PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO
FACULTAD DE CIENCIAS
INSTITUTO DE MATEMÁTICAS

Sobre el Problema de Grunwald-Wang y una Pregunta de Cassels

TESIS PARA OBTENER EL GRADO DE
MAGÍSTER EN MATEMÁTICAS

AUTOR
Danae Alejandra Soto Layana

PROFESOR GUÍA
Dr. Gabriele Ranieri

Valparaíso, Noviembre de 2018

Este trabajo fue financiado por CONICYT MAGÍSTER NACIONAL 22170657

Índice general

Introducción

En este escrito estudiamos dos problemas muy relacionados entre sí. Uno de ellos, es el principio de divisibilidad local-global sobre un grupo algebraico conmutativo definido sobre un cuerpo de números. Y el otro, es una pregunta de Cassels sobre la divisibilidad del grupo de Tate-Shafarevich.

El principio de divisibilidad local-global, considera a A un grupo algebraico conmutativo definido sobre un cuerpo de números k y q un entero positivo. Supongamos que $P \in A(k)$ es un punto tal que, para todas las completaciones v de k, existe $D \in A(k_v)$ tal que $P = qD$. ¿Cuándo podemos concluir que existe $D \in A(k)$ tal que $P = qD$?

Los primeros en estudiar el principio de divisibilidad local-global sobre grupos algebraicos conmutativos son Dvornicich y Zannier [8, 9]. Ellos obtuvieron respuestas parciales al problema trabajando particularmente con curvas elípticas. Creutz [6] también estudia este problema sobre curvas elípticas y presenta un contraejemplo donde el principio de divisibilidad local global no tiene respuesta afirmativa cuando $p \in \{2, 3\}$.

Por otro lado, sea A una variedad abeliana definida sobre un cuerpo de números k. Para todo número primo p decimos que el grupo de Tate-Shafarevich $Ш^1(G_k, A)$ es $p-$divisible en el grupo $H^1(G_k, A(\overline{k}))$ si y solo si

$$Ш^1(G_k, A(\overline{k})) \subseteq p^n H^1(G_k, A(\overline{k})), \forall n \in \mathbb{N}^*.$$

La pregunta de Cassels es: ¿cuál es el conjunto de números primos p tales que el grupo de Tate-Shafarevich es $p-$divisible?

En el año 2.013, Creutz presenta un contraejemplo donde el grupo de Tate-Shafarevich no es 2-divisible [5]. Posteriormente, Çiperiani y Stix trabajan en este problema y dan un acercamiento a una respuesta positiva, estudiando la trivialidad del grupo de Tate-Shafarevich. También, Gillibert y Ranieri [10] estudian ambas preguntas principalmente sobre variedades abelianas polarizadas y determinan condiciones para que ambos problemas tengan una respuesta positiva.

Los dos problemas mencionados, pueden ser tratados utilizando herramientas de cohomología las cuales se encuentran en el capítulo 1 y el ápendice de este escrito. Es importante mencionar, que los dos problemas tienen una interpretación en común, es decir, con la ayuda de la cohomología nos reducimos a un único problema. Lo anterior se explica en profundidad en el capítulo 2, donde nos reducimos a estudiar el principio de divisibilidad local-global sobre $H^r(G_k, A(\overline{k}))$.

En el capítulo 3, presentaremos el siguiente criterio que nos permite dar una respuesta parcial a los dos problemas expuestos anteriormente, en el caso particular de las curvas elípticas definidas sobre un cuerpo de números k.

Criterio. *Sea p un número primo. Sea k un cuerpo de números que no contiene a $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Sea E una curva elíptica definida sobre k tal que para toda E' curva elíptica definida sobre k, k-isogena a E, tal que $E'[p] \cap E'(k) = \{0\}$. Entonces, para todo $n \in \mathbb{N}$*

$$H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) = 0.$$

También vamos a explicar cómo a partir del criterio anterior y de unos resultados muy profundos de Merel [13] se cumple el siguiente teorema:

Teorema. *Para todo entero $d \geq 1$ existe una constante $C(d)$ que depende de d, tal que para todo cuerpo de números k que cumple $[k : \mathbb{Q}] \leq d$ y para toda curva elíptica definida sobre k y para todo número primo $p > C(d)$, el principio de divisibilidad local-global para p^n sobre $E(\overline{k})$ se sostiene y se cumple que el grupo de Tate-Shafarevich es $p-$divisible.*

Este criterio ya ha sido demostrado independientemente para Paladino, Ranieri y Viada [17]. Pero, la demostración presentada en esta tesis es más simple y elemental pues, las herramientas utilizadas son en gran parte teoría básica de grupos.

Capítulo 1

Definición de los Grupos de Cohomología

En este primer capítulo, definiremos los Grupos de Cohomología a través de las cadenas no homogéneas. Para esto es necesario recordar algunas definiciones, propiedades y teoremas importantes de la categoría de los G-módulos, los cuales quedan sin demostración pero pueden ser consultados en [14] y [16]. También, se presentarán distintos homomorfismos definidos sobre los Grupos de Cohomología, entre ellos el de Restricción, Inflación y Corestricción, quienes serán útiles en los próximos capítulos. Finalmente, es importante destacar que en el apéndice se mostrará la definición de los Grupos de Cohomología vía Funtores Derivados. Esta definición que utiliza resoluciones inyectivas es equivalente a la definición por cadenas no homogéneas.

1.1. Categorías de G-módulos

Definición 1.1. *Sea G un grupo. Un $G-$módulo izquierdo es un grupo abeliano M con una función*

$$\begin{array}{rccc} \bullet & : & G \times M & \to & M \\ & & (g, m) & \to & g \bullet m \end{array}$$

que satisface que, $\forall g, g' \in G, m, m' \in M$

a) $g \bullet (m + m') = g \bullet m + g \bullet m'$.

b) $g \bullet (g' \bullet m) = (gg') \bullet m$, $1_G \bullet m = m$.

De forma equivalente, un $G-$módulo izquierdo es un grupo abeliano M con un homomorfismo de grupos

$$\begin{array}{rccc} \Phi & : & G & \longrightarrow & \text{Aut(M)} \\ & & g & \longrightarrow & \Phi_g : M \to M \\ & & & & m \to g \bullet m. \end{array}$$

Observación 1.2. *A menos que se diga de otro modo, consideramos de ahora en adelante a todo $G-$módulo como izquierdo.*

Definición 1.3. *Sea G un grupo y sean M, N $G-$módulos. Un homomorfismo de $G-$módulos es una función $\alpha : M \to N$ que satisface las siguientes condiciones:*

a) $\alpha(m + m') = \alpha(m) + \alpha(m'), \quad \forall m, m' \in M$. *Es decir, α es un homomorfismo de grupos abelianos.*

b) $\alpha(g \bullet m) = g \bullet (\alpha(m)), \quad \forall g \in G, m \in M$.

1.2. Definición de $\mathbf{H}^r$ vía cadenas no homogéneas

Para esta sección consideremos M un $G-$módulo.

Definición 1.4. *Una cadena no homogénea de grado r es una función*

$$\psi : \underbrace{G \times G \times ... \times G}_{r-veces} \to M.$$

El conjunto de todas las r cadenas no homogéneas se denota $C^r(G, M)$ y es un grupo de forma natural con la suma de funciones.

Observación 1.5. *El conjunto $G^0 = 1_G$, entonces $C^0(G, M) = M$.*

Definición 1.6. *Sea $\psi \in C^r(G, M)$ se define la función*

$$d^r : C^r(G, M) \to C^{r+1}(G, M)$$

por

$$(d^r\psi)(g_1, ..., g_{r+1}) = g_1\psi(g_2, ..., g_{r+1}) + \sum_{i=1}^{r}(-1)^i\psi(g_1, ..., g_i \cdot g_{i+1}, ..., g_{r+1}) + (-1)^{r+1}\psi(g_1, ..., g_r).$$

Además, se define el grupo $r-$cociclos no homogéneos por $Z^r(G, M) = \mathrm{Ker(d^r)}$ y el grupo de los $r-$cobordes no homogéneos por $B^r(G, M) = \mathrm{Im(d^{r-1})}$. Como se cumple que $d^{r+1} \circ d^r = 0, \forall r \in \mathbb{N}$ se obtiene que $B^r(G, M)$ es un subgrupo de $Z^r(G, M)$.

