UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

El Teorema de Mordell-Weil

Eduardo Ocampo Alvarez

29 de junio de 2006

Maestro en Ciencias (Matemáticas)

Agradecimientos

Agradezco profundamente al Instituto de Matemáticas por permitirme hacer de él un segundo hogar. No fue sólo el espacio sino también su gente lo que es invaluable. Al Dr. Javier Elizondo por aceptar dirigir este trabajo. Las conversaciones contigo y tus consejos tan acertados y tan a tiempo siempre los tendré presentes.

A mis sinodales Pedro Luis del Angel, Francisco Portillo, Felipe Zaldivar y Rogelio Pérez, por pemitirse revisar este trabajo; por las sugerencias y correcciones a éste.

A mis padres Guadalupe y Paulina, por su esmero en tratar de hacer de mi una persona honesta y con valores, aunque quizá en muchas ocasiones pensaron que esa labor era todo menos divertida. Hoy es agradezco por escuchar mis necedades y también por amarme. A mis hermanas Elvia y Sandra, que amo y me han dado la oportunidad de experimentar el mejor cariño que puedo tener: el de mis sobrinos.

A lo largo de esta experiencia tuve la oportunidad de hacer grandes amigos, tanto en el IMATE como en la Facultad de Ciencias. Mi más sincero agradecimiento a todos ellos por su amistad y apoyo incondicional. He vivido con ustedes grandes experiencias y los estimo: Jorge Eduardo (Jorch), Ann Margareth, Sergio Hernandez (Checo), Grissel Santiago, Adriana de la Cruz, Emigdio Martinez (Mito), Mario Lomelí, Edgar Jasso, José Crux Zagal, José Yudico, Marisol Flores, Abraham Martín del Campo, Juan Ochoa.

A mis amigos Andrés, Bernardino, Edith, Efrain y Olga. Les agradezco su confianza y su infinita ayuda. Siempre serán mis *brothers*.

Finalmente y con especial cariño, agradezco al Dr. Fernando Barrera por permitirme ser su alumno.

Índice general

Introducción

La motivación principal del presente trabajo fue tratar de hacer mas accesible uno de los resultados mas importantes dentro de la teoría de Curvas Elípticas: El teorema de Mordell-Weil.

Desde un punto de vista muy personal, la importancia de éste resultado radica en dos puntos muy importantes: primeramente en la cantidad de áreas dentro de las Matemáticas que se relacionan directa o indirectamente con él. Desde la teoría de números algebraicos pasando por el análisis complejo y la geometría algebraica, hasta finalmente ser parte fundamental de la geometría aritmética. Por otro lado, para establecer este resultado se han mejorado (e inclusive generado) técnicas y herramientas en matemáticas que han incidido no solamente en el teorema de Mordell-Weil, sino que por si mismas han sido objeto de un profundo estudio y desarrollo.

El estudio básico de las curvas elípticas, esto es, como una curva algebraica, se desarrolla dentro del área de la geometría algebraica, y en el primer capítulo se consideran los aspectos básicos de las curvas algebraicas, hasta un resultado crucial: el teorema de Riemann-Roch.

En el segundo capítulo se introducen formalmente las curvas elípticas y una de sus características más interesantes: el conjunto de puntos tiene estructura de Grupo. Se definen también conceptos como morfismos entre curvas elípticas (isogénias), y los diferentes invariantes asociadas a las curvas elípticas. Una herramienta de creciente uso en matemáticas y de gran utilidad en este trabajo es la cohomología de grupos, particularmente la cohomología de grupos de Galois y en el capítulo cuatro se establecen los hechos de esta teoría de las cuales se hace uso.

Finalmente en el capítulo cinco se enuncia y prueba el resultado principal de este trabajo, El teorema de Mordell-Weil para $\mathbb{Q}$, el cual establece que toda el grupo de puntos $\mathbb{Q}$-racionales de una curva elíptica es finitamente generado. La prueba se divide en dos etapas, el llamado teorema de Mordell-Weil débil el cual habla sobre la finitud de cierto grupo cociente. La segunda parte nos dice que cualquier punto $\mathbb{Q}$-racional es generado por un conjunto de puntos de "*medida*" pequeña.

Capítulo 1

Preliminares

1.1. Introducción

El propósito de este capítulo es desarrollar la teoría básica de las curvas planas, tanto en su geometría como en su aritmética, hasta enunciar el teorema de Riemann-Roch. Dicho teorema es parte fundamental en el estudio de las curvas elípticas, pues nos permite dar una definición del *género algebraico* de una curva algebraica.

1.1.1. Curvas en el plano Afín

Sea K un campo y supongamos que tiene característica distinta de 2 y 3. Ocasionalmente usaremos que K esta contenido en un campo algebraicamente cerrado (por ejemplo en una cerradura algebraica $\overline{K}$).

El *plano afín sobre* K esta definido como $\mathbf{A}^2 = \mathbf{A}^2(K) := K^2$.

Una *curva plana afín* C definida sobre K es un polinomio no cero $f(x, y)$ en dos variables con coeficientes en K. Un múltiplo de f por un escalar no cero se considerará como la misma curva. El conjunto de ceros de este polinomio es lo que usualmente visualizamos como la curva. Si L es una extensión de campos de K, entonces los ceros de $f(x, y)$ con coordenadas en L se denota por

$$C(L) := \{(x, y) \in L^2 : f(x, y) = 0\}.$$

Si $L = \overline{K}$ decimos que $C(\overline{K})$ *es el conjunto de puntos de la curva* C. Si $L = K$ decimos que $C(K)$ *es el conjunto de puntos* K*-racionales de la curva* C.
Dada una curva C sobre un campo K, decimos que la curva es *irreducible* si el polinomio $f(x, y)$ que define a la curva es irreducible en $\overline{K}[x]$.

Ejemplo 1.1.1
Si $f(x, y) = x^2 + y^2$, entonces la curva que define tiene un único punto $\mathbb{Q}$-racional, a saber el punto $(0, 0)$. Por otro lado, en el campo $\mathbb{Q}(i)$, f admite una factorización $f(x, y) = (x+iy)(x-iy)$. De aquí en adelante convenimos en que curva significará curva irreducible a menos que se especifique lo contrario.

Si $(0,0)$ es un punto de la curva $C : f(x,y) = 0$, calculando la expansión de Taylor en un punto $P = (x,y)$ en una vecindad del $(0,0)$ tenemos que

$$0 = f(x,y) = f_1(x,y) + f_2(x,y) + \cdots$$

donde $f_d(x,y)$ es un polinomio homogéneo de grado d. Si d es el mínimo entero tal que $f_d(x,y) \neq 0$, entonces $f_d(x,y)$ (el cual no es necesariamente irreducible) en una aproximación a C en una vecindad de $(0,0)$ suficientemente pequeña y se llama el término principal de la expansión de Taylor de f.

La curva se dice *lisa o regular* en P si $f_1(x,y) \neq 0$, es decir, la curva puede ser aproximada por una recta en una vecindad pequeña de P. En otro caso se dice *singular*. La 1-forma lineal se escribe como

$$f_1(x,y) = Ax + By \qquad A = \partial_x f \mid_{(0,0)}, \quad B = \partial_y f \mid_{(0,0)},$$

por lo que el punto P es no singular si al menos una de las derivadas parciales es no cero en P. En tal caso decimos que $f_1 = 0$ es la *recta tangente* a C en P.

En general si la curva es singular y d es el mínimo entero tal que f_d es no cero, entonces la forma f_d se factoriza como

$$f_d = \prod_{i=1}^{d} (\alpha_i x + \beta_i y),$$

en una cerradura algebraica de K, y las d líneas

$$\alpha_i x + \beta_i y = 0$$

se llaman las rectas tangentes a C en $(0,0)$. Si las rectas tangentes a C en P son todas distintas, se dice que P es un *punto múltiple ordinario*.

Todo lo anterior se generaliza a puntos P arbitrarios de la curva considerando la expansión de Taylor en P o haciendo un cambio de coordenadas poniendo a P como origen.

Ejemplo 1.1.2 (Un nodo)
La curva cúbica $y^2 - x^3 - x^2 = 0$ es singular en el origen. El término principal en su expansión de Taylor es

$$f_2(x,y) = y^2 - x^2 = (y+x)(y-x),$$

por lo que hay 2 líneas tangentes en el origen: $y = x$ y $y = -x$.
En general, cualquier punto singular en una curva f_2 que se factoriza en rectas distintas se llama *nodo* y normalmente se le piensa como un punto doble.

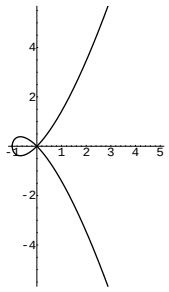


Figura 1.1: Nodo

Ejemplo 1.1.3 (Una cúspide)
La curva cúbica $y^2 - x^3 = 0$ también es singular en el origen y el término principal en la expansión de Taylor es y^2. Esto significa que el eje x es una línea tangente de multiplicidad 2. Singularidades de este tipo se llaman *cúspides*.

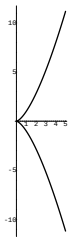


Figura 1.2: Cúspide

Todas nuestras definiciones deberán ser invariantes bajo cambios de *coordenadas afines* seguidas por traslaciones, esto es, bajo funciones de la forma:

$$v \longmapsto Mv + w, \qquad M \in \mathrm{GL}_2(K),\, w \in \mathbf{A}^2(K).$$

Si una recta L en el plano afín interseca a una curva afín C en un punto $P = (x_0, y_0)$, entonces definimos la *multiplicidad de intersección del punto*[1] P (y se denota por $I_P(C \cap L)$) como el orden del cero del polinomio

$$g(t) := f(x_0 + at, y_0 + bt)$$

en $t = 0$, donde f es el polinomio que define a la curva y la recta L se ha parametrizado como:

$$L := \{(x_0 + at, y_0 + bt) \,|\, t \in \overline{K}\}.$$

Otra manera de ver lo anterior es tomar la ecuación de la recta y substituirla directamente en la ecuación de la curva para obtener un polinomio de una sola variable, el cual se factoriza de acuerdo a la multiplicidad.

[1]Este concepto se puede definir tomando no solo rectas sino también curvas algebraicas

Ejemplo 1.1.4
Los puntos de intersección de la parábola $y = x^2 + x$ con la recta $x + y + 1 = 0$ se obtienen substituyendo una ecuación en la otra, por lo que uno llega al polinomio $x^2 + 2x + 1 = (x+1)^2 = 0$ por lo que la recta interseca a la parábola en el punto $(-1, 0)$ con multiplicidad 2.

Ejemplo 1.1.5
La recta $x = y$ y el círculo $x^2 + y^2 = 1$ se intersectan en dos puntos, ambos $\mathbb{Q}(\sqrt{2})$-racionales, pero no $\mathbb{Q}$-racionales.

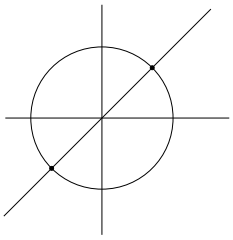


Figura 1.3: Puntos $\mathbb{Q}(\sqrt{2})$-racionales

Ejemplo 1.1.6
La curva cúbica nodal $y^2 = x^3 + x^2 = x^2(x+1)$ interseca a la recta $y = 0$ dos veces en cero y una vez en -1. Si ahora tomamos la recta $y = x$ obtenemos la ecuación $x^3 = 0$ por lo que la recta $y = x$ interseca a la curva en $(0, 0)$ con multiplicidad 3. Esto nos dice que la multiplicidad depende fuertemente de la recta.

Ejemplo 1.1.7 (Punto de Inflexión)
Tomemos la curva $y = x^3$. El origen es un punto no singular y su recta tangente es el eje $y = 0$, por lo tanto si intersectamos tal recta con la curva obtenemos la ecuación $x^3 = 0$, esto es, la recta tangente interseca a la curva en el origen 3 veces. Las rectas tangentes intersecan a la curva 2 veces en el punto de tangencia. Si la multiplicidad es mayor que 2, el punto se dice *punto de inflexión*.

1.1.2. Curvas Proyectivas

Aunque en lo concerniente a nuestro objetivo solo consideraremos curvas en el plano proyectivo, en esta introducción consideraremos curvas en el espacio proyectivo n-

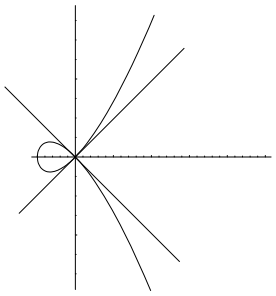


Figura 1.4: rectas tangentes en el punto nodal (multiplicidad 2)

dimensional.

Definición 1.1.1
El Espacio Proyectivo $\mathbb{P}^n(K)$ *se define como el conjunto de clases de equivalencia de* $(n+1)$*-adas* $x = (x_0, \ldots, x_n) \in \mathbf{A}^n(K)$ *bajo la siguiente relación:*

$$x \simeq \lambda x, \quad \lambda \in K, \lambda \neq 0.$$

Las clases de equivalencia se denotan $\overline{x} = (x_0 : x_2 : \cdots : x_n)$

Si consideramos el morfismo

$$\begin{aligned} \mathbf{A}^n(K) &\longrightarrow \mathbb{P}^n(K) \\ x = (x_0, \ldots, x_n) &\longmapsto (x_0 : x_2 : \cdots : x_{n-1} : 1) \end{aligned}$$

resulta que es un encaje de $\mathbf{A}^n(K)$ en $\mathbb{P}^n(K)$. Cualquier punto en el espacio proyectivo con su ultima coordenada no cero esta en la imagen de la función anterior, y el complemento de la imagen, el cual es un conjunto que consiste de todas las clases de equivalencia de puntos con $x_n = 0$ es isomorfo a $\mathbb{P}^{n-1}(K)$ y se nombrará *hiperplano al infinito*. Con lo anterior la recta proyectiva $\mathbb{P}^1(K)$ consiste de la recta afín $\mathbf{A}^1(K) = \{(x : 1) \mid x \in K\}$ junto con un simple punto.

Un *cambio de coordenadas* (llamado a veces cambio proyectivo de coordenadas) en el espacio proyectivo es una función de la forma

$$x \longmapsto Mx,$$

donde M es una matriz no singular $(n+1) \times (n+1)$; si dos matrices no singulares difieren por un escalar, entonces determinan el mismo cambio de coordenadas en $\mathbb{P}^n(K)$. Si un cambio de coordenadas manda el hiperplano al infinito en sí mismo, entonces es directo verificar que la restricción de la función al espacio afín $\mathbf{A}^n(K)$ es un cambio de coordenadas afín.

Un polinomio no cero $f(x)$, en $n+1$ variables ($f \in K[x_0, \ldots, x_n]$) se dice *homogéneo* de grado d si es una combinación lineal de monomios de grado total d. Lo anterior es equivalente a que f cumple que $f(\lambda x) = \lambda^d f(x)$ para todo $\lambda \in \overline{K}$. El conjunto de raíces del un polinomio homogéneo es un subconjunto bien definido de $\mathbb{P}^n(\overline{K})$ dado que $f(x) = 0$ es equivalente a $f(\lambda x) = 0$.

Definición 1.1.2
Una variedad algebraica *(proyectiva) se define como el conjunto de raíces en* $\mathbb{P}^n(\overline{K})$ *de una colección de polinomios homogéneos.*

Las variedades algebraicas se puede escribir como unión finita de variedades *irreducibles*. Dichas variedades son aquellas que no se pueden escribir como uniones finitas de subvariedades propias.
Si V es una variedad algebraica proyectiva el *ideal homogéneo I(V)* es el ideal en $\overline{K}[X_1, \ldots, X_n]$ generado por

$$\{f \in \overline{K}[X_1, \ldots, X_n] \mid f \text{ es homogéneo y } f(P) = 0 \,\forall\, P \in V\}.$$

En tal caso definimos el *anillo coordenado homogéneo de* V (denotado por $\Gamma_h(V)$) como el anillo cociente

$$\Gamma_h(V) := \overline{K}[X_1, \ldots, X_n]/I(V).$$

Es fácil ver que $I(V)$ es un ideal primo y por tanto $\Gamma_h(V)$ es un dominio entero.

Sea $K_h(V)$ el campo de cocientes de $\Gamma_h(V)$.Definimos el *campo de funciones de* V de V, denotado por $K(V)$, como

$$\{z \in K_h(V) \mid z = \frac{f}{g}, \text{ para algunos } f, g \in \Gamma_h(V) \text{ del mismo grado}\}.$$

Es directo ver que $K(V)$ es un subcampo de $K_h(V)$ y a sus elementos le llamaremos *funciones racionales en* V.

Sea $P \in V$, $z \in K(V)$. Decimos que z *está definida en* P si z se puede escribir como $z = \frac{f}{g}$, con f, g clases de polinomios homogéneos en $\Gamma_h(V)$ del mismo grado de tal forma que $g(P) \neq 0$. Definimos entonces el conjunto

$$\mathcal{O}_P(V) := \{z \in K(V) \mid z \text{ está definida en P}\}.$$

El conjunto $\mathcal{O}_P(V)$ resulta ser un anillo local con ideal maximal

$$M_P(V) := \{z \mid z = \frac{f}{g},\ g(P) \neq 0,\ f(P) = 0\}.$$

Definición 1.1.3
Una curva proyectiva *es una variedad algebraica irreducible de dimensión 1.*

Aquí dimensión se considera como dimensión del espacio topológico[2].

Podemos extender el concepto de recta tangente para el espacio proyectivo y entonces decimos que una curva proyectiva es *no singular* o *lisa* si para cada punto tiene una única tangente.

Nos restringiremos ahora al caso $n = 2$. Si tenemos curvas en espacios proyectivos de dimensión mayor, éstas se pueden ver en el plano proyectivo haciendo uso de la proyección desde un punto, y si esto es hecho con cuidado, muchas propiedades se preservan.

Definición 1.1.4
Una curva en el plano proyectivo $\mathbb{P}^2(K)$ *es el conjunto de ceros de un polinomio homogéneo e irreducible de* $K[x, y, z]$.

[2]Si X es un espacio topológico, definimos la *dimensión* de X (denotada $\dim X$) como el supremo de todos los enteros n tales que existe una cadena $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ de subconjuntos distintos cerrados e irreducibles de X [Har],pág. 5

Si $f \in K[x, y]$ es un polinomio de grado d, definimos su *homogeneización* como el polinomio homogéneo $f^* \in K[x, y, z]$ dado por:

$$f^*(x, y, z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right).$$

De la definición anterior se concluye que cualquier polinomio homogéneo $g(x, y, z)$ que no es divisible por z es la homogeneización del polinomio $g(x, y, 1)$, y por lo tanto una curva afín $f(x, y) = 0$ determina una curva proyectiva $f^*(x, y, z) = 0$, la cual consiste de los puntos en $\mathbf{A}^2(K)$ donde $f(x, y) = f^*(x, y, 1) = 0$ más los puntos al infinito en la línea $z = 0$, los cuales se obtienen resolviendo $f^*(x, y, 0) = 0$.

Ejemplo 1.1.8
Considere la curva afín $y^2 = x^3 + ax + b$ y su homogeneización $y^2z = x^3 + axz^2 + bz^3$. Los puntos al infinito de la curva proyectiva son aquellos donde $z = 0$, es decir $x^3 = 0$ y por lo tanto el único punto al infinito de la curva es $(0 : 1 : 0)$ y los demás puntos corresponden a puntos de la curva $y^2 = x^3 + ax + b$.

Las nociones de punto liso e intersección en un punto se extienden de los respectivos conceptos en el caso afín haciendo un cambio de coordenadas para mover el punto en consideración al punto $(0 : 0 : 1)$.

Ejemplo 1.1.9
Consideremos la curva cúbica en su forma general

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Implícitamente queremos estudiar el conjunto de ceros en el plano proyectivo del polinomio

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3 = 0.$$

De acuerdo a esto podemos contestar a las preguntas siguientes:

- *¿Cuándo el punto $P = (0 : 1 : 0)$ está en la curva?*
  Por sustitución, cuando $d = 0$.

- *¿Qué significa que el punto P sea un punto no singular?*
  La parte de grado 1 en la expansión de Taylor alrededor de P es $cx + gz$, por lo que el punto es no singular si c o g son no cero.

- *¿Qué significa que la recta al infinito sea tangente en P?*
  La recta al infinito es la recta $z = 0$, por lo que ésta es la tangente en P si $c = 0$ y $g \neq 0$

- *¿Qué significa que P sea un punto de inflexión si la recta al infinito sea la tangente en P?*
  La tangente ($z = 0$) intersecta a la curva en los puntos de la cúbica donde $ax^3 + byx^2 = 0$ y entonces tenemos multiplicidad 3 cuando $b = 0$ (Recordemos que multiplicidad > 2 significa que el punto es de inflexión).

El ejemplo anterior nos da el resultado siguiente.

Lema 1
Una curva plana cúbica tiene la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

si y solo si el punto $(0:1:0)$ *es un punto liso en la curva, además de que es punto de inflexión y tiene como tangente a la recta al infinito* $z = 0$.

1.2. Divisores y el teorema de Riemann-Roch

En lo sucesivo omitiremos las pruebas de algunos resultados ya que aunque los temas siguientes serán usados como herramienta para la parte central de este trabajo, no se consideró necesario completar estos temas.

Por un *divisor* de X entendemos una suma formal

$$D = \sum_{P \in X} n_P P, \qquad n_P \in \mathbb{Z}$$

y donde $n_P = 0$ salvo un número finito de puntos $P \in X$. El conjunto de divisores forman un grupo abeliano (es precisamente el grupo libre generado por los puntos de X).

Definimos el *grado* de un divisor D como la suma de sus coeficientes, esto es:

$$\deg\left(\sum_{p \in X} n_P P\right) = \sum_{p \in X} n_P.$$

De lo anterior podemos observar que $\deg(D + D') = \deg D + \deg D'$.

Decimos que un divisor $D = \sum_{p \in X} n_P P$ es *efectivo* si $n_P \geq 0 \, \forall \, P \in X$.
Al conjunto de divisores le damos una relación de equivalencia como sigue: dados dos divisores

$$D = \sum_{p \in X} n_P P, \quad D' = \sum_{p \in X} m_P P,$$

decimos que

$$D \succeq D' \quad \text{si} \quad n_P \geq m_P \quad \forall \, P \in X.$$

Sea C una curva plana de grado n, X un modelo no singular[3] de C y G una curva plana que no contiene a C como componente. Definimos el *divisor de* G como sigue. Calculando la deshomogeneización G_* de G se tiene que $G_* \in K(\mathbb{P}^2(K))$ y entonces

[3]Esto es, existe un morfismo birracional f de X sobre C, donde X es una curva proyectiva no singular.

nos fijamos en la imagen g de G_* en $K(X)$ y entonces tiene sentido calcular el orden $\mathrm{ord}_P(g)$ y por lo tanto definiendo $\mathrm{ord}_P(G):=\mathrm{ord}_P(g)$ de define el divisor de G como

$$\text{div } (G) := \sum_{P\in X} \mathrm{ord}_P(G).$$

Esta definición tiene sentido pues sabemos [Ful, prop 2, cap 7] que el número de intersección de las curvas G y C y el orden de G en X por la fórmula siguiente:

$$I(P, C\cap G) = \sum_{Q\in f^{-1}(P)} \mathrm{ord}_Q(G),$$

por lo tanto

$$\deg \text{div } (G) = \sum_{Q\in X} \mathrm{ord}_Q(G) = \sum_{P\in C} I(P, C\cap G) = mn,$$

donde n es el grado de C y m el grado de G. La última igualdad es el Teorema de Bezout.

En general para cualquier $z \in K(X)$ definimos

$$\text{div } (z) := \sum_{P\in X} \mathrm{ord}_P(Z)P.$$

Como z tiene solamente un número finito de ceros y de polos, se concluye que div (z) es un divisor bien definido.

Definimos de la misma manera

$$(z)_0 = \sum_{\mathrm{ord}_P(z)>0} \mathrm{ord}_P(z)P \quad \text{y} \quad (z)_\infty = \sum_{\mathrm{ord}_P(z)<0} -\mathrm{ord}_P(z)P.$$

Dichos divisores son el *divisor de ceros* y el *divisor de polos* de z respectivamente. Se concluye directamente que

$$\text{div } (z) = (z)_0 - (z)_\infty.$$

Así mismo se puede observar que

$$\begin{aligned} \text{div } (zz_1) &= \text{div } (z) + \text{div } (z_1) \\ \text{div } \left(z^{-1}\right) &= -\text{div } (z) \end{aligned}$$

para cualesquiera $z, z_1 \in K(X)$.

Proposición 1.1
Para cualquier $z \in K(X)$, el grado de div (z) *es* 0.

Demostración.
Sea C una curva de grado n. Tomemos $z = \frac{g}{h}$, con $g, h \in \Gamma_h(C)$ del mismo grado, esto es, g y h son clases de polinomios $G, H \in K[x, y, z]$ de grado m, entonces

$$\text{div } (z) = \text{div } (G) - \text{div } (H)$$

y vimos que div (G) tiene grado $m \cdot n$, por lo tanto el grado de div (z) es cero. ■

Corolario 1.2.1
Sea $z \in K(X)^*$. Los siguientes enunciados son equivalentes

1. $\text{div}\,(z) > 0$.
2. $z \in K$.
3. $\text{div}\,(z) = 0$.

Corolario 1.2.2
Sean $z_1, z_2 \in K(X)^*$, entonces $\text{div}\,(z_1) = \text{div}\,(z_2)$ si y solo si $z_2 = \lambda z_1$ para algún $\lambda \in K$.

Definición 1.2.1
Dos divisores D, D' se dicen linealmente equivalentes *si $D' = D + \text{div}\,(z)$ para algún $z \in K(X)$ y escribimos $D' \equiv D$.*

Proposición 1.2
a) La relación $\equiv$ es de equivalencia.

b) Si $D \equiv D'$ entonces $\deg D = \deg D'$.

c) Si $D \equiv D'$ y $D_1 \equiv D_1'$ entonces $D + D_1 \equiv D' + D_1'$.

d) $D \equiv 0$ si y solo si $D = \text{div}\,(z)$ con $z \in K(X)$.

e) Sea C una curva plana, Entonces $D \equiv D'$ si y solo si existen dos curvas del mismo grado G, G', tales que $D + \text{div}\,(G) = D' + \text{div}\,(G')$.

Demostración.

a) Tenemos que probar 3 propiedades básicas:

1. Claramente es reflexiva, pues $0 \in K(X)$ y por lo tanto $D = D + (0)$, esto es, $D \equiv D$.
2. Si $D \equiv D'$, existe $z \in K(X)$ tal que $D' = D + \text{div}\,(z)$ y de esto, tomando $w = z^{-1} \in K(X)$ tenemos $D = D' - (-\text{div}\,(z)) = D' - \text{div}\,(z^{-1}) = D' - \text{div}\,(w)$ por lo tanto se obtiene que $D' = D + \text{div}\,(w)$ y de esto $D' \equiv D$.
3. Si $D_1 \equiv D_2$ y $D_2 \equiv D_3$, existen $z_1, z_2 \in K(X)$ tales que

$$\begin{aligned} D_1 &= D_2 + \text{div}\,(z_1) \\ D_2 &= D_3 + \text{div}\,(z_2)\,, \end{aligned}$$

de lo cual obtenemos $D_1 = D_3 + \text{div}\,(z_2) + \text{div}\,(z_1) = D_3 + \text{div}\,(z_1 z_2)$ donde $z_1 z_2 \in K(X)$ y por lo tanto $D_1 \equiv D_3$.

b) Si $D \equiv D'$ entonces existe $z \in K(X)$ tal que $D = D' + \text{div}\,(z)$, por lo tanto

$$\deg D = \deg\left(D' + \text{div}\,(z)\right) = \deg D' + \deg\left(\text{div}\,(z)\right) = \deg D'$$

pues $\text{div}\,(z)$ tiene grado cero.

c) Si $D \equiv D'$ y $D_1 \equiv D_1'$ entonces existen $z_1, z_2 \in K(X)$ tales que $D = D' + \text{div}\ (z)$ y $D_1 = D_1' + \text{div}\ (z_1)$ lo cual implica

$$D + D_1 = D' + D_1' + \text{div}\ (z_1 z_2)$$

de lo cual se tiene que $D + D' \equiv D' + D_1'$.

d) la prueba se divide en dos partes:

($\Rightarrow$) si $D \equiv 0$ entonces tenemos que $D = \text{div}\ (z)$ para algún $z \in K(X)$.

