\mathrm{Frob}_p)$ es el coeficiente de p^{-s} en (4.1), es decir

$$a_p = \mathrm{Tr}(\rho(\mathrm{Frob}_p)).$$

Si el primo p es ramificado y $\mathcal{P}$ es un divisor primo de p en L, la preimagen de $x \mapsto x^p$ vía ϕ en (3.2) es único sólo módulo el grupo de inercia $I_{\mathcal{P}}$. Es decir, tenemos un elemento $\mathrm{Frob}_{\mathcal{P}} \in D_{\mathcal{P}}/I_{\mathcal{P}}$ bien definido. Este elemento da lugar a su vez a un elemento $\rho(\mathrm{Frob}_{\mathcal{P}}) \in \mathrm{GL}(V^{I_{\mathcal{P}}})$ bien definido. Aquí $V^{I_{\mathcal{P}}} \subseteq V$ es el subespacio de los elementos de V que quedan fijos por los elementos de $I_{\mathcal{P}}$. Podemos definir el factor de Euler asociado a p entonces como $L_p(\rho, T) := \det\left(1 - \rho(\mathrm{Frob}_{\mathcal{P}})T|_{V^{I_{\mathcal{P}}}}\right)$. El resultado no depende de la elección del divisor primo $\mathcal{P}$ ya que eligiendo otro divisor da lugar a un elemento conjugado.

La serie de Artin (4.2) formada con estos factores de Euler converge absolutamente para $\Re(s) > 1$ (usando la Proposición 2.3 (3)). Notemos que el grado de los factores de Euler $L_p(\rho, T)$ es a lo sumo $\dim V$ y es igual a $\dim V$ salvo un número finito de casos (que serán algunos de los primos ramificados). Es una conjetura de Artin que para ρ no-trivial la serie $L(\rho, s)$ se extiende a una función entera de la variable s y satisface una ecuación funcional relacionando $L(\rho, s)$ con $L(\rho, 1 - s)$.

4.2. Ejemplo I: polinomios de grado cuatro. Sea $h \in \mathbb{Z}[x]$ un polinomio irreducible de grado $n = 4$ y $\theta \in \mathbb{C}$ una raíz de h. Definimos $K := \mathbb{Q}(\theta)$ y $L \subset \mathbb{C}$ su clausura Galois. Supongamos que $G := \mathrm{Gal}(L/\mathbb{Q})$ es isomorfo al grupo S_4 de permutaciones de cuatro elementos, digamos $X := \{1, 2, 3, 4\}$. Vamos a describir las series L de Artin de $L/\mathbb{Q}$ asociadas a las representaciones irreducibles de S_4 (que ya describimos en §2.4).

Como vimos en §2.3 la acción natural de S_4 en X da lugar a una representación lineal V_0 isomorfa a $U \oplus V$, donde U es la representación trivial y V la representación estándar. Numerando las raíces de h en $\mathbb{C}$ apropiadamente la acción de G es justamente esta acción natural de S_4 en X.

Una forma más conceptual y completa del Teorema 3.2 es la siguiente

$$L(V_0, s) = \zeta_K(s) := \prod_{\mathcal{P}} (1 - \mathbb{N}\mathcal{P}^{-s})^{-1}, \tag{4.3}$$

donde el producto recorre todos los primos $\mathcal{P}$ del anillo de enteros $\mathcal{O}_K$ de K. Notar que $\mathbb{N}\mathcal{P} = |\mathcal{O}_L/\mathcal{P}| = p^f$. La función $\zeta_K(s)$ es la función zeta del cuerpo K; coincide con la función zeta de Riemann $\zeta(s)$ cuando $K = \mathbb{Q}$.

En efecto, para un primo p que no divide al discriminante de h, la factorización de h módulo p determina la factorización de p en K. Esta factorización a su vez nos da el factor de Euler en $\zeta_K(s)$ donde $\mathbb{N}\mathcal{P}$ que no es otro que $L_p(V_0, T)$. Vemos que (4.3) extiende apropiadamente el Teorema 3.2 a *todos* los primos.

La descomposición de ρ en representaciones irreducibles corresponde a la factorización

$$\zeta_K(s) = L(U, s)L(V, s),$$

de las respectivas funciones L de Artin. Como $L(U, s) = \zeta_{\mathbb{Q}}(s) = \zeta(s)$ deducimos que

$$L(V, s) = \zeta_K(s)/\zeta(s).$$

Resumimos el argumento que usamos para el caso general

Proposición 4.1. *Sea $h \in \mathbb{Q}[x]$ un polinomio irreducible de grado n y $\theta \in \mathbb{C}$ una raíz de h. Sea $L/\mathbb{Q}$ la clausura de Galois de $\mathbb{Q}(\theta)/\mathbb{Q}$ con grupo de Galois G. Sea ρ la representación de G proveniente de la acción en las raíces de h. Entonces*

$$L(\rho, s) = \zeta_K(s). \tag{4.4}$$

Para simplificar la discusión, fijemos ahora $h := x^4 + x + 1$ de discriminante 229 como en §3.3. ¿Qué podemos decir de la serie L de Artin asociada a la representación de signo U'?

Si $\theta_1, \ldots, \theta_4$ son las raíces de h en $\mathbb{C}$, su discriminante es $\operatorname{disc}(h) = \prod_{i<j}(\theta_i - \theta_j)^2$. Consideremos

$$\Delta := \prod_{i<j}(\theta_i - \theta_j).$$

Claramente $\Delta^2 = \operatorname{disc}(h) = 229$ con lo que $F := \mathbb{Q}\left(\sqrt{229}\right)$ es un subcuerpo de $L = \mathbb{Q}(\theta_1, \ldots, \theta_4)$. Por otro lado una permutación $\sigma \in S_4$ actúa en Δ como

$$\Delta^\sigma = \epsilon(\sigma)\Delta.$$

Aplicando la Proposición 4.1 al polinomio $x^2 - 229$ vemos que

$$\zeta_F(s) = \zeta(s)L(U', s)$$

y deducimos que

$$L(U', s) = L(\chi, s)$$

donde $\chi(p) := \left(\frac{229}{p}\right)$ es el símbolo de Kronecker módulo 229. Es decir, la serie L de Artin de U' es la serie clásica de Dirichlet asociada a χ.

Notemos que para un primo $p \neq 229$ se tiene que

$$\epsilon(\mathrm{Frob}_p) = \chi(p)$$

o, lo que es lo mismo, Frob_p consiste de permutaciones pares si y sólo si (gracias a la reciprocidad cuadrática) p es un cuadrado módulo 229.

Esto se puede ver en la siguiente tabla donde agregamos una columna con los valores de $\chi(p)$ a la tabla que dimos en § 3.3.

p	τ_p	$\chi(p)$
2	[4]	-1
3	[3, 1]	1
5	[3, 1]	1
7	[4]	-1
11	[3, 1]	1
13	[4]	-1
17	[3, 1]	1
19	[3, 1]	1
23	[2, 1, 1]	-1
29	[2, 1, 1]	-1
31	[4]	-1
37	[2, 2]	1
41	[4]	-1
43	[3, 1]	1
47	[2, 1, 1]	-1

La serie L de Artin de V' se deduce de lo que ya vimos usando que $V' = V \otimes U'$. Si

$$L(V, s) = \sum_{n \geq 1} a_n n^{-s}$$

entonces

$$L(V', s) = \sum_{n \geq 1} \chi(n) a_n n^{-s}.$$

Nos queda describir $L(W, s)$. En paralelo a la descripción de W que dimos en § 2.4 definimos

$$\eta_1 := (\theta_1 + \theta_2)(\theta_3 + \theta_4), \qquad \eta_2 := (\theta_1 + \theta_3)(\theta_2 + \theta_4), \qquad \eta_3 := (\theta_1 + \theta_4)(\theta_2 + \theta_3)$$

y

$$g(x) := (x - \eta_1)(x - \eta_2)(x - \eta_3).$$

El grupo de Galois G preserva el conjunto $\{\eta_1, \eta_2, \eta_3\}$ y la acción correspondiente da lugar al homomorfismo sobreyectivo $S_4 \to S_3$. En particular, g tiene coeficientes racionales; es la *resolvente cúbica* de h. Encontramos que

$$g(x) = x^3 - 4x + 1$$

que es irreducible de discriminante 229. En general, si $h = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ la resolvente es

$$g(x) = x^3 - 2a_2x^2 + (a_2^2 + a_1a_3 - 4a_0)x + a_1^2 - a_1a_2a_3 + a_0a_3^2.$$

Sea $F = \mathbb{Q}(\eta_1) \subseteq L$. Aplicando la Proposición 4.1 al polinomio g vemos que

$$L(W, s) = \zeta_F(s)/\zeta(s).$$

Denotemos con σ_p el tipo de factorización de g módulo p. Obtenemos los siguientes valores (tabulados junto a los datos anteriores para comparar)

p	σ_p	τ_p	$\chi(p)$
2	[2,1]	[4]	-1
3	[3]	[3, 1]	1
5	[3]	[3, 1]	1
7	[2,1]	[4]	-1
11	[3]	[3, 1]	1
13	[2,1]	[4]	-1
17	[3]	[3, 1]	1
19	[3]	[3, 1]	1
23	[2,1]	[2, 1, 1]	-1
29	[2,1]	[2, 1, 1]	-1
31	[2,1]	[4]	-1
37	[1,1,1]	[2, 2]	1
41	[2,1]	[4]	-1
43	[3]	[3, 1]	1
47	[2,1]	[2, 1, 1]	-1

Vemos de la tabla que tienen el mismo signo dado por χ.

4.3. Ejemplo II: polinomio de Trinks. Terminamos con el ejemplo siguiente: $h := x^7 - 7x + 3$. En los años 60 Trinks [Tri68] descubrió, justamente calculando sus tipos de factorización τ_p para suficientes primos p, que h tiene grupo de Galois $G \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. Éste es el famoso grupo simple de orden 168 asociado a Klein. Notemos que a priori un polinomio al azar de grado 7 tiene grupo de Galois S_7 de orden $7! = 5040$. Es decir que h está lejos de ser un polinomio genérico.

En efecto, calculando para los primos $p \leq 10^{10}$ vemos que sólo aparecen los siguientes tipos de factorización (rutinas en PARI-GP para estos cálculos se pueden encontrar en [RV07]):

$$[7], \quad [4,2,1], \quad [3,3,1], \quad [2,2,1,1,1].$$

(Como ya vimos en §3.3 la clase de la identidad $[1,1,1,1,1,1,1]$, aunque es igual a τ_p con densidad positiva $1/|G|$, típicamente requiere que p sea muy grande en relación a los otros tipos.)

Podemos también calcular la densidad aproximada

$$\delta_\tau(x) := \frac{\#\{p \leq x \,|\, \tau_p = \tau\}}{\#\{p \leq x\}}$$

para cada tipo τ. Con $x = 10^{10}$ la mejor aproximación racional de $\delta_\tau(x)$ nos da lo siguiente

τ	$\delta_\tau(10^{10})$
$[7]$	$2/7$
$[4,2,1]$	$1/4$
$[3,3,1]$	$1/3$
$[2,2,1,1,1]$	$1/8$

Si sumamos todas estas densidades incluyendo $1/168$ correspondiendo al tipo que falta $\tau = [1,1,1,1,1,1,1]$ obtenemos: $2/7+1/4+1/3+1/8+1/168 = 1$. Todo esto es consistente con que $G \simeq \mathrm{PSL}_2(\mathbb{F}_7)$.

De hecho, $\mathrm{PSL}_2(\mathbb{F}_7)$ tiene seis clases de conjugación pero tenemos sólo cinco tipos de factorización. Esto es el fenómeno que mencionamos anteriormente en §3.2. Dos de estas clases de conjugación ($7A$ y $7B$ en notación estándar, de orden 7) son indistinguibles vistas en S_7 vía la acción del grupo de Galois G en las raíces de h. Es decir, no hay forma de saber a cual de estas dos clases pertenece Frob_p sólo sabiendo que $\tau_p = [7]$.

Tenemos también el otro fenómeno que mencionamos en §2.3. El grupo $G = \mathrm{PSL}_2(\mathbb{F}_7)$ tiene dos representaciones de permutación no equivalentes pero isomorfas como representaciones lineales. Esto se puede ver más claro usando que $G \simeq \mathrm{PGL}_3(\mathbb{F}_2)$. Sea $U \leqslant G$ el estabilizador de un punto del plano proyectivo de Fano $\mathcal{P}^2(\mathbb{F}_2)$ y U' el estabilizador de una recta. Entonces las representaciones en las coclases de U y U' tienen esta propiedad. Concretamente podemos tomar los subgrupos

$$U := \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}, \qquad U' := \begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Estos subgrupos no son conjugados; por lo tanto los cuerpos $K, K' \subseteq L$ correspondientes por teoría de Galois no son isomorfos. Existe sin embargo una biyección $\phi : U \longrightarrow U'$, dada por transposición $u \mapsto u^t$, con la propiedad que u y $\phi(u)$ son conjugadas. (Para ser claro: dada u existe $g \in G$ tal que $gug^{-1} = u^t$ pero no es cierto que existe tal g para *toda* u simultáneamente.)

Concluimos que para cada clase de conjugación C de G se tiene que

$$\#(C \cap U) = \#(C \cap U'). \tag{4.5}$$

Esto muestra que las representaciones lineales correspondientes son isomorfas. En particular, se tiene la igualdad

$$\zeta_K(s) = \zeta_{K'}(s).$$

No es difícil dar una ecuación para el cuerpo K', por ejemplo,

$$h'(x) := x^7 + 14x^4 - 42x^2 - 21x + 9.$$

5. Extensiones de cuerpos no finitas

5.1. Correspondencia de Galois. Queremos extender la relación entre extensiones y grupos de manera que permita considerar extensiones que no sean finitas. Al hacer esto, aparece un nuevo ingrediente que pasa desapercibido al trabajar con extensiones finitas, a saber *la topología*. Recordar que dar una topología en un conjunto es determinar que subconjuntos son abiertos, y cuales cerrados, satisfaciendo un conjunto de axiomas.

Definición 5.1. Un *espacio topológico* es un par $(X, \mathcal{B})$, donde X es un conjunto, y $\mathcal{B}$ es un conjunto de subconjuntos de X que satisface las siguientes propiedades:

1. El conjunto vacío y X están en $\mathcal{B}$.
2. La unión de elementos de $\mathcal{B}$ es un elemento de $\mathcal{B}$.
3. La intersección finita de elementos de $\mathcal{B}$, es un elemento de $\mathcal{B}$.

Los elementos de $\mathcal{B}$ son los llamados *abiertos* del conjunto X, y los cerrados son por definición complementos de abiertos.

Ejemplos 5.2.
1. Los espacios métricos son espacios topológicos (tomando $\mathcal{B}$ el conjunto de abiertos). Por ejemplo, $(\mathbb{R}^n, |\,.\,|_2)$ es un espacio topológico.
2. Si X es un conjunto arbitrario, podemos tomar $\mathcal{B}$ el conjunto de partes de X. Así, todo subconjunto es abierto y cerrado. Esta es la llamada topología discreta en X.
3. Si X es un conjunto arbitrario, podemos tomar $\mathcal{B} = \{\emptyset, X\}$. Esta es la llamada topología trivial en X.

Definición 5.3. Si G es un espacio topológico, y $* : G \times G \to G$ es una operación binaria tal que $(G, *)$ es un grupo, decimos que $(G, *)$ es un grupo topológico si vale que:

- El producto: $G \times G \to G$ es continuo.
- La función inversa: $\iota : G \to G$, $\iota(g) = g^{-1}$ es continua.

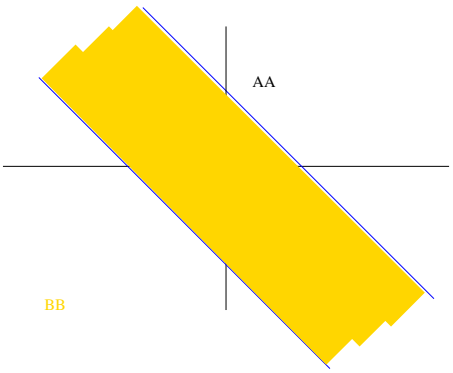


FIGURA 2. Continuidad suma

Recordar que una función es continua si vale que la preimagen de un conjunto abierto es abierto, y en $G \times G$ tomamos la topología producto (o sea un abierto es un producto de abiertos de G).

Ejemplos 5.4.
1. Si $(G, *)$ es un grupo, entonces $(G, *)$ es un grupo topológico con la topología discreta (dado que todo subconjunto de G es abierto).
2. $(\mathbb{R}, +)$ es un grupo topológico. Para ver esto, tomemos un abierto de $\mathbb{R}$, digamos (a, b), y calculemos su preimagen por la operación suma. Luego estamos buscando todos los pares $(x, y) \in \mathbb{R}^2$ tales que $a < x + y < b$. Esto claramente es un abierto (que corresponde a la parte pintada de amarillo en la Figura 2).

Ejercicio 5.5. Probar que $(\mathbb{R}, *)$ es un grupo topológico.

Si G es un grupo topológico, y $g \in G$ es un elemento cualquiera, la función dada por traslación por g es la función $m_g : G \to G$ dada por $m_g(h) = gh$. Dicha función es un homeomorfismo. La razón es que trasladar siempre es una función biyectiva (por tener inversa), y es continua por ser composición de las siguientes funciones continuas:

$$G \hookrightarrow G \times G \xrightarrow{*} G$$

$$h \longrightarrow (g, h) \longrightarrow gh$$

En particular, si $H < G$ es un subgrupo abierto, todas sus coclases (que son de la forma $gH = m_g(H)$) son también abiertas. Luego, el grupo G lo podemos escribir como la unión

$$G = H \cup \bigcup_{\substack{g \in G/H \\ g \notin H}} gH.$$

El último conjunto es abierto (por ser unión de abiertos), con lo cual H es cerrado. Con esto hemos probado lo siguiente.