Con todas las definiciones y propiedades anteriores estamos en condiciones de presentar la definición de los Grupos de Cohomología vía cadenas no homogéneas.

Definición 1.7. *Para $r \geq 0$ el grupo*

$$H^r(G, M) := \frac{Z^r(G, M)}{B^r(G, M)}$$

*es llamado el **r-ésimo Grupo de Cohomología** de G con coeficientes en M.*

Para $r = 0$ el Grupo de Cohomología $H^0(G, M) = \dfrac{Z^0(G, M)}{B^0(G, M)}$. Por definición de los cobordes no homogéneos, $B^0(G, M) = \mathrm{Im}(\mathrm{d}^{-1})$ que por convención es 0. De esta forma, el $0-$Grupo de Cohomología admite la siguiente interpretación:

$$\begin{aligned} H^0(G, M) &= Z^0(G, M) \\ &= \mathrm{Ker}(\mathrm{d}^0) \\ &= \{m \in M : g \bullet m = m, \forall g \in G\} \\ &= M^G. \end{aligned}$$

Es decir, el Grupo $H^0(G, M)$ son los elementos dejados fijos por la acción de G.

Para $r = 1$, el Primer Grupo de Cohomología es

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)}.$$

Mediante la definición de d^1 obtenemos que el grupo de $1-$cociclos no homogéneos es:

$$\begin{aligned} Z^1(G, M) &= \{\psi : G \to M : (d^1\psi)(g_1, g_2) = 0\} \\ &= \{\psi : G \to M : \psi(g_1 g_2) = g_1 \bullet \psi(g_2) + \psi(g_1)\}. \end{aligned}$$

Las funciones que cumplen la condición $\psi(g_1 g_2) = g_1 \bullet \psi(g_2) + \psi(g_1)$ son llamadas homomorfismos cruzados.

Ahora, describiremos los elementos de $B^1(G, M)$. Dado $m \in M = C^0(G, M)$ tenemos que

$$\begin{aligned} d^0(m) \ : \ G &\to M \\ g &\to (d^0(m))(g) = g \bullet m - m. \end{aligned}$$

Las funciones anteriores son llamadas homomorfismo cruzados principales.

De lo anterior, el Primer Grupo de Cohomología tiene la siguiente interpretación:

$$H^1(G, M) = \frac{\text{Homomorfismos Cruzados}}{\text{Homomorfismos Cruzados Principales}}$$

Observación 1.8. *Si la acción de G sobre M es trivial tenemos que:*

$$g \bullet m - m = 0, \forall m \in M.$$
$$\psi(g_1 g_2) = g_1 \bullet \psi(g_2) + \psi(g_1) = \psi(g_2) + \psi(g_1).$$

Entonces, $B^1(G, M) = 0$ y $Z^1(G, M) = \mathrm{Hom(G, M)}$, es decir,

$$H^1(G, M) = \mathrm{Hom(G, M)}.$$

Lema 1.9. *Sea G un grupo cíciclo de orden m con σ un generador de G. Sea M un $G-$módulo. Definamos* $\mathrm{Nm_G : M \to M}$ *por* $\mathrm{Nm_G(m) = \sum_{\sigma \in G} \sigma \bullet m}$. *Entonces, $\psi \to \psi(\sigma)$ define un isomorfismo entre*

$$H^1(G, M) \to \frac{\mathrm{Ker(Nm_G)}}{(\sigma - 1)M} \quad .$$

Demostración. Sea ψ un homomorfismo cruzado, entonces cumple lo siguiente:

$$\psi(1_G) = \psi(1_G \cdot 1_G) = 1 \bullet \psi(1_G) + \psi(1_G) = 2\psi(1_G)$$
$$\psi(1_G) = 0 \qquad (1)$$

Entonces,

$$\begin{aligned} \psi(\sigma^2) &= \sigma\psi(\sigma) + \psi(\sigma) \\ \psi(\sigma^3) &= \sigma^2\psi(\sigma) + \sigma\psi(\sigma) + \psi(\sigma) \\ &\vdots \\ \psi(\sigma^m) &= \sigma^{m-1}\psi(\sigma) + ... + \sigma\psi(\sigma) + \psi(\sigma) = \mathrm{Nm_G}(\psi(\sigma)). \end{aligned}$$

Como σ es un generador del grupo G entonces $\sigma^m = 1_G$. Utilizando (1), se obtiene que $0 = \psi(\sigma^m) = \mathrm{Nm_G}(\psi(\sigma))$. De esta forma, $\psi(\sigma) \in \mathrm{Ker(Nm_G)}$. Observemos que:

ψ es homomorfismo cruzado principal $\Leftrightarrow \psi(\sigma) = \sigma \bullet m - m$ para algún m $\Leftrightarrow \psi(\sigma) \in (\sigma - 1)M$.

Usando el primer Teorema de Homomorfismos de Grupos podemos concluir que

$$H^1(G, M) \simeq \frac{\mathrm{Ker(Nm_G)}}{(\sigma - 1)M}.$$

□

1.3. Funciones definidas sobre los Grupos de Cohomología

A continuación mostraremos algunas de las funciones más importantes definidas sobre los Grupos de Cohomología.

Sean G, G' grupos y sean M y M', G y respectivamente G' módulos. Sean

$$\alpha : G' \to G \qquad \beta : M \to M'$$

homomorfismos de grupos. Diremos que son compatibles si verifican que

$$\beta(\alpha(g') \bullet m) = g' \bullet (\beta(m)), \forall m \in M, g' \in G'.$$

Entonces, (α, β) entre los complejos $C^\bullet(G, M)$ y $C^\bullet(G', M')$ definen los siguientes homomorfismos (para definición de complejos ver [7, Section 17.1])

$$\begin{array}{rccc} F^r_{\alpha,\beta} & : & C^r(G,M) & \to & C^r(G',M') \\ & & \phi & \to & \beta \circ \phi \circ \alpha^r \end{array}$$

que hacen que el siguiente diagrama conmute.

$$\begin{array}{ccccccccc} C^0(G,M) & \xrightarrow{d^0} & C^1(G,M) & \longrightarrow \ldots \longrightarrow & C^r(G,M) & \xrightarrow{d^r} & C^{r+1}(G,M) & \longrightarrow \\ \downarrow{\scriptstyle F^0_{\alpha,\beta}} & & \downarrow{\scriptstyle F^1_{\alpha,\beta}} & & \downarrow{\scriptstyle F^r_{\alpha,\beta}} & & \downarrow{\scriptstyle F^{r+1}_{\alpha,\beta}} & \\ C^0(G',M') & \xrightarrow[d^0]{} & C^1(G',M') & \longrightarrow \ldots \longrightarrow & C^r(G',M') & \xrightarrow[d^r]{} & C^{r+1}(G,M) & \longrightarrow \end{array}$$

Además, inducen homomorfismos entre los Grupos de Cohomología

$$\begin{array}{rccc} \Phi^r & : & H^r(G,M) & \to & H^r(G',M') \\ & & [Z] & \to & [\beta \circ Z \circ \alpha^r]. \end{array}$$

Definición 1.10. *Sea H un subgrupo de G, α la inclusión de H en G y β la identidad del $G-$módulo M. Los homomorfismos α y β son compatibles e inducen en los grupos de cohomología el* ***homomorfismo restricción****.*

$$Res : H^r(G,M) \to H^r(H,M).$$

Definición 1.11. *Sea H subgrupo normal de G, $\alpha : G \to G/H$ la proyección canónica y sea β la inclusión de M^H en M. Los homomorfismos α y β son compatibles e inducen en los grupos de cohomología el* ***homomorfismo inflación****.*

$$Inf : H^r(G/H, M^H) \to H^r(G,M).$$

Para definir otro homomorfismo sobre los Grupos de Cohomología es importante conocer la definición de los módulos inducidos y el Lema de Shapiro, que se presentarán a continuación.