($\Leftarrow$) Si $D = \text{div}\ (z)$ con $z \in K(X)$ se tiene que $D \equiv 0$.

e) De manera similar como en el inciso anterior:

($\Rightarrow$) Como $D \equiv D'$ entonces existe $z \in K(X)$ tal que $D = D' + \text{div}\ (z)$. Escribiendo $z = \frac{g}{g'}$ con $g, g' \in \Gamma_h(C)$ del mismo grado, esto es, son clases de curvas G, G' del mismo grado, y por lo tanto $\text{div}\ (z) = \text{div}\ (G') - \text{div}\ (G)$, de donde se obtiene

$$D + \text{div}\ (G) = D' + \text{div}\ (G')\,.$$

($\Leftarrow$) Sea $z = \frac{g}{g'}$, donde $g', g \in \Gamma_h(C)$ son clases de G', G respectivamente, por lo que $z \in K(X)$ y de esto $\text{div}\ (z) = \text{div}\ (G') - \text{div}\ (G)$, y de esto

$$D + \text{div}\ (G) = D' + \text{div}\ (G') \quad \Rightarrow \quad D = D' + \text{div}\ (G') - \text{div}\ (G) = D' + \text{div}\ (z)$$

lo cual significa $D \equiv D'$. ■

1.2.1. Los Espacios $\mathcal{L}(D)$

Iniciemos con un divisor $D = \sum_P n_P P$ en X. De cierta manera D elige puntos P en X y les asigna el entero n_P. ¿Existirá una función racional en X con polos en los puntos elegidos por D y que además el orden de sus polos sea acotado por el orden n_P de P, y si hay, cuantas de estas funciones existen?

Definimos el conjunto

$$\mathcal{L}(D) := \{f \in K(X) \mid \text{ord}_P(f) \geq -n_P \quad \forall \quad P \in X\}.$$

Es fácil ver que una función racional f pertenece a $\mathcal{L}(D)$ si $\text{div}\ (f) + D > 0$, o si $f = 0$, por lo que $\mathcal{L}(D)$ tiene estructura de espacio vectorial sobre K; denotemos entonces la dimensión de este espacio por $\ell(D)$. La siguiente proposición muestra que $\ell(D)$ es finito.

Proposición 1.3

1) Si $D < D'$, entonces $\mathcal{L}(D) \subset \mathcal{L}(D')$ y además

$$\dim_K \left({}^{\mathcal{L}(D')}\!/_{\mathcal{L}(D)} \right) \leq \deg\,(D' - D)$$

2) $\mathcal{L}(O) = K$; $\mathcal{L}(D) = 0$ si $\deg D < 0$.

3) $\mathcal{L}(D)$ es de dimensión finita $\forall\, D$. Si $\deg D \geq 0$, entonces

$$\ell(D) \leq \deg D + 1.$$

4) Si $D \equiv D'$ entonces $\ell(D) = \ell(D')$.

Demostración.
1) Dado que $D < D'$, podemos escribir $D' = D+(P_1)+(P_2)+\cdots+(P_s)$. Si $f \in \mathcal{L}(D)$, si tiene que div $(f) + D > 0$ y por tanto con mayor razón div $(f) + (D + (P_1)) > 0$, lo cual implica que $f \in \mathcal{L}(D + (P_1))$ y de manera general,

$$\mathcal{L}(D) \subseteq \mathcal{L}(D + (P_1)) \subseteq \mathcal{L}(D + (P_1) + (P_2)) \subseteq \cdots \subseteq \mathcal{L}(D').$$

Usando los teoremas de isomorfismo para módulos, se tiene lo siguiente

$$\begin{aligned}\dim\left(\mathcal{L}\,(D')/\mathcal{L}\,(D)\right) = \dim\left(\mathcal{L}\,(D')/\mathcal{L}\,(D + (P_1) + \cdots + (P_{s-1}))\right) + \cdots \\ \cdots + \dim\left(\mathcal{L}\,(D + (P_1) + (P_2))/\mathcal{L}\,(D + (P_1))\right) + \\ + \dim\left(\mathcal{L}\,(D + (P_1))/\mathcal{L}\,(D)\right),\end{aligned}$$

Por lo tanto es suficiente probar que

$$\dim\left(\mathcal{L}\,(D + (P))/\mathcal{L}\,(D)\right) \leq 1.$$

Sea entonces $t \in \mathcal{O}_P(X)$ un parámetro y $r = n_P$ el coeficiente de P en D. Definamos

$$\begin{aligned}\varphi_P : \mathcal{L}(D + (P)) &\longrightarrow K \\ f &\longmapsto (t^{r+1}f)(P)\end{aligned}$$

Como $f \in \mathcal{L}(D+(P))$ se tiene que div $(f)+(D+(P)) > 0$, por lo que $\mathrm{ord}_P(f)+r+1 \geq 0$ y esto hace que φ_P este bien definida. Si ahora nos fijamos en $\ker\varphi_P$ se tiene que $0 = \varphi_P(f) = (t^{r+1}f)(P)$ y por tanto $\mathrm{ord}_P(f) + r + 1 > 0$, esto es $\mathrm{ord}_P(f) + r \geq 0$ lo que significa que $f \in \mathcal{L}(D)$. Recíprocamente también se cumple, y por lo tanto tenemos que $\ker\varphi_P = \mathcal{L}(D)$, de aquí que, usando un teorema de isomorfismos,

$$\mathcal{L}\,(D + P)/\mathcal{L}\,(D) \subseteq K$$

y por tanto se tiene el resultado.

2) De manera inmediata se ve que

$$f \in \mathcal{L}(0) \quad \Longleftrightarrow \quad \text{div}\,(f) \geq 0 \quad \Longleftrightarrow \quad f \in K.$$

Tomemos D tal que $\deg D < 0$ y $f \in \mathcal{L}(D)$, $f \neq 0$. Se tiene entonces que div $(f)+D \geq 0$ y por tanto, si definimos $D' = \text{div}\,(f) + D$ por un lado se observa que $\deg D' \geq 0$ y por otro lado que $\deg D' \equiv D$, y por lo tanto $\deg D' = \deg D$ lo cual es una contradicción. De esto se concluye que $\mathcal{L}(D) = 0$.

3) Sea $n = \deg D \geq 0$. Sea $P \in X$ y definamos $D' = D - ((n+1)P)$. Como $\deg D' < 0$ se tiene que $\mathcal{L}(D') = 0$ por lo tanto $\dim \left(\mathcal{L}(D) / \mathcal{L}(D') \right) = \ell(D)$. Por otro lado tenemos que $D' < D$ y por el inciso 1) tenemos que

$$\dim \left(\mathcal{L}(D) / \mathcal{L}(D') \right) = \ell(D) \leq \deg (D - D') = n + 1.$$

4) Suponga que $D' = D + \text{div } (g)$. Definamos entonces

$$\begin{array}{ccc} \mathcal{L}(D) & \xrightarrow{\psi} & \mathcal{L}(D') \\ f & \longmapsto & fg \end{array}$$

Tenemos que ψ es un isomorfismo y por tanto $\ell(D) = \ell(D')$. ■

De manera más general, para cualquier subconjunto $S \subseteq X$ y cualquier divisor $D = \sum_P n_P P$ en X, definimos

$$\deg^S(D) := \sum_{P \in S} n_P$$

y de manera similar

$$\mathcal{L}^S(D) := \{f \in K(X) \mid \text{ord}_P(f) \geq -n_P \quad \forall \quad P \in S\}.$$

Se cumple entonces un resultado más preciso que la proposición anterior:

Lema 2
Si $D < D'$, entonces $\mathcal{L}^S(D) \subset \mathcal{L}^S(D')$. Si S es finito entonces

$$\dim_K \left(\mathcal{L}^S(D') / \mathcal{L}^S(D) \right) = \deg^S(D' - D)$$

El siguiente resultado es un avance en el cálculo de las dimensiones $\ell(D)$, y su prueba utiliza elementos solamente de teoría de campos de funciones.

Proposición 1.4
Sea K un campo de funciones en una variable sobre k, $x \in K$, $x \notin k$. Sea $(x)_0$ el divisor de ceros de x, y $n = [K : k(x)]$. Entonces

1. *$(x)_0$ es un divisor efectivo de grado n.*
2. *Existe una constante τ tal que $\ell(r(x)_0) \geq rn - \tau$ para todo $r \in \mathbb{Z}$.* ■

A modo de generalización tenemos el siguiente resultado

Teorema 1.2.1 (Teorema de Riemann)
Existe una constante g tal que

$$\ell(D) \geq \deg D + 1 - g$$

para todo divisor D. Al más pequeño de tales g se le denomina el género de X *(ó de K ó de C). Tal número g es no negativo.* ■

Como consecuencia directa tenemos los corolarios siguientes.

Corolario 1.2.3
Si $\ell(D_0) = \deg(D_0) + 1 - g$ *entonces para todo* $D > D_0$ *se cumple que* $\ell(D) = \deg(D) + 1 - g$.

Corolario 1.2.4
Si $x \in K$ *pero* $x \notin k$ *entonces* $g = \deg(r(x)_0) - \ell(r(x)_0) + 1$ *para* $r > 0$ *suficientemente grande.*

Corolario 1.2.5
Existe un entero N *tal que para todo divisor* D *tal que* $\deg(D) > N$ *se cumple que* $\ell(D) = \deg(D) + 1 - g$.

Ejemplo 1.2.1
Si C es una curva cúbica no singular, entonces es proyectivamente equivalente a una curva dada por la ecuación

$$Y^2Z = X(X - Z)(X - \lambda Z) \qquad \lambda \neq 0, 1.$$

Tomando $x = \frac{X}{Z}, y = \frac{Y}{Z}$ entonces la ecuación de-homogenizada se convierte en

$$y^2 = x(x - 1)(x - \lambda).$$

si tomamos $z = x^{-1} \in K(C)$ entonces tenemos que $z \in K \backslash k$, además de que $\mathcal{L}(r(z)_0) \subseteq k[x, y]$ y $\ell(r(z)_0) = 2r$, por tanto por el corolario 1.2.4 se cumple que

$$g = \deg(r(z)_0) - \ell(r(z)_0) + 1 = 1.$$

Recíprocamente si una curva tiene género $g = 1$, aplicando el teorema de Riemann se cumple que $\ell(P) \geq 1$ para todo $P \in C$ y por la proposición 1.3 (como $\deg(P) > 1$) se tiene que

$$\ell(P) < \deg(P) + 1 = 2$$

por lo tanto $\ell(P) = 1$ y más aún $\ell(rP) = r$ (corolario 1.2.3) para todo $r > 0$.
Sea $\{1, x\}$ una base para $\mathcal{L}(2P)$. Entonces

$$\text{div}\ (x) + 2 \cdot P \geq 0$$

o lo que es lo mismo, si escribimos $\text{div}\ (x) = \sum n_P P$, entonces $n_P + 2 \geq 0$. Si $(x)_\infty = P$ entonces C sería racional, por lo tanto $(x)_\infty = 2P$ y también (lema 1.4) $[K : k(x)] = 2$.
Sea ahora $\{1, x, y\}$ base de $\mathcal{L}(3P)$. Se cumple entonces que $(y)_\infty = 3P$ de donde se concluye que $y \notin k(x)$ y por tanto $K = k(x, y)$.
Dado que $1, x, y, x^2, x^3, y^2, xy \in \mathcal{L}(6P)$ tenemos que existe una relación de la forma

$$ay^2 + (bx + c)y = Q(x),$$

donde $Q(x)$ es un polinomio de grado ≤ 3. Si calculamos ord_P en ambos lados de la igualdad forzamos a que $a \neq 0$ y además $\deg Q(x) = 3$, (de lo contrario no habría coincidencia en ord_P), y por tanto podemos suponer que $a = 1$. Sustituyendo en la igualdad anterior y por $y - \frac{1}{2}(bx + c)$ tenemos

$$\begin{aligned}(y - \frac{1}{2}(bx + c))^2 + (bx + c)(y - \frac{1}{2}(bx + c)) &= y^2 - y(bx + c) + \frac{1}{4}(bx + c)^2 \\ &\quad + y(bx + c) - \frac{1}{2}(bx + c)^2 \\ &= y^2 - \frac{1}{4}(bx + c)^2 = Q(x)\end{aligned}$$

de donde tenemos que $y^2 = \prod_{i=1}^{3}(x - \alpha_i)$.

Si $\alpha_1 = \alpha_2$ entonces $\left(\frac{y}{x-\alpha_1}\right)^2 = x - \alpha_3$ de donde $x, y \in k\left(\frac{y}{x-\alpha_1}\right)$ y por tanto X sería racional (imposible pues X es racional $\iff g = 0$). Concluimos que los $\alpha_i's$ son todos distintos y de esto $K = K(C)$, donde C es una curva cúbica no singular dada por

$$C = V\left(Y^2Z - \prod_{i=1}^{3}(X - \alpha_i Z)\right).$$

1.2.2. Derivaciones y Diferenciales

Sea R un anillo que contenga a k y M un R-módulo.

Definición 1.2.2
Una derivación de R en M sobre k *es un mapeo k-lineal $D : R \to M$ tal que*

$$D(xy) = D(x)y + xD(y)$$

para todos $x, y \in R$.

Observemos que si $F \in k[X_1, \ldots, X_n]$ y $x_1, \ldots, x_n \in R$, entonces

$$D\left(F(x_1, \ldots, x_n)\right) = \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(x_1, \ldots, x_n)D(x_i).$$

De aquí en adelante todos los anillos considerados contendrán a k por lo que omitiremos la frase "sobre k".

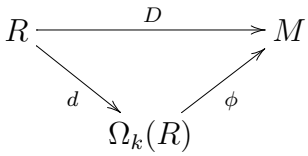
Lema 3
Si R es un dominio entero con campo de cocientes K y M es un espacio vectorial sobre K, entonces cualquier derivación $D : R \to M$ se extiende a una derivacion $\tilde{D} : K \to M$. ■

Consideremos ahora por cada $x \in R$ el símbolo $[x]$ y sea F el R-módulo libre generado por el conjunto $\{[x] \mid x \in R\}$. Tomemos N como el submódulo de F generado por los conjuntos

1. $\{[x + y] - [x] - [y] \mid x, y \in R\}$.
2. $\{[\lambda x] - \lambda[x] \mid x \in R,\ \lambda \in k\}$.
3. $\{[xy] - x[y] - y[x] \mid x, y \in R\}$.

Denotemos por $\Omega_k(R) = \frac{F}{N}$ el R-módulo cociente y dx la clase de $[x]$ en $\Omega_k(R)$. Sea $d : R \to \Omega_k(R)$ que manda a x en dx. A $\Omega_k(R)$ se le llama el *módulo de diferenciales sobre R* y claramente d es una derivación.

Lema 4
Para cualquier R-módulo M y cualquier derivación $D : R \to M$ existe un homomorfismo de módulos $\phi : \Omega_k(R) \to M$ tal que el triángulo



es conmutativo, esto es, $D(x) = \phi(dx)$, para todo $x \in R$.

Demostración.
Si definimos $\phi' : F \to M$ por

$$\phi' \left(\sum \lambda_i [x_i] \right) := \sum \lambda_i D(x_i)$$

es claro que $\phi'(N) = 0$, por lo tanto ϕ' induce el morfismo ϕ deseado. ■

Si $x_1, \ldots, x_n \in R$ y $G \in k[X_1, \ldots, X_n]$ entonces

$$d(G(x_1, \ldots, x_n)) = \sum_{i=1}^{n} \frac{\partial G}{\partial X_i}(x_1, \ldots, x_n) dx_i.$$

De ésto se sigue que si $R = k[x_1, \ldots, x_n]$, entonces $\Omega_k(R)$ es generado por $dx_1, \ldots, dx_n$ (como R-módulo).
De la misma forma supongamos que R es un dominio entero con campo de cocientes K y además tenemos una derivación $\tilde{d} : K \to \Omega_k(R)$ dada por

$$\tilde{d}z = \frac{dx - zdy}{y}$$

donde $z = \frac{x}{y}$, $x, y \in R$. Si $K = k(x_1, \ldots, x_n)$ entonces $\Omega_k(K)$ es un espacio vectorial de dimensión finita sobre k, generado por $dx_1, \ldots, dx_n$.

Proposición 1.5
1. *Sea K un campo de funciones algebraicas de una variable sobre k, entonces*

$$\dim_k (\Omega_k(K)) = 1.$$

2. *(*Char $k = 0$*) Si $x \in K$, $x \notin k$, entonces dx es una base para $\Omega_k(K)$ sobre k.*

Demostración. Sea $F \in k[X, Y]$ una curva plana afín con campo de funciones K. Sea $R = k[X, Y]/(F) = k[x, y]$, $K = k(x, y)$. Asumiendo que $\frac{\partial F}{\partial Y} \neq 0$ es directo verificar que F no divide a $\frac{\partial F}{\partial Y}$ (ya que F es irreducible), por tanto $\frac{\partial F}{\partial Y}(x, y) \neq 0$. Anteriormente habíamos visto que dx y dy generan a $\Omega_k(K)$ y además

$$0 = d(F(x, y)) = \frac{\partial F}{\partial X}(x, y) + \frac{\partial F}{\partial Y}(x, y),$$

por lo tanto $dy = udx$, con $u = -\frac{\frac{\partial F}{\partial X}(x,y)}{\frac{\partial F}{\partial Y}(x,y)}$. Se tiene entonces que dx genera a $\Omega_k(K)$ y de ésto $\dim_k(\Omega_k(K)) \leq 1$. Resta verificar que $\Omega_k(K) \neq 0$.

Por los lemas 3 y 4 basta ver que existe una derivación $D : R \to M$, con M un espacio vectorial sobre K.

Tomemos $M = K$ y para cada $G \in k[X, Y]$ sea $\bar{G}$ su imagen en R. Definamos entonces $D : R \to M$ como

$$D(\bar{G}) = \frac{\partial G}{\partial X}(x, y) - u\frac{\partial F}{\partial Y}(x, y).$$

Es directo verificar que D es una derivación y además $D(x) = 1$, por lo tanto D no es trivial y así $\Omega_k(K) \neq 0$. ■

De la proposición anterior tenemos que ($\operatorname{char} k = 0$) para cualesquier $f, t \in K$, $t \notin k$ existe $v \in K$ tal que $df = vdt$. Es natural entonces escribir $v = \frac{df}{dt}$ y decir que v es la derivada de f respecto de t.

Proposición 1.6
Con K como en la proposición anterior, $\mathcal{O}$ un subanillo de valuación discreta de K, $t \in \mathcal{O}$ un parametro uniformizador. Si $f \in \mathcal{O}$ entonces $\frac{df}{dt} \in \mathcal{O}$. ■

1.2.3. Divisores Canónicos

Sea C una curva proyectiva, X un modelo no singular de C, K su campo de funciones. Tomemos tambien $\Omega = \Omega_k(K)$ el espacio de diferenciales de K sobre k. Los elementos $\omega \in \Omega$ se llaman diferenciales en X o en C.

Sea $\omega \in \Omega$, $\omega \neq 0$ y $P \in X$. Definimos el *orden de ω en P*, $\operatorname{ord}_P(\omega)$, como sigue: sea $t \in \mathcal{O}_P(X)$ un parametro uniformizador, por tanto $\omega = fdt$ y entonces $\operatorname{ord}_P(\omega) := \operatorname{ord}_P(f)$. Ésto está bien definido pues si u es otro parametro uniformizador y $fdt = gdu$, entonces

$$\frac{f}{q} = \frac{du}{dt} \in \mathcal{O}_P(X),$$

y por lo tanto $\operatorname{ord}_P(f) = \operatorname{ord}_P(g)$.
Si $0 \neq \omega \in \Omega$, el divisor de ω, denotado por div (ω), se define como

$$\text{div } (\omega) := \sum_{P \in X} \operatorname{ord}_P(f)P.$$

Definamos el divisor $E = \sum_{P \in X}(m_P X - 1)P$ (aquí $m_P X$ es la multiplicidad del punto $P \in X$).

Proposición 1.7
Suponga que C es una curva plana de grado $n \geq 3$ con solamente puntos multiples ordinarios, entonces para cualquier curva plana G de grado $n - 3$ se tiene

$$\text{div } (G) - E = \text{div } (w)$$

para algún diferencial $\omega \in \Omega$.

El resultado anterior nos dice que div (w) es en efecto un divisor en el sentido que habíamos manejado con anterioridad. Si $\omega \neq 0$ al divisor $W = \text{div } (\omega)$ le llamaremos

divisor canónico. Si ω' es otra diferencial no cero en Ω, entonces tenemos que $\omega = f\omega'$, con $f \in K$, y por tanto

$$\text{div } (\omega) = \text{div } (\omega') + \text{div } (f) = \text{div } (\omega')$$

y por tanto div $(\omega) \equiv$ div (ω'). Por lo tanto los divisores canónicos forman una clase de equivalencia bajo equivalencia lineal, y en particular todos los divisores canónicos tienen el mismo grado.

Corolario 1.2.6
Sea W un divisor canónico. Entonces $\deg(W) = 2g - 2$ *y* $\ell(W) \geq g$.

Estamos ahora en posición de enunciar el resultado mas general, en el cual encontramos el término faltante en el teorema de Riemann.

Teorema 1.2.2 (Teorema de Riemann-Roch)
Sea W un divisor canónico en X. Entonces para cualquier divisor D se cumple

$$\ell(D) = \deg(D) + 1 - g + \ell(D - W). \qquad \blacksquare$$

Como consecuencias directas de este importante resultado tenemos que

Corolario 1.2.7
$\ell(W) = g$ *si W es un divisor canónico.*

Corolario 1.2.8
Si $\deg(D) \geq 2g - 1$, *entonces* $\ell(D) = \deg(D) + g - 1$

Corolario 1.2.9
Si $\deg(D) \geq 2g$, *entonces* $\ell(D - P) = \ell(D) - 1$ *para todo* $P \in X$.

Capítulo 2

Curvas Elípticas

2.1. Curvas Elípticas

En éste capítulo damos (¡por fin!) la definición de una curva elíptica Y establecemos las bases (o los hechos básicos) concernientes a las curvas elípticas.

Definición 2.1.1
Sea K un campo. Una curva elíptica sobre K *(E/K) es una curva proyectiva lisa de género 1 con un punto distinguido* $0 = [0 : 1 : 0]$.

En los siguientes resultados definimos la operación de grupo en una curva elíptica, usando lo establecido en el capítulo anterior.

Proposición 2.1
Sea E una curva elíptica sobre K.

a) Existen funciones $x, y \in K(E)$ tal que la función $\phi : E \to \mathbb{P}^2$ dada $\phi = [x, y, 1]$ da un isomorfismo de E/K a una curva cúbica dada por la ecuación siguiente (llamada ecuación de Weierstrass)

$$C: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

con $a_i \in K$ tal que $\phi(0) = [0, 1, 0]$.

b) Toda curva cúbica lisa C dada por una ecuación de Weierstrass es una curva elíptica con punto distinguido $0 = [0, 1, 0]$.

Demostración.
a) Como en el ejemplo 1.2.1, la idea principal es fijarse en los espacios vectoriales $\mathfrak{L}(n(0))$ asociados a la curva elíptica E. Por un corolario al teorema de Riemann-Roch con $g = 1$ se tiene que para todo divisor D efectivo

$$\ell(D) = \deg D$$

y por lo tanto tenemos que $\ell(n(0)) = \deg(n(0)) = n$ para todo $n \geq 1$. De esto podemos decir lo siguiente:

Para $n = 2$ existe $x \in K(E)$ tal que $\{1, x\}$ es base de $\mathfrak{L}(2(0))$. Notemos que x tiene un polo en 0 de orden *exactamente* 2. Similarmente para $n = 3$ existe $y \in K(E)$ tal que

$\{1, x, y\}$ es base del espacio $\mathfrak{L}(3(0))$, donde y tiene en 0 un polo de orden exactamente 3. De nueva cuenta para $\mathfrak{L}(6(0))$ tenemos las funciones que

$$1, x, y, xy, y^2, x^3, x^2 \in \mathfrak{L}(6(0))$$

por lo tanto existe una combinación lineal

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7y^3 = 0$$

donde los $A_i \in K(E)$. Notemos que $A_6A_7 \neq 0$ pues de otra forma tendríamos

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 = 0$$

ó

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + a_7x^3 = 0$$

donde cada término tiene un polo en 0 de orden distinto y por lo tanto son linealmente independientes, de donde se deduce que todos los $A_i's$ son cero. Reemplazando

$$\begin{array}{rcl} x & \rightarrow & -A_6A_7x \\ y & \rightarrow & A_6A_7^2y \end{array}$$

se tiene que

$$A_1 - A_6A_7A_2x + A_6A_7^2A_3y + A_4A_6^2A_7^2x^2 - A_5A_6^2A_7^3xy + A_6^3A_7^4y^2 - A_6^3A_7^4x^3 = 0$$

de donde dividimos entre el $A_6^3A_7^4$ obtenemos una expresión de la forma

$$-a_6 - a_4x + a_3y - a_2x^2 + a_1xy + y^2 - x^3 = 0.$$

lo siguiente es probar que la función es un isomorfismo, para lo cual basta que sea de grado 1, esto es que $K(E) = K(x, y)$.

Tomemos la función $[x, 1] : E \rightarrow \mathbb{P}^1$. Como x tiene sólo un polo doble en 0, entonces el grado de esta aplicación es 2, ésto es, $[K(E) : K(x)] = 2$. De manera similar tenemos que $[K(E) : K(y)] = 3$ pues la aplicación $[y, 1] : E \rightarrow \mathbb{P}^1$ tiene grado 3 ya que la función y tiene un polo triple en 0. Dado que estos dos grados son divididos por el grado de a la aplicación definida antes $E \rightarrow \mathbb{P}^2$, se tiene que la única posibilidad es que $\deg \phi = 1$. Por lo tanto es un isomorfismo.

b)Ejemplo 1.2.1 ■

2.2. Ecuaciones de Weierstrass

Como se estableció en la proposición 2.1, toda curva elíptica tiene asociada una ecuación de Weierstrass, por lo que es necesario establecer algunos hechos respecto de curvas elípticas dadas por dichas ecuaciones.
Si la característica de K no es 2, entonces en la forma de Weierstrass podemos completar el cuadrado en el lado izquierdo (o lo que es lo mismo hacemos la sustitución $y \mapsto \frac{1}{2}(y - a_1x - a_3)$)para obtener:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

donde

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

Definimos las cantidades siguientes

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{(discriminante)} \\ j &= \frac{c_4^3}{\Delta} \qquad \text{(invariante } j\text{)} \\ \omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \end{aligned}$$

Las cuales cumplen relaciones interesantes, como por ejemplo

$$b_2b_6 - b_4^2 = 4b_8.$$

y de la misma forma $1728\Delta = c_4^3 - c_6^2$. Si, más aún, tenemos que $\operatorname{char} K \neq 2, 3$, podemos hacer el reemplazo

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{216}\right)$$

y se elimina el término x^2.

Ejemplo 2.2.1
La ecuación cúbica $x^3 + y^3 = z^3$ (llamada de Fermat) no está en su forma de Weierstrass, sin embargo, al hacer los cambios $x = Y + 36$, $y = -Y + 36$, $z = 6X$ obtenemos la ecuación

$$Y^2 = X^3 - 432$$

la cual claramente está en la forma de Weierstrass y define entonces una curva elíptica con invariante $j = 0$ y discriminante $\Delta = -432^3$. Posteriormente explicaremos la importancia de estas cantidades.

2.3. Estructura de Grupo

Dada una curva elíptica $E(K)$, esta hereda una estructura de grupo abeliano por medio de su grupo de divisores. Iniciamos con el siguiente lema:

Lema 5
Sea C una curva de género 1, $P, Q \in C$. Entonces $(P) \equiv (Q) \iff P = Q$.