Proposición 5.6. *Si $H < G$ es un subgrupo abierto, entonces es cerrado.*

Si L/K es una extensión de Galois (no necesariamente finita), y $S \subset L$ es un conjunto finito, definimos el conjunto

$$G(S) := \mathrm{Gal}(L/K)^S = \{\sigma \in \mathrm{Gal}(L/K) \ : \ \sigma(s) = s \ \forall s \in S\}. \tag{5.1}$$

Lema 5.7. *Los conjuntos $G(S)$ satisfacen las siguientes propiedades:*
1. *$G(S)$ es un subgrupo de $\mathrm{Gal}(L/K)$.*
2. *Si S_1 y S_2 son conjuntos finitos, $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$.*

3. *Si* $S_1 \subset S_2$, $G(S_2) \subset G(S_1)$.
4. *Si* S *satisface que para todo* $\tau \in \mathrm{Gal}(L/K)$, $\tau(S) = S$, *entonces* $G(S)$ *es un subgrupo normal de* $\mathrm{Gal}(L/K)$.
5. *El subgrupo* $G(S)$ *tiene índice finito en* $\mathrm{Gal}(L/K)$.

Demostración. Las tres primeras propiedades son inmediatas de la definición. Para ver la cuarta afirmación, tomemos $\tau \in \mathrm{Gal}(L/K)$ y $\sigma \in G(S)$. Entonces $\tau(s) = \tilde{s} \in S$ por hipótesis. Luego

$$\tau^{-1}\sigma\tau(s) = \tau^{-1}(\sigma(\tilde{s})) = \tau^{-1}(\tilde{s}) = s.$$

La última afirmación se deduce de lo siguiente:
Afirmo: sin pérdida de generalidad, podemos suponer que $\tau(s) \in S$ para todo $\tau \in \mathrm{Gal}(L/K)$.

Si esto no fuera así, para cada elemento $s \in S$, el conjunto $\{\sigma(s) : \sigma \in \mathrm{Gal}(L/K)\}$ es finito, pues como L/K es algebraica, y $s \in L$, s es raíz de un polinomio con coeficientes en $K[x]$. En particular, $\sigma(s)$ debe ser otra raíz del mismo polinomio. Denotemos por $\overline{S} = \{\sigma(s) : s \in S, \sigma \in \mathrm{Gal}(L/K)\}$. Dicho conjunto es finito por ser S finito, y el ítem 3 del lema implica que $G(\overline{S}) \subset G(S)$, con lo cual si probamos que $G(\overline{S})$ tiene índice finito en $\mathrm{Gal}(L/K)$, $G(S)$ también lo tiene.

Consideremos la extensión $K(S)$, que es la mínima subextensión de L que contiene a K y a todos los elementos de S. La extensión $K(S)/K$ es finita (¿por qué?) y Galois por la hipótesis en S. Notar que todo elemento de $G(S)$ es la identidad sobre los elementos de $K(S)$ (o sea la restricción de los elementos de $G(S)$ a $K(S)$ es la identidad). Luego obtenemos una sucesión exacta:

$$0 \longrightarrow G(S) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(K(S)/K)$$

$$\sigma \longrightarrow \sigma|_{K(S)}$$

Luego el índice de $G(S)$ en $\mathrm{Gal}(L/K)$ es menor o igual que $[K(S) : K] < \infty$. En realidad no es difícil ver que la sucesión anterior es exacta en todos lados (o sea restringir es suryectivo), pero no precisamos este resultado. □

Proposición 5.8. *Existe en* $\mathrm{Gal}(L/K)$ *una única topología para la cual los conjuntos* $G(S)$, *con* $S \subset L$ *finito, forman una base de entornos abiertos de la identidad. Esta topología hace de* $\mathrm{Gal}(L/K)$ *un grupo topológico.*

Antes de demostrar la proposición, entendamos que sucede cuando L/K es finita (donde el Teorema de Galois no incluye topología alguna). En tal caso, si $\{l_1, \ldots, l_n\}$ es una base de L como K-espacio vectorial, podemos tomar $S = \{l_1, \ldots, l_n\}$. Así, $G(S) = \{1\}$ (la identidad), o sea que cada punto del conjunto (finito) $\mathrm{Gal}(L/K)$ es abierto, con lo cual obtenemos la topología discreta. Luego es claro que dicha topología nos da una estructura de grupo topológico (dado que toda función es continua para ella).

Cuando la extensión L/K no es finita, la topología obtenida no es la trivial, y es cuando realmente obtenemos algo distinto de la teoría clásica.

Demostración de la Proposición 5.8. Para abreviar la notación, denotemos por $G = \mathrm{Gal}(L/K)$, por $*$ la operación (en nuestro caso la composición) y por 1 el elemento neutro.

Por el Lema anterior, si S_1 y S_2 son conjuntos finitos, $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$. Luego $G(S)$ da una base de entornos de la identidad. Recordar que luego un entorno de un punto $g \in G$ está dado por $g * G(S)$ para $S \subset L$ finito. Debemos verificar que el producto con esta topología es continuo. Para ello debemos verificar las siguientes propiedades:

1. Si S es finito, sea $g \in G(S)$, tal que $g = \sigma\tau$, con $\sigma, \tau \in G$. Entonces existen $S_1, S_2 \subset L$ finitos tales que $(\sigma * G(S_1)) * (\tau * G(S_2)) \subset G(S)$.
2. Si S es finito y $g \in G(S)$, entonces existe $\tilde{S} \subset L$ finito tal que $g^{-1}G(\tilde{S})^{-1} \subset G(S)$.

La primer propiedad dice que el producto es continuo en un entorno del 1, mientras que la segunda dice que la función $g \mapsto g^{-1}$ es continua en un entorno del 1.

Para demostrar (1), consideremos el conjunto $G(\overline{S})$ (ver la demostración del Lema 5.7 para la notación). Claramente $G(\overline{S}) \subset G(S)$ (por la segunda propiedad del lema), y $G(\overline{S}) \lhd G$ (o sea es un subgrupo normal). Luego,

$$(\sigma * G(\overline{S})) * (\tau * G(\overline{S})) = \sigma * \tau * (\tau^{-1} * G(\overline{S}) * \tau) * G(\overline{S}) = \sigma * \tau * G(\overline{S}) = g * G(\overline{S}) \subset G(S).$$

La demostración de (2) es inmediata, dado que $G(S)$ es un subgrupo, luego $G(S)^{-1} = G(S)$ y claramente $g^{-1}G(S) \subset G(S)$ (por definición). □

Definición 5.9. Si L/K es una extensión de Galois, el grupo de Galois topológico de la extensión (que haciendo abuso de notación lo denotamos también $\mathrm{Gal}(L/K)$) es el grupo $\mathrm{Gal}(L/K)$, con la única topología para la cual una base de entornos de la identidad son los conjuntos $G(S)$. Dicha topología se denomina la *topología de Krull*.

Proposición 5.10. *Si L/K es una extensión de Galois, entonces el grupo topológico $\mathrm{Gal}(L/K)$ es Hausdorff, compacto y totalmente disconexo.*

Demostración. Veamos que es Hausdorff: sean $\sigma, \tau \in \mathrm{Gal}(L/K)$ distintos. Luego, existe $\alpha \in L$ tal que $\sigma(\alpha) \neq \tau(\alpha)$. Miremos $S = \{\alpha\}$. Luego $\sigma G(S)$ y $\tau G(S)$ son abiertos, y claramente disjuntos.

Veamos que es totalmente disconexo: alcanza con ver que la componente conexa de la identidad, denotada $\mathcal{C}_{\mathbb{1}}$, es sólo la identidad. Sea S un conjunto finito y $\mathrm{Gal}(L/K)$ estable (o sea $\sigma(S) = S$ para todo $\sigma \in \mathrm{Gal}(L/K)$). Entonces $G(S)$ es un abierto que contiene a la identidad. Como $G(S)$ es abierto, por la Proposición 5.6 $G(S)$ es también cerrado, con lo cual la componente conexa de la identidad está contenida en $G(S)$. Luego

$$\mathcal{C}_{\mathbb{1}} \subset \bigcap_{\substack{S \subset L \\ \#S < \infty}} G(S) = \{\mathbb{1}\}.$$

Probar que $\mathrm{Gal}(L/K)$ es compacto es más complicado, y proviene de dar dicho grupo de Galois como un límite inverso sobre todas las subextensiones finitas, y utilizar el Teorema de Tychonoff (ver el capítulo 1 de [FJ08] por ejemplo). □

Por completitud, enunciamos la correspondencia de Galois para extensiones de Galois arbitrarias.

Teorema 5.11 (Galois)**.** *Sea L/K una extensión Galois. Entonces existe una correspondencia biyectiva entre el conjunto de extensiones: $\{N : K \subset N \subset L\}$ y el conjunto de subgrupos cerrados de $\mathrm{Gal}(L/K)$. La biyección esta dada por:*

$$N \to \mathrm{Aut}_N(L) \subset \mathrm{Gal}(L/K) \tag{5.2}$$

$$L^H := \{\alpha \in L : \sigma(\alpha) = \alpha \, \forall \sigma \in H\} \leftarrow H \tag{5.3}$$

Además, la extensión N/K es Galois si y sólo si el grupo $\mathrm{Gal}(L/N)$ es un subgrupo normal de $\mathrm{Gal}(L/K)$. En el caso que la extensión N/K sea Galois, $\mathrm{Gal}(N/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/N)$.

5.2. Grupo de descomposición y Frobenius en extensiones infinitas. De manera análoga a lo hecho en la sección 3.2, podemos definir el anillo de enteros de $\overline{\mathbb{Q}}$, esto es:

$$\overline{\mathbb{Z}} := \{\alpha \in \overline{\mathbb{Q}} : \alpha \text{ es entero algebraico}\}. \tag{5.4}$$

Recordar que α es entero algebraico si es raíz de un polinomio con coeficientes enteros mónico. Como en el caso de extensiones finitas, $\overline{\mathbb{Z}}$ es un anillo. Sea $p \in \mathbb{Z}$ un primo, y sea $\mathfrak{p} \subset \overline{\mathbb{Z}}$ un ideal maximal que contiene a p.

Ejercicio 5.12. Probar que $\overline{\mathbb{Z}}/\mathfrak{p} \simeq \overline{\mathbb{F}_p}$.

Definición 5.13. El grupo de descomposición de $\mathfrak{p}$ es

$$D_{\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ : \ \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Claramente $D_{\mathfrak{p}}$ es un subgrupo de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A pesar de que el grupo de descomposición $D_{\mathfrak{p}}$ depende del ideal $\mathfrak{p}$, si $\mathfrak{p}, \tilde{\mathfrak{p}}$ son dos ideales que contienen a p, entonces existe $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tal que $\sigma(\mathfrak{p}) = \tilde{\mathfrak{p}}$. Luego $D_{\mathfrak{p}} = \sigma^{-1} D_{\tilde{\mathfrak{p}}} \sigma$.

Si $\sigma \in D_{\mathfrak{p}}$, σ induce una función en $\overline{\mathbb{Z}}/\mathfrak{p}$, que es la identidad sobre $\mathbb{F}_p$, con lo cual obtenemos una función

$$\varphi : D_{\mathfrak{p}} \mapsto \mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}_p}) = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p). \tag{5.5}$$

Ejercicio 5.14. Verificar las siguientes propiedades:

1. El subgrupo $D_{\mathfrak{p}}$ es un subgrupo cerrado (equivalentemente, su complemento es abierto). Luego por la correspondencia de Galois $D_{\mathfrak{p}} = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, donde $L = \overline{\mathbb{Q}}^{D_{\mathfrak{p}}}$.
2. El morfismo φ es continuo, donde miramos a $D_{\mathfrak{p}}$ como grupo topológico con la topología de subgrupo (o con la topología de Krull identificándolo con $\mathrm{Gal}(\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^{D_{\mathfrak{p}}})$).
3. El morfismo φ es suryectivo. Sugerencia: probar primero que las funciones $\varphi_n : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ (componer φ con la función cociente) es suryectivo para todo n utilizando lo visto en extensiones finitas. Deducir que la imagen de φ es densa en $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, y utilizar el ítem anterior.

Se puede ver que el grupo $D_{\mathfrak{p}}$ es isomorfo al grupo de Galois $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

Definición 5.15. El grupo de inercia $I_{\mathfrak{p}}$ de $\mathfrak{p}$ es el núcleo del morfismo φ, o sea

$$I_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ : \ \sigma(x) \equiv x \pmod{\mathfrak{p}} \text{ para todo } x \in \overline{\mathbb{Z}}\}.$$

Llamamos un *Frobenius absoluto sobre* p a cualquier elemento $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ en la preimagen de $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Claramente dos Frobenius absolutos difieren por un elemento en el subgrupo de inercia.

Como sucede con el grupo de descomposición, si $\mathfrak{p}, \tilde{\mathfrak{p}}$ son dos ideales de $\overline{\mathbb{Z}}$ que contienen a un primo p, entonces existe $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tal que $\sigma(\mathfrak{p}) = \tilde{\mathfrak{p}}$ y entonces $I_{\mathfrak{p}} = \sigma^{-1} I_{\tilde{\mathfrak{p}}} \sigma$.

Por último, obtenemos la siguiente versión del Teorema de Chebotarev.

Teorema 5.16 (Chebotarev)**.** *Para todo número primo p, salvo finitos, tomemos para cada ideal primo $\mathfrak{p}$ que contiene a p un Frobenius absoluto* $\mathrm{Frob}_{\mathfrak{p}}$*. Entonces el conjunto* $\{\mathrm{Frob}_{\mathfrak{p}}\}_{\mathfrak{p}|p} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *es denso.*

6. Representaciones de Galois

El objetivo deseado es el de poder entender el grupo $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (o su análogo para otros cuerpos como extensiones finitas de $\mathbb{Q}$ por ejemplo). Lamentablemente, dicho grupo es muy difícil de manejar (y ni siquiera está bien definido, dado que depende de elegir una clausura algebraica de $\mathbb{Q}$). Una manera de entender un grupo es mediante sus representaciones, esto es entender como actúa en espacios vectoriales de dimensión finita. En varios casos, conocer dichas representaciones es suficiente para determinar el grupo (y sus propiedades) unívocamente, por ejemplo es lo que sucede al considerar grupos finitos. A pesar de que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ no es finito, el mismo es un límite (inverso) de grupos finitos,

con lo cual es de esperar poder recuperar bastante información si logramos entender todas sus representaciones.

Durante este capítulo, K va a denotar un cuerpo topológico (principalmente nos concentraremos en los casos $\mathbb{C}$, $\mathbb{Q}_p$ o una extensión finita de $\mathbb{Q}_p$), y V un K-espacio vectorial de dimensión finita d. En particular, V admite una topología a partir de la de K. Lo mismo sucede para el grupo $\mathrm{End}_K(V)$ (grupo de transformaciones lineales de V en sí mismo), ya que una vez que elegimos una base para V, podemos identificar $\mathrm{End}_K(V)$ con el conjunto $M_{d\times d}(K)$ de matrices con d filas y d columnas, y este es isomorfo con K^{d^2}.

Definición 6.1. Una representación de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ es un morfismo continuo

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V).$$

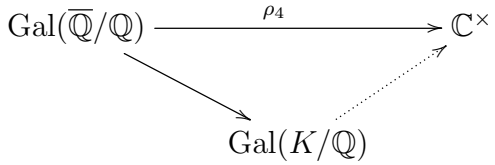
Para poder comenzar a entender que es una representación de Galois, miremos algunos ejemplos sencillos.

Ejemplos 6.2. 1. En el caso en que V tiene dimensión 1, cualquier representación es un morfismo entre $G_\mathbb{Q}$ y $K^\times$ (dado que a un elemento v de V, lo manda a un múltiplo suyo no nulo).

Sea $K = \mathbb{Q}(i)$ el cuerpo de raíces cuartas de la unidad. Si $\sigma \in G_\mathbb{Q}$, $\sigma(i) = \pm i$, con lo cual podemos definir una representación $\rho_4 : G_\mathbb{Q} \to \mathbb{C}^\times$ por

$$\rho_4(\sigma) = \frac{\sigma(i)}{i} \in \{\pm 1\}. \tag{6.1}$$

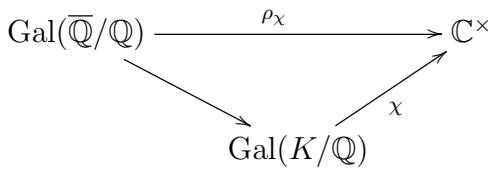
Notar que ρ_4 es trivial en el subgrupo $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, dado que dichos elementos actúan trivialmente en i. Luego ρ_4 factoriza por $\mathrm{Gal}(K/\mathbb{Q})$, o sea tenemos el siguiente diagrama



Notar que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2$, y ρ_4 es justamente la representación no trivial de dicho grupo. Esto demuestra que efectivamente ρ_4 es un morfismo de grupos. Nos resta ver que ρ_4 es continua.

El conjunto $\{\pm 1\} \subset \mathbb{C}^\times$ es discreto, con lo cual su topología es la discreta. Para verificar que ρ_4 es continua, basta con ver que $\ker(\rho_4)$ (su núcleo) es abierto. Pero $\mathrm{Gal}(\overline{\mathbb{Q}}/K) = G(\{i\})$ (siguiendo la notación del capítulo anterior), con lo cual es abierto y tiene índice finito en $G_\mathbb{Q}$ (ver Lema 5.7). De esto se deduce que $\ker(\rho_4)$ es abierto, como queríamos ver.