Definición 1.12. *Sea G un grupo y $H \leq G$. Sea M un $H-$módulo se define el siguiente conjunto de funciones* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M}) = \{\phi : \mathrm{G} \to \mathrm{M} : \phi(\mathrm{hg}) = \mathrm{h} \bullet \phi(\mathrm{g}), \forall \mathrm{h} \in \mathrm{H}\}$.

Ejemplo 1.13. *El conjunto* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M})$ *es un $G-$módulo con las siguientes operaciones:*

a) $(\phi + \psi)(x) = \phi(x) + \psi(x), \quad \forall \phi, \psi \in \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M}), \forall \mathrm{x} \in \mathrm{G}.$

b) $(g \bullet \phi)(x) = \phi(xg), \quad \forall \phi \in \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M}), \forall \mathrm{x}, \mathrm{g} \in \mathrm{G}.$

Lema 1.14 (Lema de Shapiro)**.** *Sea H un subgrupo de G. Para cualquier H-módulo N, existe un isomorfismo canónico entre*

$$H^r(G, \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{N})) \simeq \mathrm{H}^{\mathrm{r}}(\mathrm{H}, \mathrm{N}), \qquad \forall \mathrm{r} \geq 0.$$

Demostración. Ver [14, Proposition 1.11]. □

Definición 1.15. *Sea M un $G-$módulo y sabemos que $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M})$ es también un $G-$módulo. Sea H un subgrupo de índice finito de G y sea S el conjunto de representantes de las coclases izquierdas de H en G. Consideremos α como la identidad de G y consideremos β como el isomorfismo canónico de $G-$módulos dado por*

$$\begin{array}{rccc} \beta & : & \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M}) & \to & M \\ & & \phi & \to & \displaystyle\sum_{s\in S} s \bullet \phi(s^{-1}). \end{array}$$

*Los homomorfismos α y β son compatibles por lo tanto tenemos un homomorfismo entre los Grupos de Cohomología $\Phi^r : H^r(G, \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M})) \to \mathrm{H^r(G, M)}$. Además, por el Lema de Shapiro 1.14 tenemos que $H^r(H, M) \simeq H^r(G, \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{M}))$. Entonces se define el **homomorfismo corestricción** como la composición del isomorfismo de Shapiro con Φ^r. Es decir,*

$$Cor : H^r(H, M) \to H^r(G, M).$$

Teorema 1.16 (Inflación - Restricción)**.** *Sea H un subgrupo normal de G, y sea M un $G-$ módulo. Sea r un entero, con $r > 0$. Si $H^i(H, M) = 0$ para todo i con $0 < i < r$ entonces la secuencia*

$$0 \to H^r(G/H, M^H) \to H^r(G, M) \to H^r(H, M)$$

es exacta.

Demostración. Ver [14, Proposition 1.34]. □

Teorema 1.17. *Sea H un subgrupo de G de índice finito. La composición*

$$Cor \circ Res : H^r(G, M) \to H^r(G, M)$$

es multiplicación por $[G : H]$.

Demostración. Ver [14, Proposition 1.30]. □

A continuación, presentaremos un resultado muy importante, que será utilizado en varias ocasiones en los siguientes capítulos.

Corolario 1.18. *Sea G un grupo y M un $G-$módulo. Si G y M son grupos finitos y* $\mathrm{m.c.d}(|\mathrm{G}|, |\mathrm{M}|) = 1$ *entonces $H^r(G, M) = 0, \forall r \geq 1$.*

Demostración. Consideremos H subgrupo de G igual a la identidad. Al realizar la composición de los homomorfismos restricción y corestricción se obtiene por Teorema 1.17, lo siguiente:

$$Cor \circ Res(Z) = [G : H]Z = |G|Z, \quad \forall Z \in H^r(G, M).$$

Por Corolario 1.12 de [14] se cumple $H^r(H, M) = 0, \forall r \geq 1$, si $H = 1_G$. Entonces, se cumple que $Cor \circ Res(Z) = 0$ para todo cociclo $Z \in H^r(G, M)$. De ambas igualdades concluimos que $|G|H^r(G, M) = 0$. Por otro lado, sea $Z \in H^r(G, M)$ se cumple que $\forall r \geq 1$ y $\forall \sigma \in G^r, Z_\sigma \in M$ entonces $|M|Z_\sigma = 0$, lo que nos permite concluir que $|M|H^r(G, M) = 0, \forall r \geq 1$.

Luego (m.c.d(|M|, |G|))$\mathrm{H^r(G, M)} = 0, \forall \mathrm{r} \geq 1$, como el máximo común divisor es 1 por hipótesis, podemos concluir que $H^r(G, M) = 0, \forall r \geq 1$. □

Para finalizar, daremos un ejemplo del Corolario 1.18, que será citado en los capítulos siguientes.

Ejemplo 1.19. *Sea $G \leq GL_2(\mathbb{Z}/p\mathbb{Z})$ y sea M un $G-$módulo. Si p no divide al orden de G entonces $H^1(G, M) = 0$.*

Demostración. Como M es un $G-$módulo cumple que $p^n M = 0, \forall n \in \mathbb{N}$. Si $Z \in H^1(G, M)$, se cumple que $p^n Z_\sigma = 0, \forall \sigma \in G, n \in \mathbb{N}$, entonces $p^n H^1(G, M) = 0$. Por demostración del Corolario 1.18 tenemos que (m.c.d($\mathrm{p^n}$, |G|))$\mathrm{H^1(G, M)} = 0$. Como p no divide a $|G|$, entonces el máximo común divisor entre p^n y $|G|$ es 1, lo que implica que $H^1(G, M) = 0$. □

Capítulo 2

Algunas preguntas sobre el Grupo de Tate-Shafarevich

En este segundo capítulo presentaremos la definición de la sucesión de Kummer y el grupo de Tate-Shafarevich que se encuentran en [4]. Luego, expondremos el Principio de Divisibilidad Local-Global, haciendo énfasis en los casos particulares de este que son el Problema de Grunwald-Wang y el Problema de Cassels. Además, daremos a conocer los resultados más importantes sobre estos problemas y explicitaremos la relación entre ellos mediante un Teorema de Sansuc. Lo anterior puede ser consultado en [4], [9] y [10].

2.1. Definición de la Sucesión de Kummer y el Grupo de Tate Shafarevich

Comenzaremos esta sección con la definición de la sucesión de Kummer. Para esto, es importante considerar a L cuerpo perfecto y $\overline{L}$ su clausura algebraica. Presentaremos la siguiente notación que será utilizada desde esta sección en adelante.

Notación 2.1.

- $G_L := \mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L})$.

Sea n un entero positivo tal que $n \geq 2$ y sea A una variedad abeliana definida sobre L. Sea $A[n] = \{P \in A(\overline{L}) : nP = 0\}$ el subgrupo de los puntos de $n-$torsión de $A(\overline{L})$. Consideremos i como la inclusión y $\cdot n$ como la multiplicación por n. La siguiente sucesión es exacta

$$0 \to A[n] \xrightarrow{i} A(\overline{L}) \xrightarrow{\cdot n} A(\overline{L}) \to 0 \tag{2.1}$$

y es llamada sucesión de Kummer.

La sucesión de Kummer es una sucesión exacta de G_L-módulos, a la cual podemos asociar una sucesión exacta larga formada por los grupos de cohomología (para más detalles revisar la propiedad (4.4, d) del ápendice), donde obtenemos lo siguiente:

$$0 \to A[n](L) \xrightarrow{i} A(L) \xrightarrow{\cdot n} A(L) \to H^1(G_L, A[n]) \to H^1(G_L, A(\overline{L})) \to ... \to H^r(G_L, A(\overline{L})) \to ...$$

De la sucesión exacta larga anterior, podemos construir la siguiente sucesión exacta corta

$$0 \xrightarrow{i} A(L)/nA(L) \xrightarrow{\alpha} H^1(G_L, A[n]) \xrightarrow{\beta} H^1(G_L, A(\overline{L}))[n] \to 0 \quad .$$

Sea ahora k cuerpo de números y consideremos las siguientes notaciones:

Notaciones 2.2.

- M_k *conjuntos de los lugares de* k.
- $G_k := \mathrm{Gal}(\overline{\mathrm{k}}/\mathrm{k})$.
- $\forall v \in M_k, G_{k_v} := \mathrm{Gal}(\overline{\mathrm{k_v}}/\mathrm{k_v})$.