Demostración. Si $(P) \equiv (Q)$, existe $f \in \bar{K}(C)$ tal que $(P) = \text{div } (f)+(Q)$; esto último implica que $f \in \mathfrak{L}((Q))$. Por el teorema de Riemann-Roch sabemos que $\ell((Q))) = 1$, lo cual nos dice que $f = 1 \cdot k$ con $k \in \bar{K}$, de donde vemos que div $(f) = 0$ y por lo tanto $P = Q$.

Proposición 2.2
Sea $(E, 0)$ una curva elíptica.

a) Para cualquier divisor $D \in \text{Div}^{\,0}(E)$ existe un único punto $P \in E$ tal que

$$D \equiv (P) - (0).$$

Sea $\sigma : \text{Div}^{\,0}(E) \to E$ dado por

$$D \longmapsto P \qquad \textit{donde } D \equiv (P) - (0)$$

b) La función σ es suprayectiva.

c) Sean $D_1, D_2 \in \text{Div}^{\,0}(E)$. Entonces

$$\sigma(D_1) = \sigma(D_2) \quad \Longleftrightarrow \quad D_1 \equiv D_2.$$

Entonces σ induce ua biyección de conjuntos $\bar{\sigma} : \text{Pic}^0(E) \to E$.

d) La función inversa de $\bar{\sigma}$ esta dado por

$$\begin{array}{rcl} \kappa : E & \longrightarrow & \text{Pic}^0(E) \\ P & \longmapsto & [(P) - (0)]. \end{array}$$

Demostración.
a) Como E tiene género 1, el teorema de Riemann-Roch dice que

$$\ell(D + (0)) = 1. \qquad (\text{ya que } \deg D = 0)$$

Sea $f \in \bar{K}(E)$ un generador de $\mathfrak{L}(D + (0))$. Como

$$\text{div } (f) + D + (0) \geq 0 \qquad \mathbf{y} \qquad \deg(\text{div } (f)) = 0$$

existe $P \in E$ tal que

$$\text{div } (f) = -D - (0) + (P)$$

y por lo tanto $D \equiv (P) - (0)$. Si $P' \in E$ tiene la misma propiedad, resulta que $(P) \equiv (P')$ y por el lema anterior se tiene que $P = P'$.

b) Sea $P \in E$. Si tomamos $D = (P) - (0)$, se tiene que $D \in \text{Pic}^0(E)$ y $D \equiv (P) - (0)$, por lo tanto $\sigma(D) = P$.

c) Sean $P_i = \sigma(D_i)$, por lo tanto $(P_i) \equiv D_i + (0)$ de donde obtenemos que $(P_1) - (P_2) \equiv D_1 - D_2$.
$\Rightarrow$) Si $P_1 = P_2$ entonces directamente $D_1 = D_2$, en particular son equivalentes.

$\Leftarrow$) Si $D_1 \equiv D_2$, existe $f \in \bar{K}(E)$ tal que $D_1 - D_2 = \text{div}\,(f) = (P_1) - (P_2)$, esto es, $(P_1) \equiv (P_2)$ y nuevamente el lema anterior asegura que $P_1 = P_2$.

d) Es directo. ■

Notemos que en la proposición anterior la biyección $\bar{\sigma}$ traslada la estructura de grupo de $\text{Pic}^0(E)$ a la curva elíptica. Definamos ahora geométricamente una operación de grupo. Esta operación resulta ser la misma que la heredada por la biyección anterior.

Sean $P, Q \in E$, L la linea recta que conecta a P y Q (recta tangente si $P = Q$) y R el tercer punto de intersección de L con E (Bezout). Sea también L' la recta que conecta a R con 0; Entonces $P \oplus Q$ es el tercer punto de intersección de L' con E.

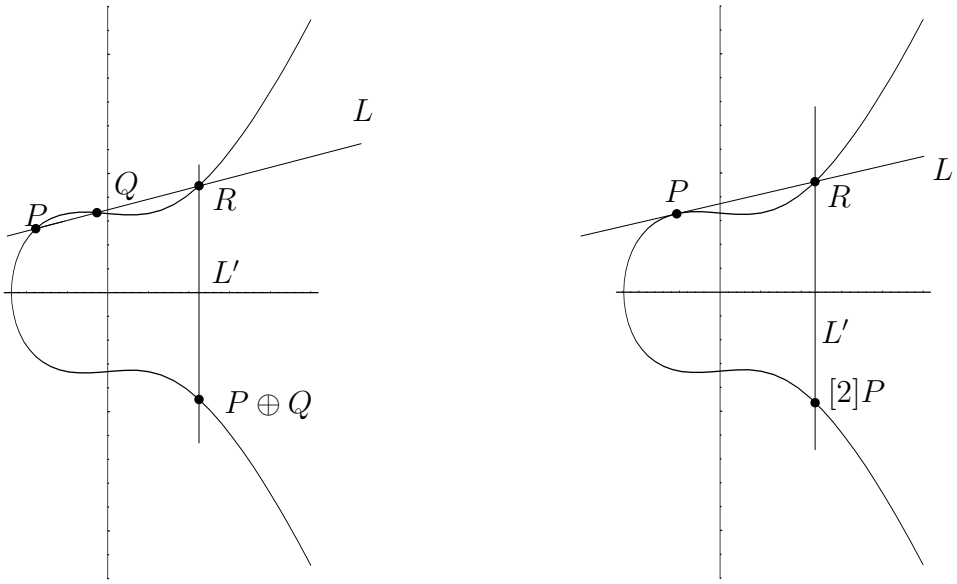


Figura 2.1: operación de grupo en una curva elíptica

Sea E una curva elíptica dada por la ecuación de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Tenemos entonces la proposición siguiente que modela la operación de grupo en E.

Proposición 2.3
La operación de grupo heredada en una curva elíptica es la misma que la construida geométricamente.

Demostración.
Es suficiente probar que

$$\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$$

donde $\oplus$ denota la suma definida de manera geométrica y $+$ la suma del grupo $\text{Pic}^0(E)$.

Sean

$$f_1(x, y, z) = \alpha x + \beta y + \gamma z = 0$$

la recta (en $\mathbb{P}^2(K)$) que une a P, Q y sea R el otro punto de intersección con E. De manera similar definamos

$$f_2(x, y, z) = lx + my + nz = 0$$

la recta que une a $0, R$. Por la definición geométrica, el tercer punto de intersección con E es precisamente $P \oplus Q$. Entonces se tiene que

$$\text{div}\left(\frac{f_1}{z}\right) = (P) + (Q) + (R) - 3(0)$$
$$\text{div}\left(\frac{f_2}{z}\right) = (R) + (P \oplus Q) - 2(0)$$

de donde, restando una igualdad de la otra, obtenemos

$$\text{div}\left(\frac{f_1}{f_2}\right) = (P) + (Q) - (P \oplus Q) \equiv 0$$

y por consiguiente (usando la función κ) se concluye que

$$\kappa(P) + \kappa(Q) - \kappa(P \oplus Q) = [0]$$

y por lo tanto se cumple la igualdad requerida. ■

En lo que resta de la sección supondremos que E está definida por una ecuación en la forma de Weierstrass.

Proposición 2.4
Sea E una curva elíptica.

a) Sea $P_0 = (x_0, y_0) \in E$, entonces $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

Supongamos ahora que $P_1 + P_2 = P_3$, con $P_i = (x_i, y_i) \in E$.

b) Si $x_1 = x_2$ y además $y_1 + y_2 + a_1x_2 + a_3 = 0$, entonces $P_1 + P_2 = 0$, de otra manera tenemos lo siguiente

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \qquad \text{si } x_1 \neq x_2$$

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \qquad \text{si } x_1 = x_2$$

(Aquí, $y = \lambda x + \nu$ es la recta que pasa por P_1 y P_2 ó tangente si $P_1 = P_2$).

c) $P_3 = P_1 + P_2$ está dado por

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

d) Como casos especiales del inciso anterior, tenemos que si $P_1 \neq \pm P_2$, entonces

$$x(P_1 + P_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 + a_1\left(\frac{y_1 - y_2}{x_1 - x_2}\right) - a_2 - x_1 - x_2$$

y la fórmula de duplicación para un punto $P = (x, y) \in E$ es

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4 + b_6}.$$

Demostración.
(a) $-P_0$ es el punto Q tal que $P_0 + Q = 0$, entonces la recta que une a P_0 con Q tiene que ser tangente a 0, esto es, tiene que ser la recta $x = x_0$ y por lo tanto, $x(Q) = x_0$. Para encontrar $y(Q)$ substituimos en la ecuación de Weierstrass donde

$$y^2 + a_1x_0y + a_3y = x_0^3 + a_2x_0^2 + a_4x_0 + a_6 = y_0^2 + a_1x_0y_0 + a_3y_0$$

de donde obtenemos una ecuación cuadrática

$$y^2 + (a_1x_0 + a_3)y - y_0(y_0 + a_1x_0 + a_3) = 0.$$

Sabemos que una raíz de esta ecuación es y_0 y por tanto la otra es precisamente $y(Q) = y_0 + a_1x_0 + a_3$.

(b) Sea $y = \lambda x + \nu$ la recta que pasa por P_1 y P_2 y supongamos que $x_1 \neq x_2$. entonces se tiene que $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ y así

$$\nu = y_1 - \lambda x_1 = y_1 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x_1 = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

Si $x_1 = x_2$ pero $y_2 \neq -y_1 - a_1x_1 - a_3$ entonces $y_2 = y_1$ y por tanto $P_1 = P_2$, por lo que $y = \lambda x + \nu$ es la recta tangente en P_1. Si derivamos implícitamente la ecuación de Weierstrass

$$2yy' + a_1(y + xy') + a_3y' = 3_x^2 + 2a_2x + a_4$$

obtenemos

$$\begin{aligned}
\lambda = y'(x_1, y_1) &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \\
\nu = y_1 - \lambda x_1 &= y_1 - \left(\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}\right)x_1 \\
&= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}
\end{aligned}$$

(c) Si substituimos la ecuación de la recta $y = \lambda x + \nu$ en la ecuación de Weierstrass tenemos

$$(y = \lambda x + \nu)^2 + a_1x(y = \lambda x + \nu) + a_3(y = \lambda x + \nu) = x^3 + a_2x^2 + a_4x + a_6$$

de donde obtenemos el polinomio de grado 3

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\nu)x + a_6 - \nu^2 - a_1\nu - a_3\nu = 0$$

y como sabemos que este polinomio se anula en x_1 y x_2, necesariamente la tercera raíz es la coordenada de $P_1 + P_2$ y utilizando las relaciones existentes entre las raíces del polinomio y sus coeficientes, vemos que

$$-(x_1 + x_2 + x_3) = a_2 - \lambda^2 - a_1\lambda$$

o lo que es lo mismo

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$

para encontrar la coordenada $y(P_1 + P_2)$ substituimos directamente en la ecuación de la recta

$$y(P_1 + P_2) = \lambda x_3 + \nu.$$

(d) Supongamos que $P_1 \neq P_2$, entonces combinando los incisos anteriores se tiene el valor para la coordenada $x(P_1+P_2)$ de manera directa. Para la formula de duplicación de un punto $P = (x, y) \in E$ tenemos que

$$x([2]P) = \left(\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\right) + a_1\left(\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}\right) - a_2 - 2x$$

de donde simplificando se obtiene el resultado. ■

2.4. Isogenias

Nos interesan ahora los morfismos entre curvas elípticas que preservan la operación de grupo definida en ellas.

Definición 2.4.1
Sean E_1, E_2 curvas elípticas. Una isogenia *entre E_1 y E_2 es un morfismo $\phi : E_1 \to E_2$ que satisface $\phi(0) = 0$.*

Notemos que una isogenia ϕ satisface que $\phi(E_1) = \{0\}$ o bien $\phi(E_1) = E_2$, pues un morfismo es constante o suprayectivo y por lo tanto una isogenia distinta de la cero es un morfismo finito de curvas, el cual induce una función inyectiva

$$\phi^* : \overline{K}(E_2) \hookrightarrow \overline{K}(E_1).$$

Notación: Usaremos la notación

$$\mathrm{Hom}_{\bar{K}}(E_1, E_2) : \{\phi : E_1 \to E_2 | \, \phi \text{ es isogenia}\}.$$

Es fácil ver que $\mathrm{Hom}_{\bar{K}}(E_1, E_2)$ es un grupo. Si $E_1 = E_2 = E$, podemos componer isogenias y $\mathrm{End}_{\bar{K}}(E) := \mathrm{Hom}_{\bar{K}}(E, E)$ se convierte en un anillo bajo suma y composición. Denotaremos por $\mathrm{Aut}_{\bar{K}}(E)$ a los elementos invertibles en $\mathrm{End}_{\bar{K}}(E)$.

Ejemplo 2.4.1
Para cada $m \in \mathbb{Z}$ podemos definir la isogenia "multiplicación por m"

$$[m] : E \to E$$

dada como sigue; si $m > 0$ tenemos

$$[m]P := P + P + \cdots + P \qquad m \text{ veces}$$

y cuando $m < 0$, la definición es

$$[m]P := [-m](-P).$$

El hecho de que es una isogenia se sigue por inducción.

Proposición 2.5

a) Sea E/K una curva elíptica y $m \in \mathbb{Z}$, con $m \neq 0$. El morfismo "multiplicación por m" no es constante.

b) Sean E_1, E_2 curvas elípticas. El grupo de isogenias $\mathrm{Hom}_{\bar{K}}(E_1, E_2)$ es un $\mathbb{Z}$-módulo libre de torsión.

c) Sea E una curva elíptica. El anillo $\mathrm{End}_{\bar{K}}(E)$ es un dominio entero. ■

Definición 2.4.2

- *Sea E una curva elíptica y $m \neq 0$ un entero. Definimos el m-ésimo* grupo de torsión de *E, denotado por $E[m]$, como el conjunto de puntos de orden m,*

$$E[m] := \{P \in E | [m]P = 0\}.$$

- *El* subgrupo de torsión de *E, denotado por $T(E)$, es el conjunto de puntos de orden finito, esto es,*

$$T(E) := \bigcup_{m=1}^{\infty} E[m].$$

Supongamos que $\mathrm{char}\, K = 0$, entonces la función

$$[\,] : \mathbb{Z} \longrightarrow \mathrm{End}\,(E)$$

es una biyección y por tanto $\mathrm{End}\,(E) \cong \mathbb{Z}$.

Capítulo 3

Curvas Elípticas sobre $\mathbb{C}$

3.1. Funciones Elípticas

Sea $\Lambda \subseteq \mathbb{C}$ una retícula, esto significa que Λ es un subgrupo discreto de $\mathbb{C}$ el cual contiene una base de $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$.

Ejemplo 3.1.1
El conjunto $\Lambda = \{x + yi \in \mathbb{C} \mid x, y \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}i$ es una retícula, llamada comúnmente *enteros gaussianos*.

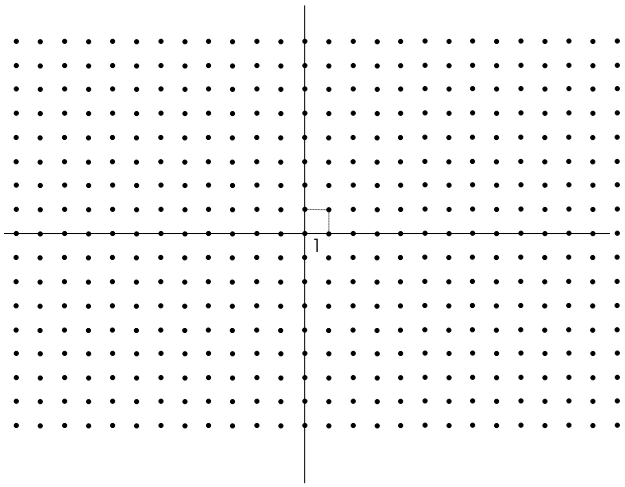


Figura 3.1: Los enteros gaussianos en $\mathbb{C}$.

Definición 3.1.1
Una función elíptica *(relativa a Λ) es una función meromorfa $f(z)$ en $\mathbb{C}$ que satisface:*

$$f(z + w) = f(z) \qquad \forall\, w \in \Lambda \quad \forall\, z \in \mathbb{C}.$$

Al conjunto de funciones elípticas se le denotará por $\mathbb{C}(\Lambda)$. Es claro que $\mathbb{C}(\Lambda)$ es un campo.

Definición 3.1.2
Un paralelogramo fundamental *para* Λ *es un conjunto de la forma*

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\},$$

donde $a \in \mathbb{C}$ *y* $\{\omega_1, \omega_2\}$ *es base de* Λ.

Es claro que la función natural $D \longrightarrow \mathbb{C}/\Lambda$ es biyectiva.

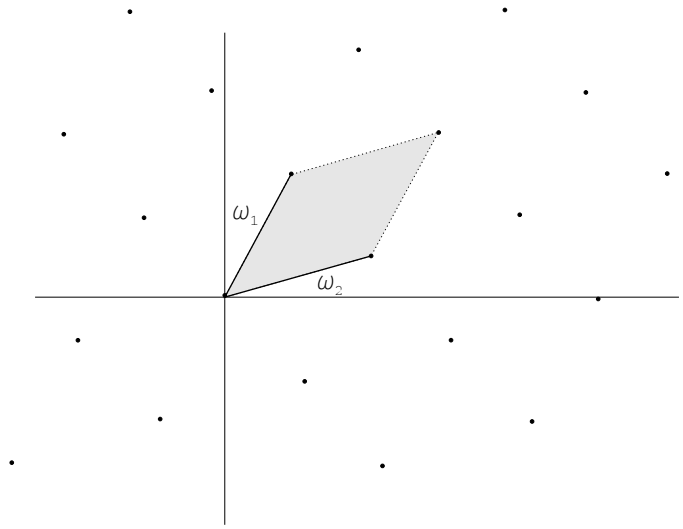


Figura 3.2: Paralelogramo fundamental

Proposición 3.1
Una función elíptica sin polos (sin ceros) es constante.

Demostración.
Suponga que f es una función elíptica y holomorfa ($f \in \mathbb{C}(\Lambda)$) y sea D un paralelogramo fundamental para Λ. Dado que f es periódica en λ se tiene que

$$\sup_{z\in\mathbb{C}} \mid f(z) \mid = \sup_{z\in\overline{D}} \mid f(z) \mid .$$

Sin embargo f es continua y $\overline{D}$ es compacto, por lo tanto $\mid f(z) \mid$ esta acotada en $\overline{D}$ y por lo tanto acotada en $\mathbb{C}$. Usando el teorema de Liouville se tiene entonces que f es constante. Si f no tiene ceros fijémonos en $1/f$. ■

Sea f una función elíptica y $w \in \mathbb{C}$. Tiene sentido definir

$$\begin{aligned} \text{ord}_w(f) &= \text{ orden del cero } w \text{ de } f. \\ \text{res}_w(f) &= \text{ residuo de } f \text{ en } w. \end{aligned}$$

Dada la periodicidad de f, el orden y el residuo de f permanecen iguales si reemplazo w por $w + \omega$, para cualquier $\omega \in \Lambda$. De esto convenimos en lo siguiente: por $\sum_{w\in\mathbb{C}/\Lambda}$ entenderemos la suma sobre $w \in D$, siendo D un paralelogramo fundamental para Λ. Es claro que la suma resultante será independiente de la elección de D.

Teorema 3.1.1
Sea $f \in \mathbb{C}(\Lambda)$,

a) $\displaystyle\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = 0.$

b) $\displaystyle\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = 0.$

c) $\displaystyle\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)\, w \in \Lambda.$

Demostración. Sea D un paralelogramo fundamental para Λ tal que f no tenga ni polos ni ceros en ∂D (la frontera de D).
a) Por el teorema del residuo se tiene que

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)dz.$$

La periodicidad de f nos dice que la integral a lo largo de los lados opuestos del paralelogramo se cancelan, por lo tanto la integral total a lo largo de la frontera de D es cero.

b) la periodicidad de f implica que f' también es periódica. En efecto,

$$f'(z) = \lim_{h\to 0} \frac{f(z+h)-f(z)}{h}$$

y por lo tanto, si $\omega \in \Lambda$, tenemos que

$$f'(z+\omega) = \lim_{h\to 0} \frac{f(z+h+\omega)-f(z+\omega)}{h} = \lim_{h\to 0} \frac{f(z+h)-f(z)}{h} = f'(z),$$

de donde se tiene que $f' \in \mathbb{C}(\Lambda)$. Por otro lado, sabemos que $\operatorname{ord}_w(f) = \operatorname{res}_w\left(\dfrac{f'}{f}\right)$, por lo tanto,

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = \sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w\left(\frac{f'}{f}\right) = \frac{1}{2\pi i}\int_{\partial D} \frac{f'(z)}{f(z)}\,dz = 0,$$

donde la última igualdad se tiene por el mismo argumento que en el inciso anterior.
c) Usando integración por partes a lo largo de ∂D tenemos que

$$\begin{aligned}
\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)\, w &= \frac{1}{2\pi i}\int_{\partial D} \frac{zf'(z)}{f(z)}\,dz \\
&= \frac{1}{2\pi i}\left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a}\right)\frac{zf'(z)}{f(z)}\,dz \\
&= \frac{1}{2\pi i}\left(\int_a^{a+\omega_1} \frac{zf'(z)}{f(z)}\,dz + \int_a^{a+\omega_2} \frac{(z-\omega_1)f'(z-\omega_1)}{f(z-\omega_1)}\,dz + \right. \\
&\quad \left. + \int_{a+\omega_1}^{a} \frac{(z-\omega_2)f'(z-\omega_2)}{f(z-\omega_2)}\,dz + \int_{a+\omega_2}^{a} \frac{zf'(z)}{f(z)}\,dz\right),
\end{aligned}$$

de lo cual simplificando resulta lo siguiente:

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)\, w = \frac{\omega_2}{2\pi i}\int_a^{a+\omega_1} \frac{f'(z)}{f(z)}\,dz + \frac{\omega_1}{2\pi i}\int_{a+\omega_2}^{a} \frac{f'(z)}{f(z)}\,dz.$$

En general, la fórmula $\dfrac{1}{2\pi i}\displaystyle\int_a^b \frac{g'(z)}{g(z)}\,dz$ calcula el índice de la trayectoria $t \mapsto g((1-t)a+tb)$ alrededor del cero, y más aún, si $g(a) = g(b)$ (el cual es nuestro caso pues f es periódica) el valor de la integral es un número entero, y por lo tanto

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)\, w = a_1\omega_1 + a_2\omega_2 \in \Lambda \qquad a_1, a_2 \in \mathbb{Z}. \quad \blacksquare$$

Definición 3.1.3
El orden *de una función elíptica f es el número de polos (con su multiplicidad) en cualquier paralelogramo fundamental. (Esto igual al número de ceros)*

Corolario 3.1.1
Una función elíptica no constante tiene orden al menos 2.

Demostración. Si f tiene un polo simple, por el resultado anterior, el residuo en ese punto es cero, por lo que en realidad es holomorfa, lo cual es una contradicción. $\blacksquare$

Definimos ahora el *grupo de divisores de* $\mathbb{C}/\Lambda$ (denotado por $\operatorname{Div}(\mathbb{C}/\Lambda)$) como el grupo libre abeliano generado por los $w \in \mathbb{C}/\Lambda$. Inmediatamente tenemos lo siguiente: si $D = \displaystyle\sum_{w\in\mathbb{C}/\Lambda} n_w(w) \in \operatorname{Div}(\mathbb{C}/\Lambda)$ se define el *grado de* D como

$$\deg D = \sum_{w\in\mathbb{C}/\Lambda} n_w,$$

y también definimos $\operatorname{Div}^0(\mathbb{C}/\Lambda)$ como el subgrupo

$$\operatorname{Div}^0(\mathbb{C}/\Lambda) = \{D \in \operatorname{Div}(\mathbb{C}/\Lambda) \mid \deg D = 0\}.$$

De un resultado anterior, para cualquier $f \in \mathbb{C}(\Lambda)^*$ definimos un divisor $\operatorname{div}(f) \in \operatorname{Div}^0(\mathbb{C}/\Lambda)$ dado por

$$\operatorname{div}(f) = \sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)\,(w).$$

La asignación anterior define un homomorfismo $\operatorname{div} : \mathbb{C}(\Lambda)^* \longrightarrow \operatorname{Div}^0(\mathbb{C}/\Lambda)$. Definimos también el *morfismo suma* como sigue: si $D = \displaystyle\sum_{w\in\mathbb{C}/\Lambda} n_w(w) \in \operatorname{Div}(\mathbb{C}/\Lambda)$ tenemos:

$$\begin{aligned} \operatorname{sum} : \operatorname{Div}^0(\mathbb{C}/\Lambda) &\longrightarrow \mathbb{C}/\Lambda \\ D &\longmapsto \sum_{w\in\mathbb{C}/\Lambda} n_w\, w \mod \Lambda \end{aligned}$$

La sucesión exacta siguiente abarca los resultados hasta ahora obtenidos incluyendo uno que se probará la sección siguiente.

Teorema 3.1.2
la sucesión

$$1 \longrightarrow \mathbb{C}^* \xrightarrow{\iota} \mathbb{C}(\Lambda)^* \xrightarrow{\text{div}} \text{Div}^{\,0}(\mathbb{C}/\Lambda) \xrightarrow{\text{sum}} \mathbb{C}/\Lambda \longrightarrow 0$$

es exacta.

Demostración. Es claro que la sucesión es exacta en $\mathbb{C}^*$. Veamos ahora que es exacta en $\mathbb{C}(\Lambda)^*$. Si $c \in \mathbb{C}^*$, se observa que $c \in \mathbb{C}(\Lambda)^*$ y $\text{ord}_w(c) = 0$ para todos $w \in \mathbb{C}/\Lambda$, por lo que $\text{div}\ (c) = 0$. ($\text{Im}\,\iota \subseteq \ker \text{div}$)

Por otro lado, sea $f \in \ker \text{div}$, esto es, $\text{div}\ (f) = 0$ lo cual significa que $\text{ord}_w(f) = 0$ para todos $w \in \mathbb{C}/\Lambda$. De un resultado anterior tenemos entonces que f es constante. ($\text{Im}\,\iota \supseteq \ker \text{div}$)

Para verificar que la sucesión es exacta en $\mathbb{C}/\Lambda$ basta ver que para cualquier $w \in \mathbb{C}/\Lambda$ el divisor $(w) - (0) \in \text{Div}^{\,0}(\mathbb{C}/\Lambda)$ es tal que

$$\text{sum}\,((w) - (0)) = 1 \cdot w - 1 \cdot 0 = w.$$

Sea $f \in \mathbb{C}(\Lambda)^*$, entonces se tiene que $\text{div}\ (f) = \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(w)$. Aplicando el morfismo sum tenemos lo siguiente

$$\text{sum}\,(\text{div}\ (f)) = \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w w \equiv 0 \mod \Lambda,$$

de lo cual concluimos que $\text{Im}\,\text{div}\ (\subseteq) \ker \text{sum}$. La otra contención se probará mas adelante. ■

3.2. La función $\wp$ de Weierstrass

Veamos ahora que existen funciones elípticas no triviales, de tal suerte que lo que hasta ahora hemos dicho no ha sido en vano.

Definición 3.2.1

a) Sea Λ una retícula. La función $\wp$ de Weierstrass relativa a Λ *esta definida por la serie*

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

b) La Serie de Eisenstein de peso $2k$ para Λ *es la serie:*

$$G_{2k} = \sum_{\substack{w \in \Lambda \\ w \neq 0}} w^{-2k}.$$

Los resultados preliminares siguientes aseguran que lo que hemos definido no se comporta *mal*:

Lema 6
Sea Λ una retícula. La serie de Eisenstein G_{2k} para Λ converge absolutamente para $k > 1$.

Demostración.
De manera general veamos que si $s > 2$, entonces la serie

$$\sum_{\substack{w\in\Lambda \\ w\neq 0}} |w|^{-s}.$$

converge.