2. Mas generalmente, si $n \in \mathbb{N}$, $n \geq 3$, y tomamos $K = \mathbb{Q}(\xi_n)$ (el cuerpo ciclotómico de raíces n-ésimas de la unidad), el grupo $\mathrm{Gal}(K/\mathbb{Q})$ es un grupo abeliano finito. En particular, todas sus representaciones irreducibles son de dimensión 1. Si $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$ es una tal representación, podemos definir $\rho_\chi : G_\mathbb{Q} \to \mathbb{C}^\times$, mediante el diagrama



Dejamos como ejercicio probar que dicho morfismo es continuo.

Proposición 6.3. *Sean ρ_1, ρ_2 dos representaciones de Galois. Si para todo número primo p, salvo finitos, y para cada ideal primo $\mathfrak{p}$ que contiene a p vale que $\rho_1(\mathrm{Frob}_\mathfrak{p}) = \rho_2(\mathrm{Frob}_\mathfrak{p})$ entonces $\rho_1 = \rho_2$.*

Demostración. Por el Teorema 5.16 el conjunto $\{\mathrm{Frob}_\mathfrak{p}\}$ es denso en $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Como las representaciones son continuas, si coinciden en un conjunto denso, coinciden en todos los elementos. □

Mas adelante veremos cómo reemplazar primos de $\overline{\mathbb{Z}}$ por primos de $\mathbb{Z}$.

Definición 6.4. Si ρ_1, ρ_2 son dos representaciones de Galois de $G_\mathbb{Q}$ en $\mathrm{Aut}_K(V)$, decimos que son equivalentes, si existe una transformación lineal $\psi \in \mathrm{Aut}_K(V)$ tal que para todo $\sigma \in G_\mathbb{Q}$ y todo $v \in V$,

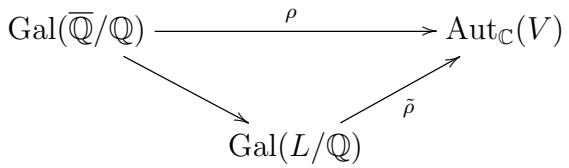
$$\rho_1(\sigma)(v) = \psi^{-1}(\rho_2(\sigma)(\psi(v))).$$

Sea ρ una representación de Galois de $G_\mathbb{Q}$ en $\mathrm{Aut}_K(V)$, donde V es un K-espacio vectorial de dimensión d. Elegir una base B de V induce un isomorfismo $V \simeq K^d$ y una representación de Galois

$$\rho_B : G_\mathbb{Q} \to \mathrm{GL}_d(K).$$

Elegir otra base de V da representaciones equivalentes, dado que si B' es otra base, y $\mathcal{C}$ es la matriz de cambio de base de B a B', entonces las representaciones ρ_B y $\rho_{B'}$ difieren en conjugar por $\mathcal{C}$. Es por esto que no vamos a distinguir entre representaciones de $G_\mathbb{Q}$ en $\mathrm{Aut}_K(V)$ o en $\mathrm{GL}_d(K)$.

Teorema 6.5. *Si V es un $\mathbb{C}$-espacio vectorial de dimensión finita, y $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_\mathbb{C}(V)$ es una representación de Galois, entonces ρ factoriza por una extensión finita; o sea existe L extensión finita de $\mathbb{Q}$, y $\tilde{\rho} : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Aut}_\mathbb{C}(V)$ tal que el siguiente diagrama conmuta*



Demostración. Supongamos primero que $d = 1$, o sea que tenemos un morfismo continuo de $G_\mathbb{Q}$ en $\mathbb{C}^\times$. Si tomamos un abierto de $\mathbb{C}^\times$ cerca del 1, digamos $U = \{z \in \mathbb{C} \,:\, |z-1| < \frac{1}{2}\}$, entonces su preimagen es un abierto de $G_\mathbb{Q}$ (por ser ρ continua). Como la función identidad está en $\rho^{-1}(U) \subset G_\mathbb{Q}$, hay un abierto centrado en la matriz identidad que esta contenido en la preimagen, o sea existe un conjunto finito $S \subset \overline{\mathbb{Q}}$ (que podemos suponer $G_\mathbb{Q}$ estable) tal que $G(S) \subset \rho^{-1}(U)$. En particular, $\rho(G(S)) \subset U$. Como $G(S)$ es un subgrupo de $G_\mathbb{Q}$ y ρ es un morfismo, $\rho(G(S))$ es un subgrupo de U. Pero el único subgrupo de U es $\{1\}$ (convencerse). En particular, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(S))$ está en el núcleo de ρ y por lo tanto ρ factoriza por $\mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$ como queríamos ver.

Cuando $d > 1$, la demostración es similar, con la dificultad de que tenemos que demostrar que existe un entorno de la matriz identidad (de $d \times d$) que no contiene subgrupos no triviales. Supongamos que tomando una bola (abierta) centrada en la identidad de radio ϵ (pequeño y fijo) tenemos un subgrupo H no trivial. Es fácil ver que todos los elementos de H son diagonalizables (¿por qué?). Si M es un elemento de H, y λ es un autovalor de M, entonces $|\lambda - 1| \leq \frac{1}{2}$ (para la elección adecuada de ϵ, que no depende de M, ver Ejercicio 6.6). Pero como $M \in H$, sus potencias también lo están, con lo cual $|\lambda^n - 1| \leq \frac{1}{2}$ para todo n entero. Luego $\lambda = 1$, y M es la matriz identidad. □

Ejercicio 6.6. Para el alumno que no vio los detalles de métricas utilizados en la última demostración, les dejamos algunas propiedades que cumplen los espacios vectoriales en dimensión finita.

1. Probar que dos normas cualesquiera en un espacio vectorial V de dimensión finita son equivalentes, esto es, si $\|.\|_1$, $\|.\|_2$ son normas en V, entonces existe una constante $C > 0$ tal que $\|v\|_1 \leq C\|v\|_2$ para todo $v \in V$.
2. Si K es un cuerpo con un valor absoluto $|.|$, y tomamos cualquiera de las normas usuales en K^d, entonces podemos asociar una norma de *operadores* en $M_{d\times d}(K)$ de la siguiente manera: si $M \in M_{d\times d}(K)$ definimos
$$\|M\| := \sup_{\substack{v\in K^d \\ \|v\|=1}} \|Mv\|.$$
Probar que $\|.\|$ es una norma.
3. Probar que si $\lambda \in K$ es un autovalor de M, entonces $|\lambda| \leq \|M\|$.
4. Completar los detalles de la demostración anterior para $d > 1$.

El Teorema 6.5 nos dice que las representaciones de Galois complejas son interesantes, pero si trabajamos exclusivamente con ellas, sólo vamos a obtener información sobre las extensiones finitas de $\mathbb{Q}$. Es por esto que hay que considerar también representaciones en espacios vectoriales sobre $\mathbb{Q}_p$ (las llamadas representaciones de Galois p-ádicas).

Si $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$ es una representación de Galois, decimos que un subespacio $W \subset V$ es *ρ-invariante* si $\rho(\sigma)(w) \in W$ para todo $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ y todo $w \in W$.

Definición 6.7. Una representación $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$ se dice *irreducible* si no existe $W \subset V$ subespacio propio y no trivial ρ-invariante. Una representación $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$ se dice *semi-simple* si V se puede descomponer como
$$V = \bigoplus_i V_i,$$
donde cada V_i es un subespacio ρ-invariante, y las representaciones $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V_i)$ son irreducibles.

Teorema 6.8. *Sea V un $\mathbb{C}$-espacio vectorial de dimensión finita y sea $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{C}}(V)$ una representación de Galois. Entonces ρ es semi-simple.*

Demostración. Por el Teorema 6.5 sabemos que ρ factoriza por una extensión finita, o sea existe $L/\mathbb{Q}$ Galois y finita y $\tilde{\rho} : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{C}}(V)$ tal que $\rho = \tilde{\rho} \circ \Pi$, donde $\Pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ es la proyección (que corresponde a restringir un automorfismo al cuerpo L). Luego el resultado sigue del Teorema de Maschke (que afirma que toda representación de un grupo G finito en un K-espacio vectorial V tal que la característica de K no divide al orden de G, es semi-simple). La demostración original de Maschke se puede ver en [Mas98], aunque hay muchas demostraciones disponibles en formato electrónico. □

Observación 6.9. No vale en general que toda representación de Galois sea semi-simple, usamos fuertemente que el cuerpo K era el cuerpo de números complejos.

Definición 6.10. Sea $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$ una representación de Galois. Dado un primo p, decimos que ρ es *no-ramificada* en p si $\rho(I_{\mathfrak{p}}) = 1$ (la identidad) para cualquier primo $\mathfrak{p} \subset \overline{\mathbb{Z}}$ que contiene a p.

Veamos que efectivamente la condición de ρ ser no-ramificada en p no depende del primo $\mathfrak{p}$. Notar que si $\mathfrak{p}$, $\tilde{\mathfrak{p}}$ son dos ideales que contienen al mismo primo p, entonces los grupos $I_{\mathfrak{p}}$, $I_{\tilde{\mathfrak{p}}}$ son conjugados, con lo cual ρ es trivial en uno de ellos si y sólo si lo es en el otro. Decimos que ρ es ramificada en p si no es no-ramificada (equivalente, la imagen del grupo de inercia es no-trivial).

Recordar que dado $\mathfrak{p} \subset \overline{\mathbb{Z}}$, un Frobenius absoluto sobre p, denotado por $\mathrm{Frob}_{\mathfrak{p}}$, es un elemento cualquiera en el grupo de descomposición $D_{\mathfrak{p}}$ cuya imagen residual corresponde

al automorfismo de Frobenius. Dos tales morfismos difieren en un elemento del grupo de inercia $I_{\mathfrak{p}}$. Ahora si ρ es no ramificada en p, entonces $\rho(I_{\mathfrak{p}}) = 1$, con lo cual el valor $\rho(\mathrm{Frob}_{\mathfrak{p}})$ depende solamente del ideal $\mathfrak{p}$. Además, si $\mathfrak{p}, \tilde{\mathfrak{p}}$ son dos ideales en $\overline{\mathbb{Z}}$ que contienen a p, entonces uno es conjugado del otro. Luego $\rho(\mathrm{Frob}_{\mathfrak{p}})$ y $\rho(\mathrm{Frob}_{\tilde{\mathfrak{p}}})$ son matrices conjugadas (identificando $\mathrm{Aut}_K(V)$ con el grupo de matrices). En particular, sus polinomios característicos son iguales.

Dada una matriz cuadrada M, denotemos por $\mathrm{car}(M) = \det(1 - T \cdot M)$ a su polinomio característico. De lo expuesto anteriormente, tenemos que si ρ es no ramificada en p, podemos definir

$$\mathrm{car}(\rho(\mathrm{Frob}_p)) := \mathrm{car}(\rho(\mathrm{Frob}_{\mathfrak{p}})), \tag{6.2}$$

donde $\mathfrak{p} \subset \overline{\mathbb{Z}}$ es cualquier ideal maximal tal que $p \in \mathfrak{p}$.

Para los primos ramificados, la situación es igual que lo expuesto en la Sección 4 para extensiones finitas: dado un primo $\mathfrak{p} \subset \overline{\mathbb{Z}}$, el grupo de inercia $I_{\mathfrak{p}}$ actúa en V. Denotemos por $V^{I_{\mathfrak{p}}}$ al subespacio de vectores donde la inercia actúa trivialmente. Por ejemplo, si p es un primo no ramificado de ρ, entonces $V^{I_{\mathfrak{p}}} = V$.

Ejercicio 6.11. Probar que el subespacio $V^{I_{\mathfrak{p}}}$ es invariante por la acción de ρ, o sea si $v \in V^{I_{\mathfrak{p}}}$ y $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ entonces $\rho(\sigma)(v) \in V^{I_{\mathfrak{p}}}$.

La restricción $\rho|_{V^{I_{\mathfrak{p}}}}$ da una acción de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ en el subespacio $V^{I_{\mathfrak{p}}}$. Por definición, $I_{\mathfrak{p}}$ actúa trivialmente en $V^{I_{\mathfrak{p}}}$, con lo cual la matriz $\rho|_{V^{I_{\mathfrak{p}}}}(\mathrm{Frob}_{\mathfrak{p}})$ está bien definida (o sea no depende de la preimage de $\mathrm{Frob}_{\mathfrak{p}}$ escogida). Mas aún, dicho valor depende exclusivamente del primo p contenido en $\mathfrak{p}$.

Ejercicio 6.12. Sean $\mathfrak{p}$ y $\tilde{\mathfrak{p}}$ son dos primos en $\overline{\mathbb{Z}}$ que contienen al mismo primo p. En particular, existe $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tal que $\tau\tilde{\mathfrak{p}} = \mathfrak{p}$.

- Probar que $\tau I_{\mathfrak{p}} \tau^{-1} = I_{\tilde{\mathfrak{p}}}$ y que $\tau V^{I_{\mathfrak{p}}} = V^{I_{\tilde{\mathfrak{p}}}}$.
- Probar que el polinomio $\mathrm{car}(\rho|_{V^{I_{\mathfrak{p}}}}(\mathrm{Frob}_{\mathfrak{p}}))$ no depende de $\mathfrak{p}$.

Luego podemos definir $\mathrm{car}(\rho|_{V^{I_p}}(\mathrm{Frob}_p))$ como $\mathrm{car}(\rho|_{V^{I_{\mathfrak{p}}}}(\mathrm{Frob}_{\mathfrak{p}}))$ para cualquier $\mathfrak{p} \subset \overline{\mathbb{Z}}$ maximal que contenga a p.

Teorema 6.13 (Brauer-Nesbitt)**.** *Sean $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$, $i = 1, 2$ dos representaciones semi-simples. Si para todo elemento s de un conjunto denso $S \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ vale*

$$\mathrm{car}(\rho_1(s)) = \mathrm{car}(\rho_2(s)),$$

entonces ρ_1 y ρ_2 son isomorfas.

Demostración. Ver [CR06, 30.16]. Ver también el Teorema 2.4.6 de las notas de Gabor Wiese (en `math.uni.lu/~wiese/notes/GalRep.pdf`). La demostración involucra todos los elementos de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, pero por ser las representaciones continuas, basta verificarla en un conjunto denso. □

Si el cuerpo K tiene característica cero, además basta con verificar que las trazas de las representaciones son iguales, sin necesidad de calcular todo el polinomio característico.

Corolario 6.14. *Sean $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$, $i = 1, 2$ dos representaciones semi-simples. Supongamos que ambas representaciones son ramificadas solamente en un conjunto finito de primos S. Si*

$$\mathrm{car}(\rho_1(\mathrm{Frob}_p)) = \mathrm{car}(\rho_2(\mathrm{Frob}_p)),$$

para todo primo $p \notin S$, entonces ρ_1 y ρ_2 son isomorfas. Además, si K tiene característica 0, basta verificar que $\mathrm{Tr}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_p))$ para todo $p \notin S$.

Una pregunta natural es cuando las representaciones de Galois son ramificadas solamente en un conjunto finito de primos.

Proposición 6.15. *Si $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{C}}(V)$ es una representación de Galois, entonces ρ es no ramificada fuera de un conjunto finito de primos.*

Demostración. Por Teorema 6.5 ρ factoriza por una extensión Galois finita $L/\mathbb{Q}$, o sea existe una representación $\tilde{\rho} : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{C}}(V)$ tal que $\rho = \tilde{\rho} \circ \Pi$, donde $\Pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ es la proyección. Es conocido que en una extensión finita hay un conjunto finito de primos que ramifican (precisamente aquellos que dividen al discriminante de la extensión). Luego $\tilde{\rho}$ es no ramificada fuera de un conjunto finito de primos y por consiguiente ρ también lo es. □

Para un cuerpo general, no es cierto que una representación de Galois semi-simple sea no ramificada fuera de un conjunto finito de primos (ver por ejemplo [Ram00]). Sin embargo, el conjunto de primos ramificados siempre tiene densidad cero (ver [KR01]), con lo cual el Teorema de Brauer-Nesbitt se puede aplicar en general.

6.1. Series L asociadas a representaciones del grupo de Galois absoluto. Las series L son objetos analíticos, que se utilizan para *codificar* información asociada a diversos objetos geométricos/aritméticos/algebraicos. Un primer ejemplo es la función zeta de Riemann, definida como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C}.$$

Es fácil ver que dicha serie converge en el semiplano $\Re(s) > 1$. Riemann en 1859 demostró que dicha función se puede extender de forma analítica a todo el plano complejo, probando que la misma satisface una ecuación funcional que relaciona el valor en s con el valor en $1 - s$. La importancia de la función zeta de Riemann es que admite una descomposición como

$$\zeta(s) = \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}},$$

con lo cual la misma da mucha información sobre la distribución de los números primos. Existen muchas generalizaciones de la función zeta de Riemann, como la asociada a caracteres por Dirichlet, la asociada a cuerpos de números por Dedekind y muchas otras (como vimos en la Sección 4). El objetivo nuestro es asociarle a una representación de Galois una función analítica similar.

Definición 6.16. Dada $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$, definimos la L-serie $L(\rho, s)$ asociada a ρ como:

$$L(\rho, s) = \prod_{p\text{primo}} L_p(\rho, p^{-s})^{-1} = \prod_{p \text{ primo}} \frac{1}{\mathrm{car}(\rho|_{V^{I_p}}(\mathrm{Frob}_p))(p^{-s})}, \tag{6.3}$$

donde $\mathrm{car}(\rho|_{V^{I_p}}(\mathrm{Frob}_p))$ es el polinomio característico definido en el Ejercicio 6.12, evaluado en p^{-s}.