Podemos construir la sucesión de Kummer para k y para todas las completaciones k_v de k. Realizando el mismo proceso anterior obtenemos las siguientes sucesiones exactas cortas:

$$0 \xrightarrow{i} A(k)/nA(k) \xrightarrow{\alpha} H^1(G_k, A[n]) \xrightarrow{\beta} H^1(G_k, A(\overline{k}))[n] \to 0 \quad . \tag{2.2}$$

$$0 \xrightarrow{i} A(k_v)/nA(k_v) \xrightarrow{\alpha} H^1(G_{k_v}, A[n]) \xrightarrow{\beta} H^1(G_{k_v}, A(\overline{k_v}))[n] \to 0, \forall v \in M_k. \tag{2.3}$$

Aplicando el homomorfismo restricción [Definición 1.10] entre la sucesión (2.2) y el producto de la sucesión (2.3) para cada lugar $v \in M_k$, obtenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc}
0 & \xrightarrow{i} & A(k)/nA(k) & \xrightarrow{\alpha} & H^1(G_k, A[n]) & \xrightarrow{\beta} & H^1(G_k, A(\overline{k}))[n] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \prod_v i_v} & & \downarrow{\scriptstyle \prod_v res_v} & & \downarrow{\scriptstyle \prod_v res_v} & & \\
0 & \xrightarrow{i} & \prod_{v\in M_k} A(k_v)/nA(k_v) & \xrightarrow{\alpha} & \prod_{v\in M_k} H^1(G_{k_v}, A[n]) & \xrightarrow{\beta} & \prod_{v\in M_k} H^1(G_{k_v}, A(\overline{k_v}))[n] & \longrightarrow & 0
\end{array}$$

Definiremos el grupo de Tate-Shafarevich para los puntos de $n-$torsión de una variedad abeliana A como el kernel del primer homomorfismo $\prod_v res_v$ del diagrama anterior, es decir,

$$Ш^1(G_k, A[n]) = \mathrm{Ker}\Big(\mathrm{H}^1(\mathrm{G_k}, \mathrm{A[n]}(\overline{\mathrm{k}})) \xrightarrow{\prod_{\mathrm{v}} \mathrm{res_v}} \prod_{\mathrm{v}\in \mathrm{M_k}} \mathrm{H}^1(\mathrm{G_{k_v}}, \mathrm{A[n]}(\overline{\mathrm{k_v}}))\Big)$$

con los homomorfismos restricción res_v inducidos por la incrustación de $k \hookrightarrow k_v$. La definición anterior del Grupo de Tate-Shafarevich es equivalente a

$$Ш^1(G_k, A[n]) = \bigcap_{v \in M_k} \mathrm{Ker}\Big(\mathrm{H^1(G_k, A[n](\overline{k}))} \xrightarrow{\mathrm{res_v}} \mathrm{H^1(G_{k_v}, A[n](\overline{k_v}))}\Big).$$

Por lo tanto, podemos entender al Grupo de Tate-Shafarevich como los elementos del grupo $H^1(G_k, A[n])$ que se vuelven triviales en todas las completaciones v de k.

Para finalizar esta sección, definiremos también, el grupo de Tate-Shafarevich para $A(\overline{k})$ por lo siguiente:

$$Ш^1(G_k, A(\overline{k})) = \mathrm{Ker}\Big(\mathrm{H^1(G_k, A(\overline{k}))} \xrightarrow{\prod_{\mathrm{v}} \mathrm{res_v}} \prod_{\mathrm{v} \in \mathrm{M_k}} \mathrm{H^1(G_{k_v}, A(\overline{k_v}))}\Big).$$

2.2. Problema de Grunwald-Wang y Problema de Cassels

Consideremos k un cuerpo de números, $\overline{k}$ su clausura algebraica, A una variedad abeliana definida sobre el cuerpo k y n y r enteros no negativos. Diremos que un elemento ρ del grupo de cohomología $H^r(G_k, A(\overline{k}))$ es divisible por n si existe $\rho' \in H^r(G_k, A(\overline{k}))$ tal que $n\rho' = \rho$. Además, ρ es localmente divisible por n si, para todos los lugares v de k, existe $\rho'_v \in H^r(G_{k_v}, A(\overline{k}))$ tal que $n\rho'_v = res_v(\rho)$. La pregunta natural que surge en este momento es, ¿todo elemento localmente divisible por n es globalmente divisible? Cuando se tiene respuesta positiva a esta pregunta, diremos que el principio de divisibilidad local-global para n se sostiene sobre $H^r(G_k, A(\overline{k}))$ [Ver 6].

A continuación, daremos condiciones necesarias para que el principio de divisibilidad local-global tenga una respuesta positiva. Para lograr este objetivo, es necesario extender las definiciones de los grupos de Tate-Shafarevich, presentadas en la sección anterior, para $r > 1$. Por lo tanto, se define el r-ésimo grupo de Tate-Shafarevich para una variedad abeliana A definida sobre un cuerpo de números k como:

$$Ш^r(G_k, A(\overline{k})) = \mathrm{Ker}\Big(\mathrm{H^r(G_k, A(\overline{k}))} \xrightarrow{\prod_{\mathrm{v}} \mathrm{res_v}} \prod_{\mathrm{v} \in \mathrm{M_k}} \mathrm{H^r(G_{k_v}, A(\overline{k_v}))}\Big).$$

Y se define el $r-$ésimo grupo de Tate-Shafarevich para $A[n]$ como:

$$Ш^r(G_k, A[n]) = \mathrm{Ker}\Big(\mathrm{H^r(G_k, A[n](\overline{k}))} \xrightarrow{\prod_{\mathrm{v}} \mathrm{res_v}} \prod_{\mathrm{v} \in \mathrm{M_k}} \mathrm{H^r(G_{k_v}, A[n](\overline{k_v}))}\Big).$$

También, consideremos el siguiente diagrama conmutativo formada por dos sucesiones

de Kummer, cuyos grupos son G_k y G_{k_v} módulos respectivamente:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[n] & \xrightarrow{i} & A(\overline{k}) & \xrightarrow{\cdot n} & A(\overline{k}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in M_k} A[n](\overline{k_v}) & \xrightarrow{i_v} & \prod_{v\in M_k} A(\overline{k_v}) & \xrightarrow{\cdot n_v} & \prod_{v\in M_k} A(\overline{k_v}) & \longrightarrow & 0 \end{array} .$$

Por propiedad (4.4, e) del ápendice, podemos asociar a cada sucesión de Kummer una sucesión exacta larga formada por grupos de cohomología, los cuales respetan la conmutatividad del diagrama, es decir, obtenemos lo siguiente:

$$\begin{array}{ccccccccc} \ldots & \longrightarrow & H^r(G_k, A(\overline{k})) & \xrightarrow{\cdot n} & H^r(G_k, A(\overline{k})) & \xrightarrow{\delta_n} & H^{r+1}(G_k, A[n]) & \longrightarrow & \ldots \\ & & \downarrow \prod_v res_v & & \downarrow \prod_v res_v & & \downarrow \prod_v res_v & & \\ \ldots & \longrightarrow & \prod_{v\in M_k} H^r(G_{k_v}, A(\overline{k_v})) & \xrightarrow{\cdot n_v} & \prod_{v\in M_k} H^r(G_{k_v}, A(\overline{k_v})) & \xrightarrow{\delta_{n_v}} & \prod_{v\in M_k} H^{r+1}(G_{k_v}, A[n]) & \longrightarrow & \ldots \end{array}$$

Notar que $\rho \in H^r(G_k, A(\overline{k}))$ es divisible por n si existe $\rho' \in H^r(G_k, A(\overline{k}))$ tal que $n\rho' = \rho$, entonces por la exactitud de la sucesión tenemos que $\rho \in \mathrm{Ker}(\delta_{\mathrm{n}})$, es decir, $\delta_n(\rho) = 0$. En cambio, ρ es localmente divisible si para todos los lugares v de k, existe $\rho'_v \in H^r(G_{k_v}, A(\overline{k_v}))$ tal que $n_v\rho'_v = res_v(\rho)$, nuevamente por la exactitud de la sucesión, se cumple que $res_v(\rho) \in \mathrm{Ker}(\delta_{\mathrm{n_v}})$. Usando la conmutatividad del diagrama se obtiene que $\delta_n(\rho) \in \mathrm{Ker}(\mathrm{res_v})$, para todo $v \in M_k$, es decir, $\delta_n(\rho) \in Ш^{r+1}(G_k, A[n])$. Por lo tanto, podemos concluir que el principio de divisibilidad local-global para n se sostiene sobre $H^r(G_k, A(\overline{k}))$, si el grupo $Ш^{r+1}(G_k, A[n])$ es trivial.