Sea $\widetilde{D}$ la unión de los cuatro paralelogramos fundamentales trasladados de tal manera que rodean el origen:

$$\tilde{D} = D \cup (-w_1 + D) \cup (-w_2 + D) \cup (-w_1 - w_2 + D).$$

La frontera de $\widetilde{D}$ es compacto y no contiene al origen, por lo que elegimos $c > 0$ tal que $|z| \geq c$ para todo $z \in \partial\widetilde{D}$. Si $|m| \geq |n| > 0$ entonces se tiene que

$$|mw_1 + nw_2| = |m| \left| w_1 + \frac{n}{m} w_2 \right| \geq c|m|,$$

pues $w_1 + \dfrac{n}{m} w_2 \in \partial\widetilde{D}$. Fijémonos ahora en la serie que nos interesa. Si escribimos $w = mw_1 + nw_2$, los términos con $n = 0$ contribuyen con

$$\sum_{\substack{w\in\Lambda \\ w\neq 0, n=0}} |w|^{-s} = \sum_{m\neq 0} \frac{1}{|mw_1|^s} = \frac{1}{|w_1|^s} \sum_{m\neq 0} \frac{1}{|m|^s} = 2|w_1|^{-s} \sum_{m=1}^{\infty} \frac{1}{m^s} < \infty$$

y de la misma manera los términos con $m = 0$ contribuyen con

$$2|w_2|^{-s} \sum_{n=1}^{\infty} \frac{1}{n^s} < \infty.$$

Según las estimaciones hechas anteriormente, los términos con $|m| \geq |n| > 0$ contribuyen en

$$\sum_{|m|\geq|n|>0} \frac{1}{|mw_1 + nw_2|^s} \leq \frac{1}{c^s} \sum_{|m|\neq 0} \frac{1}{|m|^s} = \frac{2}{c^s} \sum_{m=1}^{\infty} \frac{1}{m^s} < \infty.$$

y los términos con $|n| > |m|$ hacen una contribución similar, por lo tanto se tiene el resultado. ■

Lema 7
Si $s > 2$ y $R > 0$ la serie

$$\sum_{|w|>R} \frac{1}{(z-w)^s}$$

converge absoluta y uniformemente en el disco $|z| \leq R$.

Demostración.
Consideremos todos los $w \in \Lambda$ con $|w| > R$ y elijamos el que tiene modulo mínimo, digamos $|w_0| = R + d$, donde $d > 0$. Entonces si $|z| \leq R$ y $|w| \geq R + d$ tenemos

$$\left|\frac{z-w}{w}\right| = \left|1 - \frac{z}{w}\right| \geq 1 - \left|\frac{z}{w}\right| \geq 1 - \frac{R}{R+d},$$

y por lo tanto

$$\left|\frac{z-w}{w}\right|^s \geq \left(1 - \frac{R}{R+d}\right)^s.$$

Definiendo entonces

$$M = \left(1 - \frac{R}{R+d}\right)^{-s}$$

se tiene que

$$\frac{1}{|z-w|^s} \leq \frac{M}{|w|^s} \tag{3.1}$$

para todo w con $|w| > R$ y para todo z con $|z| \leq R$, y por el lema anterior se tiene el resultado. ■

Teorema 3.2.1

a) La función $\wp$ de Weierstrass converge absolutamente y uniformemente en cualquier compacto de $\mathbb{C} \setminus \Lambda$. Define además una función meromorfa en $\mathbb{C}$ con un polo de orden 2 en cada punto de Λ y solamente ahí.

b) La función $\wp$ de Weierstrass es una función elíptica par.

Demostración.
a) Cada término en la serie tiene norma:

$$\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| = \left|\frac{w^2 - (z-w)^2}{w^2(z-w)^2}\right| = \left|\frac{z(2w-z)}{w^2(z-w)^2}\right|.$$

Ahora consideremos un disco compacto $\mid z \mid \leq R$. Existen sólo un número finito de periodos w en ese disco. Si excluimos de la serie que define a $\wp$ los sumandos de esos periodos, por la desigualdad 1 del lema 7,

$$\left|\frac{1}{(z-w)^2}\right| \leq \frac{M}{|w|^2},$$

donde M es una constante que depende solo de R. Tenemos entonces la estimación

$$\left|\frac{z(2w-z)}{w^2(z-w)^2}\right| \leq \frac{MR(2|w|+R)}{|w|^4} \leq \frac{MR(2+R/|w|)}{|w|^3} \leq \frac{3MR}{|w|^3}$$

dado que $R < |w|$ para w fuera del disco $|z \mid |R$. Esto muestra que la serie truncada converge uniformemente y absolutamente ene el disco $|z| \leq R$ y por tanto es analítica en ese disco y los términos restantes dan un polo de orden 2 en cada w dentro del disco. De lo anterior $\wp$ es meromorfa con un polo de orden 2 en cada periodo.

b) Es fácil ver que

$$\begin{aligned}\wp(-z) &= \frac{1}{z^2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \left(\frac{1}{(-z-w)^2} - \frac{1}{w^2}\right) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \left(\frac{1}{(-z+w)^2} - \frac{1}{w^2}\right)\\ &= \wp(z),\end{aligned}$$

esto es, la función $\wp$ es par.

Si calculamos la derivada de $\wp(z)$, tenemos que

$$\wp'(z) = \frac{-2}{z^3} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \frac{-2}{(z-w)^3} = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3},$$

la cual cumple que

$$\wp'(z+l) = -2\sum_{w\in\Lambda} \frac{1}{(z+l-w)^3} = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3} = \wp'(z) \quad \forall\, l \in \Lambda,$$

lo cual significa que $\wp'(z)$ es una función elíptica. Tomemos entonces $w \in \Lambda$ y derivando la expresión $\wp(z+w) - \wp(z)$ se tiene que $\wp'(z+w) - \wp'(z) = 0$. Se sigue que $\wp(z+w) - \wp(z) = cte$. Evaluando ésta expresión en $z = -\frac{1}{2}w_1$ y tomando $w = w_1$ se tiene que

$$\text{cte} = \wp\left(\tfrac{1}{2}w_1\right) - \wp\left(-\tfrac{1}{2}w_1\right) = \wp\left(\tfrac{1}{2}w_1\right) - \wp\left(\tfrac{1}{2}w_1\right) = 0$$

y por tanto $\wp(z)$ también es una función elíptica. ■

El teorema siguiente es de particular importancia, la cual se verá mas adelante.

Teorema 3.2.2

a) Toda función elíptica par (relativa a los periodos w_1 y w_2) es una función racional de $\wp(z)$.

a) Cualquier función elíptica es de la forma $f(z) = g(\wp(z)) + \wp'(z)\, h(\wp(z))$, con g y h funciones racionales.

Demostración.
Observemos que el inciso b) se sigue directamente del inciso a) dado que, escribiendo a $f = f_p + f_i$ con

$$f_p(z) = \frac{1}{2}\left(f(z) + f(-z)\right) \qquad f_i(z) = \frac{1}{2}\left(f(z) - f(-z)\right),$$

(partes par e impar respectivamente) y dado que $f_i = \wp' \dfrac{f_1}{\wp'}$ donde $\dfrac{f_1}{\wp'}$ también es par, por lo que se verifica la observación y es suficiente demostrar solamente el inciso a).

El teorema siguiente establece la relación entre las curvas elípticas y las funciones elípticas.

Teorema 3.2.3
la función $w = \wp(z)$ cumple la ecuación diferencial

$$\left(\frac{dw}{dz}\right)^2 = 4w^3 - g_2 w - g_3,$$

donde g_2 y g_3 son constantes dadas por

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \qquad g_3 = g_3(\Lambda) = 140G_6(\Lambda).$$

Demostración.
Por un teorema anterior las series $G_4(\Lambda)$ y $G_6(\Lambda)$ convergen absolutamente, por lo que g_2 y g_3 están bien definidos. Para la prueba del teorema se hará uso del lema siguiente.

Lema 8
Suponga que

$$f_n(z) = \sum_{k=0}^{\infty} a_k^{(n)(z-z_0)^k}$$

es analítica para $|z - z_0| < r$ y suponga que la serie

$$F(z) = \sum_{n=0}^{\infty} f_n(z)$$

converge uniformemente para $|z - z_0| \leq \rho$ donde $\rho < r$. Entonces los coeficientes en cada columna *forman una serie convergente, y mas aun, si*

$$A_k = \sum_{n=0}^{\infty} a_k^{(n)}$$

es la suma de los coeficientes de la columna k-ésima, entonces la serie

$$\sum_{k=1}^{\infty} A_k (z - z_0)^k$$

es la serie de Taylor para $f(z)$ en $z = z_0$ y converge para $|z| < r$.

Aplicaremos el lema a la función

$$\wp(z) - \frac{1}{z^2} = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

En un disco alrededor del cero tenemos

$$\begin{aligned} \frac{1}{(z-w)^2} &= \frac{1}{w^2 \left(1 - \frac{z}{w}\right)^2} = \frac{1}{w^2} \left(1 + 2\frac{z}{w} + 3\frac{z^2}{w^2} + \cdots \right) \\ &= \frac{1}{w^2} + \frac{1}{w^2} \sum_{k=1}^{\infty} (k+1) \left(\frac{z}{w}\right)^k, \end{aligned}$$

de donde vemos que

$$\wp(z) - \frac{1}{z^2} = \sum_{\substack{w\in\Lambda\\ w\neq 0}} \left(\frac{1}{w^2} \sum_{k=1}^{\infty} (k+1) \left(\frac{z}{w}\right)^k \right) = \sum_{\substack{w\in\Lambda\\ w\neq 0}} \left(\sum_{k=1}^{\infty} \frac{(k+1)}{w^{k+2}} z^k \right).$$

Como la serie $\displaystyle\sum_{\substack{w\in\Lambda\\ w\neq 0}} \left(\frac{1}{(w-z)^2} - \frac{1}{w^2} \right)$ es uniformemente convergente y la serie $\displaystyle\sum_{k=1}^{\infty} \frac{(k+1)}{w^{k+2}} z^k$ es analítica (todo dentro de un disco pequeño con centro en el origen) por el lema anterior se tiene que la serie $G_{k+2}(\lambda)$ converge (lo cual ya sabíamos) y además

$$\wp(z) - \frac{1}{z^2} = \sum_{k=1}^{\infty} (k+1) G_{k+2}(\lambda) z^k$$

donde $G_m = 0$ para m impar, por lo tanto,

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_6 z^6 + \cdots$$

De esto último podemos hacer los cálculos siguientes directamente:

$$\begin{aligned}
\wp'(z) &= -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \cdots \\
(\wp'(z))^2 &= \frac{4}{z^6} - 24G_4 \frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8) z^2 + \cdots \\
(\wp(z))^2 &= \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + (14G_8 + 9G_4^2) z^4 + \cdots \\
(\wp(z))^3 &= \frac{1}{z^6} + 9G_4 \frac{1}{z^4} + 15G_6 z^2 + (21G_8 + 27G_4^2) z^2 + \cdots
\end{aligned}$$

de lo cual vemos que se cumple la relación

$$(\wp'(z))^2 - 4(\wp(z))^3 + 60G_4 \wp(z) + 140G_6 = O(z^2).$$

Lo anterior nos dice que el lado derecho de la igualdad es una función elíptica sin polos, y por tanto, por un resultado anterior, es cero. ■

Teorema 3.2.4
La funcion $\mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C})$ *dado por*

$$z \mod \Lambda \overset{\varphi}{\longmapsto} \begin{cases} (\wp(z), \wp'(z), 1) & \text{para } z \notin \Lambda \\ (0,1,0) & \text{para } z \in \Lambda \end{cases}$$

es holomorfo y establece una correspondencia biyectiva a una curva proyectiva plana $E(\mathbb{C})$ *la cual en su forma afín está dada por la ecuación*

$$y^2 = 4x^3 - g_2 x - g_3.$$

Demostración.
Del resultado anterior vemos que la imagen de la función esta contenida en $E(\mathbb{C})$. Sea ahora $(x, y) \in E(\mathbb{C})$. Tenemos entonces que $\wp(z) - x$ es una función elíptica no constante, por lo tanto tiene un cero, digamos en $z = a$. Se sigue entonces que $(\wp'(a))^2 = y^2$ y por lo tanto $\wp'(a) = y$ (posiblemente después de reemplazar a por $-a$), por lo tanto $a \mapsto (x, y)$.

Supongamos ahora que $\varphi(z_1) = \varphi(z_2)$ y supongamos también que $2z_1 \notin \Lambda$, entonces la función $\wp(z) - \wp(z_1)$ tiene orden 2 y ceros en $z_1, -z_1, z_2$, por lo tanto $z_2 \equiv \pm z_1 \mod \Lambda$. Por otro lado tenemos que

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$$

de donde deducimos que $z_1 \equiv z_2 \mod \Lambda$ (cabe notar que $\wp(z_1) \neq 0$). Lo anterior nos dice que φ es inyectiva.

Para probar que es un isomorfismo analítico calculemos el efecto en el espacio cotangente. En cada punto de $E(\mathbb{C})$, $\frac{dx}{y}$ es una 1-forma diferencial no nula y holomorfa. Dado que

$$\varphi^* : \Omega(E(\mathbb{C})) \longrightarrow \Omega(\mathbb{C}/\Lambda)$$

donde

$$\varphi^*\left(\frac{dx}{y}\right) = \frac{d\wp(z)}{\wp'(z)} = \frac{\wp'(z)}{\wp'(z)}\,dz = dz$$

es igualmente una 1-forma no nula holomorfa en cada punto de $\mathbb{C}/\Lambda$, vemos que φ es un isomorfismo local y como a su vez es inyectiva, es un isomorfismo global.

Finalmente, para ver que es un isomorfismo de grupos, sean $z_1, z_2 \in \mathbb{C}$. Entonces existe una función elíptica $f \in \mathbb{C}(\Lambda)$ cuyo divisor es

$$\text{div } (f) = (z_1 + z_2) - (z_1) - (z_2) + (0).$$

Sabemos que $f(z) = F(\wp(z), \wp'(z))$ para alguna función racional $F(u, v) \in \mathbb{C}(u, v)$. Considerando a $F(x, y) \in \mathbb{C}(x, y) = \mathbb{C}(E)$, tenemos que

$$\text{div } (F) = (\varphi(z_1 + z_2)) - (\varphi(z_2)) - (\varphi(z_2)) - (\varphi(0))$$

el cual es un divisor principal, por lo tanto se tiene

$$\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2). \quad \blacksquare$$

Veamos ahora cual es el efecto de considerar aplicaciones analíticas en el toro $\mathbb{C}/\Lambda$. Veremos que en realidad tienen una forma muy simple y que inducen a las correspondientes isogenias de curvas elípticas sobre $\mathbb{C}$.

Sean Λ_1, Λ_2 retículas en $\mathbb{C}$. Si $\alpha \in \mathbb{C}$ tiene la propiedad que $\alpha\Lambda_1 \subset \Lambda_2$, entonces tenemos la función *multiplicación por escalar* α dado por

$$\begin{aligned} \phi_\alpha : \mathbb{C}/\Lambda_1 &\longrightarrow \mathbb{C}/\Lambda_2 \\ z &\longmapsto \alpha z \mod \Lambda_2 \end{aligned}$$

el cual además es un homomorfismo holomorfo. El resultado siguiente nos dice que en esencia son las únicas aplicaciones de este estilo.

Teorema 3.2.5

a) La asociación

$$\begin{array}{rcl}\{\alpha \in \mathbb{C} | \alpha\Lambda_1 \subset \Lambda_2\} & \longrightarrow & \left\{ \begin{smallmatrix}\text{aplicaciones}\\ \text{holomorfas}\end{smallmatrix} \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 | \phi(0) = 0 \right\} \\ \alpha & \longmapsto & \phi_\alpha \end{array}$$

es una biyección

b) Sean E_1, E_2 curvas elípticas sobre $\mathbb{C}$ correspondientes a las retículas Λ_1, Λ_2. Entonces la inclusión natural

$$\{\text{isogenias } \phi : E_1 \to E_2\} \hookrightarrow \left\{ \begin{smallmatrix}\text{aplicaciones}\\ \text{holomorfas}\end{smallmatrix} \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 | \phi(0) = 0 \right\}$$

es una biyección.

Demostración.
a) Sean $\alpha, \beta \in \mathbb{C}$ tales que $\phi_\alpha = \phi_\beta$, lo cual significa que $z\alpha = z\beta \mod \Lambda_2$. Esto nos dice que $z \mapsto (\alpha - \beta)z$ manda $\mathbb{C}$ en Λ_2 y por lo tanto es constante, pues Λ_2 es un conjunto discreto. Si sustituimos $z = 0$ vemos que la constante es precisamente cero, y si ponemos $z = 1$ vemos que $\alpha = \beta$, probando que la asignación definida es inyectiva.

Sea ahora $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ holomorfo con $\phi(0) = 0$. Como $\mathbb{C}$ es simplemente conexo, existe $f : \mathbb{C} \to \mathbb{C}$ con $f(0) = 0$ tal que el diagrama

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow[\phi]{} & \mathbb{C}/\Lambda_2 \end{array} \qquad \begin{pmatrix} \phi \text{ se levanta a } f \\ p_2 \circ f = \phi \circ p_1 \end{pmatrix}$$

es conmutativo. Para cualquier $w \in \Lambda_1$ tenemos que $z + w \equiv z \mod \Lambda_1$ y por lo tanto $f(z + w) \equiv f(z) \mod \Lambda_2$ para todo $z \in \mathbb{C}$. Entonces $z \mapsto f(z + w) - f(z)$ manda a $\mathbb{C}$ en Λ_2 y nuevamente es constante. De lo anterior deducimos que

$$f'(z + w) = f'(z) \qquad \forall\, w \in \Lambda_1 \,\text{y}\, \forall\, z \in \mathbb{C}.$$

Esto nos dice que f' es una función elíptica holomorfa, y por lo tanto constante; juntando toda la información tenemos que

$$f(z) = \alpha z + \gamma, \qquad \alpha, \gamma \in \mathbb{C}.$$

Como $f(0) = 0$ tenemos que $\gamma = 0$ y entonces $f(z) = \alpha z$. Dado que el diagrama es conmutativo entonces $\forall\, w \in \Lambda_1$ tenemos que

$$(p_2 \circ f)(w) = (\phi \circ p_1)(w) = \phi(0) = 0 \mod \Lambda_2$$

por lo que $f(w) \in \Lambda_2$ y por lo tanto $\alpha\Lambda_1 \subset \Lambda_2$, de donde deducimos que $\phi = \phi_\alpha$. La aplicación es entonces suprayectiva.

b) La asignación es claramente inyectiva. Sea ahora $\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ una aplicación holomorfa con $\phi(0) = 0$. Por el inciso anterior es suficiente suponer que $\phi = \phi_\alpha$. Este mapeo $E_1 \to E_2$ a nivel de las ecuaciones de Weierstrass está dado por

$$[\wp(z, \Lambda_1), \wp'(z, \Lambda_1), 1] \longmapsto [\wp(\alpha z, \Lambda_2), \wp'(\alpha z, \Lambda_2), 1]$$

por lo tanto basta mostrar que $\wp(\alpha z, \Lambda_2)\,\&\,\wp'(\alpha z, \Lambda_2)$ se pueden expresar como funciones racionales de $\wp(z, \Lambda_1)\,\&\,\wp'(z, \Lambda_1)$. Usando el hecho de que $\alpha\Lambda_1 \subset \Lambda_2$ tenemos que para todo $w \in \Lambda_1$

$$\wp(\alpha(z + w), \Lambda_2) = \wp(\alpha z + \alpha w, \lambda_2) = \wp(\alpha z, \Lambda_2),$$

y de manera similar para $\wp'(\alpha z, \Lambda_2)$, por lo tanto $\wp(\alpha z, \Lambda_2), \wp'(\alpha z, \Lambda_2)$ son funciones elípticas, esto es, pertenecen a $\mathbb{C}(\Lambda_1)$ lo cual termina la prueba. ■

Hasta aquí hemos expuesto los resultados básicos de las curvas elípticas sobre $\mathbb{C}$.

Capítulo 4

Cohomología de Grupos

Sea G un grupo arbitrario (considerado multiplicativamente) y M un grupo abeliano (aditivo). Decimos que M es un *G-Módulo* si M es un $\mathbb{Z}G$-módulo izquierdo (aquí $\mathbb{Z}G$ es el anillo de grupo[1] generado por G). Notemos que la definición anterior es equivalente a decir que existe un homomorfismo de grupos $\varphi : G \to \mathrm{Aut}\,(M)$ (una *acción* de G en M). De la misma forma es equivalente decir que existe un homomorfismo de grupos $G \times M \xrightarrow{\Phi} M$ (denotada por $\Phi(\sigma, m) := \sigma m$) que cumple las propiedades siguientes

1. $\sigma(m + m') = \sigma m + \sigma m'$ para todos $\sigma \in G$, $m, m' \in M$.
2. $(\sigma\tau)m = \sigma(\tau m)$ para todos $\sigma, \tau \in G$, $m \in M$.
3. $1m = m$ para todo $m \in M$.

Ejemplo 4.0.1
Sea L una extensión de Galois finita de un campo K y sea $G = \mathrm{Gal}\,(L/K)$ y E una curva elíptica sobre L. Entonces de manera natural $L, L^\times$ y $E(L)$ son G-módulos.

Si M y N son G-módulos, un G-morfismo $\phi : M \to N$ es un $\mathbb{Z}G$-homomorfismo, y para lo cual usaremos la notación

$$\hom_G(M, N) := \hom_{\mathbb{Z}G}(M, N)$$

Dado M un G-módulo consideremos el submódulo de M formado por aquellos elementos que quedan *fijos* bajo la acción:

$$M^G := \{m \in M | \sigma m = m \quad \forall\, \sigma \in G\}.$$

Lema 9
Sea G un grupo y consideremos la asignación:

$$(\quad)^G : G\text{-}\mathbf{Mod} \longrightarrow \mathbf{Ab}.$$

1. $(\quad)^G$ es un funtor covariante exacto izquierdo.

[1] $\mathbb{Z}G$ consiste de de elementos de la forma $\sum_{\sigma \in G} n_\sigma \sigma$ con $n_\sigma \in \mathbb{Z}$ todos cero salvo un número finito.

2. Existe un isomorfismo natural

$$(\quad)^G \longrightarrow \mathbf{Hom}_G(\mathbb{Z}, \quad).$$

Demostración.
1) Si $\theta : M \to N$ es un G-morfismo veamos que la restricción de θ a M^G tiene su imagen en N^G. Sea $x \in M^G$, entonces

$$\sigma\theta(x) = \theta(\sigma x) = \theta(x),$$

y por tanto $\theta(x) \in N^G$ y es fácil ver entonces que $(\quad)^G$ es un funtor covariante. Veamos ahora que es exacto izquierdo. Sea

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

una sucesión exacta de G-módulos. Tenemos que mostrar que la sucesión

$$0 \longrightarrow M'^G \xrightarrow{\tilde{\phi}} M^G \xrightarrow{\tilde{\psi}} M''^G$$

también es exacta.

El morfismo $\tilde{\phi}$ es inyectivo ya que es la restricción del morfismo ϕ el cual es inyectivo. Sea ahora $x \in \operatorname{Im}\tilde{\phi}$, entonces

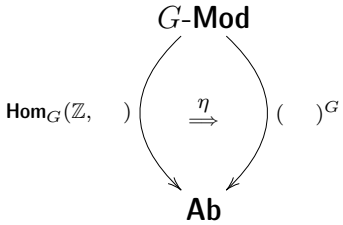
$$\tilde{\psi}(\tilde{\phi}) = \psi(\phi(x)) = 0,$$

esto último pasa pues las funciones $\tilde{\psi}, \tilde{\phi}$ son restricciones de ψ y ϕ respectivamente. Esto demuestra que $\operatorname{Im}\tilde{\phi} \subseteq \ker\tilde{\psi}$.
Por último, sea ahora $x \in \ker\tilde{\psi} \subseteq \ker\psi$ y por la exactitud de la primera sucesión existe $y \in M'$ tal que $\phi(y) = x$. Tal elemento y pertenece a M'^G pues

$$\phi(\sigma y) = \sigma\phi(y) = \sigma x = x = \phi(y)$$

Para todo $\sigma \in G$ y como ϕ es inyectiva, se cumple que $\sigma y = y$ para todo $\sigma \in G$.

2) Tenemos que construir una transformación natural η tal que



Sea M un G-módulo, entonces definimos $\eta_M : \hom_G(\mathbb{Z}, M) \longrightarrow M^G$ como $\eta_M(\phi) = \phi(1)$. Es directo ver que esto define un isomorfismo natural. ■

Definición 4.0.2
Sea M un G-módulo y $q \geq 0$ un entero. Definimos el q-ésimo grupo de cohomología de G con coeficientes en M *como*

$$\mathbf{H}^q(G, M) := \mathbf{Ext}^q_{\mathbb{Z}G}(\mathbb{Z}, M)$$

Observe que la definición es tan sólo tomar los funtores derivados derechos del funtor $\mathbf{Hom}_G(\mathbb{Z}, \quad)$. Los grupos de cohomología se calculan por medio de una resolución proyectiva de $\mathbb{Z}$ como G-módulo

$$\mathcal{P}: \quad \cdots P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

Después quitamos el G-módulo $\mathbb{Z}$ del complejo $\mathcal{P}$ y aplicamos el funtor $\mathbf{Hom}_G(\quad, M)$, el cual es contravariante, para formar el complejo

$$\mathbf{Hom}_G(P_0, M) \xrightarrow{d_1^*} \mathbf{Hom}_G(P_1, M) \xrightarrow{d_2^*} \mathbf{Hom}_G(P_2, M) \xrightarrow{d_3^*} \cdots$$

cuya cohomología es

$$\mathbf{H}^q(G, M) := \mathbf{Ext}^q_{\mathbb{Z}G}(G, M) = \ker d^*_{q+1} \big/ \operatorname{Im} d^*_q$$

Observación: Las propiedades usuales de funtores derivados se traducen en este contexto como sigue:

1. $\mathbf{H}^0(G, M) = \mathbf{hom}_G(\mathbb{Z}, M) \simeq M^G$.
2. $\mathbf{H}^q(G, M) = 0 \quad \forall\, q \geq 1$ si M es un G-módulo inyectivo.
3. Dada cualquier sucesión exacta corta de G-módulos

   $$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

   se tiene asociada una sucesión exacta larga en cohomología

   $$0 \longrightarrow M'^G \xrightarrow{\tilde{\phi}} M^G \xrightarrow{\tilde{\psi}} M''^G \xrightarrow{\delta} \mathbf{H}^1(G, M') \xrightarrow{\phi^*} \mathbf{H}^1(G, M) \xrightarrow{\psi^*} \mathbf{H}^1(G, M'') \longrightarrow \cdots$$

   donde los morfismos de conexión δ dependen de la sucesión exacta de G-módulos dada.

Ejemplo 4.0.2
En el ejemplo anterior tenemos $\mathbf{H}^0(G, L) = K$, $\mathbf{H}^0(G, L^\times) = K^\times$ y por último $\mathbf{H}^0(G, E(L)) = E(K)$.

4.0.1. Resoluciones Estándar

Tomemos la resolución proyectiva (de hecho libre) de $\mathbb{Z}$ dada de la siguiente manera: Sea P_n el $\mathbb{Z}$-módulo libre con base el conjunto de $(n+1)$-adas de la forma $(\sigma_0, \sigma_1, \ldots, \sigma_n)$ de elementos de G y donde G actúa por traslaciones, es decir, si $\sigma \in G$, definimos

$$\sigma \cdot (\sigma_0, \sigma_1, \ldots, \sigma_n) := (\sigma\sigma_0, \ldots, \sigma\sigma_n)$$

y así los P_n son G-módulos libre con una base dada por las $(n+1)$-adas de la forma $(e, \sigma_1, \ldots, \sigma_n) \in G^{n+1}$. Los morfismos $d_n : P_n \longrightarrow P_{n-1}$ se definen en los generadores:

$$d_n(\sigma_0, \ldots, \sigma_n) := \sum_{j=0}^{n} (-1)^j (\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_n)$$

y finalmente el morfismo $\epsilon : P_0 \longrightarrow \mathbb{Z}$ se define enviando cada generador al 1 ($\epsilon(\sigma_0) = 1$). Observemos que $P_0 = \mathbb{Z}G$ y el morfismo $\epsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$ es el llamado *morfismo de aumentación* y es suprayectivo de manera directa.

Proposición 4.1
La sucesión de G-módulos libres

$$\mathcal{P} : \cdots \xrightarrow{d_{i+1}} P_i \xrightarrow{d_i} P_{i-1} \xrightarrow{d_{i-1}} \cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

es exacta.