Ejemplo 6.17. Sea $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_K(V)$ la representación trivial, con $\dim(V) = 1$, o sea $\rho(\sigma)(v) = v$. Entonces todos los primos son no ramificados y vale que $\chi(\rho(\mathrm{Frob}_p)) = 1 - t$. Luego,

$$L(\rho, s) = \prod_{p \text{ primo}} \frac{1}{(1 - p^{-s})} = \zeta(s).$$

Se puede ver que las L-series de Dedekind y de Dirichlet se obtienen como casos particulares de esta construcción mas general (las de Dirichlet corresponden a otras representaciones de dimensión 1, mientras que las de Dedekind corresponden a tomar representaciones de Galois de grupos $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, para $K/\mathbb{Q}$ finita).

Las L-series mas estudiadas son las que corresponden a los siguientes dos casos: $K = \mathbb{C}$, que corresponden a representaciones de Galois complejas y fueron estudiadas por Artin (vistas en la Sección 4); y $K = \mathbb{Q}_p$, las llamadas representaciones de Galois p-ádicas. En general dichas L-series convergen sólo en un semiplano como sucede con la función zeta de Riemann. Un problema muy difícil es estudiar si dicha función se puede extender a todo el plano complejo, y otro problema muy interesante es poder calcular valores en puntos *especiales*, donde se espera que el valor de $L(\rho, s_0)$ contenga información del objeto geométrico/aritmético/algebraico a partir del cual se construyó ρ (para el lector interesado, ver el Teorema de Dedekind, y la conjetura de Birch y Swinnerton-Dyer).

En lo que respecta a las representaciones de Galois complejas, tenemos la siguiente conjetura.

Conjetura 6.18. *Si $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{C}}(V)$ es una representación irreducible y no trivial, entonces ρ se extiende de manera holomorfa a todo el plano complejo.*

Al día de hoy no se conoce ninguna demostración de dicha conjetura. Brauer (en 1946) usando teoría de caracteres inducidos, logró demostrar que la L-serie se puede extender de manera meromorfa a todo el plano complejo, pero a priori podría tener polos. Los únicos casos que se conocen de la conjetura es cuando V tiene dimensión 2, y la representación es "impar" (esto quiere decir que el determinante de la imagen de conjugación compleja es -1), como corolario de la demostración de las conjeturas de Serre dado por Khare y Wintenberger.

En el próximo capítulo veremos cómo construir algunas representaciones de Galois p-ádicas. Dichas construcciones provienen en general de variedades algebraicas proyectivas (veremos el caso de curvas elípticas). La conjetura de Fontaine-Mazur predice que todas las representaciones p-ádicas que ramifiquen en un conjunto finito y satisfagan una cierta condición técnica, se obtienen a partir de variedades algebraicas. Al día de hoy se conocen muy pocos casos de dicha conjetura.

7. Curvas algebraicas

En el presente capítulo vamos a estudiar la *aritmética de las curvas elípticas*. La palabra *aritmética* está directamente asociada a los números enteros y sus propiedades, mientras que una *curva* es un objeto geométrico de dimensión 1, que en nuestro caso estará contenida en un plano. También podríamos decir que lo que vamos a hacer es *teoría de números de ciertas curvas*.

Las curvas que consideraremos serán *curvas algebraicas planas*, y aunque no vamos a dar la definición formal de las mismas, momentáneamente llamaremos así a aquellas curvas C descritas por una ecuación polinómica en dos variables $F(x, y) = 0$, donde los coeficientes del polinomio F serán números de algún cuerpo, como bien podrían ser $\mathbb{R}$ o $\mathbb{C}$, pero como vamos a hacer aritmética nos interesará sobre todo que estén en $\mathbb{Q}$.

Aunque inevitablemente al esbozar la gráfica de una curva tengamos que "dibujar" *todos* sus puntos, es decir, tanto los racionales como aquellos con alguna o ambas coordenadas irracionales, momentáneamente estos últimos no existirán para nuestros fines (serán como si no estuvieran).

También tendremos que considerar para una curva definida sobre los racionales sus puntos con coordenadas que sean enteros algebraicos, al menos, algunos de tales puntos.

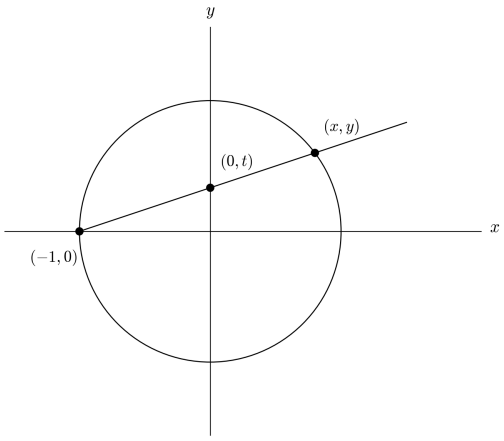


FIGURA 3. Cónica

7.1. Cónicas. Podríamos comenzar considerando *rectas*, en vista de que son el tipo de curvas más simple, pero las dejaremos de lado y pasaremos directamente a las *cónicas*, que son las curvas descritas por un polinomio en dos variables y de segundo grado. Implícitamente estamos midiendo el *nivel de complejidad* de una curva por el grado del polinomio F cuya ecuación polinómica $F(x, y) = 0$ la define. Así, las rectas están descritas por polinomios de primer grado y las cónicas (circunferencia, elipse, parábola e hipérbola) por polinomios de segundo grado. En un nivel de complejidad posterior al de las cónicas se ubican las *curvas elípticas* y en el siguiente y último escalón están las *curvas de mayor complejidad*, que ni siquiera tienen un nombre específico. En realidad, para ser un poco más precisos, las singularidades (puntos dobles por ejemplo) también deben tenerse en cuenta para medir esta complejidad, pero eso ya lo veremos más adelante.

Detengámonos entonces en las cónicas, que en relación a nuestras necesidades, se comportan todas de igual modo, la principal diferencia será que, sobre los racionales, algunas tienen puntos y otras no. Apoyaremos esta última afirmación viendo cómo se pueden poner de manifiesto los puntos racionales de una cónica, y llegaremos a la conclusión que en todas, éstos se "manifiestan" igual.

Sea, por ejemplo, la cónica C descrita por la siguiente ecuación:

$$C: \qquad x^2 + y^2 = -1. \tag{7.1}$$

Trivialmente, en este caso es $C(\mathbb{Q}) = \emptyset$. Pero veremos a continuación que si hay algún punto racional en una cónica, entonces hay infinitos. Para ello consideremos la circunferencia C con centro en el origen de coordenadas y radio 1, junto con uno de sus puntos racionales, como por ejemplo el $P(-1, 0)$. Si elegimos sobre el eje y un punto racional $T(0, t)$, con $t \in \mathbb{Q}$ y trazamos la recta ℓ que pasa por P y T, veremos que la misma corta a C en un punto R racional (ver Figura 3).

En efecto, la ecuación de ℓ es $y = tx + t$ y su intersección con

$$C: \qquad x^2 + y^2 = 1 \tag{7.2}$$

es el punto $R\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, que claramente es racional. Recíprocamente, dado un punto racional R de C, la recta que pasa por él y P corta al eje y en un punto T racional. De modo que a partir de P podemos *generar todos* los puntos racionales de C considerando todas las rectas de pendiente racional que pasan por P:

$$C(\mathbb{Q}) = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\} \cup \{P\}. \tag{7.3}$$

Por otro lado, digamos que siempre una recta corta a una cónica en dos puntos (reales o complejos), contados por su multiplicidad (más generalmente, un teorema de la Geometría Proyectiva debido a E. Bézout afirma que: una curva de grado m y una curva de grado n siempre se cortan en mn puntos). Esto último nos permite interpretar que:

- una *recta tangente* a una circunferencia, por ejemplo, también corta a ésta en dos puntos, o como diremos ahora, en un punto *doble* (o *de multiplicidad* 2); y que
- una *recta exterior* a una cónica también corta a ésta en dos puntos, aunque imaginarios, pues sus coordenadas serán números complejos.

Observemos ahora que el problema *geométrico* resuelto recién al hallar todos los puntos del conjunto $C(\mathbb{Q})$ en el caso de la circunferencia unitaria también nos da la solución de un problema *aritmético* de vieja data, cual es el de obtener todas las ternas de números enteros tales que la suma de los cuadrados de los dos primeros sea igual al cuadrado del tercero. Tales ternas se denominan ternas Pitagóricas, dada su relación evidente con las longitudes de los lados de los triángulos rectángulos (en los cuales se verifica el teorema de Pitágoras). En efecto, el problema de hallar todas las ternas (x, y, z) de números enteros tales que $x^2 + y^2 = z^2$ puede considerarse resuelto por el problema anterior dado que la precedente ecuación homogénea (en tres variables y de grado 2) puede deshomogeneizarse respecto de z (esto es: podemos en ella pasar dividiendo z^2 al primer miembro si desechamos la solución trivial $x = y = z = 0$) para obtener la ecuación

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1, \tag{7.4}$$

la cual, en vista de los elementos de $C(\mathbb{Q})$ dados por (7.3), tiene las soluciones: $\frac{x}{z} = \frac{1-t^2}{1+t^2}$ y $\frac{y}{z} = \frac{2t}{1+t^2}$, con $t \in \mathbb{Q}$, lo que nos termina por dar (suponiendo $t = \frac{r}{s}, 0 \leq t \leq 1$):

$$x = s^2 - r^2, \qquad y = 2rs, \qquad z = s^2 + r^2, \qquad \text{con } r, s \in \mathbb{Z}, \tag{7.5}$$

como familia de ternas Pitagóricas (primitivas si r y s son primos relativos y de distinta paridad).

El procedimiento que acabamos de describir para la circunferencia unitaria puede extenderse al resto de las cónicas: partiendo de un punto racional en cualquiera de ellas (si lo hubiera) y trazando por él todas las rectas con pendiente racional, los puntos en que éstas cortan a la cónica serán todos los puntos racionales de la misma.

Como vimos en el caso de la cónica descrita por la ecuación $x^2 + y^2 = -1$, a veces una curva algebraica no tiene puntos racionales. Un caso menos evidente es el de la siguiente cónica:

$$C: \qquad x^2 + y^2 = 3, \tag{7.6}$$

para la cual ya no es obvio que $C(\mathbb{Q}) = \emptyset$. Veamos que sin embargo es así: expresando los posibles puntos racionales de C como cociente de enteros y homogeneizando vía común denominador obtenemos que $C(\mathbb{Q}) = \emptyset$ si y sólo si la ecuación

$$x^2 + y^2 = 3z^2 \tag{7.7}$$

no tiene soluciones en números enteros (distintas de la trivial $(0, 0, 0)$).

Podemos ver esto último, que es un resultado negativo, encontrando un número primo p para el cual la congruencia

$$x^2 + y^2 \equiv 3z^2 \qquad (\text{mód} p) \tag{7.8}$$

no tenga solución (dado que, evidentemente, una congruencia es más débil que una igualdad: dos enteros pueden ser congruentes sin ser iguales, pero no al revés). Este enfoque, que a priori podría parecer arbitrario, sorpresivamente funciona siempre para polinomios

homogéneos de grado 2. En general tenemos el siguiente resultado (que generaliza un teorema de Legendre): si $F(x_1, \ldots, x_n) = 0$ no tiene solución en números enteros (donde F es un polinomio homogéneo de grado 2) entonces existe al menos un primo p para el cual la congruencia

$$F(x_1, \ldots, x_n) \equiv 0 \qquad (\text{mód} p) \tag{7.9}$$

tampoco tiene solución. La recíproca es trivial (y vale para cualquier función F), pero la veracidad de la afirmación precedente es una "grata sorpresa". Decimos esto último porque hay igualdades (de grado superior al 2) que no tienen solución y sin embargo todas sus correspondientes congruencias (módulo todos los primos) sí la tienen. Un ejemplo concreto de esta última afirmación fue encontrado en 1951 por E. Selmer (y publicado en la referencia [Sel51], pero realmente se "terminó de entender" en la década de 1980) y lo constituye la siguiente curva algebraica:

$$A: \qquad 3x^3 + 4y^3 + 5z^3 = 0. \tag{7.10}$$

La misma no tiene puntos racionales distintos del $(0, 0, 0)$ a pesar de que para todo primo p hay puntos módulo p en ella.

Retomando nuestro problema de ver que la forma cuadrática $x^2+y^2-3z^2$ no representa a cero para ninguna terna de racionales $(x, y, z) \neq (0, 0, 0)$ utilizando la estrategia de hallar un primo p (adecuado) para el cual la congruencia $x^2 + y^2 - 3z^2 \equiv 0$ no tenga solución módulo p, debemos empezar por buscar dicho primo. Así por ejemplo, si elegimos arbitrariamente $p = 7$ veremos que la congruencia se cumple (existen, por ejemplo, $x = 1, y = 2$ y $z = 2$ tales que $x^2 + y^2 - 3z^2 = 1 + 4 - 12 = -7 \equiv 0\,(\text{mód}7)$). De modo que $p = 7$ no es adecuado para nuestro propósito. Sí lo será $p = 3$.

Empecemos observando que si $a \not\equiv 0\,(\text{mód}3)$ entonces $a^2 \equiv 1\,(\text{mód}3)$. De modo que si $x \not\equiv 0$ e $y \not\equiv 0\,(\text{mód}3)$ entonces $x^2+y^2 \equiv 2\,(\text{mód}3)$, y como para todo z es $3z^2 \equiv 0\,(\text{mód}3)$ resulta que $x^2 + y^2 - 3z^2 \not\equiv 0\,(\text{mód}3)$.

Resta ver el caso $x \equiv 0$ ó $y \equiv 0\,(\text{mód}3)$. Pero (siempre trabajando en módulo 3): $x \equiv 0 \Rightarrow x^2 \equiv 0$, lo cual, junto con el hecho de que $3z^2 \equiv 0$ nos da que $x^2 - 3z^2 \equiv 0$, es decir, que $y^2 \equiv 0\,(\text{mód}3)$, lo cual a su vez implica que $y \equiv 0\,(\text{mód}3)$. Hemos probado que en nuestra ecuación: $x \equiv 0\,(\text{mód}3) \Leftrightarrow y \equiv 0\,(\text{mód}3)$. Luego, en el caso que nos resta ver, sólo pueden ser simultáneamente $x \equiv 0$ e $y \equiv 0\,(\text{mód}3)$. Además, bajo estas condiciones también z debe ser múltiplo de 3, porque si no lo fuera tendríamos la contradicción de que x^2 e y^2 serían múltiplos de 9 (y por ende también su suma), sin serlo su "igual" $3z^2$. Por otro lado, como el polinomio es homogéneo, si admite una solución no trivial, también admite una solución primitiva, esto es, una en la cual $\text{mcd}\{x, y, z\} = 1$. Y además, como acabamos de explicar, en una tal solución primitiva no pueden ser x e y múltiplos de 3 a la vez (porque eso también forzaría a que lo sea z, dejando de ser, entonces, primitiva). Y si uno no lo es, ninguno puede serlo (ya visto), pero en tal caso (también visto) la congruencia no tiene solución.

Lo que hemos dado en llamar una "grata sorpresa" es un profundo teorema, extremadamente fuerte, que llamaremos de Hasse-Minkowski (*teorema de H-M* en adelante. El mismo está demostrado en la referencia [Ser73], IV, Theorem 8), el cual afirma que $C(\mathbb{Q}) \neq \emptyset$ si y sólo si se verifican estas dos condiciones:

- para todo primo p hay puntos módulo p en la cónica C, y
- hay al menos un punto real (esto es: de coordenadas reales) en C.

Se suele decir que la segunda condición es la primera aplicada al *primo al infinito*.

Hay otra forma de enunciar el teorema de H-M en términos de los cuerpos p-ádicos $\mathbb{Q}_p$, diciendo que $C(\mathbb{Q}) \neq \emptyset$ si y sólo si se verifican estas dos condiciones:

- para todo primo p hay puntos de $\mathbb{Q}_p$ en la cónica C, y
- hay al menos un punto real (esto es: de coordenadas reales) en C.

También se suele expresar la segunda condición en lenguaje análogo a la primera, diciendo que debe haber puntos de $\mathbb{Q}_\infty$ en la curva. El teorema de H-M es un ejemplo de aplicación de lo que suele llamarse *"principio global* versus *local"*.

Ejercicio 7.1. Mostrar que para cada número natural e existe un entero x solución de la congruencia $x^2 + 1 \equiv 0 \,(\text{mód} 5^e)$.

Digamos también, y sólo a título informativo, que la "lista" (o sucesión) de las infinitas soluciones de la congruencia del Ejercicio 7.1 (una para cada $e \in \mathbb{N}$) es un número 5-ádico, esto es, es un elemento del cuerpo $\mathbb{Q}_5$.

El teorema de H-M es válido para cónicas (y así lo hemos enunciado), pero deja de serlo para curvas más complejas (como la del ejemplo encontrado por Selmer).

7.2. Curvas Elípticas. Como dijimos anteriormente, las cónicas son curvas que poseen un primer nivel de dificultad (en lo referido a la forma de hallar sus puntos racionales). Hay una definición topológica del nivel de complejidad de una curva, que es el llamado *género*. Así, las cónicas (como las rectas) tienen género 0, mientras que las curvas elípticas poseen el siguiente nivel, o sea género 1. De modo que las curvas elípticas estarán definidas por ecuaciones polinómicas de grado 3. Pero ¡cuidado!, porque no toda ecuación de grado 3 define una verdadera curva elíptica.

Con mayor precisión, llamaremos curva elíptica (sobre un cuerpo de característica distinta de 2) a toda aquella curva plana E cuyos puntos (x, y) verifiquen una ecuación de la forma

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{7.11}$$

en la cual f es un polinomio con coeficientes enteros, de grado 3 y sin raíces múltiples (o, como también se suele decir: sin *singularidades*). Simbolizaremos $E(\mathbb{Q})$ al conjunto de los puntos racionales de una curva elíptica E.