Es importante mencionar, que si $r \geq 2$ el principio de divisibilidad local-global sobre $H^r(G_k, A(\overline{k}))$ se sostiene [22, Theorem 3.1]. Debido a esta razón, nos interesa estudiar los casos en que $r = 0$ o $r = 1$. Para ello, expondremos los resultados de los autores Çiperiani y Stix, Dvornicich y Zannier, Gillibert y Ranieri.

Para contestar la pregunta del principio de divisibilidad local-global para cualquier entero positivo q, nos interesa estudiar los grupos $Ш^1(G_k, A[q])$ y $Ш^2(G_k, A[q])$. Por la identidad de Bézout, basta resolverlo para potencias de primos, es decir, para los grupos $Ш^1(G_k, A[p^n])$ y $Ш^2(G_k, A[p^n])$. Consideremos ahora, A^t la variedad dual de A [15, Definition 2.8, page 74]. Un profundo Teorema llamado dualidad de Poitou-Tate [16, Theorem 8.6.7] nos dice que si $Ш^1(G_k, A^t[p^n])$ es trivial entonces $Ш^2(G_k, A[p^n])$ es trivial.

Por lo tanto, la pregunta natural que nos surge en estos momentos es, ¿cómo aseguramos la trivialidad de $Ш^1(G_k, A[p^n])$? Para dar una respuesta, expondremos la siguiente definición de Sansuc que puede ser encontrada en [19]:
Consideremos Σ un subconjunto de lugares de M_k, se define

$$Ш^1_\Sigma(G_k, A[p^n])) = \bigcap_{v \notin \sum} \mathrm{Ker}(\mathrm{H^1(G_k, A[p^n]) \to H^1(G_{k_v}, A[p^n]))} \quad \text{y}$$
$$Ш^1_\omega(G_k, A[p^n])) = \bigcup_{\Sigma \text{ finito}} Ш^1_\Sigma(G_k, A[p^n]).$$

Sansuc observó que $Ш^1_\omega(G_k, A[p^n])$ es un grupo y es claro que, $Ш^1(G_k, A[p^n])$ es un subgrupo de $Ш^1_\omega(G_k, A[p^n])$ para todo $n \in \mathbb{N}^*$. Entonces, nos reducimos a estudiar la trivialidad de $Ш^1_\omega(G_k, A[p^n])$.

Sansuc [19, Lemme 1.2] y Dvornicich y Zannier [8] muestran que $Ш^1_\omega(G_k, A[p^n])$ es isomorfo a un cierto subgrupo de $H^1(\mathrm{Gal(k(A[p^n]), k), A[p^n])}$ llamado $H^1_{\mathrm{loc}}(\mathrm{Gal(k(A[p^n])/k), A[p^n])}$, definido de la siguiente forma:

$$H^1_{\mathrm{loc}}(\mathrm{Gal(k(A[p^n])/k), A[p^n])} = \bigcap_{\substack{\mathrm{C \leq Gal(k(A[p^n])/k)} \\ \text{C cíclico}}} \mathrm{Ker(H^1(Gal(k(A[p^n])/k), A[p^n]) \to H^1(C, A[p^n])}.$$

Además, los autores Dvornicich y Zannier [8] dan una definición equivalente al grupo $H^1_{\mathrm{loc}}(\mathrm{Gal(k(A[p^n])/k), A[p^n])}$. Para ello, explican que un coclico $Z \in H^1(\mathrm{Gal(k(A[p^n])/k), A[p^n])}$ satisface la condición local si para todo $\gamma \in \mathrm{Gal(k(A[p^n])/k)}$ existe un $m_\gamma \in A[p^n]$ tal que $Z_\gamma = \gamma \bullet m_\gamma - m_\gamma$. El conjunto de todas las clases de cociclos que satisfacen la condición local es el grupo $H^1_{\mathrm{loc}}(\mathrm{Gal(k(A[q])/k), A[q])}$.

Gracias al resultado anterior de Sansuc, podemos presentar un teorema y un corolario que dan una respuesta positiva al principio de divisibilidad local-global para $r = 0$ y $r = 1$.

Teorema 2.3. *Sea k un cuerpo de números, A una variedad abeliana definida sobre k y A^t la variedad dual de A. Sea p número primo y $n \in \mathbb{N}^*$. Entonces, si $H^1_{loc}(\mathrm{Gal(k(A[p^n])/k), A[p^n])}$ es trivial, el principio de divisibilidad local-global para p^n se sostiene sobre $H^0(G_k, A[p^n])$. Además, si $H^1_{\mathrm{loc}}(\mathrm{Gal(k(A^t[p^n])/k), A^t[p^n])} = 0$, el principio de divisibilidad local-global para p^n se sostiene sobre $H^1(G_k, A[p^n])$.*

Corolario 2.4. *Con las mismas notaciones del Teorema 2.3. Sea E una curva elíptica definida sobre k. Entonces si $H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k), E[p^n])} = 0$, la divisibilidad local-global para p^n se sostiene sobre $H^0(\mathrm{Gal(k(E[p^n])/k), E[p^n])}$ y sobre $H^1(\mathrm{Gal(k(E[p^n])/k), E[p^n])}$.*

Demostración. Toda curva elíptica es autodual. □

Para finalizar esta sección, expondremos un poco de historia sobre el estudio del problema de divisibilidad local-global. Para ello, mostraremos algunos resultados de los autores mencionados anteriormente.

Cuando $r = 0$, el principio anterior es conocido como el problema de Grunwald-Wang. Los autores Dvornicich y Zannier son unos de los primeros en trabajar este problema sobre curvas elípticas, con la diferencia de que ellos consideran el problema de la divisibilidad local-global, para todos los lugares, salvo una cantidad finita [8, 9].

Por otro lado, Çiperiani y Stix [4] trabajan el siguiente Problema de Cassels: sea k un cuerpo de números y A una variedad abeliana definida sobre k. Para todo número primo p decimos que el Grupo de Tate-Shafarevich $Ш^1(G_k, A(\overline{k}))$ es p-divisible en el Grupo $H^1(G_k, A(\overline{k}))$ si y solo si

$$Ш^1(G_k, A(\overline{k})) \subseteq p^n H^1(G_k, A(\overline{k})), \forall n \in \mathbb{N}^*.$$

La pregunta que surge es, ¿cuál es el conjunto de números primos p tales que el Grupo de Tate-Shafarevich es $p-$divisible? Los autores dan un acercamiento a responder este problema estudiando la trivialidad del grupo $Ш^1(G_k, A(\overline{k}))$. Notar que si $Ш^1(G_k, A(\overline{k})) = 0$ el problema de Cassels tiene respuesta afirmativa y el problema de divisibilidad local-global para p^n se sostiene sobre $H^0(G_k, A(\overline{k}))$.

Además, los autores Çiperiani y Stix presentan la siguiente proposición que también da una respuesta positiva al problema de Cassels: Si A es una variedad abeliana definida sobre un cuerpo de números k, A^t variedad abeliana dual de A, p un número primo. Si para todo $n \in \mathbb{N}$ tenemos que $Ш^1(G_k, A^t[p^n]) = 0$. Entonces

$$Ш^1(G_k, A) \text{ es p divisible sobre } H^1(G_k, A(\overline{k})) \quad [4, \text{Proposition 13}].$$

Notar que si $Ш^1(G_k, A^t[p^n]) = 0$ por la dualidad de Poitou-Tate [16, Theorem 8.6.7] tenemos que $Ш^2(G_k, A[p^n]) = 0$, es decir, si el problema de divisibilidad local global para p^n se sostiene sobre $H^1(G_k, A[p^n])$ implica respuesta positiva al problema de Cassels.