Demostración. directa. ■

El paso siguiente es identificar los $\mathbf{Hom}_G(P_i, M)$. Un elemento $\phi \in \mathbf{Hom}_G(P_i, M)$ está determinado por los valores que toma en los generadores $(\sigma_0, \ldots, \sigma_i) \in P_i$ y como debe ser un G-morfismo, se cumple también

$$\phi(\sigma \cdot (\sigma_0, \ldots, \sigma_i)) = \sigma \cdot (\phi(\sigma_0, \ldots, \sigma_i)).$$

los morfismos $d_i : P_i \longrightarrow P_{i-1}$ inducen homomorfismos

$$d_i^* : \mathbf{Hom}_G(P_{i-1}, M) \longrightarrow \mathbf{Hom}_G(P_i, M)$$

dados por

$$d_i^*(\phi)(\sigma_0, \ldots, \sigma_i) = \phi(d_i(\sigma_0, \ldots, \sigma_i)) = \sum_{j=0}^{i} (-1)^j \phi(\sigma_0, \ldots, \widehat{\sigma_j}, \ldots, \sigma_i)$$

Notemos que de la propiedad de G-morfismo de ϕ podemos notar que

$$\phi(\sigma_0, \ldots, \sigma_i) = \phi(\sigma_0(1, \sigma_0^{-1}\sigma_1, \ldots, \sigma_0^{-1}\sigma_i)) = \sigma_0 \cdot \phi(1, \sigma_0^{-1}\sigma_1, \ldots, \sigma_0^{-1}\sigma_i),$$

lo cual significa que ϕ en realidad está determinado por sus valores en generadores de P_i de la forma $(1, \sigma_1, \ldots, \sigma_i)$, por lo tanto consideramos otra resolución $\mathbb{Z}G$-libre de $\mathbb{Z}$ de la manera siguiente:

Si $n > 0$ tomemos Q_n el $\mathbb{Z}G$-módulo libre con base el conjunto

$$\{[\sigma_1, \ldots, \sigma_n] \in G^n\};$$

si $n = 0$, sea Q_0 el G-módulo libre generado por el símbolo $[\,]$.

Lema 10
Para todo entero $n \geq 0$ se cumple que $P_n \cong Q_n$ como $\mathbb{Z}G$-módulos.

Demostración.
Si definimos los morfismos

$$\begin{aligned} \phi_n : Q_n &\longrightarrow P_n \\ [\sigma_1, \ldots, \sigma_n] &\longmapsto (1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \cdots \sigma_n) \\ \psi_n : P_n &\longrightarrow Q_n \\ (\sigma_0, \ldots, \sigma_n) &\longmapsto \sigma_0[\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n] \end{aligned}$$

se demuestra que ϕ_n es un isomorfismo de G-módulos, con inversa ψ_n, para todo $n \geq 0$. ■

Corolario 4.0.1
Existen morfismos únicos $\delta_n : Q_n \longrightarrow Q_{n-1}$ tales que los diagramas

$$\begin{array}{ccc} P_n & \xrightarrow{d_n} & P_{n-1} \\ \downarrow{\scriptstyle \psi_n} & & \downarrow{\scriptstyle \psi_{n-1}} \\ Q_n & \xrightarrow[\delta_n]{} & Q_{n-1} \end{array}$$

conmutan.

Demostración.
Escribiendo $\delta_n := \psi_{n-1} \circ d_n \circ \phi_n$ se tiene la conclusión. Explícitamente

$$\delta_n[\sigma_1, \ldots, \sigma_n] = \sigma_1[\sigma_2, \ldots, \sigma_n] + \sum_{i=0}^{n-1} (-1)^i [\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] + (-1)^n [\sigma_1, \ldots, \sigma_{n-1}] \quad \blacksquare$$

Proposición 4.2
La sucesión de G-módulos libres

$$\mathcal{Q} : \cdots \xrightarrow{\delta_{i+1}} Q_i \xrightarrow{\delta_i} Q_{i-1} \xrightarrow{\delta_{i-1}} \cdots \xrightarrow{\delta_2} Q_1 \xrightarrow{\delta_1} Q_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

es exacta.

Demostración.
Se tiene directamente del complejo $\mathcal{P}$. $\blacksquare$

Observación Importante:
Para el complejo $\mathcal{Q}$ anterior los morfismos $\phi \in \mathbf{Hom}_G(Q_n, M)$ son funciones G-covariantes $\phi : Q_n \to M$ determinadas por sus valores en los generadores $[\sigma_1, \ldots, \sigma_n] \in Q_n$ y por tanto podemos ver dichos morfismos como funciones G-covariantes

$$\phi : G \times \cdots \times G \longrightarrow M.$$

Entonces los morfismos δ_n^* quedan totalmente determinados

$$\begin{aligned} \delta_n^*([\sigma_1, \ldots, \sigma_n]) &= \phi(\delta_n([\sigma_1, \ldots, \sigma_n])) \\ &= \sigma_1\phi([\sigma_2, \ldots, \sigma_n]) + \sum_{i=1}^{n-1} (-1)^i \phi([\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n]) \\ &\quad + (-1)^n \phi([\sigma_1, \ldots, \sigma_{n-1}]). \end{aligned}$$

4.0.2. El grupo $\mathbf{H}^1(G, M)$.

La parte del complejo $\mathbf{Hom}_G(\mathcal{Q}, M)$ que nos interesa es

$$\mathbf{Hom}_G(Q_0, M) \xrightarrow{\delta_1^*} \mathbf{Hom}_G(Q_1, M) \xrightarrow{\delta_2^*} \mathbf{Hom}_G(Q_2, M) \xrightarrow{\delta_2^*}$$

dado que

$$\mathbf{H}^1(G,M) = {}^{\ker \delta_2^*}\!/_{\operatorname{Im} \delta_1^*}.$$

Sea $\phi \in \ker \delta_2^*$. Se tiene entonces

$$\begin{aligned} 0 = \delta_2^*(\phi)([\sigma,\tau]) &= \phi(\delta_2([\sigma,\tau])) \\ &= \sigma\phi([\tau]) + (-1)^1\phi([\sigma\tau]) + (-1)^2\phi([\sigma]) \\ &= \sigma\phi(\tau) - \phi(\sigma\tau) + \phi(\sigma). \end{aligned}$$

Definición 4.0.3
Sea G un grupo, M un grupo abeliano. Por un homomorfismo cruzado (o 1-cociclo) de G en M *entenderemos una función $f : G \to M$ tal que*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

para todo $\sigma, \tau \in G$. Al conjunto de homomorfismos cruzados le denotamos por $Z^1(G,M)$.

Sea ahora $\phi \in \operatorname{Im} \delta_1^*$, esto es, existe un $\phi' \in \mathbf{Hom}_G(Q_0, M)$ tal que $\delta_1^*(\phi') = \phi$. Este ϕ' está determinado por su valor en el generador $[\,]$ de Q_0

$$\phi'([\,]) =: x \in M.$$

Por lo tanto

$$\begin{aligned} \phi([\sigma]) &= \delta_1^*(\phi')([\sigma]) \\ &= \phi'(\delta_1([\sigma])) \\ &= \sigma\phi'([\,]) + (-1)^1\phi([\,]) \\ &= \sigma x - x. \end{aligned}$$

Entonces tenemos que $\phi(\sigma) = \sigma x - x$ para algún $x \in M$.

Definición 4.0.4
Sea $\alpha \in M$ y definamos la función $f_\alpha : G \to M$ dada por

$$f_\alpha(\sigma) = \sigma\alpha - \alpha.$$

Es directo ver que f_α es un homomorfismo cruzado por lo que las funciones f_α forman un subgrupo de $Z^1(G,M)$ denotado por $B^1(G,M)$.

Se tiene entonces que el primer grupo de cohomología de G con coeficientes en M es

$$\mathbf{H}^1(G,M) = {}^{Z^1(G,M)}\!/_{B^1(G,M)}.$$

4.0.3. Cambio de Grupos

Sea $f : G' \to G$ un homomorfismo de grupos y M un G-módulo. Podemos hacer de M un G'-módulo de la manera siguiente. Extendamos f a un homomorfismo de anillos

$$\begin{array}{c} f : \mathbb{Z}G' \longrightarrow \mathbb{Z}G \\ \sum m_\sigma \cdot \sigma \longmapsto \sum m_\sigma \cdot f(\sigma) \end{array}$$

y entonces definimos la acción de G' en M como $\sigma' \cdot m := f(\sigma') \cdot m$ para todo $\sigma' \in G'$.

A nivel de submódulos fijos existe una contención de grupos abelianos dada por $M^G \subseteq M^{G'}$, ya que si $m \in M^G$, entonces para todo $\sigma' \in G'$ se cumple que

$$\sigma' m := f(\sigma') m = x$$

y así que $x \in M^{G'}$; la contención $\mathbf{H}^0(G, M) \subseteq \mathbf{H}^0(G', M)$ junto con la propiedad universal de los funtores derivados induce un morfismo de funtores de cohomología

$$\mathbf{H}^q(G, M) \xrightarrow{f^*} \mathbf{H}^q(G', M)$$

el cual es llamado morfismo inducido por el cambio de grupos $f : G' \to G$.

Ejemplo 4.0.3
Sea H un subgrupo de G. Entonces todo G-módulo es naturalmente un H-módulo y el mapeo inclusión $i : H \hookrightarrow G$ induce los morfismos

$$i^* : \mathbf{H}^q(G, M) \longrightarrow \mathbf{H}^q(H, M)$$

llamados *morfismos de restricción* y denotados por

$$i^* =: \mathbf{Res}^G_H.$$

Para el caso $q = 1$ tenemos que

$$\mathbf{H}^1(G, M) = \frac{\text{homomorfismos cruzados}}{\text{hom. cruzados principales}}$$

por lo tanto el morfismo $\mathbf{Res}^G_H$ está dado por

$$\begin{array}{c} \mathbf{Res}^G_H : \mathbf{H}^1(G, M) \longrightarrow \mathbf{H}^1(H, M) \\ \overline{\phi} \longmapsto \overline{\phi|_H} \end{array}$$

La construcción del morfismo inducido por el cambio de grupos se generaliza ahora considerando un homomorfismo de grupos $f : G' \to G$ y un homomorfismo de grupos abelianos $g : M \to M'$ tal que M es un G-módulo y M' es un G'-módulo; en esta situación decimos que f y g son *compatibles* si para toda $x \in M$ y todo $\sigma' \in G'$ se cumple que

$$g(f(\sigma') \cdot x) = \sigma' g(x),$$

esto es, si g es un G'-morfismo de f^*M (M como G'-módulo) a M'. Dicho morfismo induce morfismos en cohomología

$$\mathbf{H}^q(G, f^*M) \xrightarrow{g^*} \mathbf{H}^q(G', M')$$

y por otro lado se tiene el homomorfismo inducido por el cambio de grupos

$$\mathbf{H}^q(G, M) \xrightarrow{f^*} \mathbf{H}^q(G', M')$$

de donde, junto con el morfismo anterior, se obtiene la composición

$$\mathbf{H}^q(G, M) \longrightarrow \mathbf{H}^q(G', M')$$

los cuales denotaremos por $(f, g)^*$

Ejemplo 4.0.4
Supongamos que, en el ejemplo anterior, H es un subgrupo normal ($H \lhd G$) y $p : G \to G/H$ es la proyección natural. Se observa que M^H automáticamente adquiere estructura de G/H-módulo con la acción definida por

$$(\sigma H) \cdot m := \sigma \cdot m.$$

Resta verificar que la acción anterior está bien definida y que los morfismos $i : M^H \hookrightarrow M$ y p son compatibles. Para lo primero, observemos que para todo $m \in M^H$ y $h \in H$ se tiene lo siguiente

$$h[(\sigma H) \cdot m] = h(\sigma \cdot m) = (h\sigma) \cdot m = (\sigma h') \cdot m = \sigma(h' \cdot m) = \sigma \cdot m.$$

donde la igualdad $h\sigma = \sigma h'$ se obtiene por la normalidad de H. Veamos ahora que i y p son compatibles; sean $m \in M^H$ y $\sigma \in G$, se cumple entonces que

$$i(p(\sigma) \cdot m) = i[(\sigma H) \cdot m] = g(\sigma \cdot m) = \sigma \cdot m = \sigma \cdot (i(m)).$$

De esto obtenemos morfismos

$$\mathbf{H}^q({}^{G}\!/_{H}, M^H) \xrightarrow{(p,i)^*} \mathbf{H}^q(G, M)$$

los cuales llamaremos *morfismos de inflación* y se denotarán por $(p, i)^* = \mathbf{Inf}_G^{G/H}$. Para $q = 0$ se tiene que

$$\mathbf{H}^0({}^{G}\!/_{H}, M^H) = \left(M^H\right)^{G/H} = M^G$$

y por tanto se tiene que $\mathbf{Inf}_G^{G/H} = \mathrm{Id}_{M^G}$.

Para $q = 1$ se tiene que todo homomorfismo cruzado $\lambda : {}^{G}\!/_{H} \to M^H$ induce un homomorfismo cruzado $\tilde{\lambda}$ dado por el diagrama siguiente:

$$\begin{array}{ccc} G & \overset{\tilde{\lambda}}{\dashrightarrow} & M \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ {}^{G}\!/_{H} & \xrightarrow{\lambda} & M^H \end{array}$$

entonces el morfismo inflación está dado por

$$\begin{aligned} \mathbf{Inf}_G^{G/H} : \mathbf{H}^1({}^{G}\!/_{H}, M^H) &\longrightarrow \mathbf{H}^1(G, M) \\ \overline{\lambda} &\longmapsto \overline{i \circ \lambda \circ p} = \overline{\tilde{\lambda}}. \end{aligned}$$

De manera natural podemos componer los morfismos $\mathbf{Inf}_G^{G/H}$ y $\mathbf{Res}_H^G$ y para $q = 1$ se cumple la siguiente proposición (si no hay ambigüedad utilizaremos $\mathbf{Inf} = \mathbf{Inf}_G^{G/H}$ y de manera similar $\mathbf{Res} = \mathbf{Res}_H^G$).

Proposición 4.3
Dado G un grupo, $H \lhd G$ y M un G-módulo, entonces se tiene que la sucesión siguiente es exacta

$$0 \longrightarrow \mathbf{H}^1\left({}^{G}\!/_{H}, M^H\right) \xrightarrow{\mathbf{Inf}} \mathbf{H}^1(G, M) \xrightarrow{\mathbf{Res}} \mathbf{H}^1(H, M).$$

Demostración.
Veamos que la sucesión es exacta en $\mathbf{H}^1\left({}^{G}\!/_{H}, M^H\right)$, es decir, que el morfismo $\mathbf{Inf}$ es inyectivo.
Sea entonces $[\lambda] \in \mathbf{H}^1\left({}^{G}\!/_{H}, M^H\right)$ tal que $\mathbf{Inf}([\lambda]) = \bar{0} = [i \circ \lambda \circ p]$. Esto significa que $i \circ \lambda \circ p(\sigma) = \sigma m - m$ para algún $m \in M$. Observemos que $m \in M^H$, ya que si $h \in H$ se tiene que

$$(\sigma h) \cdot m - m = i \circ \lambda \circ p(\sigma h) = i \circ \lambda(\sigma h H) = i \circ \lambda(\sigma H) = i \circ \lambda \circ (\sigma) = \sigma \cdot m - m$$

de donde se observa que $(\sigma h) \cdot m = \sigma \cdot m$ y de esto $h \cdot m = m \quad \forall\, h \in H$. Se concluye entonces que λ es cohomólogo a 0 en $\mathbf{H}^1\left({}^{G}\!/_{H}, M^H\right)$ y por tanto $[\lambda] = \bar{0}$.

Veamos ahora la exactitud en $\mathbf{H}^1(G, M)$.
Tomemos $[\lambda] \in \mathbf{H}^1\left({}^{G}\!/_{H}, M^H\right)$. Por lo tanto se tiene que $\mathbf{Inf}([f]) = [i \circ \lambda \circ p] \in \operatorname{Im} \mathbf{Inf}$. Si ahora aplicamos el morfismo restricción, se obtiene

$$\mathbf{Res}(\mathbf{Inf}([\lambda])) = \mathbf{Res}([i \circ \lambda \circ p]) = [(i \circ \lambda \circ p)|_H] = \bar{0},$$

pues $(i \circ \lambda \circ p)|_H(\tau) = \lambda(\bar{\tau}) = 0$ para todo $\tau \in H$. De esto se concluye que $\operatorname{Im} \mathbf{Inf} \subseteq \ker \mathbf{Res}$.
Sea ahora $[\tilde{\lambda}] \in \mathbf{H}^1(G, M)$ tal que $\mathbf{Res}([\tilde{\lambda}]) = [\tilde{\lambda}|_H] = \bar{0}$, esto es,

$$\lambda(h) = h \cdot m - m$$

para todo $h \in H$ y para algún $m \in M$ fijo. Definamos $\bar{\lambda} : G \to M$ como

$$\bar{\lambda}(\sigma) = \tilde{\lambda}(\sigma) - (\sigma \cdot m - m).$$

Es claro que $\bar{\lambda}$ es un homomorfismo cruzado y más aún, se observa que $[\bar{\lambda}] = [\tilde{\lambda}]$.
Por otro lado, se tiene que $\bar{\lambda}(h) = 0$ para todo $h \in H$ y entonces definimos $\lambda : {}^{G}\!/_{H} \to M^H$ como $\lambda(\sigma H) := \bar{\lambda}(\sigma)$. Esto está bien definido pues si por ejemplo $\sigma H = \sigma_1 H$ esto implica que $\sigma = \sigma_1 h$ para algún $h \in H$ y como $\bar{\lambda}$ es un homomorfismo cruzado, entonces

$$\lambda(\sigma H) = \bar{\lambda}(\sigma) = \bar{\lambda}(\sigma_1 h) = \sigma_1 \cdot \bar{\lambda}(h) + \bar{\lambda}(\sigma_1) = \bar{\lambda}(\sigma_1) = \lambda(\sigma_1 H).$$

También vemos que $\operatorname{Im} \lambda \subseteq M^H$ ya que

$$h\lambda(\sigma H) = h\bar{\lambda}(\sigma) = \bar{\lambda}(h\sigma) - \bar{\lambda}(h) = \bar{\lambda}(h\sigma) = \lambda(h\sigma H) = \lambda(\sigma H).$$

Por último, λ es un homomorfismo cruzado de manera directa y de tal forma que satisface que $\bar{\lambda} = i \circ \lambda \circ p$, por lo que

$$[\tilde{\lambda}] = [\bar{\lambda}] = [i \circ \lambda \circ p] = \mathbf{Inf}([\lambda]),$$

de donde se obtiene finalmente que $[\tilde{\lambda}] \in \operatorname{Im} \mathbf{Inf}$ ■

4.0.4. Módulos Co-inducidos

Dados G un grupo, H un subgrupo de G y N un H-módulo, podemos obtener de manera natural un G-módulo con características cohomológicas bastante útiles.

Sea G un grupo, $H \subseteq G$ un subgrupo de G y N un H-módulo. Definimos

$$\mathbf{Ind}_G^H(N) := \{f : G \to N | f(h\sigma) = h \cdot f(\sigma) \quad \forall h \in H\}.$$

Notemos que $\mathbf{Ind}_G^H(N)$ es un grupo abeliano con la suma usual de funciones (usando la suma de N). Esto significa que si $f, g \in \mathbf{Ind}_G^H(N)$, entonces la suma está definida por

$$(f + g)(\sigma) = f(\sigma) + g(\sigma)$$

y como N tiene una estructura de grupo abeliano, entonces $\mathbf{Ind}_G^H(N)$ también es grupo abeliano. Más aún, $\mathbf{Ind}_G^H(N)$ adquiere una estructura de G-módulo izquierdo mediante la siguiente acción: Sean $f \in \mathbf{Ind}_G^H(N)$ y $\sigma \in G$, entonces $\sigma \cdot f : G \to N$ es la función dada por

$$(\sigma \cdot f)(\tau) := f(\tau\sigma) \quad \forall \tau \in G.$$

1. Es claro que $e \cdot f = f$ para todo $f \in \mathbf{Ind}_G^H(N)$ pues

$$(e \cdot f)(\sigma) = f(\sigma e) = f(\sigma).$$

2. Veamos que $\sigma \cdot (f_1 + f_2) = \sigma \cdot f_1 + \sigma \cdot f_2$; en efecto, pues para cada $\tau \in G$ se cumple que

$$[\sigma \cdot (f_1 + f_2)](\tau) = (f_1 + f_2)(\tau\sigma) = f_1(\tau\sigma) + f_2(\tau\sigma) = \sigma \cdot f_1(\tau) + \sigma \cdot f_2(\tau).$$

3. Se cumple que $(\sigma_1\sigma_2) \cdot f = \sigma_1 \cdot (\sigma_2 \cdot f)$. Dado $\tau \in G$ tenemos que

$$[(\sigma_1\sigma_2) \cdot f](\tau) = f(\tau\sigma_1\sigma_2) = (\sigma_2 \cdot f)(\tau\sigma_1) = [\sigma \cdot (\sigma_2 \cdot f)](\tau).$$

En el caso de $H = \{e\}$ usaremos la notación $\mathbf{Ind}_G(N) := \mathbf{Ind}_G^{\{e\}}(N)$, tomando en cuenta que un $\{e\}$-módulo es simplemente un grupo abeliano.

Definición 4.0.5
Un G-módulo Q se dice co-inducido *si $Q \simeq \mathbf{Ind}_G(N)$ para algún grupo abeliano N.*

Se tiene el siguiente lema auxiliar

Lema 11
Sean G un grupo, $H \subseteq G$ un subgrupo de G, N un H-módulo y M un G-módulo.

1. *Se tiene un isomorfismo natural*

$$\mathbf{Hom}_G(M, \mathbf{Ind}_G^H(N)) \cong \mathbf{Hom}_H(M, N)$$

donde M tiene una estructura natural de H-módulo por cambio de grupos.

2. En particular, cuando $M = \mathbb{Z}G$ se tiene que

$$\mathbf{Ind}_G^H(N) \cong \mathbf{Ind}_H(\mathbb{Z}G, N)$$

de tal forma que si $H = \{e\}$, tenemos

$$\mathbf{Ind}_G(N) \cong \mathbf{Hom}_{\mathbb{Z}}(\mathbb{Z}G, N).$$

Demostración.
(1) Definamos $\Phi : \mathbf{Hom}_G(M, \mathbf{Ind}_G^H(N)) \longrightarrow \mathbf{Hom}_H(M, N)$. Tomemos un G-morfismo $\eta : M \to \mathbf{Ind}_G^H(N)$, entonces sabemos que $\eta(m)(\sigma) \in N$ para todo $m \in M$ y para todo $\sigma \in G$. Definimos entonces

$$\begin{aligned} \Phi(\eta) : M &\longrightarrow N \\ m &\longmapsto \eta(m)(e) \end{aligned}$$

Es directo ver que $\Phi(\eta) \in \mathbf{Hom}_H(M, N)$, esto es, $\Phi(\eta)$ es H-covariante, pues si $h \in H$, se tiene

$$h \cdot [\Phi(\eta)(m)] = h \cdot \eta(m)(e) \overset{*}{=} \eta(h \cdot m)(e) = \Phi(\eta)(h \cdot m),$$

donde la igualdad (*) se tiene pues η es un G-morfismo.
Definamos ahora un morfismo $\Psi : \mathbf{Hom}_H(M, N) \longrightarrow \mathbf{Hom}_G(M, \mathbf{Ind}_G^H(N))$. Para tal efecto sea $\lambda : M \to N$ un H-morfismo. Deseamos definir un G-morfismo $\Psi(\lambda) : M \to \mathbf{Ind}_G^H(N)$. Entonces definimos

$$\begin{aligned} \Psi(\lambda) : M &\longrightarrow \mathbf{Ind}_G^H(N) \\ m &\longmapsto \Psi(\lambda)(m) : G \longrightarrow N \\ &\qquad\qquad\quad \sigma \longmapsto \lambda(\sigma \cdot m). \end{aligned}$$

Veamos que $\Psi(\lambda)$ es G-covariante.
Sea $\sigma \in G$. Entonces para todo $m \in M$ y para todo $\tau \in G$ se tiene que

$$[\sigma \cdot \Psi(\lambda)(m)](\tau) \overset{**}{=} \Psi(\lambda)(m)(\tau\sigma) = \lambda[(\tau\sigma) \cdot m] = \lambda[\tau \cdot (\sigma \cdot m)] = [\Psi(\lambda)(\sigma \cdot m)](\tau),$$

por tanto, para todo $\sigma \in G$ se cumple que $\sigma \cdot \Psi(\lambda)(m) = \Psi(\lambda)(\sigma \cdot m)$. Notemos que la igualdad (**) se tiene por la definición de $\mathbf{Ind}_G^H(N)$ como G-módulo. Es directo verificar que los morfismos Ψ y Φ son inversos uno del otro.

(2) Sabemos que hay un G-morfismo de manera natural

$$\mathbf{Ind}_G^H(N) \cong \mathbf{Hom}_G(\mathbb{Z}G, \mathbf{Ind}_G^H(N)),$$

por tanto el enunciado se cumple aplicando el inciso anterior. ■

El par de resultados siguiente es de particular importancia e imitan a resultados conocidos para módulos inyectivos.

Proposición 4.4
Para todo G-módulo M existe un G-módulo co-inducido Q y un G-monomorfismo $\gamma : M \hookrightarrow Q$.

Demostración.
Sea $Q := \mathbf{Ind}_G(M)$ considerando a M como grupo abeliano. Definamos el morfismo $\gamma : M \to Q$ como sigue: sea $m \in M$ y consideremos $\gamma(m) : G \to M$ dada por $\gamma(m)(\sigma) := \gamma(\sigma \cdot M)$. Es directo que γ es un G-morfismo ya si $\tau \in G$, se tiene

$$\tau \cdot \gamma(m)(\sigma) = \gamma(m)(\sigma\tau) = (\sigma\tau) \cdot m = \sigma \cdot (\tau \cdot m) = \gamma(\tau \cdot m)(\sigma)$$

y esto para todo $\sigma \in G$, por lo que $\tau \cdot \gamma(m) = \gamma(\tau \cdot m)$ para todo $m \in M$ y para todo $\sigma \in G$.
Por último, γ es inyectivo pues si $\gamma(m) = 0 : G \to M$, en particular para $e \in G$ se cumple que $\gamma(m)(e) = e \cdot m = m = 0$, de donde se tiene la conclusión. ■

Proposición 4.5
Sea G un grupo. Si Q es un G-módulo co-inducido, entonces

$$\mathbf{H}^q(G, Q) = 0 \qquad \forall\, q \geq 1.$$

Demostración.
Sea M un G-módulo tal que $Q = \mathbf{Ind}_G(M)$. Por el lema anterior tenemos isomorfismos naturales

$$\mathbf{Hom}_G(\quad, Q) = \mathbf{Hom}_G(\quad, \mathbf{Ind}_G(M)) \cong \mathbf{Hom}_{\mathbb{Z}}(\quad, M).$$

Tomemos una resolución proyectiva del G-módulo $\mathbb{Z}$

$$\mathcal{P}_{\mathbb{Z}} : \quad \cdots P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

Quitando el G-módulo $\mathbb{Z}$ del complejo $\mathcal{P}_{\mathbb{Z}}$ y aplicando el funtor $\mathbf{Hom}_G(\quad, Q)$ tenemos

$$\begin{array}{ccccccccc}
\mathbf{Hom}_G(P_0, Q) & \longrightarrow & \mathbf{Hom}_G(P_1, Q) & \longrightarrow & \cdots & \longrightarrow & \mathbf{Hom}_G(P_i, Q) & \longrightarrow & \cdots \\
\cong\downarrow & & \cong\downarrow & & & & \downarrow\cong & & \\
\mathbf{Hom}_{\mathbb{Z}}(P_0, M) & \longrightarrow & \mathbf{Hom}_{\mathbb{Z}}(P_1, M) & \longrightarrow & \cdots & \longrightarrow & \mathbf{Hom}_{\mathbb{Z}}(P_i, M) & \longrightarrow & \cdots
\end{array}$$

donde los cuadrados conmutan por la naturalidad de los isomorfismos. Entonces para todo $q \geq 1$ se cumple que

$$\mathbf{H}^q(G, Q) = \mathbf{H}^q(\mathbf{Hom}_G(\mathcal{P}_{\mathbb{Z}}, Q)) \cong \mathbf{H}^q(\mathbf{Hom}_{\mathbb{Z}}(\mathcal{P}_{\mathbb{Z}}, M)) = \mathbf{Ext}^q_{\mathbb{Z}}(\mathbb{Z}, M) = 0$$

y esto último se debe a que $\mathbb{Z}$ es $\mathbb{Z}$-proyectivo. ■

4.0.5. Restricción y corestricción

Sea $H \subseteq G$ un subgrupo de índice finito $[G : H] = n$ y M un G-módulo. Anteriormente definimos el morfismo restricción

$$\mathbf{Res}^H_G : \mathbf{H}^q(G, M) \longrightarrow \mathbf{H}^q(H, M) \qquad \forall\, q \geq 0.$$

Nuestro objetivo es ahora definir morfismos que van en la dirección opuesta

$$\mathbf{Cor} : \mathbf{H}^q(H, M) \longrightarrow \mathbf{H}^q(G, M).$$

Sea $G = \bigcup_{i=1}^{n} \sigma_i H$ una descomposición de G en clases laterales izquierdas. La definición de $\mathbf{Cor}$ se realizará de manera inductiva.