No es elíptica, por ejemplo, la curva definida por la ecuación $y^2 = x^2(x + 1)$, pues a pesar de ser cúbico el polinomio $f(x) = x^2(x + 1)$, tiene una *raíz doble* en $x = 0$. Este hecho (el de poseer f raíces múltiples) hace que la curva se parezca más a una cónica que a una curva elíptica (con esto último queremos decir que su género es 0, como en las cónicas, en lugar de 1 como en las verdaderas curvas elípticas).

A continuación veremos una forma "analítica" para determinar singularidades. Consideremos una curva C definida por una ecuación de la forma $y^2 = f(x)$. Si escribimos la misma como $F(x, y) = y^2 - f(x) = 0$ y calculamos sus derivadas parciales,

$$\frac{\partial F}{\partial x} = -f'(x), \qquad \frac{\partial F}{\partial y} = 2y \tag{7.12}$$

entonces por definición la curva es no singular si y sólo si no existen puntos sobre la misma que anulen simultáneamente ambas derivadas parciales. Geométricamente, eso significará que todo punto sobre la curva tiene una recta tangente bien definida.

- Si las derivadas parciales se anulan simultáneamente en un punto (x_0, y_0) de la curva entonces $y_0 = 0$ y $f'(x_0) = 0$, como asimismo $f(x_0) = 0$ (pues $0 = y_0^2 = f(x_0)$). Ahora bien: el hecho de que $f(x_0) = f'(x_0) = 0$ implica que x_0 es una raíz doble de $f(x)$.
- Recíprocamente, si f tuviera una raíz doble en x_0, entonces el punto $(x_0, 0)$ sería un punto singular de la curva (pues su multiplicidad 2 implica que $f(x_0) = f'(x_0) = 0$).

En resumen, una curva C definida por una ecuación polinómica $F(x, y) = 0$ posee una singularidad en (x_0, y_0) si y sólo si:

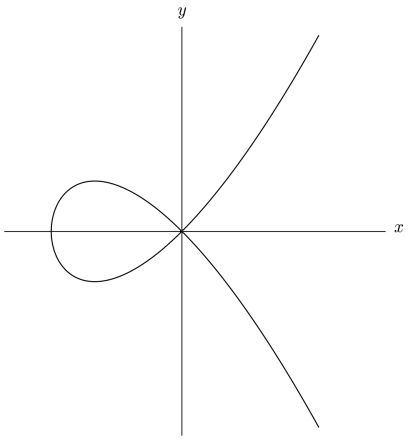


FIGURA 4. Cubica Singular

- $F(x_0, y_0) = 0$ (esto es: $(x_0, y_0) \in C$), y
- $\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$.

En el caso de la curva precedente tenemos que $F(x, y) = y^2 - x^2(x + 1)$ y un punto singular de la misma es $(x_0, y_0) = (0, 0)$. Procediendo como en las cónicas, a partir de éste (que es racional) también podemos hallar infinitos puntos racionales de la curva (que en este caso los habrá) haciendo pasar por $(0, 0)$ rectas con pendiente racional: aquellos puntos donde éstas corten a la curva serán puntos racionales. De modo que ahora la condición "nueva" es que la recta debe pasar por el punto singular (que asumiremos que será racional). Y vemos que el procedimiento es muy similar al ya descrito para las cónicas (y habíamos ejemplificado con cierto detalle en la circunferencia unitaria). Ver la Figura 4.

En el caso que ahora nos ocupa, tales rectas tienen ecuación $y = rx$, con $r \in \mathbb{Q}$, y si buscamos sus puntos de intersección con C obtendremos los puntos (x, y) con $x = r^2 - 1$ e $y = r(r^2 - 1)$, que evidentemente son racionales.

De modo que las dos "patologías" que pueden hacer que una ecuación de la forma $y^2 = f(x)$, con f polinomio a coeficientes enteros de tercer grado, no sea una curva elíptica son:

- que f posea dos raíces iguales, o
- que f posea sus tres raíces iguales.

Ejercicio 7.2. Consideremos la ecuación $y^2 = x^3$.

1. Dibujar su conjunto de puntos reales en el plano,
2. Indicar si dicha curva es singular (esto es: si posee un punto singular),
3. Indicar si la curva posee puntos racionales, y en caso afirmativo, calcularlos.

Para que una ecuación polinómica en dos variables $F(x, y) = 0$ represente a una curva elíptica, también es suficiente que exista un cambio de variables (adecuado) que permita llevarla a la llamada *forma normal de Weierstrass* (o simplemente *forma normalizada* o *forma tipo*) como en (7.11) donde f es un polinomio cúbico con coeficientes enteros y sus tres raíces distintas.

Otra manera de concluir lo mismo es verificando que $F(x, y) = 0$ es una ecuación cúbica no singular, con el agregado (y este es un requisito *sine qua non*) de que sea $C(\mathbb{Q}) \neq \emptyset$.

Dada una cúbica $F(x, y) = 0$ no singular con un punto racional, se puede ver (usando por ejemplo el Teorema de Riemann-Roch) que existe un función que manda la cúbica en una ecuación normalizada como en (7.11), con lo cual nos restringiremos a trabajar únicamente con dicho tipo de ecuaciones.

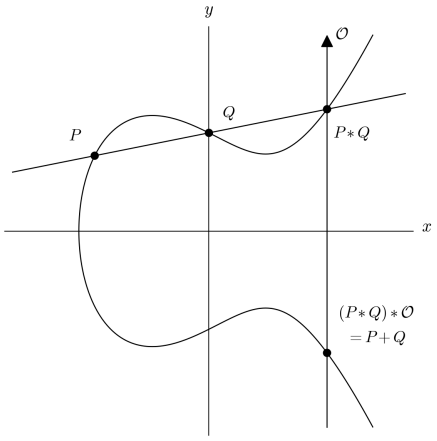


FIGURA 5. Suma en Curvas Elípticas

Para poder unificar el estudio de curvas, es preciso salir de la geometría clásica y trabajar con la llamada *Geometría Proyectiva*. En ella una curva consta no sólo de sus *puntos afines*, sino también de sus *puntos proyectivos*. Así por ejemplo el *plano proyectivo* se obtiene agregando al plano afín un *punto al infinito* por cada dirección. Luego en el plano proyectivo todas las rectas se cortan: las que no en un punto afín (antes llamadas *paralelas*), sí en el punto al infinito (correspondiente a la dirección de las mismas). Para los puntos al infinito interesa la dirección pero no el sentido: yendo "para arriba" o "para abajo" por una misma recta, nos encontramos con el mismo punto al infinito, que en adelante simbolizaremos $\mathcal{O}$. En las curvas elípticas normalizadas, se dice que las rectas verticales son rectas "que pasan por $\mathcal{O}$". Además $\mathcal{O}$ tiene coordenadas ¡proyectivas!, y es racional: $\mathcal{O} \in E(\mathbb{Q})$.

La ventaja de trabajar con el plano proyectivo es que en él, toda recta corta corta a una curva elíptica E en tres puntos (contados con multiplicidad).

Así como en las cónicas y en las cúbicas con puntos singulares, en las curvas elípticas también existen *métodos propagadores* que permiten, a partir de uno o más de sus puntos racionales conocidos, generar otros. Lo importante es, siempre, encontrar el o los puntos de partida y saber que los que generaremos por estos métodos pueden no ser todos. Dado que una recta corta a una curva elíptica en tres puntos, necesitaremos partir de dos de sus puntos racionales (dos puntos de $E(\mathbb{Q})$) para ir generando otro u otros puntos racionales de las mismas. Esto dará lugar a una "operación", a dos puntos de la curva le podremos asociar un tercero, que le otorgará al conjunto $E(\mathbb{Q})$ la estructura, antes anunciada, de grupo Abeliano.

Dados los dos puntos (racionales) de partida sobre E, que llamaremos P y Q, comenzaremos por definir una operación $*$ (que leeremos *estrella*) entre ellos cuyo resultado se obtiene trazando la recta pasante por P y Q e intersectando a E : dicho punto de intersección R^* será el resultado de $P * Q$. Si ésta fuera la "operación" en $E(\mathbb{Q})$, no habría estructura de grupo (la estructura todavía está ausente). A continuación "unimos" R^* con $\mathcal{O}$ trazando por R^* una recta vertical (y en general: paralela a la asíntota) y el punto de intersección de esta última con E, punto que llamaremos R, será el resultado de la "verdadera" operación entre P y Q, operación que denominaremos *suma* y le otorga a $E(\mathbb{Q})$ estructura de grupo Abeliano. En síntesis: $P + Q = (P * Q) * \mathcal{O} = R$ (ver Figura 5). La conmutatividad de la operación suma entre P y Q es evidente, no así su asociatividad.

Ejercicio 7.3. Probar que $\mathcal{O}$ es el neutro para la suma en la curva E.

Supongamos ahora que una curva elíptica E está dada por la ecuación normalizada (7.11), y que los puntos racionales de partida sobre E sean los puntos P y Q, de coordenadas (afines) $P = (x_1, y_1), Q = (x_2, y_2)$. La recta que pasa por ellos tiene por ecuación $y = \lambda x + \nu$, donde $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ y $\nu = y_1 - \lambda x_1$ (desde luego, el caso $x_2 = x_1$ hay que hacerlo aparte. Es un caso más fácil y lo consideraremos más adelante). Reemplazando en la ecuación de E, con el fin de hallar $R^*(x_3, y_3)$, resulta la igualdad

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c, \tag{7.13}$$

y la abscisa x_3 de R^* es la "tercera" raíz (diferente de x_1 y x_2) del polinomio mónico de tercer grado

$$x^3 + \left(a - \lambda^2\right) x^2 + (b - 2\lambda\nu) x + \left(c - \nu^2\right) = 0. \tag{7.14}$$

Si recordamos la relación que existe entre las raíces de un polinomio y los coeficientes del mismo, observaremos que:

$$x_1 + x_2 + x_3 = \lambda^2 - a, \tag{7.15}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = b - 2\lambda\nu, \tag{7.16}$$

$$x_1x_2x_3 = \nu^2 - c, \tag{7.17}$$

planteado lo cual, podemos hallar sus raíces resolviendo un sistema de ecuaciones. En este caso resultará:

$$x_1 + x_2 + x_3 = \lambda^2 - a \quad \Rightarrow \quad x_3 = \lambda^2 - a - x_1 - x_2. \tag{7.18}$$

Una vez obtenida x_3 hallamos la ordenada y_3 de R^* vía la ecuación de la recta: $y_3 = \lambda x_3 + \nu$. Finalmente, como $R(x_r, y_r)$ es simétrico a R^* respecto del eje de las abscisas, sus coordenadas serán $x_r = x_3$ e $y_r = -y_3$. Denominaremos a la expresión (7.18) la *fórmula de la adición.*

A los efectos de ver el caso pendiente ($x_1 = x_2$), correspondiente a la fórmula para x_3 cuando sumamos un punto S con sí mismo, suma que abreviaremos $2S := S + S$ conviene proceder como a continuación indicaremos (pues la expresión anterior de la pendiente λ exigía que los puntos tuvieran abscisas distintas).

Dado $S = (x_0, y_0) \in E$, queremos encontrar las coordenadas de $2S$ a las que llamaremos (x_3, y_3). Primero necesitamos encontrar la ecuación de la recta que une S con S, es decir, de la recta tangente a la cúbica en S. Para ello, a partir de la relación

$$F(x, y) = y^2 - f(x) = y^2 - x^3 - ax^2 - bx - c = 0, \tag{7.19}$$

encontramos, derivando en forma implícita, que $\lambda = \frac{dy}{dx} = -\frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}} = -\frac{-f'(x)}{2y} = \frac{f'(x)}{2y}$, y valorizando en S obtenemos dicha pendiente:

$$\lambda = \frac{f'(x_0)}{2y_0}, \tag{7.20}$$

y la ecuación de la recta tangente será entonces $y = \lambda x + \nu$ con $\nu = y_0 - \lambda x_0$. A los efectos de obtener una fórmula explícita para el valor de las coordenadas de $2S$ en términos de las coordenadas de S, sustituimos la expresión (7.20) de λ en la expresión (7.15). Sacando común denominador y reemplazando y_0^2 por $f(x_0)$ encontraremos que:

$$x_3 = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + (b^2 - 4ac)}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}, \tag{7.21}$$

obteniéndose su ordenada y_3 en consecuencia. La expresión (7.21) es la llamada *fórmula de duplicación.*

Lo que nos interesa destacar de todas estas expresiones, es que las coordenadas del punto "suma" de otros dos, son *funciones racionales* (esto es: cociente de polinomios, y ¡a

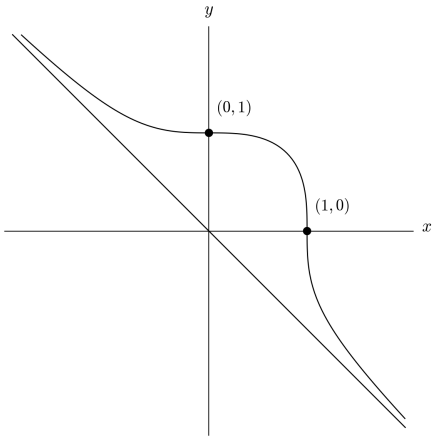


FIGURA 6. Cubica Fermat

coeficientes enteros!) en las coordenadas de los sumandos, de modo que si $P, Q \in E(\mathbb{Q})$ entonces $P + Q \in E(\mathbb{Q})$.

Teorema 7.4 (Mordell)**.** *Sea E una curva elíptica sobre $\mathbb{Q}$, y $E(\mathbb{Q})$ el grupo Abeliano de sus puntos racionales. Entonces $E(\mathbb{Q})$ es finitamente generado.*

Recordar que cuando un grupo Abeliano está finitamente generado su estructura se puede "controlar", pues al existir un número finito de *generadores* (o "puntos privilegiados"), conociéndolos (esto es: conociendo una cantidad "finita" de información referida al grupo), podemos calcular ¡todo! Desde ya que lo anterior no quiere decir que vaya a haber un número finito de puntos racionales en la curva, como tampoco lo contrario.

Los resultados del siguiente ejercicio nos permitirán exhibir dos pares de números (ciertamente "no triviales") tales que la diferencia entre el cubo de uno de ellos y el cuadrado del otro es igual a 17.

Ejercicio 7.5. Dada la curva elíptica definida por la ecuación normalizada $y^2 = x^3 + 17$ y sabiendo que $P_1(-1, 4)$ y $P_2(2, 5)$ son dos de sus puntos racionales, calcular (por el procedimiento descrito de las tangentes y secantes):

1. $P_1 + P_2$,
2. $2P_1$

7.3. Puntos de Torsión. Consideremos la ecuación cúbica $x^3 + y^3 = 1$, que como afirmó P. de Fermat y demostró L. Euler sólo tiene un número finito de puntos racionales, que corresponden a sus dos soluciones "triviales" $(x = 0, y = 1)$ y $(x = 1, y = 0)$ y al punto al infinito $\mathcal{O}$ (que también es racional por ser racional la pendiente de la asíntota, recta cuya dirección define a $\mathcal{O}$). De modo que estos tres son los únicos puntos racionales de la curva definida por $x^3 + y^3 = 1$ (ver Figura 6). Puede verse que $x^3 + y^3 = 1$ representa una curva elíptica E. En efecto: el cambio de variables que nos permite expresarla en la forma normal es el siguiente:

$$x = \frac{36 + Y}{6X}, \qquad y = \frac{36 - Y}{6X}. \tag{7.22}$$

Luego de llevarlo a cabo (¡hacerlo!) obtendremos $Y^2 = X^3 - 432$.

Pero a pesar de la existencia de tal cambio de variable (o cambio de coordenadas, ¡y racional!) que la lleva a la forma normalizada de Weierstrass, la dejaremos simplemente expresada así, como $x^3 + y^3 = 1$ (digamos que "en honor a su fama").

El hecho de que $P(0, 1), Q(1, 0)$ y $\mathcal{O}$ sean sus tres únicos puntos racionales (debido al resultado de L. Euler), hace que si operamos con ellos como aprendimos (esto es, si calculamos $P + Q, 2P, 2Q$, etc.) el resultado siempre será uno de ellos tres y consecuentemente

estará en el conjunto:

$$E(\mathbb{Q}) = \{P, Q, \mathcal{O}\}. \tag{7.23}$$

También hemos dicho que toda recta corta a una curva elíptica en tres puntos y pareciera que en este caso, una recta tangente a E por P cortará a la curva en sólo dos (porque los puntos de tangencia de una recta, son dobles). Pero en esta curva se da el caso que P y Q son, además, *puntos de inflexión* de la misma, lo que hace que en realidad sean puntos *triples*.

Sabemos que $E(\mathbb{Q})$ tiene estructura de grupo Abeliano, de modo que en este caso $E(\mathbb{Q})$ es el (único) grupo de orden tres, el cual es cíclico y por lo tanto Abeliano. Concretamente

$$2P = Q, \qquad 2Q = P, \qquad 3P = \mathcal{O}, \qquad 3Q = \mathcal{O}. \tag{7.24}$$

De modo que P y Q (y desde ya, también $\mathcal{O}$) son los puntos de la curva que tienen *orden finito*. Tales puntos son raros (porque no es frecuente que un punto sumado una cantidad finita de veces consigo mismo tenga por resultado él mismo) y se denominan *puntos de torsión* de la curva elíptica. Como en este caso P y Q tienen orden tres, esto se expresa diciendo que son puntos de 3-torsión de E.

Ampliemos momentáneamente el campo de variación de los puntos de una curva permitiendo que tengan coordenadas reales e incluso complejas. Y lo interesante es que los tres conjuntos de puntos $E(\mathbb{Q}), E(\mathbb{R})$ y $E(\mathbb{C})$ tienen estructura de grupo Abeliano con la misma operación "suma de puntos". De modo que ahora nos van a interesar, por ejemplo, no sólo los puntos racionales de orden 3 de E, sino *todos* los puntos de E de orden 3 (con coordenadas reales o complejas). Para nuestros fines, considerar el conjunto más amplio $\mathbb{C}$, tendrá una ventaja doble: la de tratar con un conjunto que es a la vez *algebraicamente cerrado* y *topológicamente completo* (recordemos que $\mathbb{Q}$ no posee ninguna de ambas propiedades, y que $\mathbb{R}$ reúne sólo la segunda).