Finalmente, Gillibert y Ranieri [10] profundizan en estos temas trabajando principalmente en variedades abelianas polarizadas. Explicitan también, utilizando el teorema de Sansuc la relación entre el Problema de Cassels y el Problema Grunwald-Wang que fue estudiado por Çiperiani y Stix [4] previamente. Los autores establecen que, al demostrar que el grupo $H^1_{\mathrm{loc}}(\mathrm{Gal(k(A[p^n])/k), A[p^n])}$ es trivial o que $Ш^1_\omega(G_k, A[p^n])$ lo es, tenemos respuesta positiva tanto al problema de Grunwald-Wang como al problema de Cassels.

Capítulo 3

Demostración de los principales resultados

En el segundo capítulo hemos demostrado que si k es un cuerpo de números, A una variedad abeliana definida sobre k, p un número primo y $n \in \mathbb{N}$, el problema de Grunwald-Wang tiene respuesta positiva si el grupo $Ш^1_\omega(\mathrm{G_k}, \mathrm{A[p^n]})$ es trivial. También, hemos demostrado que si $Ш^1(\mathrm{G_k}, \mathrm{A^t[p^n]}) = 0$ para todo $n \in \mathbb{N}$, entonces el problema de Cassels tiene respuesta afirmativa. Es por eso, que en esta sección queremos encontrar un criterio para que el grupo $Ш^1_\omega(G_k, E[p^n])$ sea trivial, donde E es una curva elíptica definida sobre el cuerpo de números k.

Más precisamente, vamos a demostrar que fuera de un conjunto finito de números primos S que depende sólo del grado de la extensión de $k/\mathbb{Q}$, para toda curva elíptica E, para todo número primo $p \notin S$ y para todo $n \in \mathbb{N}$, el grupo $H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]})$ es trivial. Es decir, fuera del conjunto finito S tenemos respuesta positiva tanto al problema de Cassels como al problema de Grunwald-Wang.

3.1. Teorema de Dvornicich-Zannier

A continuación se presentará una generalización de un teorema de Dvornicich y Zannier que puede ser consultado en [9].

Teorema 3.1. *Sea p un número primo, sea ζ_p una raíz $p-$ésima primitiva de la unidad, sea k un cuerpo de números que no contiene a $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Sea E una curva elíptica definida sobre k tal que E no admite una isogenia de grado p definida sobre k. Entonces, tenemos que para todo $n \in \mathbb{N}$*

$$H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) = 0.$$

Demostración. Sea $q = p^n$, sea $K = k(E[q])$ el cuerpo k adjuntado el grupo de los puntos de $q-$torsión de la curva elíptica. Considerando $\sigma \in \mathrm{Gal(K/k)}$ y $P \in E(q)$ se

cumple que

$$0 = \sigma(0) = \sigma(qP) = \sigma(q)\sigma(P) = q\sigma(P)$$

es decir, $\sigma(P)$ es un punto de $q-$ torsión. Por lo tanto, la extensión K/k es una extensión de Galois.

Por Corolario 2.4 basta probar que $H^1_{\mathrm{loc}}(\mathrm{Gal(K/k)}, \mathrm{E[q]}) = 0$. En este caso probaremos que $H^1(\mathrm{Gal(K/k)}, \mathrm{E[q]})$ es trivial, lo que es una condición más fuerte pues $H^1_{\mathrm{loc}}(\mathrm{Gal(K/k)}, \mathrm{E[q]})$ es un subgrupo de $H^1(\mathrm{Gal(K/k)}, \mathrm{E[q]})$.

Sabemos que $E[q] \simeq (\mathbb{Z}/q\mathbb{Z})^2$, es decir, si $P \in E[q]$ existe un único $(x, y) \in (\mathbb{Z}/q\mathbb{Z})^2$ tal que $P \simeq (x, y)$ y viceversa. Entonces, debido al isomorfismo anterior podemos definir un homomorfismo inyectivo Φ de la siguiente forma:

$$\begin{array}{rccc} \Phi & : & \mathrm{Gal(K/k)} & \to & \mathrm{Aut}((\mathbb{Z}/\mathrm{q}\mathbb{Z})^2) \simeq \mathrm{Aut(E[q])} \\ & & \sigma & \to & \Phi_\sigma : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \\ & & & & (x, y) \to (\sigma(x), \sigma(y)) = \sigma(P). \end{array}$$

Como $\mathrm{Aut}((\mathbb{Z}/\mathrm{q}\mathbb{Z})^2) \simeq \mathrm{GL}_2(\mathbb{Z}/\mathrm{q}\mathbb{Z})$ por el homomorfismo anterior Φ se cumple que cualquier subgrupo G del grupo de Galois $\mathrm{Gal(K/k)}$ se representa como un subgrupo de las matrices $\mathrm{GL}_2(\mathbb{Z}/\mathrm{q}\mathbb{Z})$, que por abuso de notación se llamará también G.

Consideremos el siguiente homomorfismo ϕ llamado reducción módulo p

$$\begin{array}{rccc} \phi & : & \mathbb{Z}/q\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & & x & \to & x \bmod \mathrm{p}. \end{array}$$

Aplicando el homomorfismo ϕ a cada coeficiente de las matrices del grupo G, obtenemos un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/\mathrm{p}\mathbb{Z})$ que llamaremos G_0, y su imagen en $\mathrm{PGL}_2(\mathbb{Z}/\mathrm{p}\mathbb{Z})$ la llamaremos H_0.

Por [21, Corollary 8.1.1] los cuerpos $k(E[p])$ y K contienen a la raíz $p-$ésima primitiva de la unidad ζ_p. Las propiedades básicas del emparejamiento de Weil [21, Proposition III:8.1] implican que la acción de G sobre ζ_p esta dada por $g(\zeta_p) = \zeta_p^{\det(\mathrm{g})}$ para todo $g \in G$. Declaramos que como k no contiene a $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ la imagen del determinante tiene por lo menos 3 elementos. En efecto, si k no contiene al cuerpo $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ entonces $\zeta_p + \overline{\zeta_p} \notin k$, por lo tanto el grado de la extensión de cuerpos $[k(\zeta_p + \overline{\zeta_p}) : k]$ es mayor que 1. Supongamos entonces que el grado de la extensión $k(\zeta_p + \overline{\zeta_p})/k$ es 2 y sabemos que todo $\sigma \in \mathrm{Gal(k(\zeta_p)/k)}$ cumple que $\sigma(\zeta_p) = \zeta_p^i$. Como el grado de la extensión es 2 es igual al grado del polinomio irreducible de $\zeta_p + \overline{\zeta_p}$ sobre k, el cual es $(x - \zeta_p)(x - \sigma(\zeta_p)) = x^2 - (\zeta_p + \zeta_p^i)x + \zeta_p^{i+1}$ para algún $\sigma \in \mathrm{Gal(k(\zeta_p)/k)}$. Si $i = -1$ tenemos que $\zeta_p + \zeta_p^i = \zeta_p + \zeta_p^{-1} = \zeta_p + \overline{\zeta_p} \in k$, lo que es una contradicción. Ahora, si

$i \neq -1$ se debe cumplir que $\zeta_p \in k$ para que $\zeta_p^i \in k$, lo que también es una contradicción. Por lo tanto, el grado de la extensión de $k(\zeta_p + \overline{\zeta_p})/k$ es mayor o igual a 3, ya que de lo contrario concluimos que ζ_p o $\zeta_p + \overline{\zeta_p}$ pertenecen a k por ser coeficientes del polinomio irreducible.