Para $q = 0$ se define

$$\begin{aligned} \mathbf{Cor}^0 : M^H = \mathbf{H}^0(H, M) &\longrightarrow \mathbf{H}^0(G, M) \\ x &\longmapsto \mathrm{N}_{G/H}(x) := \sum_{i=1}^{n} \sigma_i \cdot x. \end{aligned}$$

Esto está bien definido, es decir, no depende de los representantes de las clases laterales y la imagen de $\mathbf{Cor}$ realmente sí está contenida en M^G. En efecto, para lo primero tomemos $\tau_i \in G$ otros representantes de las clases laterales; entonces $\tau_i = \sigma_i h_i$ para algunos h_i, donde $i = 1, \cdots n$. Por otro lado

$$\sum_{i=1}^{n} \tau_i \cdot x = \sum_{i=1}^{n} (\sigma_i h_i) \cdot x = \sum_{i=1}^{n} \sigma_i \cdot (h_i \cdot x) = \sum_{i=1}^{n} \sigma_i \cdot x.$$

De igual manera veamos que $\mathrm{N}_{G/H}(x) \in M^G$. Sea $\sigma \in G$, entonces

$$\sigma \cdot \sum_{i=1}^{n} \sigma_i \cdot x = \sum_{i=1}^{n} \sigma \cdot (\sigma_i \cdot x) = \mathrm{N}_{G/H}(x).$$

Por último observemos también que $\mathbf{Cor}^0 : M^H \to M^G$ es un homomorfismo de grupos abelianos.

Sea $q \geq 1$ y supongamos que $\mathbf{Cor}^j$ está definido para $j = 0, 1, \ldots, q-1$. Tomemos Q un G-módulo co-inducido tal que $M \hookrightarrow Q$. Consideremos la sucesión exacta

$$0 \longrightarrow M \longrightarrow Q \longrightarrow Q/M \longrightarrow 0$$

de la cual obtenemos las sucesiones exactas largas

$$\begin{array}{ccccccccc} \longrightarrow \mathbf{H}^{q-1}(H, Q) & \longrightarrow & \mathbf{H}^{q-1}(H, Q/M) & \xrightarrow{\delta} & \mathbf{H}^{q}(H, M) & \longrightarrow & \mathbf{H}^{q}(H, Q) & \longrightarrow \\ \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \mathbf{Cor}^{q-1}} & & \downarrow{\scriptstyle \mathbf{Cor}^{q}} & & \downarrow{\scriptstyle 0} & \\ \longrightarrow \mathbf{H}^{q-1}(H, Q) & \longrightarrow & \mathbf{H}^{q-1}(H, Q/M) & \xrightarrow{\delta} & \mathbf{H}^{q}(H, M) & \longrightarrow & \mathbf{H}^{q}(H, Q) & \longrightarrow \end{array}$$

En el diagrama anterior los cuadrados conmutan y como $\mathbf{H}^q(G, Q) = 0$ para todo $q \geq 0$, se induce de manera natural $\mathbf{Cor}^q : \mathbf{H}^q(H, M) \to \mathbf{H}^q(G, M)$ pues los morfismos de conexión δ se convierten en isomorfismos.

Una de las propiedades más importantes del morfismo de corestricción es la siguiente.

Teorema 4.0.6
Sea $H \subseteq G$ un subgrupo de G de índice finito n. Entonces para todo G-módulo M y para toda $Q \geq 0$, la composición $\mathbf{Cor} \circ \mathbf{Res}$ es multiplicación por n en $\mathbf{H}^q(G, M)$, es decir el diagrama siguiente

$$\begin{array}{ccc} \mathbf{H}^q(G, M) & \xrightarrow{\quad n \quad} & \mathbf{H}^q(G, M) \\ & {\scriptstyle \mathbf{Res}} \searrow \quad \nearrow {\scriptstyle \mathbf{Cor}} & \\ & \mathbf{H}^q(H, M) & \end{array}$$

conmuta para todo $q \geq 0$.

Demostración.
Sea $G = \bigcup_{i=1}^{n} \sigma_i H$ una descomposición de G en clases laterales izquierdas. Procederemos por inducción sobre q. Si $q = 0$, estudiemos la composición

$$M^G \xrightarrow{\mathsf{Res}} M^H \xrightarrow{\mathsf{Cor}} M^G.$$

Sea $x \in M^G$, entonces

$$\mathsf{Cor} \circ \mathsf{Res}(x) = \sum_{i=1}^{n} \sigma_i \cdot x \overset{*}{=} \sum_{i=1}^{n} x = nx,$$

donde la igualdad $*$ se tiene pues $x \in M^G$.

Sea ahora $q > 0$ y supongamos que para todo $0 \leq j < q$ se cumple que $\mathsf{Cor}^j \circ \mathsf{Res} = n$ para todo G-módulo. Tomemos Q un G-módulo co-inducido tal que $M \hookrightarrow Q$; como antes, tenemos la sucesión exacta

$$0 \longrightarrow M \longrightarrow Q \longrightarrow {}^{Q}\!/_{M} \longrightarrow 0$$

de la cual obtenemos las sucesiones exactas largas

$$\begin{array}{ccccccccc}
\longrightarrow & \mathbf{H}^{q-1}(H,Q) & \longrightarrow & \mathbf{H}^{q-1}(H,{}^{Q}\!/_{M}) & \xrightarrow{\delta} & \mathbf{H}^{q}(H,M) & \longrightarrow & \mathbf{H}^{q}(H,Q) & \longrightarrow \\
 & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \mathsf{Cor}^{q-1}} & & \downarrow{\scriptstyle \mathsf{Cor}^{q}} & & \downarrow{\scriptstyle 0} & \\
\longrightarrow & \mathbf{H}^{q-1}(H,Q) & \longrightarrow & \mathbf{H}^{q-1}(H,{}^{Q}\!/_{M}) & \xrightarrow{\delta} & \mathbf{H}^{q}(H,M) & \longrightarrow & \mathbf{H}^{q}(H,Q) & \longrightarrow
\end{array}$$

en donde los morfismo nuevamente δ se convierten en isomorfismos. Por lo tanto la conmutatividad del diagrama y la hipótesis implican la igualdad

$$\mathsf{Cor}^q \circ \mathsf{Res} = n. \quad \blacksquare$$

Corolario 4.0.2
Si G es un grupo finito de orden n, entonces

$$n \cdot \mathbf{H}^q(G,M) = 0$$

para todo $q \geq 1$ y para todo G-módulo M.

Demostración.
Si $H = \{e\} \leq G$ entonces H es de índice finito n y por el resultado anterior el diagrama

$$\begin{array}{ccc}
\mathbf{H}^q(G,M) & \xrightarrow{\quad n \quad} & \mathbf{H}^q(G,M) \\
 & {\scriptstyle \mathsf{Res}} \searrow \quad \nearrow {\scriptstyle \mathsf{Cor}} & \\
 & \mathbf{H}^q(\{e\},M) &
\end{array}$$

conmuta para toda $q \geq 0$, sin embargo $\mathbf{H}^q(\{e\},M) = 0$ para toda $q \geq 1$. Se sigue entonces que multiplicación por n es igual a cero. $\blacksquare$

4.1. Cohomología de Galois

Sea F/K una extensión de Galois finita de campos y tomemos $G = \mathrm{Gal}\,(F/K)$. Calculemos entonces la cohomología de G con coeficientes en algunos G-módulos importantes.

Ejemplo 4.1.1 (Teorema 90 de Hilbert)
Sea F/K una extensión de Galois finita con $G = \mathrm{Gal}\,(F/K)$. Entonces

$$\mathbf{H}^1\,(G, F^*) = \{1\}.$$

Demostración.
Sea $f \in Z^1(G, F^*)$. Dado que F^* es un grupo multiplicativo, se tiene que

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

Sea entonces $\alpha \in F^*$ y definamos

$$\beta = \sum_{\sigma\in G} f(\sigma)\sigma(\alpha).$$

Dado que G es un conjunto linealmente independiente podemos elegir un $\alpha_0 \in F^*$ tal que $\beta \neq 0$. Entonces, tomando $\tau \in G$ se tiene que

$$\begin{aligned}\tau(\beta) &= \sum_{\sigma\in G} \tau(f(\sigma))\tau\sigma(\alpha_0) = \sum_{\sigma\in G} f(\tau)^{-1} f(\tau\sigma)\tau\sigma(\alpha_0)\\ &= f(\tau)^{-1}\sum_{\sigma\in G} f(\tau\sigma)\tau\sigma(\alpha_0) = f(\tau)^{-1}\sum_{\sigma\in G} f(\sigma)\sigma(\alpha_0)\\ &= f(\tau)^{-1}\beta\end{aligned}$$

por lo tanto

$$f(\tau) = \frac{\beta}{\tau(\beta)} = \frac{\tau(\beta^{-1})}{\beta^{-1}},$$

es decir $f \in B^1(G, F^*)$ y de esto se tiene directamente que $\mathbf{H}^1\,(G, F^*) = \{1\}$. ∎

Ejemplo 4.1.2
Si para un campo L denotamos por $\mu_n(L)$ las n-raíces de la unidad, tenemos la siguiente sucesión exacta

$$1 \longrightarrow \mu_n(\bar{K}) \longrightarrow \bar{K}^+ \xrightarrow{n} \bar{K}^+ \longrightarrow 1$$

por lo tanto se induce una sucesión exacta en cohomología

$$1 \longrightarrow \mu_n(K) \longrightarrow K^+ \xrightarrow{n} K^+ \longrightarrow \mathbf{H}^1\,(G, \mu_n(\bar{K})) \longrightarrow 1$$

donde $G = \mathrm{Gal}\,(K(\zeta_n)/K)$. De donde se concluye directamente que

$$\mathbf{H}^1\,(G, \mu_n(\bar{K})) \cong \frac{K^+}{(K^+)^n}.$$

4.1.1. Cohomología de Galois infinita

A todo campo K se le puede construir una extensión de Galois canónica: La cerradura separable $\overline{K}/K$. Su grupo de Galois $\mathrm{Gal}\,(\overline{K}/K)$ es llamado el *grupo de Galois absoluto de* K. Esta extensión tiene grado infinito en casi todos los casos, pero se tiene la ventaja de que uno puede considerar dentro de ésta todas las extensiones de Galois finitas. Sin embargo, uno se encuentra con el problema de que el teorema fundamental de la teoría de Galois no se cumple para este caso. Esto se visualiza en el siguiente ejemplo.

Ejemplo 4.1.3
El grupo de Galois absoluto $G = \mathrm{Gal}\,(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ del campo $\mathbb{F}_p$ de p elementos contiene el automorfismo de Frobenius φ el cual está definido por

$$\varphi(x) = x^p \qquad \forall\, x \in \overline{\mathbb{F}}_p.$$

El subgrupo $(\varphi) = \{\varphi^n : n \in \mathbb{Z}\}$ claramente tiene el mismo campo fijo $\mathbb{F}_p$ que G, pero en contraste con lo que pasa en las extensiones de Galois finitas, se tiene que $(\varphi) \neq G$. Para ver esto, se construye un elemento $\psi \in G$ que no pertenezca a (φ) como sigue:

Se elige una sucesión $\{a_n\}$ de enteros tal que

$$a_n \equiv a_m \mod m \qquad \text{siempre que } m \mid n,$$

y también que no exista entero a tal que las congruencias $a_n \equiv a \mod n$ se cumplan para todo n. Por ejemplo, escribiendo $n = n' \cdot p^{v_p(n)}$, con $(n', p) = 1$ y $1 = n'x_n + p^{v_p(n)}y_n$, entonces tomando $a_n = n'x_n$, tenemos que a_n cumple con lo requerido. En efecto, se tiene lo siguiente: Si $n = n' \cdot p^{v_p(n)}$ con $(n', p) = 1$ y $m = m' \cdot p^{v_p(m)}$ con $(m', p) = 1$, además, $a_n = n'x_n$ y $a_m = m'x_m$ se tiene que

$$\begin{aligned} 1 &= n'x_n + p^{v_p(n)}y_n = a_n + p^{v_p(n)}y_n \\ 1 &= m'x_m + p^{v_p(m)}y_m = a_m + p^{v_p(m)}y_m \end{aligned}$$

Por lo tanto, si $m \mid n$, se tiene que $m' \mid n'$ y $v_p(m) \leq v_p(n)$. Más aún, se cumple que

$$a_n - a_m = p^{v_p(m)}y_m - p^{v_p(n)}y_n = p^{v_p(m)}\left(y_m - p^{v_p(n)-v_p(m)}y_n\right),$$

por lo que $p^{v_p(m)} \mid a_n - a_m$. Por otro lado,

$$a_n - a_m = n'x_n - m'x_m = m'\left(\frac{n'}{m'}x_n - x_m\right),$$

entonces $m' \mid a_n - a_m$, y como $(m', p) = 1$, se concluye que

$$m' \cdot p^{v_p(m)} = m \mid a_n - a_m,$$

esto es, $a_n \equiv a_m \mod m$. Suponga ahora que existe a entero tal que $a_n \equiv a \mod n$ para todo n, se tiene entonces que $n \mid a_n - a$, y como $n = n' \cdot p^{v_p(n)}$, se tiene que $n' \mid a_n - a$. Por otro lado, dado que $a_n = n'x_n$ se tiene que $n' \mid a_n$. De lo anterior se tiene que $n' \mid a$ para todo n, pero esto sólo se cumple cuando $a = 0$. De lo anterior se

tendría que $a_n \equiv 0 \mod n$ para todo n. Entonces $n \mid a_n$ y de esto, $n' \cdot p^{v_p(n)} \mid n' x_n$, por lo tanto $p^{v_p(n)} \mid x_n$, lo cual es imposible, ya que son primos relativos. Entonces no existe a entero tal que $a_n \equiv a \mod n$ para todo n. Sea entonces

$$\psi_n = \varphi^{a_n} \mid_{\mathbb{F}_{p^n}} \in \mathrm{Gal}\,(\mathbb{F}_{p^n}/\mathbb{F}_p).$$

Si $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, entonces $m \mid n$, es decir $a_n \equiv a_m \mod m$ y por lo tanto

$$\psi_n \mid_{\mathbb{F}_{p^m}} = \varphi^{a_n} \mid_{\mathbb{F}_{p^m}} = \varphi^{a_m} \mid_{\mathbb{F}_{p^m}} = \psi_m,$$

dado que $\varphi \mid_{\mathbb{F}_{p^m}}$ tiene orden m. Por lo tanto ψ_n define un automorfismo ψ de $G = \overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$. El elemento ψ no pertenece a (φ), pues si así fuera, $\psi = \varphi^a$, para algún $a \in \mathbb{Z}$, es decir, $\psi \mid_{\mathbb{F}_{p^n}} = \varphi^{a_n} \mid_{\mathbb{F}_{p^n}} = \varphi^a \mid_{\mathbb{F}_{p^n}}$, entonces, $a_n \equiv a \mod n$ para todo n, lo cual contradice la elección de ψ.

El teorema fundamental de la teoría de Galois se corregirá ahora tomando en consideración una topología para el grupo de Galois $G = \mathrm{Gal}\,(\Omega/K)$ de una extensión de Galois cualquiera Ω/K. Esta topología es llamada la *topología de Krull* y se obtiene como sigue. Sea $\Re$ la familia de todos los subgrupos $\mathrm{Gal}\,(\Omega/F)$ de G donde $K \subseteq F \subseteq \Omega$ y $[F : K]$ es finito. Entonces se toma $\Re$ como *un sistema fundamental de vecindades de la identidad*. Para cada $\sigma \in G$, se toman las clases laterales $\sigma\mathrm{Gal}\,(\Omega/F)$ como un base de vecindades de σ. La función de multiplicación

$$G \times G \to G, \qquad (\sigma,\, \tau) \mapsto \sigma\tau$$

es continua, dado que la imagen inversa del elemento de la base de la topología $\sigma\tau\mathrm{Gal}\,(\Omega/F)$ contiene la vecindad abierta

$$\sigma\mathrm{Gal}\,(\Omega/F) \times \tau\mathrm{Gal}\,(\Omega/F)$$

de $(\sigma,\, \tau)$. De la misma forma la función

$$G \to G, \qquad \sigma \mapsto \sigma^{-1}$$

es continua, por lo que G se convierte en un grupo topológico.

Para poder determinar ciertas propiedades importantes de G, es necesario introducir los conceptos de sistemas proyectivos y límites inversos.

Definición 4.1.1
Por un conjunto dirigido I *entenderemos un conjunto parcialmente ordenado en el cual sus elementos cumplen la propiedad de Moore-Smith:*

$$\forall\, \alpha,\, \beta \in I,\ \exists\, \gamma \in I \ \ \textit{tal que}\ \alpha \leq \gamma \ \ \textit{y} \ \ \beta \leq \gamma.$$

Ejemplo 4.1.4

1a. Los conjuntos $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ son conjuntos dirigidos con el orden usual.

2a. Considere $\mathbb{N}$ con el orden dado por $m \leq n \iff m \mid n$. Se tiene que si $m,\, n \in \mathbb{N}$, entonces $r = nm \in \mathbb{N}$ y además $n \leq r$ y $m \leq r$, por lo que $\mathbb{N}$ visto desde esta forma también es un conjunto dirigido.

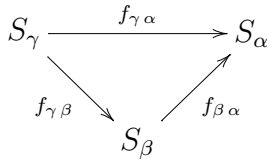
3a. Dado un grupo G y Λ la familia de subgrupos G ordenada por la inclusión. Entonces Λ es un conjunto dirigido, pues si $H,\ K$ son subgrupos de G, se tiene que tomando $M = \langle H,\ K\rangle$, se cumple que $M \in \Lambda$ y además $H \leq M$ y también $K \leq M$.

4b. Tomando G y Λ de la misma forma que en el inciso anterior, el orden es definido como sigue: si $H,\ K \in \Lambda$, $H \preceq K \iff K \leq H$ como subgrupos. Con lo anterior Λ es un conjunto dirigido, ya que para todos $H,\ K \in \Lambda$, y tomando $L = H \cap K$, se tiene que $L \in \Lambda$ y también $H \preceq L,\ K \preceq L$.

Suponga ahora que para todo $\alpha \in I$, S_α es un conjunto (grupo, anillo, etc.) y se cumple que para todos $\alpha,\ \beta \in I$ con $\alpha \leq \beta$ existe una función (homomorfismo) $f_{\beta\,\alpha} : S_\beta \to S_\alpha$ con la propiedad que para todos $\alpha \leq \beta \leq \gamma$ se cumple que

$$f_{\gamma\,\alpha} = f_{\beta\,\alpha} \circ f_{\gamma\,\beta},$$

esto es, el diagrama siguiente



es conmutativo. Además, $f_{\alpha\,\alpha} = id$, para todo α.

Cualquier sistema como el descrito anteriormente, será llamado un *sistema proyectivo (o inverso) de conjuntos (grupos, anillos, etc.)* y se denotará por $\{S_\alpha,\ f_{\beta\,\alpha}\}$.

Ejemplo 4.1.5

1b. Sea $I = \mathbb{N}$, $S_\alpha = \mathbb{Z}$ y $l \geq 0$; sean $f_{n+l,\,n} : \mathbb{Z} \to \mathbb{Z}$ dadas por $a \mapsto p^l a$, donde p es un número primo fijo. Se tiene entonces que, si $n \leq m \leq r$

$$\begin{aligned} f_{r\,n}(a) &= p^{r-n}a = p^{r-m+m-n}a \\ &= p^{r-m}p^{m-n}a = f_{m\,n}(p^{r-m}a) \\ &= f_{m\,n}(f_{r\,m}(a)) = (f_{m\,n} \circ f_{r\,m})(a). \end{aligned}$$

por lo anterior, $\{\mathbb{Z},\ f_{r\,n}\}$ es un sistema inverso.

2b. Considere $I = \mathbb{N}$ como en el ejemplo 2a. Sean $n,\ m \in \mathbb{N}$ con $m \leq n$. Definamos

$$f_{n\,m} : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{m\mathbb{Z}} \quad \text{como} \quad a + n\mathbb{Z} \mapsto a + m\mathbb{Z}.$$

estas funciones están bien definidas, pues si $a + n\mathbb{Z} = b + n\mathbb{Z}$ entonces $n \mid a - b$. Por otro lado, dado que $m \leq n$ se tiene que $m \mid n$, por lo tanto $m \mid a - b$ y de esto $a + m\mathbb{Z} = b + m\mathbb{Z}$. La consistencia de las funciones $f_{n\,m}$ es directa.

3b. Sea G un grupo, I la familia de todos los subgrupos normales de índice finito. Entonces si $\alpha \in I$, tomando $S_\alpha = G/\alpha$, se tiene que S_α es un grupo finito. Consideremos a I con el orden dado como en el ejemplo 4.1.4 y, dados $\alpha,\ \beta \in I$ con $\alpha \preceq \beta$, sean $f_{\beta\,\alpha} : G/\beta \to G/\alpha$ dadas por $g\beta \mapsto g\alpha$, es decir las proyecciones

naturales. Con lo anterior, $\{S_\alpha,\ f_{\beta\,\alpha}\}$ es un sistema inverso. En efecto, es preciso verificar que las funciones estén bien definidas y que sean consistentes. Sean $\alpha,\ \beta \in I$ con $\alpha \preceq \beta$, esto es $\beta \leq \alpha$ como subgrupos. Si $g\beta = g_1\beta$ se tiene que $gg_1^{-1} \in \beta$, por lo que $gg_1^{-1} \in \alpha$, esto es, $g\alpha = g_1\alpha$, y de esto se verifica que

$$f_{\beta\,\alpha}(g_1\beta) = g_1\alpha = g\alpha = f_{\beta\,\alpha}(g\beta).$$

Por lo último sean $\alpha \preceq \beta \preceq \gamma$, por lo tanto dado $g \in G$, se tiene que $g\gamma \in S_\gamma$ y de esto $f_{\gamma\,\beta}(g\gamma) = g\beta$, por lo tanto para todo $g \in G$

$$f_{\beta\,\alpha} \circ f_{\gamma\,\beta}(g\gamma) = f_{\beta\,\alpha}(g\beta) = g\alpha = f_{\gamma\,\alpha}(g\gamma).$$

Sea $\{S_\alpha,\ f_{\beta,\,\alpha}\}$ un sistema inverso de conjuntos (grupos anillos, etc.) y sea el producto directo $X = \prod_\alpha S_\alpha$. Definamos el conjunto $S \subseteq X$ como sigue:

$$(x_\alpha) \in S \iff (\forall\ \gamma,\ \beta) \quad (\gamma \leq \beta \Longrightarrow f_{\beta\,\gamma}(x_\beta) = x_\gamma).$$

Al conjunto S se le llama *límite inverso* del sistema inverso de conjuntos (grupos, anillos, etc.), y se le denota por

$$S = \varprojlim_{\alpha \in I} S_\alpha.$$

Definición 4.1.2
Por un grupo profinito *G, entenderemos el límite inverso de un sistema inverso de grupos finitos.*

Observaciones

1. Sabemos que a todo conjunto finito se le puede asociar una topología de manera natural, a saber la *topología discreta*, con la cual dicho conjunto es compacto. Por lo anterior, cualquier grupo finito está dotado de la topología discreta, con la cual las operaciones del grupo son funciones continuas, por lo que los grupos finitos se considerarán como grupos topológicos compactos.

2. Para el resto de la sección, supondremos que G es un grupo profinito, esto es, el límite inverso de un sistema $\{G_\alpha,\ f_{\beta\,\alpha}\}$ de grupos finitos. Con lo anterior, existe un homomorfismo $\phi_\beta : G \to G_\beta$ dado por $\phi_\beta((x_\alpha)) = x_\beta$ (este homomorfismo es la restricción a G de la β-ésima proyección, por lo que es continua) . Notemos entonces que para $\beta,\ \gamma \in I$ con $\beta \leq \gamma$ se tiene que

$$\begin{aligned} f_{\gamma\,\beta} \circ \phi_\gamma((x_\alpha)) &= f_{\gamma\,\beta}(x_\gamma) \\ &= x_\beta = \phi_\beta((x_\alpha)) \end{aligned}$$

Se tiene entonces el siguiente resultado importante.

Proposición 4.6
Si G es un grupo profinito, entonces G es un grupo compacto y totalmente disconexo en el cual la familia de subgrupos normales abiertos es un sistema fundamental de vecindades de la identidad.

Demostración. Dado que G es profinito, existen grupos finitos G_α y homomorfismos $f_{\beta\,\alpha} : G_\beta \to G_\alpha$ tales que

$$G = \varprojlim_{\alpha \in I} G_\alpha.$$

con I un conjunto dirigido de índices. Por la observación anterior, cada G_α es compacto y por el teorema de Tychonov $X = \prod_{\alpha\in I} G_\alpha$ es compacto. Es suficiente ver entonces que G es cerrado en X, o lo que es lo mismo, que su complemento G^{c} es abierto en X.

Sea entonces $(x_\alpha) \in G^{\mathrm{c}}$. Debemos encontrar una vecindad de (x_α) que no interseque a G. Dado que $(x_\alpha) \notin G$, existen un par de índices β, $\gamma \in I$ con $\beta \leq \gamma$ tales que $f_{\gamma\,\beta}(x_\gamma) \neq x_\beta$. Como G_β es un espacio Hausdorff (por ser discreto), existen vecindades M_β de x_β y N_β de $f_{\gamma\,\beta}(x_\gamma)$ tales que $N_\beta \cap M_\beta = \emptyset$. Sea $N_\gamma = f_{\gamma\,\beta}^{-1}(N_\beta)$, dado que $f_{\gamma\,\beta}$ es continua entonces N_γ es abierto en G_γ y $x_\gamma \in N_\gamma$. Sea

$$V = \prod_{\alpha\in I} X_\alpha$$

donde $X_\beta = M_\beta$, $X_\gamma = N_\gamma$ y $X_\alpha = G_\alpha$ si $\alpha \notin \{\beta, \gamma\}$. Se tiene que V es abierto en X, y $(x_\alpha) \in V$. Además si $(y_\alpha) \in V$ se tiene que $y_\gamma \in N_\gamma$, $y_\beta \in M_\beta$, por lo que $f_{\gamma\,\beta}(y_\gamma) \in N_\beta$, entonces $f_{\gamma\,\beta}(y_\gamma) \neq y_\beta$ y de esto se tiene que $V \cap G = \emptyset$, es decir G es cerrado en X. Siendo X compacto y por lo anterior se concluye que G es también compacto.