Ante todo vamos a hacer una observación respecto del lenguaje que adoptaremos. Es frecuente encontrar en algunos libros la definición de *orden de un elemento* P de un grupo como el *mínimo* natural m tal que

$$\underbrace{P + \ldots + P}_{m \text{ veces}} = mP = \mathcal{O}. \tag{7.25}$$

Los *puntos de m-torsión* de una curva elíptica E (con $m \in \mathbb{N}$) serán aquellos para los cuales $mP = \mathcal{O}$. La curva elíptica del ejemplo precedente ($x^3 + y^3 = 1$) tiene tres puntos de 3-torsión racionales (P, Q y $\mathcal{O}$).

Analicemos propiedades que caracterizan a los puntos de 2-torsión de cualquier curva elíptica E, esto es, de aquellos puntos $P \in E(\mathbb{C})$ tales que $2P = \mathcal{O}$. Por lo pronto, de esto se deduce que $P = -P$. Luego: si un punto P es de 2-torsión entonces está en el eje de simetría de la curva, que será el eje x si la curva esta normalizada. Si simbolizamos con $E(\mathbb{C})[m]$ al conjunto de todos los puntos de m-torsión de E, resulta que el mismo también tiene estructura de grupo Abeliano. Concretamente, en el caso que estamos considerando, $E(\mathbb{C})[2]$ es un grupo Abeliano con cuatro elementos: $\mathcal{O}$ y los tres puntos con ordenada $y = 0$, que son $(\alpha_1, 0), (\alpha_2, 0)$ y $(\alpha_3, 0)$, donde α_1, α_2 y α_3 son las raíces del polinomio $f(x)$. Pero no es el grupo *cíclico* de cuatro elementos, pues éstos deben ser de orden 2 (¡por ser puntos de 2-torsión!); sino que se trata del otro grupo de cuatro elementos, el isomorfo a la *suma directa* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, grupo cuyo conjunto subyacente, lo decimos rápidamente, es el producto cartesiano $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\} \times \{\overline{0}, \overline{1}\} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ y cuya "suma" (la operación que le otorga estructura de grupo) está definida por componentes. En resumidas cuentas:

$$E(\mathbb{C})[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \tag{7.26}$$

(con $\cong$ indicamos *isomorfismo de grupos*).

Pasemos a continuación a analizar los puntos de 3-torsión de una curva elíptica E. Éstos tienen la propiedad de que $3P = \mathcal{O}$, o equivalentemente, que $2P = -P$. Recordando que la abscisa de $-P$ es igual que la abscisa de P, resulta que $2P$ tiene la misma abscisa que P y por lo tanto está sobre la curva, en la misma vertical que P. Dicho brevemente: si P es un punto de 3-torsión de E entonces $2P$ es el otro punto de E que está en la misma vertical que P.

Recordemos la fórmula de duplicación (7.21) que nos permite calcular la abscisa de la suma de un punto con sí mismo y apliquémosla a $2P$. Como en este caso ésta (la abscisa de $2P$) coincide con la de P, igualándolas llegaremos a que:

Teorema 7.6. *$P(x,y) \in E(\mathbb{C})[3]$ si y sólo si $P = \mathcal{O}$ o su abscisa es raíz del polinomio*

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right). \tag{7.27}$$

Puede probarse que el polinomio $\psi_3(x)$ posee 4 raíces distintas (el hecho de que $\psi_3(x)$ no posee raíces múltiples no es un resultado trivial). Combinando estos cuatro valores de x con los dos posibles valores de y (el dado por la fórmula $y = \lambda x + \nu$ y su opuesto), tenemos los ocho puntos afines de 3-torsión de E, que junto con el punto al infinito $\mathcal{O}$ nos dan los 9 puntos de 3-torsión de E. De modo que $E(\mathbb{C})[3]$ es un grupo Abeliano de 9 elementos ($|E(\mathbb{C})[3]| = 9$) e isomorfo (dado que todos sus elementos son de orden 3) a la suma directa de los *enteros módulo* 3:

$$E(\mathbb{C})[3] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}. \tag{7.28}$$

(así que no es, por ejemplo, isomorfo al grupo cíclico de 9 elementos $\mathbb{Z}/9\mathbb{Z}$, etc.)

Ejercicio 7.7. Calcular todos los puntos de 3-torsión (racionales o no) de la curva elíptica definida por la ecuación $x^3 + y^3 = 1$.

El análisis que hemos llevado a cabo sobre los puntos de 2 y de 3-torsión de una curva elíptica E nos induce a pensar que puede haber un resultado general al respecto, y efectivamente es así.

Teorema 7.8. *Sea E una curva elíptica sobre $\mathbb{Q}$, y $m \in \mathbb{N}$. Entonces:*

1. $|E(\mathbb{C})[m]| = m^2$, *y*
2. $E(\mathbb{C})[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

El teorema precedente describe la estructura del grupo de los puntos de m-torsión (o de *m-división*, como también se los denomina) de una curva elíptica cuya ecuación (normalizada) tiene coeficientes racionales: es la suma directa de dos grupos cíclicos de orden m. En dicho grupo puede o no haber puntos racionales.

Recordar que el Teorema de Mordell (7.4) afirma que $E(\mathbb{Q})$ es finitamente generado. Pero sucede que en Teoría de Grupos existe un teorema que describe la estructura de cualquier grupo Abeliano finitamente generado, el cual informalmente afirma que: todo grupo Abeliano finitamente generado está generado por un número finito r de elementos de orden infinito y por otro número finito c de elementos de orden finito. Esto quiere decir que todo grupo Abeliano finitamente generado es isomorfo a r copias de $\mathbb{Z}$ (que es un grupo libre de rango 1 con respecto a la suma: más precisamente su generador es el entero 1, pues sumando el número 1 con sí mismo cualquier cantidad de veces, siempre obtenemos un número distinto de $\mathbb{Z}$), más c elementos de torsión (que en nuestro caso concreto son los c elementos que contenga dicho grupo finito, que simbolizaremos $E_{tor}(\mathbb{Q})$). Simbólicamente, vale el siguiente isomorfismo:

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r \text{ veces}} \oplus E_{tor}(\mathbb{Q}) = \mathbb{Z}^{\oplus r} \oplus E_{tor}(\mathbb{Q}) \tag{7.29}$$

Como acabamos de decir, con $E_{tor}(\mathbb{Q})$ estamos representando a los puntos racionales de torsión (que son "unos pocos", esto es: un número finito que sólo se generan entre ellos mismos). Por ejemplo, en el caso de la curva elíptica $x^3 + y^3 = 1$, de sus nueve puntos de torsión, sólo tres son racionales.

La expresión (7.29) nos está diciendo que $E(\mathbb{Q})$ tiene "dos partes": una libre y una de torsión, y "la parte de torsión, se puede calcular", pero "calcular la parte libre" es más difícil.

Digamos también que hay curvas elípticas en las cuales $r = 0$ y también las hay en las cuales $r > 0$ (y en principio, tan grande como se quiera). Si por ejemplo fuera $r = 20$ (y ya se han encontrado curvas elípticas con este valor de r), nos expresaremos diciendo que la curva es *de rango* 20.

Lo bueno, para nosotros, es que la parte de torsión es bien conocida. Y puntos de m-torsión los hay para todo $m \in \mathbb{N}$. En relación con esto, Beppo Levi conjeturó (en el año 1908, ver [Lev09]) que, aunque puntos de m-torsión puede haber para cualquier m, los que son racionales "no pueden ser tantos", "ni darse para cualquier valor de m". Este trabajo de B. Levi quedó en el olvido y más de 40 años después la misma propiedad fue re-conjeturada por T. Nagell [Nag52], y aún posteriormente, en la década de 1970 era ampliamente conocida como conjetura de Ogg [Ogg71]. Finalmente, en el año 1976, B. Mazur [Maz77] confirmó la *conjetura de B. Levi* (como en realidad mereció haberse llamado) demostrando el Teorema 7.9 que a continuación enunciaremos.

En relación con la *conjetura de B. Levi* , su historia y su alcance resulta muy instructiva la lectura del trabajo de Norbert Schappacher y René Schoof titulado *Beppo Levi and the Arithmetic of Elliptic Curves* [SS96][1]. En el mismo está claramente documentado que B. Levi había intuido lo mismo que otros sospecharon mucho después que él, sólo que a principios del siglo XX todo esto se expresaba en un lenguaje algo diferente del actual.

Teorema 7.9 (Mazur)**.** *El conjunto $E_{tor}(\mathbb{Q})$ de los puntos racionales de torsión de una curva elíptica E sólo puede ser isomorfo a los siguientes grupos finitos:*

1. $\mathbb{Z}/n\mathbb{Z}$ *si* $1 \leq n \leq 10$ *o* $n = 12$*, o bien a*
2. $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *si* $n = 2, 4, 6$ *u* 8*.*

Pero volvamos ahora al Teorema 7.8 y al isomorfismo de su tesis:

$$E(\mathbb{C})[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}. \tag{7.30}$$

Para tratar de "entenderlo" del todo y ver porqué siempre es cierto (o ver más claramente su significado geométrico, o ver una interpretación donde este isomorfismo sea "evidente") nos conviene mirar todos los puntos *complejos* de la curva elíptica E y efectuar

[1]En el mismo podremos leer pasajes como los siguientes, en los cuales refiriéndose a B. Levi, expresan los autores:

- *... his work on the arithmetic of elliptic curves has not received the attention it deserves. He occupied himself with this subject from 1906 to 1908. His investigations, although duly reported by him at the 1908 International Congress of Mathematicians in Rome, appear to be all but forgotten. This is striking because in this work Beppo Levi anticipated explicitly, by more than 60 years, a famous conjecture made again by Andrew P. Ogg in 1970, and proved by Barry Mazur in 1976.* (página 57);
- *More than 40 years later T. Nagell made the same conjecture* [Nag52]*. In our days the conjecture became widely known as Ogg's conjecture, after Andrew Ogg, who formulated it 60 years after Beppo Levi. The problem studied by Beppo Levi and later by Billing, Mahler, Nagell and Ogg has been very important in the development of arithmetic algebraic geometry.* (página 65).

la "construcción" de $E(\mathbb{C})[m]$ desde el punto de vista del Análisis Complejo. Esto significa, en principio, que las variables x e y de la ecuación de E pueden tomar libremente valores en $\mathbb{C}$.

La genuina y original ecuación de K. Weierstrass normalizada para una curva elíptica E es:

$$E: \qquad y^2 = 4x^3 - g_2 x - g_3, \tag{7.31}$$

donde g_2 y g_3 serán, como veremos, dos funciones de "peso" 2 y 3 respectivamente (de ahí los símbolos asignados). A partir de esta E se demuestra que existen dos números complejos ω_1 y ω_2, linealmente independientes sobre $\mathbb{R}$, tales que si consideramos el *retículo* (*lattice* en inglés) generado por el conjunto $\{\omega_1, \omega_2\}$, retículo que se simboliza $L[\omega_1, \omega_2] = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ (y que se denomina *retículo asociado a* E), entonces las funciones

$$g_2 = 60 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^4} \qquad \text{y} \qquad g_3 = 140 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^6}$$

hacen que $x = \wp(u)$ e $y = \wp'(u)$, con $u \in \mathbb{C}$, verifiquen la ecuación de E, donde a su vez $\wp(u)$ (que se lee *p de u*, siendo $\wp$ la llamada *función* $\wp$ *de Weierstrass*) es la siguiente *función elíptica con respecto al retículo* L (lo cual significa que es una función *doblemente periódica*, de períodos ω_1 y ω_2) :

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in L, \omega \neq 0} \left[\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right], \qquad u \in \mathbb{C}.$$

Dado un retículo $L[\omega_1, \omega_2]$ existe todo un "universo" de funciones doblemente periódicas de períodos ω_1 y ω_2, pero la función $\wp$ recién definida "controla" a todas ellas (¡es la principal!).

Que $\wp(u)$ sea doblemente periódica con respecto al retículo $L[\omega_1, \omega_2]$ significa que

$$\forall u \in \mathbb{C}, \omega \in L: \qquad \wp(u + \omega) = \wp(u). \tag{7.32}$$

La ecuación diferencial que verifica $\wp$ es, por lo tanto

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3 \tag{7.33}$$

y es ella la que nos dice que los puntos $P(u)$ de coordenadas $(\wp(u), \wp'(u))$ están en la curva definida por (7.31):

$$P(u) = (\wp(u), \wp'(u)) \in E. \tag{7.34}$$

La precedente, constituye una parametrización con parámetro $u \in \mathbb{C}$, de todos los puntos ¡complejos! de la curva elíptica E (así como (7.3), con parámetro $t \in \mathbb{Q}$, era una parametrización de todos los puntos ¡racionales! de la circunferencia unitaria).

De modo que la correspondencia

$$\mathbb{C} \longrightarrow E(\mathbb{C}), u \mapsto P(u) = (\wp(u), \wp'(u)) \tag{7.35}$$

es un homomorfismo de grupos, que se transforma en isomorfismo si pasamos al cociente entre $\mathbb{C}$ y el retículo L (y aquí utilizamos la doble periodicidad de $\wp$ respecto de L):

$$\mathbb{C}/L \longrightarrow E(\mathbb{C}), u \mapsto P(u) = (\wp(u), \wp'(u)). \tag{7.36}$$

El cociente $\mathbb{C}/L$ no es más que el *toro* (o más precisamente: isomorfo al toro, debido a la doble periodicidad de $\wp$), que es una superficie de Riemann de género 1 (porque tiene 1 "agujero"). La *esfera de Riemann* (sobre la cual hemos considerado las rectas y las cónicas) tiene género 0 (porque no tiene agujeros).

La relación de equivalencia en $\mathbb{C}$ que se considera al pasar al espacio cociente se basa en la doble periodicidad de la función $\wp$ de Weierstrass, y define a dos puntos $u_1, u_2 \in \mathbb{C}$ como *equivalentes* si y sólo si $\wp(u_1) = \wp(u_2)$.

Además, al ser el toro una superficie compacta, resulta que todas las funciones meromorfas en él definidas son *funciones racionales* y por lo tanto están en correspondencia con una *curva algebraica* (en el toro, el punto al infinito de $\mathbb{C}$ aparece como un punto más ¡y cualquiera! de su superficie).

Ahora bien: si calculamos $P(u_1+u_2)$ aplicando (7.34) (donde u_1+u_2 es la suma habitual de dos números complejos) obtendremos ¡oh coincidencia! la función $P(u_1)+P(u_2)$, donde ahora el signo $+$ se refiere a la suma de puntos sobre E definida por el proceso geométrico descrito en la primera clase *de las tangentes y secantes*. Algo informalmente podríamos escribir que:

$$P(u_1+u_2)=P(u_1)+P(u_2). \tag{7.37}$$

Finalmente (y para llegar a esto hicimos la presentación de la función $\wp$) los m^2 puntos de m-división de E (recordemos la tesis 1. del Teorema 7.8) se corresponden con los m^2 números complejos z tales que

$$mz\equiv 0\,(\text{mód}L), \tag{7.38}$$

esto es, con los $z\in\mathbb{C}$ tales que sumados con sí mismo m veces "caen" en el mismo lugar "relativo" dentro del retículo L. Una imagen geométrica que puede ayudar a ver esto que estamos diciendo (o tal vez: que estamos "tratando de decir"), es considerar un *paralelogramo fundamental* de L, dividir dos de sus lados no paralelos en m partes iguales cada uno y trazar rectas paralelas a los lados por cada uno de estos $2m$ puntos. En el paralelogramo fundamental quedan así determinados m^2 puntos z tales que si los sumamos con sí mismos m veces a cada uno de ellos, el resultado mz de esta suma será un punto de otro paralelogramo del retículo (no "el fundamental" de partida), pero dentro de este otro paralelogramo el punto mz ocupará la misma posición (relativa) que ocupa el 0 en el fundamental.

8. Curvas Elípticas sobre cuerpos finitos

Sea E una curva elíptica dada por

$$E:\qquad y^2=x^3+Bx+C,\qquad \text{con } B,C\in\mathbb{Z}, \tag{8.1}$$

ecuación a la que le "falta" el término en x^2, pero puede verse que siempre hay un cambio de variables que permite expresar toda curva elíptica E sobre los racionales con una ecuación de Weierstrass de esta forma. Pero ahora estamos considerando el caso en que los coeficientes B y C del polinomio cúbico $f(x)=x^3+Bx+C$ son números enteros, y como siempre (para que realmente se trate de una curva elíptica) pedimos que f no tenga raíces dobles ni triples (o como también se suele decir: que f sea no singular). Esta última condición equivale a pedir la no anulación de su *discriminante* D :

$$D(f)=\prod_{\alpha_i\neq\alpha_j,i<j}(\alpha_i-\alpha_j)^2=(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2\neq 0,$$

donde $\alpha_i\,(i=1,2,3)$ representan las raíces de f (el discriminante de un polinomio es un buen *invariante*). Por otro lado, también tenemos el *discriminante* Δ de la curva elíptica E definido por:

$$\Delta(E)=-16D(f)=-16\left(4B^3+27C^2\right), \tag{8.2}$$

el cual también va a ser distinto de cero si el discriminante de f lo es.