Recordemos que Gal(k(E[p])/k) es isomorfo a un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/\mathrm{p}\mathbb{Z})$ entonces podemos definir el homomorfismo determinante vía el homomorfismo anterior, desde Gal(k(E[p])/k) a $(\mathbb{Z}/p\mathbb{Z})^*$ donde Ker(det) = $\{\sigma \in \mathrm{Gal(k(E[p])/k)} : \det(\sigma) = 1\}$. Aplicando el primer teorema de homomorfismo de grupos, concluimos que

$$\mathrm{Im(det)} \simeq \mathrm{Gal(k(E[p])/k)/Ker(det)}.$$

Declaramos que Ker(det) = $\mathrm{Gal(k(E[p])/k(\zeta_p))}$, pues si $\sigma \in$ Ker(det) tenemos que $\zeta_p^\sigma = \zeta_p^{\det \sigma} = \zeta_p$ por el emparejamiento de Weil [21, Proposition 8.1] entonces σ pertenece a $\mathrm{Gal(k(E[p])/k(\zeta_p))}$. La otra inclusión es análoga pues, si $\sigma \in \mathrm{Gal(k(E[p])/k(\zeta_p))}$ se cumple que $\zeta_p^\sigma = \zeta_p$ lo que implica $\det(\sigma) = 1$. Por lo tanto, concluimos que

$$\mathrm{Im(det)} \simeq \mathrm{Gal(k(\zeta_p)/k)}$$

entonces la imagen del homomorfismo determinante es mayor o igual que 3.

Comenzaremos con el caso en que G_0 contiene un múltiplo no trivial de la matriz identidad. Esto sucede cuando G contiene un elemento g congruente módulo p a un múltiplo no trivial de la identidad, es decir, $g \equiv \lambda_0 I_2$ mod p, con $\lambda_0 \in (\mathbb{Z}/p\mathbb{Z})^*$ y $\lambda_0 \neq 1$. Sea d el orden de λ_0 entonces $d > 1$ y d divide al orden del grupo $(\mathbb{Z}/p\mathbb{Z})^*$ que es $p-1$. Como $g \equiv \lambda_0$ mod p se cumple que $g = \begin{pmatrix} \lambda_0' & 0 \\ 0 & \lambda_0' \end{pmatrix} + pB$ con $\lambda_0' \equiv \lambda_0$ mod p y $B \in M_2(\mathbb{Z}/q\mathbb{Z})$. Declaramos que el grupo generado por g contiene un elemento g' de orden d, donde la reducción módulo p de g' será una matriz escalar. En efecto, basta considerar $g' = g^\mu$ con μ una potencia adecuada de p, entonces por el Teorema del binomio obtenemos que

$$g' = g^\mu = \left(\lambda_0' I_2 + pB\right)^\mu \equiv (\lambda_0')^\mu I_2 \bmod p^n$$

donde llamaremos $\mu_0 = (\lambda_0')^\mu$. De esta forma g' es una matriz escalar módulo p. Lo que nos falta probar es que el orden de g' es d. Para esto sabemos que $\lambda_0' \equiv \lambda_0$ mod p entonces se cumple que $(\lambda_0')^\mu \equiv \lambda_0$ mod p, es decir, $\mu_0 \equiv \lambda_0$ mod p, lo que implica que $\mathrm{ord}(\mu_0) = \mathrm{ord}(\lambda_0) \cdot \mathrm{p^b}$ entonces $\mu_0^{p^b} \equiv \lambda_0$ mod p lo que implica que $\mathrm{ord}(\mu_0^{\mathrm{p^b}}) = \mathrm{ord}(\lambda_0)$. Es decir, la potencia adecuada de g es considerar $\mu = p^b$ así se cumple que g' tiene el mismo orden de λ_0 que es d y g' es una matriz escalar.

En particular el subgrupo generado por g, son matrices escalares que estan contenidas en el centro de G, entonces $\langle g\rangle$ es un subgrupo normal de G.

Usando Inflacción-Restricción tenemos la siguiente sucesión exacta [ver Teorema 1.16]

$$0 \to H^1(G/\langle g\rangle, E[q]^{\langle g\rangle}) \to H^1(G, E[q]) \to H^1(\langle g\rangle, E[q]) \quad .$$

El grupo $H^1(\langle g\rangle, E[q]) = 0$ pues el ord(g) = ord(λ) = d, que es coprimo con p entonces es coprimo con q, [ver Ejemplo 1.19]. Por lo tanto, la sucesión anterior queda de la siguiente forma:

$$0 \to H^1(G/\langle g\rangle, E[q]^{\langle g\rangle}) \to H^1(G, E[q]) \to 0 \quad .$$

Por lo tanto, $H^1(G/\langle g\rangle, E[q]^{\langle g\rangle}) \simeq H^1(G, E[q])$. Como $g - I_2 = (\lambda - 1)I_2$ tiene kernel trivial en $(\mathbb{Z}/q\mathbb{Z})^2$ pues $\lambda \neq 1$, entonces $E[q]^{\langle g\rangle} = 0$ lo que implica que $H^1(G, E[q]) = 0$.

Entonces podemos suponer que G_0 no contiene una matriz escalar no trivial, lo que implica que la función $G_0 \to PGL_2(\mathbb{Z}/p\mathbb{Z})$ es inyectiva, es decir, $G_0 \simeq H_0$. Usaremos la clasificación de Serre sobre los subgrupos de $PGL_2(\mathbb{Z}/p\mathbb{Z})$ que la podemos encontrar en [20, Proposition 15 and Proposition 16]. Supongamos primero que p divide al orden de G_0, entonces puede suceder que G_0 contiene a $SL_2(\mathbb{Z}/p\mathbb{Z})$ o que G_0 está contenido en un subgrupo de Borel. Si G_0 contiene a $SL_2(\mathbb{Z}/p\mathbb{Z})$ contiene a $-I_2$ lo que implica que contiene a una matriz escalar no trivial, lo que es una contradicción. Ahora, supongamos que G_0 está contenido en un subgrupo de Borel, por [21, Proposition 4.12 y Remark 4.13.2] existe ϕ isogenia de grado p definida sobre k tal que Ker$\phi = \langle$P$\rangle$ con $P \in E[p]$, lo que es una contradicción.

Supongamos que $G_0 \simeq H_0$ y que p no divide al orden de G_0. Entonces por la clasificación de Serre [20, Proposition 15 and Proposition 16] el grupo H_0 puede ser cíclico, diédrico o isomorfo a A_4, A_5 o S_5. Analicemos cada uno de los casos anteriores. Supongamos primero que G_0 es el grupo diédrico, es decir,

$$G_0 = D_n = \langle s, r : s^2 = r^n \wedge sr = r^{-1}s\rangle = \langle s, sr : s^2 = r^n \wedge sr = r^{-1}s\rangle \quad .$$

Notar que los elementos s, sr tienen orden 2 entonces det(s) = ± 1 y det(sr) = ± 1 entonces det(G_0) $\subseteq \{\pm 1\}$, lo que implica que la imagen de la función determinante es menor o igual que 2, esto contradice el hecho que la imagen del determinante es mayor o igual que 3, por lo tanto, G_0 no puede ser el grupo diédrico.

Supongamos ahora que G_0 es isomorfo a A_4, A_5 o S_5, como $A_4 \subseteq A_5 \subseteq S_5$, G_0 contiene a un subgrupo isomorfo A_4. El conjunto $L = \{(12)(34), (13)(24), (14)(23), 1\}$

es un subgrupo de A_4, que es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ entonces G_0 contiene al siguiente subgrupo $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ que contiene a $-I_2$ que es una matriz escalar no trivial, lo que es una contradicción, de esta forma G_0 no puede ser isomorfo a A_4, A_5 o S_5.