Consideremos ahora los homomorfismos continuos ϕ_α y definamos $U_\alpha = \ker \phi_\alpha$. De inmediato se observa que cada U_α es normal en G. Por otro lado, como $U_\alpha = \phi_\alpha^{-1}(\{1\})$, se tiene que cada U_α es abierto en G. Por lo anterior, la proposición se tendrá completamente probada si se cumple que $\cap_\alpha U_\alpha = \{1\}$. Sea entonces $(x_\alpha) \in \cap_\alpha U_\alpha$, por la definición de cada U_α se tiene que $\phi_\beta((x_\alpha)) = x_\beta = 1$ para todo β, por lo que $(x_\alpha) = 1$. Resta probar que G es totalmente disconexo.

Veamos que cada U_α es cerrado. Sabemos que $\{1\}$ es cerrado en G_α, por tener éste la topología discreta, y como cada ϕ_α es continua se tiene que U_α es la imagen inversa de un conjunto cerrado bajo una función continua, de lo cual se concluye que U_α es cerrado para todo $\alpha \in I$. Alternativamente se tiene que

$$G = \bigcup_{g\in G} gU_\alpha$$

y como G es compacto existen $g_1, \ldots, g_n \in G$ tales que

$$G = \bigcup_{i=1}^{n} g_i U_\alpha,$$

de lo cual se tiene que

$$g_i U_\alpha = G \setminus \bigcup_{j\neq i} g_j U_\alpha = \left(\bigcup_{j\neq i} g_j U_\alpha\right)^C$$

de lo cual se concluye que $g_i U_\alpha$ es cerrado y por lo tanto U_α también es cerrado. Sea ahora $C = C(1)$ la componente conexa de la identidad, debemos ver que $C = \{1\}$. Notemos que

$$C = C \cap (U_\alpha \cup U_\alpha^C) = (C \cap U_\alpha) \cup (C \cap U_\alpha^C).$$

Sean $A = C \cap U_\alpha$ y $B = C \cap U_\alpha^C$. Se tiene que A y B son abiertos en C y también $A \cap B = \emptyset$, por lo tanto, como C es conexo se tiene que $B = \emptyset$, y de esto vemos que $C = C \cap U_\alpha$, es decir, $C \subseteq U_\alpha$ para todo α, de lo cual se concluye que $C \subseteq \bigcap U_\alpha = \{1\}$. ■

Regresando ahora a una extensión de Galois (finita o infinita) Ω/K y su grupo de Galois $G = \mathrm{Gal}\,(\Omega/K)$. Si $H \in \Re$, se observa que $H \lhd G$ (proposición 4.6), por lo que podemos tomar a $\Re$ como un conjunto dirigido y referirnos al ejemplo 3b para construir un sistema inverso tomando como $S_H = G/H$ para todo $H \in \Re$. Pero ahora considerando que $H = \mathrm{Gal}\,(\Omega/F)$ con F campo que cumple $K \subseteq F \subseteq \Omega$ y también que $[F : K]$ es finito, tenemos que

$$S_H = \frac{\mathrm{Gal}\,(\Omega/K)}{\mathrm{Gal}\,(\Omega/F)} \cong \mathrm{Gal}\,(F/K),$$

por lo que

$$G = \varprojlim_F \mathrm{Gal}\,(F/K).$$

Como consecuencia directa de la proposición anterior, se tiene el siguiente corolario.

Corolario 4.1.1
Si Ω/K es una extensión de Galois (finita o infinita), entonces el grupo de Galois $G = \mathrm{Gal}\,(\Omega/K)$ es compacto y totalmente disconexo con respecto a la topología de Krull.

Se tiene la siguiente proposición.

Proposición 4.7
Sea H un subgrupo de G y denotemos su cerradura por $\bar{H}$, si L es el campo fijo de H entonces se tiene que $\mathrm{Gal}\,(\Omega/L) = \bar{H}$.

Demostración. Sean $\sigma \in \bar{H}$, $a \in L$ y $H' = \mathrm{Gal}\,(\Omega/K(a))$. Como $[K(a) : K]$ es finito, $H' \in \Re$, es decir, $\sigma H'$ es una vecindad de σ, por lo que $H \cap \sigma H' \neq \emptyset$. Sea entonces $\tau \in H \cap \sigma H'$. Como $\tau \in H$, observamos que τ deja fijo a todo elemento de L y como $\tau \in \sigma H'$ lo cual implica que $\sigma^{-1}\tau \in H'$, por lo tanto $\sigma^{-1}\tau$ deja fijo a todo elemento de $K(a)$. De lo anterior vemos que $\sigma(a) = \tau(a) = a$, esto es, σ deja fijo a todo elemento de L, por lo que obtenemos que $\bar{H} \subseteq \mathrm{Gal}\,(\Omega/L)$.

Sea ahora $\sigma \in \mathrm{Gal}\,(\Omega/L)$. Mostraremos que $\sigma \in \bar{H}$ lo cual es equivalente a que $H \cap \sigma H' \neq \emptyset$ para todo $H' \in \Re$. Sea entonces $H' \in \Re$, de lo cual vemos que el campo fijo de H' es una extensión finita y separable de K por lo que el teorema del elemento primitivo asegura que existe $\theta \in \Omega$ tal que $K(\theta)$ es el campo fijo de H'. Sea F una extensión finita y normal de L tal que $\theta \in F$. Si $\rho \in H$ se tiene que $\rho|_F \in \mathrm{Gal}\,(F/L)$. Vemos también que si $\rho' \in \mathrm{Gal}\,(F/L)$ existe $\rho \in \mathrm{Gal}\,(\Omega/L)$ tal que $\rho|_F \equiv \rho'$. El elemento ρ en realidad pertenece a H, pues L es el campo fijo de H. Entonces la

restricción de σ a F es un elemento de $\mathrm{Gal}\,(F/L)$ por lo que existe $\tau \in H$ tal que $\tau|_F = \sigma|_F$; en particular $\sigma(\theta) = \tau(\theta)$, es decir $\sigma^{-1}\tau$ deja fijo a todo elemento de $K(\theta)$, por lo que $\tau \in \sigma H'$, de lo que se concluye que $\tau \in H \cap \sigma H'$. ■

Sea H un subgrupo cerrado de G y Ω^H el campo fijo de H. Por la proposición anterior, si $\Omega^{H_1} = \Omega^{H_2}$ vemos que $H_1 = \bar{H}_1 = \mathrm{Gal}\,(\Omega/\Omega^{H_1}) = \mathrm{Gal}\,(\Omega/\Omega^{H_2}) = \bar{H}_2 = H_2$, lo cual prueba la inyectividad de la función

$$H \mapsto \Omega^H$$

del conjunto de subgrupos cerrados de G al conjunto de subcampos de Ω que contienen a K, por lo que resta probar que dicha función es suprayectiva. Sea F un campo tal que $K \subseteq F \subseteq \Omega$ y sea $H = \mathrm{Gal}\,(\Omega/F)$. Probaremos que $F = \Omega^H$. Notemos que por la proposición anterior H es un conjunto cerrado y claramente se cumple que $F \subseteq \Omega^H$, por lo que es suficiente mostrar que $\Omega^H \subseteq F$, esto es, todo elemento de Ω que queda fijo bajo los elementos de H pertenece F, o equivalentemente, si $a \notin F$ existe $\sigma \in H$ tal que $\sigma(a) \neq a$. Sea $a \notin F$ y sea F' una extensión normal y finita de F tal que $a \in F'$. Existe entonces $\tau \in \mathrm{Gal}\,(F'/F)$ tal que $\tau(a) \neq a$. De lo anterior existe $\sigma \in \mathrm{Gal}\,(\Omega/F)$ tal que $\sigma|_F = \tau$ de lo cual concluimos que $\sigma(a) \neq a$.

La correspondencia inversa de la función $H \mapsto \Omega^H$ está dada por

$$F \mapsto \mathrm{Gal}\,(\Omega/F).$$

Estamos ahora en posición de establecer la forma más general del teorema fundamental de la teoría de Galois.

Teorema 4.1.1
Sea Ω/K es una extensión de Galois (finita o infinita). Entonces existe una correspondencia biyectiva entre los subgrupos cerrados de $\mathrm{Gal}\,(\Omega/K)$ *y los subcampos F de Ω que contienen a K. Esta correspondencia esta dada por*

$$H \mapsto \Omega^H, \qquad F \mapsto \mathrm{Gal}\,(\Omega/F).$$

Regresando al caso cuando G es un grupo profinito,un G-módulo se dice *discreto* si la función que determina la acción es continua, donde M lo consideramos con la topología discreta y G la topología natural. Lo anterior es equivalente a que

$$M = \bigcup_H M^H, \qquad \text{con } H \text{ subgrupo abierto de } G;$$

en efecto, ya que la continuidad de $G \times M \to M$ implica que para cada par $(\sigma, m) \in G \times M$ existe un abierto H de G tal que la vecindad $\sigma H \times m$ va a dar al conjunto $\{\sigma m\} \subset M$ y esto a su vez equivale a que $m \in M^H$.

Recordemos que si $\{H_\alpha, f_{\alpha\beta}\}$ es la familia de subgrupos normales abiertos de G, se tiene el isomorfismo

$$G \cong \varprojlim_\alpha {}^G\!/_{H_\alpha}$$

y si M es un G-módulo discreto, entonces

$$M = \bigcup_\alpha M^{H_\alpha} \cong \varinjlim_\alpha M^{H_\alpha},$$

donde el isomorfismo es natural. Fijemos ahora $q \geq 0$. Para cada $\alpha \preceq \beta$ las proyecciones canónicas

$$f_{\beta\,\alpha} : {}^{G}\!/_{H_\beta} \longrightarrow {}^{G}\!/_{H_\alpha}$$

inducen los morfismos de inflación

$$\mathbf{Inf}_\alpha^\beta : \mathbf{H}^q\left({}^{G}\!/_{H_\alpha}, M^{H_\alpha}\right) \longrightarrow \mathbf{H}^q\left({}^{G}\!/_{H_\beta}, M^{H_\beta}\right)$$

de donde formamos un sistema directo

$$\left\{\mathbf{H}^q\left({}^{G}\!/_{H_\alpha}, M^{H_\alpha}\right); \mathbf{Inf}_\alpha^\beta\right\},$$

y entonces estamos en posición de extender la definición de los grupos de cohomología como sigue:

Definición 4.1.3
Sea G un Grupo profinito, y M un G-módulo discreto. El grupo

$$\mathbf{H}^q(G, M) := \varinjlim_H \mathbf{H}^q\left({}^{G}\!/_{H}, M^H\right)$$

se llama el q-ésimo grupo de cohomología de G en M *(aquí H se recorre sobre todos los subgrupos normales abiertos de G).*

Ejemplo 4.1.6
Sea Ω/K una extensión de Galois con grupo de Galois G, el cual ya vimos, es un grupo profinito (4.1.1). De hecho, si tomamos las sub-extensiones F_α/K finitas de Galois de Ω/K y $H_\alpha = \mathrm{Gal}\,(F_\alpha/K)$, se cumple que

$$G = \mathrm{Gal}\,(\Omega/K) \cong \varprojlim_\alpha {}^{G}\!/_{H_\alpha}$$

Consideremos ahora el grupo multiplicativo Ω^* el cual también es un G-módulo discreto ya que $(\Omega)^{H_\alpha} = F_\alpha$, y entonces

$$\Omega^* = \cup_\alpha F_\alpha^*.$$

Se sigue entonces del teorema 90 de Hilbert que

$$\mathbf{H}^1(G, \Omega^*) \cong \varinjlim_\alpha \mathbf{H}^1\left(\mathrm{Gal}\,(F_\alpha/K), F_\alpha^*\right) = 0,$$

ya que cada extensión F_α/K es finita de Galois.

Capítulo 5

Teorema de Mordell

5.1. Introducción o el teorema del descenso

El primer resultado importante en curvas elípticas E sobre campos de números K es el teorema de Mordell-Weil, el cual dice que $E(K)$ es un grupo abeliano finitamente generado. En otras palabras, $E(K) \cong \mathbb{Z}^r \oplus F$, donde F es un grupo abeliano finito, su subgrupo de torsión. Este resultado fue probado por Mordell para $K = \mathbb{Q}$ y por Weil de manera general. La prueba se divide en dos partes, y a la primera parte se le llama teorema de Mordell-Weil débil, el cual dice que el grupo $E(K)/mE(K)$ es finito (aquí $mE(K)$ es la imagen del morfismo $E(K) \xrightarrow{m} E(K)$). Para probar el teorema en su totalidad trataremos de encontrar un tipo de "altura" en $E(K)$ con las propiedades siguientes:

- haya solamente un número de elementos en $E(K)$ con altura acotada y
- Si tenemos representantes $\{P_1, \ldots, P_r\}$ de las clases laterales del grupo finito $E(K)/mE(K)$, para cualquier $P \in E(K)$ uno puede restarle una combinación lineal de los $P_i's$ de tal suerte que la resta resultante tiene altura acotada por una constante C independiente de P.

Veamos por que el teorema de Mordell-Weil débil y dicha función altura son suficientes para demostrar el teorema de Mordell-Weil.

Sean A un grupo abeliano y $m \in \mathbb{N}$. La función $A \xrightarrow{m} A$ es un homomorfismo con imagen

$$mA := \{b \in A | b = ma \text{ para algún } a \in A\}.$$

Si A es finitamente generado, entonces el índice $[A : mA]$ del subgrupo mA en A es finito para cualquier entero $m \neq 0$.

Definición 5.1.1
Una función altura *h en un grupo abeliano A es una función $h : A \to \mathbb{R}$ que cumple:*

1. *Dado Q en A existe una constante C_1, dependiente de A y Q tal que para todo P en A se cumple*
$$h(P + Q) \leq 2h(P) + C_1.$$

2. *Existe un entero $m \geq 2$ y una constante C_2, dependiente de A, tal que todo $P \in A$ cumple*

$$h(mP) \geq m^2 h(P) - C_2.$$

3. *Para cualquier constante C_3 se cumple que el conjunto*

$$\{P \in A \mid h(p) \leq C_3\}$$

es finito.

Proposición 5.1
Sea A un grupo abeliano. Suponga que existe una función altura h definida en A. Suponga además que para el entero m del inciso 2 de la definición anterior el grupo cociente A/mA es finito. entonces A es finitamente generado.

Demostración.
Sean $Q_1, \ldots, Q_r \in A$ representantes de las distintas clases del grupo A/mA. Tomemos ahora un punto $P \in A$ arbitrario. Se cumple entonces que $P = mP_1 + Q_{i_1}$ para algún $1 \leq i_1 \leq r$. De la misma manera $P_1 = mP_2 + Q_{i_1}$ y siguiendo con ese proceso tenemos que

$$\begin{aligned} P &= mP_1 + Q_{i_1} \\ P_1 &= mP_2 + Q_{i_2} \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n} \end{aligned}$$

y regresando a la expresión original se tiene que

$$\begin{aligned} P &= mP_1 + Q_{i_1} = m(mP_2 + Q_{i_2}) + Q_{i_1} = m^2 P_2 + mQ_{i_2} + Q_{i_1} \\ &= m^2(mP_3 + Q_{i_3}) + mQ_{i_2} + Q_{i_1} = m^3 P_3 + m^2 Q_{i_3} + mQ_{i_2} + Q_{i_1} \\ &\vdots \\ &= m^n P_n + m^{n-1} Q_{i_n} + \cdots + Q_{i_1} = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}. \end{aligned}$$

Por otro lado aplicando la función altura definida en A, se tiene que para todo índice j se tiene

$$\begin{aligned} m^2 h(P_j) &\leq h(mP_j) + C_2 = h(P_{j-1} - Q_{i_j}) + C_2 \\ &\leq 2h(P_{j-1}) + C_1' + C_2 \end{aligned}$$

donde $C_1' = \max_{1\leq j\leq r}\{h(Q_j)\}$. De lo anterior, se cumple lo siguiente

$$\begin{aligned}
h(P_n) &\leq \frac{1}{m^2}\left[2h(P_{n-1}) + C_1' + C_2\right] = \frac{2}{m^2}h(P_{n-1}) + \frac{1}{m^2}(C_1' + C_2) \\
&\leq \frac{2}{m^2}\left[\frac{1}{m^2}\left(2h(P_{n-2}) + C_1' + C_2\right)\right] + \frac{1}{m^2}(C_1' + C_2) \\
&= \left(\frac{2}{m^2}\right)^2 h(P_{n-2}) + (C_1' + C_2)\left(\frac{1}{m^2} + \frac{2}{m^4}\right) \\
&\vdots \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + (C_1' + C_2)\left(\frac{1}{m^2} + \frac{2}{m^4} + \cdots + \frac{2^{n-1}}{m^{2n}}\right) \\
&\leq \left(\frac{1}{2}\right)^n h(P) + \frac{C_1' + C_2}{2}
\end{aligned}$$

y por lo tanto para n suficientemente grande se tiene que

$$h(P_n) \leq 1 + \frac{C_1' + C_2}{2}.$$

Finalmente de la primera igualdad establecida se cumple que P es una combinación lineal de los elementos del conjunto

$$\{Q_1, \ldots, Q_r\} \cup \{P \in A \mid h(P) \leq 1 + \frac{C_1' + C_2}{2}\}$$

el cual es un conjunto finito, y entonces A es finitamente generado. ■

5.2. Teorema de Mordell-Weil débil

En lo sucesivo usaremos la siguiente notación:

K	un campo de números
M_K	un conjunto completo de valores absolutos no equivalentes en K
M_K^∞	los valores absolutos arquimedianos en M_K
M_K^0	los valores absolutos no arquimedianos de M_K
$\nu(x)$	$= -\log \mid x \mid_\nu$ para valores absolutos $\nu \in M_K$
ord_ν	valuación normalizada para $\nu \in M_K^0$
R	el anillo de enteros de K
R^*	El grupo de unidades de R
K_ν	la completación de K en $\nu \in M_K$
$R_\nu, \mathfrak{M}_\nu, k_\nu$	el anillo de enteros, ideal maximal y campo de residuos asociados a K_ν para $\nu \in M_K^0$

Nuestro objetivo en esta sección es probar que para cualquier curva elíptica E definida sobre un campo de números K y $m \geq 2$ un entero se cumple que

$$E(K)/mE(K)$$

es finito. Para lo anterior necesitamos algunos hechos de la teoría de curvas elípticas sobre campos locales.

5.2.1. El grupo Formal de una curva elíptica

Sea R un anillo.

Definición 5.2.1
Un Grupo Formal (conmutativo y de un parámetro) $\mathcal{F}$ definido sobre R *es una serie de potencias* $F(X,Y) \in R[[X,Y]]$ *que satisface:*

1. $F(X,Y) = X + Y +$ *términos de grado* ≥ 2.
2. $F(X,F(Y,Z)) = F(F(X,Y),Z)$ *(asociatividad).*
3. $F(X,Y) = F(Y,X)$ *(conmutatividad).*
4. *Existe una única serie de potencias* $i(T) \in R[[T]]$ *tal que* $F(T,i(T)) = 0$ *(inversa).*
5. $F(X,0) = X$ *y* $F(0,Y) = Y$.

Llamaremos a $F(X,Y)$ *la ley de grupo formal de* $\mathcal{F}$.

Definición 5.2.2
Sean $(\mathcal{F},F),(\mathcal{G},G)$ *grupos formales definidos sobre* R. *Un* homomorfismo de $\mathcal{F}$ a $\mathcal{G}$ definido sobre R *es una serie de potencias (sin término constante)* $f(T) \in R[[T]]$ *que satisface:*

$$f(F(X,Y)) = G(f(X),f(Y)).$$

$\mathcal{F}$ *y* $\mathcal{G}$ *se dicen* isomorfos sobre R *si existen* $f : \mathcal{F} \to \mathcal{G}$ *y* $g : \mathcal{G} \to \mathcal{G}$ *definidos sobre* R *tales que*

$$f(g(T)) = g(f(T)) = T.$$

Ejemplo 5.2.1

1. El *grupo formal aditivo*, denotado por $\widehat{\mathbb{G}}_a$ esta dado por

$$F(X,Y) = X + Y.$$

2. El *grupo formal multiplicativo*, denotado por $\widehat{\mathbb{G}}_a$ esta dado por

$$F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$$

Ejemplo 5.2.2
Sea E una curva elíptica definida por una ecuación de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

con coeficientes en R. Podemos definir el *grupo formal asociado a* E, denotado por $\hat{E}$ de acuerdo a la construcción siguiente: haciendo la sustitución $z = -\dfrac{x}{y}, w = -\dfrac{1}{y}$ en la ecuación de Weierstrass obtenemos

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3,$$

y usando substituciones repetidas se puede expresar a w como una serie de potencias formal en $\mathbb{Z}[a_1, \ldots, a_6][[z]]$ dada por

$$w(z) = z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1 a_2 + a_3)z^6 + \cdots$$

y por consiguiente podemos expresar a x y y como serie de potencias en z y por lo tanto la operación de grupo también esta dada por una serie de potencias $F_E(z_1, z_2)$ en dos variables cuyos primeros términos están dados por

$$F_E(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) + \cdots .$$

De esta manera el grupo formal $\hat{E}$ asociado a E es el grupo formal definido por la serie de potencias $F_E(z_1, z_2) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$.

En general un grupo formal es una operación de grupo, sin tener un Grupo propiamente. Sin embargo si R es un anillo local y completo, y si a las variables se les asignan valores en el ideal maximal $\mathfrak{M}$ de R, entonces las series de potencias formales del grupo formal convergen.

Definición 5.2.3
El grupo asociado a $\mathcal{F}/R$, *denotado por* $\mathcal{F}(\mathfrak{M})$, *es el conjunto* $\mathfrak{M}$ *con las operaciones de grupo*

1. $x \oplus_{\mathcal{F}} y = F(x, y)$ *(suma) para* $x, y \in \mathfrak{M}$.
2. $\ominus_{\mathcal{F}} x = i(x)$ *(inverso) para* $x \in \mathfrak{M}$.

Ejemplo 5.2.3
Sea $\hat{E}$ el grupo formal asociado a una curva elíptica E/k, donde k es el campo de cocientes de R. Si tomamos $z \in \mathfrak{M}$ el ideal maximal de R, se tiene una función

$$\begin{aligned} \mathfrak{M} &\longrightarrow E(K) \\ z &\longmapsto (x(z), y(z)) \end{aligned}$$

que se convierte en un homomorfismo de grupos de $\hat{E}(\mathfrak{M})$ a $E(K)$.

El siguiente resultado es una propiedad general de grupos formales.

Proposición 5.2
Sea $p = \operatorname{char} k$. *Entonces todo elemento de torsión de* $\mathcal{F}(\mathfrak{M})$ *tiene orden potencia de* p. *Equivalentemente si* $m \not\equiv 0 mod \pi$, *entonces* $\mathcal{F}(\mathfrak{M})$ *no tiene puntos de orden* m *no triviales.*

5.2.2. Curvas elípticas sobre campos locales

Sea K un campo local (completo con respecto a una valuación discreta ν), R su anillo de enteros con ideal maximal $\mathfrak{M} = (\pi)$ y k su campo residual de R dado por $k = R/\mathfrak{M}$. Asumamos que la valuación ν está normalizada $\nu(\pi) = 1$ y que K y k son campos perfectos.
Sea E/K una curva elíptica dada por una ecuación de Weierstrass

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

Dado que si realizamos en la ecuación de Weierstrass una sustitución

$$(x, y) \Longrightarrow (u^{-2}x, u^{-3}y)$$

se obtiene que cada a_i se transforme en $u^i a_i$, si elegimos a u que sea divisible por una potencia grande de π, podemos elegir una ecuación de Weierstrass con todos sus coeficientes $a_i \in R$. De este modo el discriminante satisface que $\nu(\Delta) \leq 0$ y dado que ν es una valuación discreta, nos podemos fijar en una ecuación de Weierstrass con $\nu(\Delta)$ lo más pequeño posible. A tal ecuación le llamaremos *mínima*.

Observemos que cada vez que hacemos un cambio de coordenadas obtenemos una nueva ecuación de Weierstrass donde su discriminante esta dado por $\Delta' = u^1 2\Delta$, por lo tanto $\nu(\Delta)$ cambia por múltiplos de 12, y por tanto podemos decir que si $a_i \in R$ para todo i y además $\nu(\Delta) < 12$, entonces la ecuación es mínima. De manera análoga, un cálculo directo nos dice que $c_4' = u^4 c_4$ y también $c_6' = u^6 c_6$, por lo que tenemos que si $a_i \in R$ para todo i y además

$$\nu(c_4) < 4 \text{ ó } \nu(c_6) < 6,$$

entonces la ecuación de Weierstrass es mínima.

Ejemplo 5.2.4
Sea p un primo y consideremos la ecuación de Weierstrass

$$y^2 + xy + y = x^3 + x^2 + 22x - 9$$

Sobre el campo $\mathbb{Q}_p$. El discriminante de esta ecuación esta dado por $\Delta = -2^{15} \cdot 5^2$ y también $c_4 = -5 \cdot 211$, por lo que esta ecuación es mínima para todo primo $p \in \mathbb{Z}$.

Definimos la *reducción de E módulo π*, denotada por $\tilde{E}$, como la curva sobre k definida por la ecuación

$$y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6},$$

donde la tilde significa reducción módulo π. La curva $\tilde{E}/k$ puede ser singular, sin embargo su conjunto de puntos no singulares forma un grupo y será denotado por $\tilde{E}_{ns}(k)$. Decimos entonces que E tiene *buena reducción* si $\tilde{E}/k$ es no singular. Definimos los siguientes subconjuntos de E(K):

$$E_0(K) = \{P \in E(K) | \tilde{P} \in \tilde{E}_{ns}(k)\};$$
$$E_1(K) = \{P \in E(K) | \tilde{P} = \tilde{0}\}.$$

Se tiene entonces que $E_0(K)$ son los puntos con reducción no singular y $E_1(K)$ el núcleo de la reducción.

Proposición 5.3

1. *La sucesión de grupos abelianos*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0$$

   es exacta

2. *Existe un isomorfismo $E_1(K) \cong \hat{E}(\mathfrak{M})$.*

Regresemos ahora a nuestro objetivo (el teorema de Mordell-Weil débil). Para esto necesitamos el lema de reducción siguiente.

Lema 12 (de reducción)
Sea L/K una extensión de Galois finita. Si ${}^{E(L)}/_{mE(L)}$ es finito, entonces ${}^{E(K)}/_{mE(K)}$ es finito.

Demostración.
Sea

$$ {}^{E(K)}/_{mE(K)} \xrightarrow{\psi} {}^{E(L)}/_{mE(L)} $$

y tomemos $\Phi = \ker\psi$. Tenemos entonces que $\Phi = {}^{(mE(L)\cap E(K))}/_{mE(K)}$. Para cada $P \mod mE(K) \in \Phi$ podemos elegir $Q_P \in E(L)$ tal que $[m]Q_P = P$. Con lo anterior podemos definir una función:

$$ \begin{aligned} \lambda_P : \mathrm{Gal}(L/K) &\longrightarrow E[m] \\ \sigma &\longmapsto Q_P^\sigma - Q_P, \end{aligned} $$

la cual esta bien definida pues

$$ \begin{aligned} [m](Q_P^\sigma - Q_P) &= [m]Q_P^\sigma - [m]Q_P = ([m]Q_P)^\sigma - ([m]Q_P) \\ &= P^\sigma - P = 0 \end{aligned} $$

Ya que $P \in E(K)$ y de hecho $\lambda_p \in \mathbf{B}^1(\mathrm{Gal}(L/K), E[m])$.