Vamos a empezar a *controlar módulo* p, con p primo (o como también se dice: a *reducir módulo* p) una curva elíptica. Esto es, dado un primo p, en lugar de E como está dada en (8.1), vamos a trabajar con $E\,(\text{mód}p)$, que no será más que la propia E pero considerando que tanto los coeficientes B y C que la definen, como sus puntos (x,y), están en el conjunto $\mathbb{Z}/p\mathbb{Z}$ de los *enteros módulo* p. Recordemos que este conjunto, al que

simbolizaremos $\mathbb{F}_p$, tiene estructura de cuerpo (pues p es primo): es un cuerpo finito con p elementos. Si lo pensamos "proyectivamente", en él también podemos "agregar" un *punto al infinito*. Usaremos el símbolo $E\,(\text{mód}p)$ para indicar una tal curva elíptica, en cuyo caso, la "igualdad" de (8.1) pasa a ser (aún cuando por comodidad o costumbre sigamos poniendo el signo igual) una congruencia módulo p :

$$E\,(\text{mód}p): \qquad y^2 \equiv x^3 + Bx + C, \qquad \text{con } B, C \in \mathbb{F}_p, \tag{8.3}$$

y también, como estamos diciendo: $x, y \in \mathbb{F}_p$ (esto es: no miramos a los enteros x e y sino a sus restos luego de dividirlos por p). Ahora bien: luego de este drástico cambio de punto de vista puede suceder que, módulo p, ya no sea $\Delta\,(E) \neq 0$ (o más precisamente: no sea $\Delta\,(E) \not\equiv 0\,(\text{mód}p)$) y la curva, que pensada en $\mathbb{Z}$ es elíptica, deje de serlo en $\mathbb{F}_p$ por fallar dicha condición.

Este hecho ya "divide las aguas" entre los primos, y diremos que p será un *primo de buena reducción* si al considerar $E\,(\text{mód}p)$ se verifica o mantiene la condición $\Delta\,(E) \neq 0$ (o más precisamente: $\Delta\,(E) \not\equiv 0\,(\text{mód}p)$). En caso contrario p será *de mala reducción* (estos últimos primos son, entonces, aquellos que dividen (módulo p) al discriminante de la curva elíptica, esto es, aquellos primos p tales que $p|\Delta$).

Fijada una curva elíptica de partida E del tipo (8.1), a la misma podemos reducirla módulo cada primo p y resultará que (sin variar la E de partida) la ecuación reducida $E\,(\text{mód}p)$ seguirá siendo una curva elíptica (ahora sobre $\mathbb{F}_p$) si y sólo si p es un primo de buena reducción para E. Se sabe que para cada curva del tipo (8.1), los primos de mala reducción sólo son un número finito (dado que sólo puede haber un número finito de primos que dividen al discriminante $\Delta\,(E)$). Para ser más precisos, conviene aclarar que antes de reducir modulo p una ecuación de una curva elíptica E, hay que asegurarse que la ecuación escogida es una ecuación minimal en p, pero omitiremos los detalles de la construcción de una tal ecuación minimal.

En lo que sigue, nos interesaremos por los primos de buena reducción. Una primera pregunta y que nos parece bastante natural es: si p es un primo de buena reducción (y por lo tanto $E\,(\text{mód}p)$ es una curva elíptica sobre $\mathbb{F}_p$) ¿cuántos puntos (x, y) con $x, y \in \mathbb{F}_p$ posee $E\,(\text{mód}p)$? Si simbolizamos $E/\mathbb{F}_p$ a tal conjunto, lo que nos preguntamos es: ¿cuál es la cardinalidad del conjunto $E/\mathbb{F}_p$?, esto es: ¿cuánto vale $\#E/\mathbb{F}_p$? Un primer procedimiento para determinarlo podría consistir en darle a x todos sus posibles valores en $\mathbb{F}_p : 0, 1, \ldots, p-1$, reemplazar cada uno de ellos en la ecuación de $E\,(\text{mód}p)$ y ver para cuáles existe un $y \in \mathbb{F}_p$ tal que la congruencia (8.3) se cumple. Por cada valor de x pueden haber a lo sumo dos valores de y (debido a que está elevada al cuadrado), de modo que una primera cota (la más burda) para el número de puntos de $E/\mathbb{F}_p$ resulta ser $2p+1$ y así tenemos que $\#E/\mathbb{F}_p \leq 2p+1$ (ponemos $2p+1$ en lugar de $2p$ porque estamos teniendo en cuenta el punto al infinito). Apenas nos detenemos un poco más en la cuestión podemos hacer el siguiente razonamiento heurístico (que luego nos lo confirmará el Teorema 8.2): como y está elevada al cuadrado, esta potencia 2 de y "pega" la mitad de las y, o dicho más precisamente (dejamos como ejercicio la prueba de esta propiedad):

Ejercicio 8.1. Dado un primo p, los residuos distintos de 0 módulo p son la mitad cuadrados y la mitad no. Esto es: existen $r = \frac{p-1}{2}$ elementos de $\mathbb{F}_p^*$ tales que $r \equiv x^2\,(\text{mód}p)$ al variar x en $\mathbb{F}_p$.

Entonces, de los p valores que puede asumir el segundo miembro al variar x en $\mathbb{F}_p$ (supongamos en principio que todos son posibles), la mitad no van a estar en correspondencia con ningún y que al cuadrado sea congruente con ellos, de modo que sólo "para la otra mitad" habrá dos y por cada valor, y en definitiva la cota se reduce aproximadamente a $p+1$, esto es: $\#E/\mathbb{F}_p \approx p+1$.

Teorema 8.2 (Hasse)**.** *Dada una curva elíptica E y un primo p de buena reducción para E, entonces para $E\,(\text{mód}p)$ se verifica que:*

$$|\#E/\mathbb{F}_p - (p+1)| < 2\sqrt{p}. \tag{8.4}$$

Digamos, antes de continuar, que:

- al número de puntos módulo p que están en la curva elíptica para cada primo p de buena reducción se lo simboliza N_p, esto es: $N_p := \#E/\mathbb{F}_p$, y
- se simboliza a_p a la siguiente diferencia: $a_p := (p+1) - N_p$, que representa el número de puntos de la curva "controlados" por la cota $2\sqrt{p}$.

Ejemplo 8.3. Una curva elíptica peculiar

$$E: \qquad y^2 = x^3 - x. \tag{8.5}$$

Esta curva tiene una particularidad, que es que sobre $\mathbb{C}$ (o cualquier cuerpo donde -1 admita una raíz cuadrada) la curva admite la transformación $(x, y) \to (-x, iy)$ (que se puede verificar preserva la estructura de grupo abeliano).

Veremos a continuación la fórmula para calcular exactamente (esto es: ¡no sólo acotarlos!) los a_p de esta curva elíptica. Tal fórmula se debe a P. de Fermat, quien alrededor de 1630 demostró cuáles enteros se pueden escribir como suma de los cuadrados de otros dos, y cuáles no. A nosotros nos interesará saber qué *primos* son igual a la suma de dos cuadrados, cuestión a la que P. de Fermat dio la siguiente respuesta: si p es primo, entonces

$$p = x^2 + y^2 \iff (p = 2 \quad \text{o} \quad p \equiv 1\,(\text{mód}4))\,, \tag{8.6}$$

siendo esta descomposición, además, esencialmente única (salvo signos y/u orden de los términos). Concretamente, entonces, para la curva peculiar en consideración, el 2 es el único (¡confirmar la unicidad como ejercicio!) primo de mala reducción, y resulta que

$$E\,(\text{mód}p) \rightsquigarrow a_p = \begin{cases} 2\alpha & \text{si} \quad p \equiv 1\,(\text{mód}4) \ \text{ y } p = \alpha^2 + \beta^2, \\ 0 & \text{si} \quad p \equiv 3\,(\text{mód}4)\,. \end{cases} \tag{8.7}$$

Para verificar la igualdad, notemos que si $p \equiv 3 \pmod 4$, entonces -1 no es un cuadrado, con lo cual si al evaluar el polinomio $p(x) = x^3 - x$ en un $x_0 \in \mathbb{F}_p$ obtenemos un valor no nulo, entonces sólo uno de los valores $p(x_0)$ o $p(-x_0)$ puede ser un cuadrado. En particular, el número de puntos de $E/\mathbb{F}_p$ es $3 + 1 + 2 \cdot \frac{p-3}{2}$, donde el 3 corresponde a las raíces de $p(x)$ $(0, 1, -1)$, el 1 corresponde al punto del infinito, y los otros a los valores donde $p(x_0)$ es un cuadrado no nulo (que aporta dos posibilidades para y). En particular, $E/\mathbb{F}_p$ tiene $p + 1$ puntos con lo cual $a_p = 0$. La otra demostración es un poco mas avanzada, ver [Cox13, Theorem 14.16], donde siguiendo su notación, $\mathcal{O} = \mathbb{Z}[i]$, y la condición $p = \pi\bar{\pi}$ es exactamente escribir $p = (\alpha + \beta i)(\alpha - \beta i)$. Notar la ambigüedad entre α y β, una sola corresponde a la elección correcta.

Digamos de paso, que este resultado de P. de Fermat también viene a decirnos qué naturales pueden ser *normas* de enteros algebraicos del cuerpo $\mathbb{Q}\,(i)$ y, en el fondo, con esto último tiene que ver (luego de que C. Gauss publicara sus *Disquisitiones Arithmeticae*, en 1801) el teorema de P. de Fermat sobre los números que se pueden escribir como suma de dos cuadrados.

Ejercicio 8.4. Calcular los puntos que tiene la curva elíptica $E : y^2 = x^3 + x + 1$ sobre $\mathbb{F}_5$.

Además, sobre un cuerpo finito, obviamente todos los puntos de la curva son de torsión.

9. Acción del grupo de Galois en puntos de torsión

Tengamos presente estos tres resultados ya vistos:

1. $E(\mathbb{C})[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ (Teorema 7.8),
2. $E(\mathbb{Q})$ es un grupo Abeliano finitamente generado (Teorema 7.4),
3. $E_{tor}(\mathbb{Q})$ es un grupo Abeliano cuyo orden $|E_{tor}(\mathbb{Q})|$ está acotado "universalmente" (Teorema 7.9).

A pesar de que la demostración del Teorema 7.8 involucra trabajar en el cuerpo $\mathbb{C}$ como cuerpo de variación de los puntos de una curva elíptica, en realidad las coordenadas de cualquier punto de m-torsión $P \in E(\mathbb{C})[m]$ estarán en la *clausura algebraica de* $\mathbb{Q}$. De esta última observación y también de las propiedades de los puntos de m-torsión de E saldrán las representaciones del grupo de Galois.

Como los únicos números de $\mathbb{C}$ que hemos manejado y manejaremos son sus *números algebraicos* (cuyo conjunto se simboliza $\overline{\mathbb{Q}}$, al que también se lo denomina la *clausura algebraica de* $\mathbb{Q}$), simbolizaremos $E\left(\overline{\mathbb{Q}}\right)[m]$ (en lugar de $E(\mathbb{C})[m]$) al conjunto de (todos) los puntos de m-torsión de una curva elíptica E con coordenadas algebraicas (ya sean reales o complejas). Sabemos que dicho conjunto contiene m^2 números algebraicos, tiene estructura de grupo Abeliano, y es isomorfo a la suma directa de los enteros módulo $m : E\left(\overline{\mathbb{Q}}\right)[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

Sin pretender desarrollar la *Teoría de Galois* en toda su generalidad, ni mucho menos, lo que haremos será construir, a partir de los puntos de m-división de una curva elíptica E, su respectivo grupo de Galois.

Recordemos que con cada N_p había asociado un a_p y que dada una curva elíptica $E/\mathbb{Q}$ considerábamos un "primo bueno" p y efectuábamos la "reducción módulo p" de E, obteniendo así $E(\text{mód}p)$: una curva elíptica tal que el polinomio que la define tiene, ahora, todos sus coeficientes en el cuerpo finito $\mathbb{F}_p$. Recordemos también que la relación que vincula los N_p y los a_p es la siguiente:

$$a_p = p + 1 - N_p. \tag{9.1}$$

Sea ahora K un cuerpo de números Galoisiano sobre $\mathbb{Q}$, sea G el grupo de Galois de K ($G = \text{Gal}(K/\mathbb{Q})$) y como hasta ahora, $E(K)$ el conjunto de todos los puntos de una curva elíptica E con coordenadas en K. Sea $P(x,y) \in E(K)$ y $\sigma \in G$. Entonces:

1. $\sigma(P) \in E(K)$, donde obviamente $\sigma(P) = (\sigma(x), \sigma(y))$. Estamos afirmando que si $P \in E(K)$ entonces $\sigma(P) \in E(K)$ o lo que es lo mismo: si P es un punto de E, también lo es su transformado por cualquier automorfismo del grupo de Galois de K.
2. Por ser σ un automorfismo de cuerpos, $\sigma(\mathcal{O}) = \mathcal{O}$.

Teorema 9.1. *Sea E una curva elíptica sobre $\mathbb{Q}, K$ un cuerpo Galoisiano sobre $\mathbb{Q}$ y $G = \text{Gal}(K/\mathbb{Q})$ su grupo de Galois. Entonces:*

1. *$E(K)$ es un subgrupo de $E(\mathbb{C})$,*
2. *$P \in E(K) \Longrightarrow \forall \sigma \in G : \sigma(P) \in E(K)$,*
3. *$\forall P \in E(K), \forall \sigma, \tau \in G : (\sigma \circ \tau)(P) = \sigma(\tau(P)), \qquad id \in G, id(P) = P$*
4. *Interacción con la estructura de grupo. $\forall P, Q \in E(K)$:*
   a) $\sigma(P+Q) = \sigma(P) + \sigma(Q)$,
   b) $\sigma(-P) = -\sigma(P)$,
   c) $\sigma(nP) = n\sigma(P)$.
5. *$P \in E(K)[m] \Longrightarrow \sigma(P) \in E(K)[m]$, donde queremos decir lo siguiente: si P es un punto de m-torsión de E y de orden exactamente m (en esta propiedad m sí*

es minimal: es el orden mínimo de P) entonces $\sigma(P)$ también es un punto de m-torsión de E y de orden exactamente m. O sea que no sólo se preserva lo propiedad de "ser punto de torsión", sino que también se preserva su "orden" (exacto).

Demostración. Veremos la prueba de las dos últimas partes de Teorema, dejando las otras como ejercicio.

4. Esta parte del Teorema nos está diciendo que la estructura de grupo de los puntos de la curva elíptica $E(K)$ (con la suma de puntos definida geométricamente por el método de las tangentes y secantes) es compatible con la acción del grupo de Galois de K.

   Sean $P = (x_1, y_1), Q = (x_2, y_2)$ y $(P + Q) = (x_3, y_3)$. Entonces, por la fórmula de adición (7.18) es $x_3 = \lambda^2 - a - x_1 - x_2$, con $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, de modo que:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2, \qquad y_3 = \lambda x_3 + \nu \tag{9.2}$$

   (donde, recordemos, $\nu = y_1 - \lambda x_1$, y por lo tanto determinando la abscisa x_3, la ordenada y_3 queda automáticamente determinada), y por ser σ un automorfismo resultará:

$$\sigma(x_3) = \ldots = \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}\right)^2 - a - \sigma(x_1) - \sigma(x_2), \qquad \sigma(y_3) = \ldots \tag{9.3}$$

   de modo que:

$$\sigma(P + Q) = (\sigma(x_3), \sigma(y_3)), \qquad \text{y} \tag{9.4}$$

$$\sigma(P) + \sigma(Q) = (\sigma(x_1), \sigma(y_1)) + (\sigma(x_2), \sigma(y_2)) = \ldots \tag{9.5}$$

   y por lo tanto $\sigma(P + Q) = \sigma(P) + \sigma(Q)$, como queríamos ver.

   Las partes b) y c) se dejan como ejercicio.

5. Sabemos que $mP = \mathcal{O}$ con m minimal. Entonces por la parte 4. recién demostrada:

$$m\sigma(P) = \sigma(mP) = \sigma(\mathcal{O}) = \mathcal{O}, \tag{9.6}$$

   de modo que $\sigma(P)$ tiene orden dividiendo a m. Para ver el orden de $\sigma(P)$ es también m, debemos considerar $\sigma^{-1}(\sigma(P))$ y proceder en consecuencia (lo cual se deja como Ejercicio).

□

Para entender el grupo de Galois que se obtiene agregando a $\mathbb{Q}$ todos los puntos de m-torsión de una curva elíptica E, sólo hacen falta las partes 4. y 5. del Teorema 9.1.

En el grupo $E(\mathbb{C})$ se define el siguiente morfismo (que no sólo es un homomorfismo de grupos, sino también un morfismo en el sentido más general de la Geometría Algebraica, en donde se definen los morfismos sobre curvas), llamado *multiplicación por m* (con $m \in \mathbb{N}$):

$$\lambda_m : E(\mathbb{C}) \longrightarrow E(\mathbb{C}), P \mapsto \lambda_m(P) = mP, \tag{9.7}$$

el cual, como tal, respeta la estructura de grupo de $E(\mathbb{C})$. Pues bien: el grupo de los puntos de m-torsión de la curva elíptica E no es más que el núcleo del morfismo λ_m precedente:

$$\ker(\lambda_m) = E(\mathbb{C})[m]. \tag{9.8}$$

Estos morfismos λ_m se denominan *morfismos triviales* y los poseen todas las curvas elípticas (por tener estructura de grupo abeliano). Sea $E[m]$ el conjunto de todos sus puntos de m-torsión distintos del punto al infinito $\mathcal{O}$, y sea S el conjunto de las $2(m^2 - 1)$ coordenadas (x_i, y_i), $1 \leq i \leq m^2 - 1$, de estos puntos (esto es: S es un conjunto de $2(m^2 - 1)$ números algebraicos), entonces el cuerpo K de números algebraicos en consideración será

la siguiente extensión algebraica de los racionales: $K = \mathbb{Q}(S)$. También se lo simboliza $K = \mathbb{Q}(E[m])$.