Supongamos que $\lambda_{P'} = \lambda_P$ para algunos $P, P' \in E(K) \cap mE(L)$, entonces se tiene $(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$ para todo $\sigma \in \mathrm{Gal}(L/K)$ y por tanto $Q_P - Q_{P'} \in E(K)$. Esto ultimo implica que

$$ P - P' = [m](Q_P - Q_{P'}) \in mE(K), $$

esto es, $P \mod mE(K) = P' \mod E(K)$. Tenemos entonces una asignación inyectiva

$$ \begin{aligned} \Phi &\longrightarrow \mathbf{B}^1(\mathrm{Gal}(L/K), E[m]) \\ P &\longmapsto \lambda_P. \end{aligned} $$

Como $\mathrm{Gal}(L/K)$ y $E[m]$ son grupos finitos $\mathbf{B}^1(\mathrm{Gal}(L/K), E[m])$ es finito y por tanto se tiene la siguiente sucesión exacta:

$$ 0 \longrightarrow \Phi \longrightarrow {}^{E(K)}/_{mE(K)} \longrightarrow {}^{E(L)}/_{mE(L)} $$

donde ${}^{E(K)}/_{mE(K)}$ queda situado entre dos grupos finitos, y por tanto él también es finito. ■

Asumamos ahora que $E[m] \subset E(K)$. A la luz del teorema anterior probaremos el teorema de Mordell-Weil débil verificando una condición similar para cierta extensión finita de K. Para esto necesitamos la siguiente herramienta

Definición 5.2.4 (función de Kummer)
Sea $P \in E(K)$ y $Q \in E(K)$ tal que $[m]Q = P$, entonces se define la función de Kummer *como sigue:*

$$\begin{aligned} \kappa : E(K) \times \mathrm{Gal}\,(\overline{K}/K) &\longrightarrow E[m] \\ (P, \sigma) &\longmapsto Q^\sigma - Q \end{aligned}$$

Proposición 5.4

1. *La función de Kummer esta bien definida.*

2. *La función de Kummer es bilineal.*

3. *El núcleo por la izquierda de la función de Kummer es $mE(K)$.*

4. *El núcleo por la derecha de la función de Kummer es $\mathrm{Gal}\,(\overline{K}/L)$, donde $L = K([m]^{-1}E(K))$, esto es, es el campo compuesto sobre todos los campos $K(Q)$, donde Q varía en $E(\overline{K})$ y tal que $mQ \in E(K)$.*

   Entonces la función de Kummer define un apareamiento bilineal perfecto

$$E(K)/_{mE(K)} \times \mathrm{Gal}\,(L/K) \longrightarrow E[m].$$

Demostración.

(a) Veremos que $\kappa(P, \sigma)$ no depende de la elección de $Q \in E(K)$ y que $\kappa(P, \sigma) \in E[m]$; En efecto,

$$[m]\kappa(P, \sigma) = [m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = P - P = 0.$$

Por otro lado, notemos que cualquier otro elemento $Q' \in E(\overline{K})$ que cumpla que $[m]Q' = P$ es de la forma[1] $Q' + T$ con $T \in E[m]$ de tal forma que

$$\begin{aligned} \kappa(Q', \sigma) &= (Q')^\sigma - Q' = (Q + T)^\sigma - (Q + T) = Q^\sigma + T^\sigma - Q - T \\ &= (Q^\sigma - Q) + (T^\sigma - T) = (Q^\sigma - Q) \end{aligned}$$

ya que $E[m] \subseteq E(K)$ (y por tanto $T^\sigma = T \,\forall\, \sigma \in \mathrm{Gal}\,(\overline{K}/K)$).

(b) La linealidad en $E(K)$ es directa. Para $\mathrm{Gal}\,(\overline{K}/K)$ se tiene que

$$\begin{aligned} \kappa(P, \sigma\tau) &= Q^{\sigma\tau} - Q = Q^{\sigma\tau} - Q^\tau + Q^\tau - Q = (Q^\sigma - Q)^\tau - (Q^\tau - Q) \\ &= \kappa(P, \sigma)^\tau + \kappa(P, \tau) = \kappa(P, \sigma) + \kappa(P, \tau) \end{aligned}$$

esto ultimo ya que $\kappa(P, \sigma) \in K[m] \subseteq E(K)$.

(c) Sea $P \in E(K)$ tal que $\kappa(P, \sigma) = 0$ para todo $\sigma \in \mathrm{Gal}\,(\overline{K}/K)$; entonces $Q^\sigma = Q \,\forall\, \sigma \in \mathrm{Gal}\,(\overline{K}/K)$ de donde $Q \in E(K)$ y entonces $[m]Q = P \in mE(K)$.

[1] En efecto, si $Q' = Q + T$ entonces $[m]Q' = [m]Q + [m]T = [m]Q = P$ y si $Q' \in E(\overline{K})$ es tal que $[m]Q' = P$, entonces [m](Q'-Q)=0, por lo que $Q' - Q = T \in E[m]$.

(d) Sea $\sigma \in \mathrm{Gal}\,(\overline{K}/K)$ tal que $\kappa(P,\sigma) = 0$ para todo $P \in E(K)$. Entonces $Q^\sigma = Q$ para todo $Q \in E(\overline{K})$ tal que $[m]Q = P$ de igual forma para todo $P \in E(K)$. Se concluye que $Q \in E(L)$ y $\sigma \in \mathrm{Gal}\,(\overline{K}/L)$.

Recíprocamente, si $\sigma \in \mathrm{Gal}\,(\overline{K}/L)$ se tiene que $\kappa(P,\sigma) = Q^\sigma - Q = 0$, ya que $Q \in E(L)$. ■

Alternativamente:
Tomemos la sucesión exacta de G-módulos (con $G = \mathrm{Gal}\,(\overline{K}/K)$)

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0$$

donde $m \geq 2$ es un entero. Tomando la correspondiente sucesión en cohomología de grupos se tiene

$$0 \longrightarrow E[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} \mathbf{H}^1\left(G, E[m]\right) \longrightarrow \mathbf{H}^1\left(G, E(\overline{K})\right) \xrightarrow{[m]} \mathbf{H}^1\left(G, E(\overline{K})\right)$$

y finalmente de aquí extraemos la sucesión exacta corta

$$0 \longrightarrow {E\,(K)}/{mE\,(K)} \xrightarrow{\delta} \mathbf{H}^1\left(G, E[m]\right) \longrightarrow \mathbf{H}^1\left(G, E(\overline{K})\right)[m] \longrightarrow 0$$

a la cual llamaremos *sucesión de Kummer* para E/K.
El morfismo δ en la sucesión exacta anterior es el morfismo de conexión en la sucesión exacta larga en cohomología, el cual podemos calcular explícitamente como sigue.
Sea $P \in E(K)$ y $Q \in E(\overline{K})$ tal que $[m]Q = P$. Anteriormente vimos que $Q^\sigma - Q \in E[m]$ para todo $\sigma \in \mathrm{Gal}\,(\overline{K}/K)$, y por tanto definimos el homomorfismo cruzado:

$$\begin{aligned} f : \mathrm{Gal}\,(\overline{K}/K) &\longrightarrow E[m] \\ \sigma &\longmapsto Q^\sigma - Q \end{aligned}$$

el cual es precisamente el morfismo de Kummer fijando la primera entrada, de donde $f(\sigma) = \kappa(\_\_, \sigma) =: \kappa_P$ y finalmente se tiene $\delta(P) = [\kappa_P]$.
Si suponemos ahora que $E[m] \subseteq E(K)$, entonces $P^\sigma = P$ para todo $\sigma\mathrm{Gal}\,(\overline{K}/K)$ y para todo $P \in E[m]$, de donde concluimos que $\mathbf{B}^1(\mathrm{Gal}\,(\overline{K}/K), E[m]) = 0$. Si ahora nos fijamos en un homomorfismo cruzado $f : \mathrm{Gal}\,(\overline{K}/K) \to E[m]$ se tiene que

$$f(\sigma\tau) = f(\sigma)^\tau + f(\tau) = f(\sigma) + f(\tau)$$

de donde obtenemos que $\mathbf{H}^1\left(\mathrm{Gal}\,(\overline{K}/K), E[m]\right) = \mathbf{Hom}(\mathrm{Gal}\,(\overline{K}/K), E[m])$. Esto ultimo nos dice que δ define un homomorfismo inyectivo

$$0 \longrightarrow {E\,(K)}/{mE\,(K)} \xrightarrow{\delta} \mathbf{Hom}(\mathrm{Gal}\,(\overline{K}/K), E[m])$$

dado por $P \mapsto \kappa(P, \_\_)$ y con esto se proporciona la prueba alterna para los incisos (a),(b),(c) de la proposición anterior.

Ahora si L/K es una extensión de Galois finita, entonces $\mathrm{Gal}\,(\overline{K}/L)$ es normal en $\mathrm{Gal}\,(\overline{K}/K)$ y además

$$\mathrm{Gal}\,(L/K) \cong {\mathrm{Gal}\,(\overline{K}/K)}/{\mathrm{Gal}\,(\overline{K}/L)}$$

y por lo tanto se tiene la sucesión inflación-restricción en cohomología para el G-módulo $E[m]$

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbf{H}^1\left(\mathrm{Gal}\left(L/K\right), E[m]\right) & \xrightarrow{\inf} & \mathbf{H}^1\left(\mathrm{Gal}\left(\overline{K}/K\right), E[m]\right) & \xrightarrow{\mathrm{Res}} & \mathbf{H}^1\left(\mathrm{Gal}\left(\overline{K}/L\right), E[m]\right) \\ & & \uparrow \rho & & \uparrow \delta & & \uparrow \\ 0 & \longrightarrow & \Phi & \longrightarrow & E\left(K\right)/mE\left(K\right) & \longrightarrow & E\left(K\right)/mE\left(K\right) \end{array}$$

y como $\mathrm{Gal}\left(L/K\right)$ y $E[m]$ son finitos, el subgrupo Φ es finito y por tanto se tiene una prueba alternativa del lema anterior pues $\mathbf{H}^1\left(\mathrm{Gal}\left(L/K\right), E[m]\right)$ es finito.

Usando lo anterior podemos probar el teorema de Mordell-Weil débil verificando una condición similar para la extensión L/K. Estudiaremos ahora esta extensión.

Definición 5.2.5
Sea K un campo de números y E/K una curva elíptica. Sea $\nu \in M_K^0$ una valuación discreta. Entonces E se dice que tiene buena reducción *(respectivamente* mala reducción *en ν si E tiene buena reducción (resp. mala reducción) cuando se considera en K_ν.*

Sea $\tilde{E}_\nu/k_\nu$ la ecuación reducida sobre el campo de residuos cuando tomamos una ecuación mínima de Weierstrass para E.

Observación 1
Tomando cualquier ecuación de Weierstrass de E/K, digamos

$$E \quad : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

con discriminante Δ. Entonces para todos salvo un número finito de $\nu \in M_K^0$ se cumple que $\nu(a_i) \geq 0$ para todo i y $\nu(\Delta) = 0$ Por tanto para una tal valuación la ecuación de Weierstrass ya es minimal y por tanto la ecuación reducida $\tilde{E}_\nu/k_\nu$ es no singular. Esto no dice que E tiene buena reducción en ν para todos salvo un número finito de $\nu \in M_K^0$.

Como una implicación directa de 5.3 se tiene el corolario siguiente.

Corolario 5.2.1
Sea $\nu \in M_\nu^0$, de tal forma que $\nu(m) = 0$ y E tiene buena reducción en ν; entonces la aplicación reducción

$$E(K)[m] \longrightarrow \tilde{E}_\nu(k_\nu)$$

es inyectiva.

Proposición 5.5
Sea $L = K([m]^{-1}E(K))$ antes definido.

1. *L/K es una extensión abeliana de exponente m (esto es, $\mathrm{Gal}\left(L/K\right)$ es abeliano y todo elemento de ahí tiene orden un divisor de m).*

2. *Sea*

   $$S = \{\nu \in M_K^0 \mid E \text{ tiene mala reducción en } \nu\} \cup \{\nu \in M_K^0 \mid \nu(m) \neq 0\} \cup M_K^\infty,$$

   Entonces L/K es no ramificada en el complemento de S.

Demostración.
a) Si fijamos $\sigma \in \mathrm{Gal}\,(\overline{K}/K)$ la función de Kummer induce un homomorfismo

$$\begin{aligned} \mathrm{Gal}\,(\overline{K}/K) &\longrightarrow \mathbf{Hom}(E(K), E[m]) \\ P &\longmapsto \kappa(P,\sigma) \end{aligned}$$

cuyo núcleo son aquellos $\sigma \in \mathrm{Gal}\,(\overline{K}/K)$ tales que $\kappa(P,\sigma) = 0$ para todo $P \in E(K)$ y esto si y sólo si $Q^\sigma - Q = 0$ para todo $Q \in E(K) \iff \sigma \in \mathrm{Gal}\,(\overline{K}/L)$. Esto último nos dice que $\mathrm{Gal}\,(\overline{K}/L)$ es normal y por tanto L/K es una extensión de Galois con grupo de Galois

$$\mathrm{Gal}\,(L/K) \cong {\mathrm{Gal}\,(\overline{K}/K)}/{\mathrm{Gal}\,(\overline{K}/L)}$$

y entonces se induce un monomorfismo

$$\rho : \mathrm{Gal}\,(L/K) \longrightarrow \mathbf{Hom}(E(K), E[m])$$

y de aquí que $\mathrm{Gal}\,(L/K)$ es abeliano de exponente m pues si $\sigma \in \mathrm{Gal}\,(L/K)$ se tiene que

$$\begin{aligned} \rho(\sigma^m) &= \kappa(\_\_, \sigma^m) \\ &= \kappa(\_\_, \sigma) + \cdots + \kappa(\_\_, \sigma) \\ &= m\kappa(\_\_, \sigma) = \kappa(m(\_\_), \sigma) \\ &= \kappa(0, \sigma) = 0 \end{aligned}$$

y como ρ es inyectiva, $\sigma^m = 0$.

b) Sea $\nu \in M_K$ con $\nu \notin S$. Tomemos un punto $Q \in E(\overline{K})$ que cumpla $[m]Q \in E(K)$ y la extensión $K' = K(Q)$ de K. Es suficiente ver que K'/K es no ramificada en ν, pues L es el campo compuesto de tales campos K'. Sea $\nu' \in M_{K'}$ un lugar en K' que se extiende a ν y $k'_{\nu'}/k_\nu$ la extensión de los correspondientes campos de residuos. Como E tiene buen reducción en ν, tomando la misma ecuación de Weierstrass se observa que E también tiene buena reducción en ν' y por tanto se tiene la función reducción

$$E(K') \longrightarrow \widetilde{E}_{\nu'}(k'_{\nu'}).$$

la cual por una proposición anterior es inyectiva.

Sea ahora $I_{\nu'/\nu} \subset \mathrm{Gal}\,(K'/K)$ el subgrupo de inercia para ν'/ν y sea $\sigma \in I_{\nu'/\nu}$. De la definición de grupo de inercia se tiene que $\sigma(x) = x$ para todo $x \in k'_{\nu'}$ y por tanto σ actúa trivialmente en $E(k'_{\nu'})$, por lo tanto

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = \tilde{Q} - \tilde{Q} = \tilde{0}$$

Por otro lado se tiene que

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - ([m]Q) = [m]Q - [m]Q = 0$$

y por tanto $Q^\sigma - Q$ es un punto de $E(K')$ de orden m y pertenece al núcleo de la función reducción; siendo ésta aplicación inyectiva, se cumple que $Q^\sigma - Q = 0$, lo cual

significa que todo elemento del subgrupo de inercia actúa trivialmente en K', y por lo tanto es no ramificada en ν'; finalmente L/K es no ramificada en todo $M_K \setminus S$. ■

El siguiente resultado de teoría de números algebraicos nos garantiza que una extensión de campos que goza de las propiedades nombradas en la proposición anterior, debe ser finita.

Proposición 5.6
Sea K un campo de números,$m \geq 2$ un entero y sea también $S \subset M_K$ con $M_K^\infty \in S$, con S finito. Sea L/K la extensión abeliana maximal de exponente m no ramificada fuera de S. Entonces L/K es una extensión finita.

Demostración.
Si la proposición se cumple para una extensión K'/K finita de K, donde $S' \subset M_{K'}$ son los lugares que se restringen a los de S, entonces LK'/K' es finita, ya que es una sub-extensión de la extensión abeliana maximal para K', la cual es finita y de lo anterior L/K es una extensión finita. Entonces podemos asumir que K contiene a μ_m, ya que $K(\mu_m)/K$ es finita y de Galois.

Por otro lado, como el grupo de clases de ideales de K es finito podemos agregar elementos a S de tal forma que el conjunto

$$R_S := \{a \in K | \nu(a) \geq 0 \, \forall \, \nu \in M_K, \, \nu \notin S\}$$

sea un dominio de ideales principales[2] (a R_S le llamaremos el *anillo de S-enteros de K*) y tal que $\nu(m) = 0$ para todo $\nu \notin S$.

El teorema principal de la teoría de Kummer nos dice que en un campo que contiene las raíces m-ésimas de la unidad (μ_m) y donde $\operatorname{char} K \nmid m$, entonces su extensión abeliana maximal de exponente m se obtiene adjuntando raíces m-ésimas (ver por ejemplo [Za, 5.17]). Entonces el campo L es el subcampo más grande de

$$K(\sqrt[m]{a} | a \in K)$$

que es no ramificado fuera de S.

Sea $\nu \in M_K \setminus S$. Si nos fijamos en la ecuación $X^m - a = 0$ en el campo K_ν, es claro que $K_\nu(\sqrt[m]{a})/K_\nu$ es no ramificada si y solo si $\operatorname{ord}_\nu((a)) \equiv 0 \mod m$ (recordemos que $\nu(m) = 0$ y ord_ν es la valuación normalizada asociada a ν). De lo anterior basta escoger un representante por cada clase en $K^*/(K^*)^m$ y por todo lo anterior vemos que

$$L = K(\sqrt[m]{a} | a \in T_S)$$

donde

$$T_S = \{a \in K^*/(K^*)^m | \operatorname{ord}_\nu(a) \equiv 0 \mod m \, \forall \nu \in M_K \setminus S\}.$$

Para terminar la prueba, resta verificar que el conjunto T_S es finito.

Consideremos la función natural

$$R_S^* \longrightarrow T_S;$$

[2] a saber, un lugar por cada ideal primo representante de las diferentes clases de ideales en K.

Este función es suprayectiva. En efecto, sea $a \in K^*$ tal que sea representante de un elemento de T_S. Entonces el ideal aR_S es potencia m-ésima de un ideal no cero en R_S, pues los ideales primos en R_S corresponden precisamente a las valuaciones $\nu \notin S$. Ahora, como R_S es un dominio de ideales principales, existe $b \in K^*$ tal que $aR_S = b^m R_S$, de donde

$$a = ub^m$$

para algún $u \in R_S^*$. Tomando órdenes, se tiene que a y u representan al mismo elemento en T_S, y por lo tanto se cumple la afirmación. Es directo darse cuenta que el núcleo del morfismo contiene al conjunto $(R_S^*)^m$ y por tanto se tiene una función biyectiva

$$R_S^*/(R_S^*)^m \longrightarrow T_S.$$

Por el teorema de las S-unidades de Dirichlet sabemos que R_S^* es finitamente generado, y por tanto T_S es finito, completando la prueba. ■

Ahora estamos en posición de completar la demostración del Teorema de Mordell-Weil débil:

Teorema 5.2.1
Sea K un campo de números, E/K una curva elíptica y $m \geq 2$ un entero. Entonces

$$E(K)/mE(K)$$

es finito.

Demostración.
Sea $L = K([m]^{-1}E(K))$ el campo definido en la proposición 5.4. Dado que $E[m]$ es finito, el apareamiento bilineal perfecto dado en 5.4 nos dice que $E(K)/mE(K)$ es finito si y solo si $\mathrm{Gal}(L/K)$ es finito. Por la proposición 5.5 la extensión L/K tiene ciertas propiedades que según la proposición 5.6 implican que la extensión dada es finita.

5.3. Teorema de Mordell-Weil sobre $\mathbb{Q}$

Fijemos una ecuación de Weierstrass para $E/\mathbb{Q}$ de la forma

$$E : y^2 = x^3 + Ax + B$$

con $A, B \in \mathbb{Z}$. De la sección anterior sabemos que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. Resta entonces definir una función altura en $E(\mathbb{Q})$.

Definición 5.3.1
1. *Sea $t \in \mathbb{Q}$, $t = \frac{p}{q}$ con $(p, q) = 1$. Definimos la* altura *de t, por*

$$H(t) := \text{máx}\{|p|, |q|\}.$$

2. *La* función altura en $E(\mathbb{Q})$ *(relativa a la ecuación de Weierstrass dada) es la función* $h_x : E(\mathbb{Q}) \to \mathbb{R}$ *dada por*

$$h_x(P) = \begin{cases} \log H(x(P)) & si\ P \neq 0 \\ 0 & si\ P = 0 \end{cases}$$

El siguiente lema enuncia las propiedades adecuadas que tiene la función altura antes definida.

Lema 13

1. *Sea* $P_0 \in E(\mathbb{Q})$*. Existe una constante* $C_1 \in \mathbb{R}$*, dependiente de* P_0, A, B*, tal que para todo* $P_0 \in E(\mathbb{Q})$ *se cumple*

$$h_x(P + P_0) \leq 2h_x(P) + C_1.$$

2. *Existe una constante* C_2*, dependiente de* A, B *tal que para todo* $P \in E(\mathbb{Q})$

$$h_x([2]P) \geq 4h_x(P) - C_2.$$

3. *Para cualquier constante* C_3 *el conjunto*

$$\{P \in E(\mathbb{Q}) | h_x(P) \leq C_3\}$$

es finito.

Demostración.
(1) Considerando una constante $C_1 \geq \text{máx}\{h_x(P_0), h_x([2]P_0)\}$ podemos asumir que $P_0 \neq 0$ y $P \neq 0, \pm P_0$. Escribamos

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \quad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$$

donde las fracciones ya están en su forma más reducida. La fórmula para la coordenada homogénea x de suma de dos puntos nos dice que

$$\begin{aligned} x(P + P_0) &= \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0 = \frac{(y - y_0)^2 - (x + x_0)(x - x_0)^2}{(x - x_0)^2} \\ &= \frac{(x + x_0)(xx_0 + A) + 2B - 2yy_0}{(x - x_0)^2} \\ &= \frac{(ad_0^2 + a_0d^2)(aa_0 + Ad_0^2d^2) + 2Bd^4d_0^4 - 2bb_0dd_0}{(ad_0^2 - a_0d^2)^2}. \end{aligned}$$

Al momento de que la fracción se reduce, la altura de $x(P + P_0)$ también se reduce y por tanto se puede estimar que

$$H(x(P + P_0)) \leq C_1' \,\text{máx}\{|a|^2, |d|^2, |bd|\},$$

donde C_1' es una combinación de A, B, a_0, d_0, b_0. El término que sobra es $|bd|$, sin embargo esto se arregla recordando que $P = (\frac{a}{d^2}, \frac{b}{d^3})$ pertenece a la curva elíptica y por tanto se tiene que $b^2 = a^2 + Aad^4 + Bd^6$, de donde se observa que

$$|b| \leq C_1'' \,\text{máx}\{|a|^{3/2}, |d|^3\}$$

y comparando con la primera desigualdad obtenida, llegamos a

$$H(x(P+P_0)) \leq C_1 \max\{|a|^2, |d|^4\} = C_1 H(x(P))^2.$$

Tomando logaritmos se obtiene la conclusión.

(2) Tomemos $C_2 \geq 4h_x(T)$ para todo $E(\mathbb{Q})[2]$; Entonces

$$h_x([2]T) = h_x(0) = 0 \geq 4h_x(T) - C_2 \qquad \text{para } T \in E(\mathbb{Q})[2].$$

Supongamos ahora que $[2]P \neq 0$ y sea $P = (x, y)$. La formula de duplicación está dada por

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Definamos los polinomios homogéneos

$$\begin{aligned} F(X,Y) &= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4 \\ G(X;Z) &= 4X^3Z + 4AXZ^3 + 4BZ^4, \end{aligned}$$

entonces, si $X = x(P) = \frac{a}{b}$ está escrito en su forma más reducida, entonces resulta que

$$x([2]P) = \frac{F(a,b)}{G(a,b)}$$

como cociente de enteros, sin embargo la fracción no está en su forma reducida, además de que buscamos una cota inferior para $H(x([2]P))$, por tanto necesitamos estimar cuanto se pueden cancelar el denominador y el numerador.

Usando el hecho de que los polinomios $F(x,1), G(x,1) \in \mathbb{Q}[x]$ son primos relativos, un cálculo directo nos muestra que existen polinomios $f_1(X,Z), f_2(X,Z) \in \mathbb{Q}[X,Z]$ dados explícitamente por

$$\begin{aligned} f_1(X,Z) &= 12X^3Z + 16aZ^3 \\ g_1(X,Z) &= 3X^3 - 5AXZ^2 - 27BZ^3 \\ f_2(X,Z) &= 4(4A^3 + 27B^2)X^3 - 4A^2BX^2Z + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3 \\ g_2(X,Z) &= A^2BX^3 + A(5A^3 + 32B^2)X^2Z + 2B(13A^3 + 96B^2)XZ^2 - 3A^2(A^3 + 8B^2)Z^3 \end{aligned}$$

de tal suerte que se cumplen las relaciones siguientes en $\mathbb{Q}[X,Z]$:

$$\begin{aligned} f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) &= 4\Delta Z^7 \\ f_2(X,Z)F(X,Z) - g_2(X,Z)G(X,Z) &= 4\Delta X^7, \end{aligned}$$

donde $\Delta = 4A^3 + 27B^2$. Si tomamos $\delta = \gcd(F(a,b), G(a,b))$ (es el término que se cancela en la fracción $x([2]P)$), y de las relaciones anteriormente obtenidas, se observa que δ divide 4Δ y por tanto $|\delta| \leq |4\Delta|$, de donde obtenemos directamente que

$$H(x([2]P)) \geq \frac{\max\{F(a,b), G(a,b)\}}{|4\Delta|}.$$

Por otro lado, las mismas identidades antes obtenidas nos dan las estimaciones siguientes:

$$|4\Delta b^7| \leq 2\,\text{máx}\{f_1(a,b), g_1(a,b)\}\,\text{máx}\{F(a,b), G(a,b)\},$$
$$|4\Delta a^7| \leq 2\,\text{máx}\{f_2(a,b), g_2(a,b)\}\,\text{máx}\{F(a,b), G(a,b)\}.$$

Nuevamente de las expresiones para f_1, f_2, g_1, g_2 se cumple que

$$\text{máx}\{f_1(a,b), f_2(a,b), g_1(a,b), g_2(a,b)\} \leq C\,\text{máx}\{|a|^3, |b|^3\},$$

donde C es una constante que dependiente de A, B. Combinando las últimas tres desigualdades se tiene

$$\text{máx}\{|4\Delta a^7|, |4\Delta b^7|\} \leq 2C\,\text{máx}\{|a|^3, |b^3|\}\,\text{máx}\{F(a,b), G(a,b)\},$$

y cancelando máx$\{|a|^3, |b^3|\}$ obtenemos

$$\frac{\text{máx}\{F(a,b), G(a,b)\}}{|4\Delta|} \geq (2C)^{-1}\,\text{máx}\{|a|, |b|\}.$$

Dado que máx$\{|a|, |b|\} = H(x(P))$, hemos obtenido la estimación requerida

$$H(x([2]P)) \geq (2C)^{-1} H(x(P)).$$

(c) Para cualquier constante C, el conjunto

$$\{t \in \mathbb{Q} | H(t) \leq C_3\}$$

es finito, ya que es directo ver que tiene $(2C+1)^2$ elementos. Ahora, dado cualquier valor de x, hay a lo más 2 valores para y de tal forma que el punto (x, y) es un punto de E. De lo anterior

$$\{P \in E(\mathbb{Q}) | h_x(P) \leq C_3\}$$

es también un conjunto finito. ■

Bibliografía

[Har] Hartshorne R., *Algebraic Geometry*, Graduate Texts in Mathematics, **52**, Springer Verlag, 1987.

[Hüs] usemöller D. *Elliptic Curves*,Graduate Texts in Mathematics, **111**, Springer Verlag, 1987.

[Ful] Fulton W., *Algebraic Curves*, Addison-Wesley, 1989.

[Ap] Apostol Tom M., *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Mathematics, **41**, Springer Verlag (1990).

[Sil] Silverman J. H., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **106**, New York: Springer Verlag (1986).

[Rub] Rubin K., *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer*, Lecture Notes in Mathematics, **1716**, pp. 166-234 (1997)

[Ta] Tate John, *The arithmetic of Elliptic Curves*, Invent. Math., **23**, 179-206 (1974).

[Za] Zaldivar Felipe, *Cohomología de Galois de Campos Locales*, Aportaciones Matemáticas, Sociedad Matemática Mexicana, **17**, 2001.

[McThy] McCarthy Paul J., *Algebraic Extensions of Fields*, Dover Publications Inc., 1991

Índice alfabético