Teorema 9.2. *Bajo las hipótesis precedentes, $K/\mathbb{Q}$ es una extensión de Galois.*

Demostración. Por lo pronto, observemos que todo automorfismo $\sigma : K \longrightarrow \mathbb{C}$ queda determinado por sus valores sobre los números algebraicos x_i, y_i del conjunto S.

Por el Teorema 9.1, parte 5., si $P_i \in E[m]$ entonces $\sigma(P_i) \in E[m]$ y tiene el mismo orden exacto que el propio punto P_i de partida. Además: $P_i \neq \mathcal{O} \Longrightarrow \sigma(P_i) \neq \mathcal{O}$, de modo que si $P_i \neq \mathcal{O}$ entonces P_i es alguno de los listados en $E[n]$ y su imagen por σ también será uno de los listados en $E[m] : \sigma(P_i) = P_j$, donde las coordenadas de P_j, que son (x_j, y_j) están en S y por lo tanto en K. De modo que $\sigma(K) \subset K$ y por lo tanto la extensión $K/\mathbb{Q}$ es Galois. □

Ahora nos interesaremos en describir el grupo de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ de esta extensión. Tales grupos de Galois, en general, no van a ser conmutativos. Como

$$(P \in E[m], \sigma \in G) \Longrightarrow \sigma(P) \in E[m], \tag{9.9}$$

en particular el automorfismo σ (y por lo tanto: inyectivo) induce una permutación de los puntos de $E[n]$ que respeta la estructura de grupo:

$$\sigma(P+Q) = \sigma(P) + \sigma(Q), \qquad \sigma(-P) = -\sigma(P). \tag{9.10}$$

De modo que cada $\sigma \in G$ da lugar a un homomorfismo del grupo $E[m]$ en sí mismo.

En general, el conjunto $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ de los enteros módulo m es un anillo conmutativo (con la suma y producto habitual de clases) y con divisores de cero si m no es primo (y consecuentemente $\mathbb{Z}_m$ no es un cuerpo si m no es primo). Pero si $m = p$ es primo, entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito de p elementos, el cual acostumbra simbolizarse $\mathbb{F}_p$ (como en las secciones anteriores). Esto hace que el grupo Abeliano $E[m]$ sea:

- un *módulo libre* de dimensión 2 sobre $\mathbb{Z}_m$ (cuando m no es primo), y
- un *espacio vectorial* de dimensión 2 sobre $\mathbb{F}_p$ (cuando p es primo).

Luego, $\sigma \in G$ actuando sobre $E[p]$ es, para p primo, una transformación lineal de un espacio vectorial. Y esto es lo que se denomina una *representación* del grupo G (como las vistas en la sección 2.2). No todo grupo admite una representación como en este caso, y que G la admita es una gran ventaja. Para toda $\sigma \in G : \sigma^{-1}$ induce el morfismo inverso, y por lo tanto la representación tiene inversa.

Cuando m no es primo lo que estamos haciendo es "álgebra lineal sobre un anillo", y entonces las cosas se complican, porque allí hay elementos que no tienen inverso. Miremos entonces el caso $m = p$ primo (como veremos, si entendemos este caso vamos a entender todo). Si tomamos en $E[p]$ dos puntos P_1 y P_2 "independientes", obtenemos una base de $E[p]$, dado que

$$E[p] = \{a_1P_1 + a_2P_2 : a_1, a_2 \in \mathbb{F}_p\}, \tag{9.11}$$

y entonces toda transformación lineal $h : E[p] \longrightarrow E[p]$ queda completamente definida por sus valores sobre P_1 y P_2 (que, como acabamos de decir, constituyen una base para el espacio vectorial $E[p]$) :

$$h(P_1) = \alpha_h P_1 + \gamma_h P_2, \qquad h(P_2) = \beta_h P_1 + \delta_h P_2, \tag{9.12}$$

de modo que h queda caracterizada por la matriz $M \in \mathrm{GL}_2(\mathbb{F}_p)$ de la transformación lineal en la base $\{P_1, P_2\}$.

Volvemos ahora al caso general (m primo o no). Dada $\sigma \in G$, induce una transformación lineal $\sigma : E[m] \longrightarrow E[m], P \mapsto \sigma(P)$ (que es la acción de σ en $E[n]$). Como dicha transformación lineal tiene inversa, si elegimos una base de $E[m]$ (como $\mathbb{Z}_m$-módulo) le podemos asociar una matriz $M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. En particular $\det(M) \in (\mathbb{Z}/m\mathbb{Z})^\times$, donde

con $(\mathbb{Z}/m\mathbb{Z})^\times$ representamos el grupo multiplicativo de los elementos inversibles del anillo $\mathbb{Z}/m\mathbb{Z}$.

Estas representaciones que hemos construido se enmarcan dentro de las representaciones de Galois definidas anteriormente, pero provienen de la curva elíptica E en cuestión.

$$G^m := \mathrm{Gal}\left(\mathbb{Q}\left(E\left[m\right]\right)/\mathbb{Q}\right) \rightsquigarrow \rho_m : G^m \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right). \tag{9.13}$$

Además, la anterior también se denomina *construcción fiel*, dado que las ρ_m resultan inyectivas. Pero en general no son exhaustivas (o suryectivas).

Recordar que vimos que el anillo de números p-ádicos se podía obtener como "pegar" los anillos $\mathbb{Z}/p^r$ para distintos valores de r (esto es truncar las series (1.3)). Queremos hacer un proceso similar para construir representaciones de Galois con coeficientes en los enteros p-ádicos $\mathbb{Z}_p$ a partir de las representaciones ρ_{p^r}. Pues bien, para los anillos $\mathbb{Z}/p^r$ tenemos definidas las respectivas representaciones ρ_{p^r} :

$$\begin{aligned}
\rho_p &: G^p \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)\\
\rho_{p^2} &: G^{p^2} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/p^2\mathbb{Z}\right)\\
&\vdots\\
\rho_{p^r} &: G^{p^r} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/p^r\mathbb{Z}\right)\\
&\vdots
\end{aligned}$$

Notar que $\mathbb{Q}(E[p]) \subset \mathbb{Q}(E[p^2]) \subset \ldots$. En particular, G^p es un cociente de G^{p^2} (dado por restringir los automorfismos al cuerpo $\mathbb{Q}(E[p])$) y así sucesivamente. Si elegimos las bases de $E[p]$, $E[p^2]$, etc de manera "compatible", o sea que si $\{Q_1, Q_2\}$ es base de $E[p^2]$ entonces la base elegida en ρ_p es exactamente $\{pQ_1, pQ_2\}$, entonces si a los coeficientes de la representación ρ_{p^2} los coeficientes módulo p, obtenemos ρ_p. Esto se debe a que si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, entonces para construir ρ_{p^2} debemos escribir $\sigma(Q_1) = \alpha Q_1 + \beta Q_2$, y así obtenemos la primer columna de la matriz. Pero como σ preserva suma, $\sigma(pQ_1) = \alpha pQ_1 + \beta pQ_2$, lo que da la primer columna de la matriz de ρ_p. Mirando todas las representaciones a juntas, podemos obtener una matriz en $\mathrm{GL}_2(\mathbb{Z}_p)$ a partir de ellas (de la misma manera como construimos los números p-ádicos en (1.3). Este proceso como ya mencionamos corresponde a tomar un *límite inverso* (que es una construcción general). Así obtenemos una representación, que se simboliza ρ_{p^∞} :

$$\rho_{p^\infty} : G^{p^\infty} \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_p\right). \tag{9.14}$$

Otra forma de obtener dicha representación, es a partir de los $\mathbb{Z}/p^r$-módulos $E[p^r]$, hacer una construcción similar, tomando límite inverso, lo que da un $\mathbb{Z}_p$-módulo de rango 2, llamado el *módulo de Tate* de E, y que se denota por $T_p(E)$. Así, podemos pensar la representación como $\rho_{p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E))$. Como vimos en la sección de representaciones de Galois, a veces es preferible con trabajar con espacios vectoriales en lugar de módulos. Como $\mathbb{Z}_p \subset \mathbb{Q}_p$, simplemente podemos pensar a nuestra representación como

$$\rho_{p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_p). \tag{9.15}$$

El criterio de Néron-Ogg-Shafarevich dice que la extensión $\mathbb{Q}(E[p^r])/\mathbb{Q}$ es no ramificada fuera de p y de los primos que dividen a $\Delta(E)$, para todo valor de r. Luego por el Teorema de Chebotarev, el conjunto $\{\mathrm{Frob}_\ell\}$, para todo primo ℓ con $\ell \neq p$ es denso en G^{p^∞}.

Teorema 9.3. *Sean $E/\mathbb{Q}$ es una curva elíptica, p un número primo y $\rho_{p^\infty} : G^{p^\infty} \to \mathrm{GL}_2(\mathbb{Z}_p)$. Si ℓ es un primo bueno para E, entonces el polinomio característico de $\rho_{p^\infty}(\mathrm{Frob}_\ell) = x^2 - a_\ell x + \ell$.*

Demostración. Ver por ejemplo [Sil09] Proposición 8.6. □

Lo sorprendente de este resultado está en que este polinomio característico no depende del primo p, sino solamente del primo ℓ, y que la traza coincide con el invariante a_ℓ que definimos asociado al número de puntos de una curva elíptica sobre el cuerpo $\mathbb{F}_\ell$. De modo que si hubiéramos montado toda la construcción precedente a partir de otro primo $q \neq p$, al pasar al límite (proyectivo) hubiéramos llegado a la aplicación ρ_{q^∞} que a los Frobenius $\{Frob_\ell\}$ para ℓ primo, $\ell \neq p$ y $\ell \neq q$, le hubiera hecho corresponder la matriz de $\mathrm{GL}_2(\mathbb{Z}_q)$ cuyo polinomio característico hubiera coincidido con el anterior.

Ejercicio 9.4. A la representación de Galois ρ_{p^∞} le podemos definir una L-serie denotada $L(\rho_{p^\infty}, s)$. Probar que dicha L-serie converge absolutamente si $\Re(s) > \frac{3}{2}$.

Pregunta: dada la representación ρ_{p^∞}, ¿que podemos decir de su imagen?

En general, los únicos morfismos de curvas elípticas son los triviales λ_m (9.7). Cuando hay más endomorfismos, además de ellos (que siempre existen), se dice que la curva elíptica E tiene *multiplicación compleja* (MC en adelante). Estas últimas son curvas "raras". Una de ellas, por ejemplo, es $y^2 = x^3 + x$. Las curvas que tienen MC tiene la propiedad de que las representaciones de Galois ρ_{p^∞} asociadas tienen imagen "no muy grande" para todo p. De hecho, se sabe que la mitad de los a_p son iguales a 0, y esto fuerza al grupo de matrices imagen a ser "casi abeliano", más precisamente, es un grupo que contiene un subgrupo abeliano normal de índice 2 .

Para enunciar el teorema de Serre nos ponemos, por el contrario, en el caso (el más frecuente) de curvas sin MC. Nos preguntamos:

- ρ_p ¿es suryectiva ?(es decir, su imagen es todo $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$),
- ρ_{p^∞} ¿es suryectiva?

En primer lugar, se tiene el siguiente resultado (ver [Ser89]):

Lema 9.5 (Serre)**.** *Si $p > 3$, ρ_p es sobreyectiva si y sólo si ρ_{p^∞} es sobreyectiva.*

A partir de este lema, basta estudiar el problema de las imágenes para las representaciones ρ_p, que tienen la ventaja de que su imagen es un grupo finito, si se desea probar que las imágenes son grandes. Es así como comienza la prueba del siguiente resultado.

Teorema 9.6 (Serre)**.** *si E no tiene MC entonces ρ_{p^∞} es suryectiva para casi todo p (esto es: para todo primo p, salvo un número finito). El conjunto finito donde esto falla es un conjunto a veces llamado de primos excepcionales.*

El Ejemplo (8.5), de la *curva elíptica peculiar* $y^2 = x^3 - x$, lo era porque la misma ¡tiene multiplicación compleja! Otro ejemplo similar es el de la curva dada por la ecuación $y^2 = x^3 + x$, que también tiene MC, el endomorfismo extra es el siguiente: $\phi(x, y) = (-x, iy)$.

El teorema de Serre nos dice por lo tanto que las curvas sin MC tienen grupos de Galois asociados $\mathrm{Gal}(\mathbb{Q}(E[p^\infty]/\mathbb{Q})) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ para casi todo primo p. En cambio, las curvas con MC (y esto se sabía con anterioridad al resultado de Serre) tienen grupo de Galois $\mathrm{Gal}(\mathbb{Q}(E[p^\infty]/\mathbb{Q}))$ "casi conmutativo" para todo primo p.

10. Puntos racionales en curvas de género mayor que 1

En la década de 1920, L. Mordell conjeturó que todas las curvas de complejidad superior (las de nivel siguiente al de las elípticas) poseen sólo un número finito de puntos racionales, esto es, que para ellas $\#C(\mathbb{Q}) < \infty$. Esta propiedad resultó ser cierta y fue probada por G. Faltings en 1983 (quien en 1986 recibió la medalla Fields por demostrar esta conjetura de L. Mordell y otras, debidas a J. Tate, a I. Shafarevich, etc.).

La famosa afirmación de P. de Fermat, conocida como "la Conjetura de Fermat" ó "el Último Teorema de Fermat" (se supone que del año 1637) de que para todo $n \geq 3$, no existen soluciones en números enteros para la ecuación $x^n + y^n = z^n$ fuera de las triviales (que son: $(1,0,1)$ y $(0,1,1)$ cuando n es impar, y $(\pm 1, 0, \pm 1), (\pm 1, 0, \mp 1), (0, \pm 1 \pm 1)$ y $(0, \pm 1 \mp 1)$ cuando n es par, además del $(0,0,0)$ en ambos casos), equivale (deshomogeneizando) a la afirmación de que para todo $n \geq 3$, no existen soluciones en números racionales (fuera de las triviales) para la ecuación $x^n + y^n = 1$. Esta familia de ecuaciones define: una curva elíptica (cuando $n = 3$) e infinitas curvas de complejidad superior (cuando $n \geq 4$).

Aunque en la época en que G. Faltings demostró la conjetura de Mordell, el Último Teorema de Fermat no había sido probado, la misma significó un avance en favor de la veracidad de este último, pues podía asegurarse, al menos, que de existir soluciones para la ecuación $x^n + y^n = z^n$ (con $n \geq 4$), éstas sólo podrían ser un número finito para cada n.

Hoy ya sabemos que la Conjetura de Fermat es cierta. Fue probada en sus primeros casos particulares por el propio P. de Fermat (para $n = 4$, quien indicó el método a seguir en una carta), por L. Euler (alrededor de 1740, para $n = 3$), por A-M. Legendre y G. Dirichlet (en 1823, para $n = 5$), etc.; y en toda su generalidad por A. Wiles, en 1994 (ver [Wil95]), quien en 1998 recibió un premio especial, otorgado por la Unión Matemática Internacional, en reconocimiento a su trabajo.

Concretamente, por ejemplo, la curva C de complejidad superior definida por la ecuación $x^5 + y^5 = 1$ no tiene puntos racionales aparte de los triviales $(0,1)$ y $(1,0)$ que constituyen $C(\mathbb{Q})$ en este caso. Además, el conjunto finito $C(\mathbb{Q})$ de las curvas de complejidad superior no posee ningún tipo de "estructura" (esto es: sus puntos no forman grupo, etc.) y también por eso se hace realmente difícil abordar el estudio de los mismos en dichas curvas.

Referencias

[Cox12] David A. Cox. *Galois theory*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2012.

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[Kob84] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[KR01] Chandrashekhar Khare and C. S. Rajan. The density of ramified primes in semisimple p-adic Galois representations. *Internat. Math. Res. Notices*, (12):601–607, 2001.

[Lev09] Beppo Levi. Sull'equazione indeterminata del 3° ordine. *Atti del IV Congresso Internaz. dei Matematici Roma 6-11 Aprile 1908*, II:173–177, 1909.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. pages 409–464, 1977.

[Mas98] Heinrich Maschke. Ueber den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen. *Math. Ann.*, 50(4):492–498, 1898.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Nag52] Trygve Nagell. Problems in the theory of exceptional points on plane cubics of genus one. In *Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949*, pages 71–76. Johan Grundt Tanums Forlag, Oslo, 1952.

[Ogg71] A. P. Ogg. Rational points of finite order on elliptic curves. *Invent. Math.*, 12:105–111, 1971.

[Ram00] Ravi Ramakrishna. Infinitely ramified Galois representations. *Ann. of Math. (2)*, 151(2):793–815, 2000.

[Rot98] Joseph Rotman. *Galois theory*. Universitext. Springer-Verlag, New York, second edition, 1998.

[RS94] Michael Rubinstein and Peter Sarnak. Chebyshev's bias. *Experiment. Math.*, 3(3):173–197, 1994.

[RV07] Fernando Rodriguez Villegas. *Experimental number theory*, volume 13 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2007.

[Sel51] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser89] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, second edition, 1989. With the collaboration of Willem Kuyk and John Labute.

[Ser12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[SL96] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[SS96] Norbert Schappacher and René Schoof. Beppo Levi and the arithmetic of elliptic curves. *Math. Intelligencer*, 18(1):57–69, 1996.

[Ste15] Ian Stewart. *Galois theory*. CRC Press, Boca Raton, FL, fourth edition, 2015.

[Tri68] Wolfgang Trinks. *Ein Beispiel eines Zahlkörpers mit der Galoisgruppe* PSL$(3, 2)$ *über* $\mathbb{Q}$. Manuscript Univ. Karlsruhe. 1968.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, España

Email address: ldieulefait@ub.edu

FaMAF-CIEM, Universidad Nacional de Córdoba. C.P:5000, Córdoba, Argentina.

Email address: apacetti@famaf.unc.edu.ar

ICTP Trieste.

Email address: villegas@ictp.it