Finalmente, supongamos que G_0 es un grupo cíclico generado por $g \in G_0$. Tenemos dos posibilidades, la primera de ellas es que al menos un autovalor de g esta en $\mathbb{Z}/p\mathbb{Z}$, lo que implica que el otro autovalor también pertenece a $\mathbb{Z}/p\mathbb{Z}$, esto permite que g se escriba como una matriz diagonal pues su orden es primo relativo con p entonces G_0 esta contenido en un subgrupo de Borel, lo que implica que E admite una isogenia de grado p definida sobre k, lo que es una contradicción. La otra posibilidad es que los valores propios $\lambda, \mu \in \mathbb{F}_{p^2}$ y no a $\mathbb{Z}/p\mathbb{Z}$ entonces son conjugados sobre $\mathbb{Z}/p\mathbb{Z}$, es decir, $\lambda = \mu^p$. Ahora, $\mu^{p+1} = \lambda \cdot \mu = \det(g)$ en $\mathbb{Z}/p\mathbb{Z}$ pero $\lambda^{p+1} = (\mu^p)^{p+1} = (\mu^{p+1})^p = \mu^{p+1}$ en $\mathbb{Z}/p\mathbb{Z}$ entonces g^{p+1} tiene dos valores propios iguales en $(\mathbb{Z}/p\mathbb{Z})^*$. Como g es diagonalizable entonces g^{p+1} también lo es, pero es una matriz escalar sobre $\mathbb{Z}/p\mathbb{Z}$, por la suposición de que G_0 no contiene matrices escalares no triviales concluimos que $g^{p+1} = I_2$, entonces, $1 = \det(g^{p+1}) = (\det(g))^{p+1}$, lo que equivale a que $\det(g) = 1$. Por lo tanto, la imagen de G_0 por el homomorfismo determinante tiene cardinal uno, que es una contradicción. □

Lema 3.2. *Sea p un número primo, sea k un cuerpo de números que no contiene a $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ y sea E curva elíptica definida sobre k. Si existe $n \in \mathbb{N}$ tal que $H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) \neq 0$ entonces existe una base de $E[p]$ tal que $\mathrm{Gal(k(E[p])/k)}$ es un subgrupo de $\left\langle \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$, con $\lambda_1, \lambda_2 \in (\mathbb{Z}/p\mathbb{Z})^*$.*

Demostración. Sea $G = \mathrm{Gal(k(E[p^n])/k)}$. Si $H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) \neq 0$ entonces E tiene una isogenia cíclica de grado p definida sobre k [ver Teorema 3.1]. Por [21, Proposition 4.12 and Remark 4.13.2] se cumple que la reducción de G módulo p, que llamaremos G_0, está contenido en un subgrupo de Borel. Si G_0 contiene matrices escalares distintas de las triviales, implica que $H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) = 0$, por demostración del teorema 3.1, esto contradice nuestra hipótesis. De esta forma, el grupo G_0 no contiene matrices escalares no triviales. Demostraremos la siguiente afirmación que nos permitirá concluir el resultado:

Afirmación 1. *Sea T el subgrupo de las matrices diagonales de $GL_2(\mathbb{Z}/p\mathbb{Z})$. Si $D \leq T$ tal que no contiene matrices escalares no triviales entonces D es cíclico.*

Demostración. Como T es el subgrupo de las matrices diagonales de $GL_2(\mathbb{Z}/p\mathbb{Z})$ se cumple que $T \simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$. Supongamos que D no es un subgrupo cíclico, entonces existe l número primo tal que l divide a $p-1$ y D contiene a un subgrupo isomorfo a $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, entonces D contiene a todas las matrices de orden l en T.

Entonces, sea $\lambda \in (\mathbb{Z}/p\mathbb{Z})^*$ de orden l entonces $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in D$, lo que es una contradicción pues, D no contienen matrices escalares no triviales. De esta forma, D debe ser cíclico. □

Entonces, como G_0 está contenido en un subgrupo de Borel, el cual es generado por el siguiente conjunto

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} b_1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & b_2 \end{pmatrix} : b_1, b_2 \in (\mathbb{Z}/p\mathbb{Z})^* \right\}.$$

Por la Afirmación 1, tenemos que las matrices diagonales que no contienen matrices escalares no triviales es un subgrupo cíclico, lo que implica que G_0 es un subgrupo de $\left\langle \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$, con $\lambda_1, \lambda_2 \in (\mathbb{Z}/p\mathbb{Z})^*$. □

Observación 3.3. *Se tienen contrajemplos donde el principio de divisibilidad local-global no se sostiene, cuando el cuerpo de números k contiene a* $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ [18, Theorem 2].

3.2. Lemas importantes

A continuación se presentarán algunos teoremas, lemas, corolarios y proposiciones que se encuentran en el artículo de Gillibert y Ranieri [10] que son necesarios para el criterio de la siguiente sección. Estos resultados permiten demostrar que si existe p número primo, $n \in \mathbb{N}$, k cuerpo de números que no contiene a $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ y E curva elíptica definida sobre k tal que $H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) \neq 0$ entonces si $\mathrm{Gal(k(E[p])/k)}$ contiene una matriz diagonal, esta matriz tiene por lo menos un valor propio igual a 1.

Proposición 3.4. *Sea* $V_{n,d}$ *el grupo* $(\mathbb{Z}/p^n\mathbb{Z})^{2d}$ *y sea* G *un subgrupo de* $GL_{2d}(\mathbb{Z}/p^n\mathbb{Z})$ *quien actúa sobre* $V_{n,d}$ *de la forma usual. Supongamos que el normalizador del* $p-$*Sylow subgrupo* H *de* G *contiene un elemento* g *de orden que divide a* $p-1$ *tal que* $g - I_{2d}$ *es biyectiva. Entonces* $H^1_{\mathrm{loc}}(G, V_{n,d}) = 0$

Para demostrar la Proposición 3.4 son necesarios algunos elementos previos, que se presentan a continuación:

Definición 3.5. *Sea* H *un* $p-$*grupo. El subgrupo de Frattini* $\phi(H)$ *de* H *es la intersección de todos los subgrupos maximales de* H.

Proposición 3.6. *Sea* p *un número primo y sea* G *un grupo finito tal que* $G = \langle g, H \rangle$, *donde* $H \trianglelefteq G$ *y* H *es un* $p-$*Sylow de* G *y* g *tiene orden que divide a* $p-1$. *Entonces existe*

$r \in \mathbb{N}$ y un conjunto generador $\{h_1, h_2, ..., h_r\}$ de H tales que, para todo $1 \leq i \leq r$, existe $\lambda_i \in \mathbb{Z}$ tales que

$$gh_ig^{-1} = h_i^{\lambda_i}$$

Demostración. Supongamos que $|H| = p^m, m \in \mathbb{N}$. La demostración será por inducción sobre m.
Si $m = 1$ tenemos que H es un grupo cíclico generado por h_1. Por hipótesis H es un subgrupo normal de G entonces se cumple que $gh_1g^{-1} = h_1^{\lambda_1}$ para $\lambda_1 \in \mathbb{Z}$, así que no hay nada que probar. Supongamos que asumimos que la proposición es cierta para todo número natural $j < m$. Declaramos que el grupo de Frattini $\phi(H)$ es normal en H y que $H/\phi(H)$ es $p-$elementalmente abeliano, es decir, es isomorfo a un producto finito de grupos isomorfos a $\mathbb{Z}/p\mathbb{Z}$. Para probar lo anterior utilizaremos los siguientes lemas:

Lema 3.6.1 *Todo subgrupo maximal de un $p-$grupo G es de índice p y normal en G.*

Demostración. Ver [7, Section 6.1]. □

Lema 3.6.2 Sea G un grupo y H un subgrupo de G. El conmutador de G, $G^{(1)}$ *es un subgrupo de H si y solo si H es un subgrupo normal de G y G/H es abeliano.*

Demostración. Ver [2, Section 8.8]. □

Como H es un $p-$grupo y M un subgrupo maximal de H entonces por el Lema 3.6.1 tenemos que $[H : M] = p$ y que M es un subgrupo normal de H. Entonces $\phi(H)$ es normal en H, pues cada subgrupo M lo es. Además, como $[H : M] = p$ tenemos que $H/M \simeq \mathbb{Z}/p\mathbb{Z}$, es decir, el cuociente es abeliano para todo subgrupo maximal de H, entonces usando el Lema 3.6.2 tenemos que $H^{(1)}$ es un subgrupo de M, para todo M, entonces $H^{(1)}$ es un subgrupo de $\phi(H)$. Usando nuevamente el Lema 3.6.2 tenemos que $\phi(H)$ es normal en H y $H/\phi(H)$ es abeliano. Finalmente, como $H/M \simeq \mathbb{Z}/p\mathbb{Z}$, $h^p \in M$, para todo $h \in H$, y para todo M subgrupo maximal de H, entonces $h^p \in \phi(H)$, lo que prueba que $H/\phi(H)$ es $p-$elementalmente abeliano.

Ahora probaremos que $\phi(H)$ es un subgrupo normal de G, para esto notar que para todo $g \in G$ se cumple que

$$g\phi(H)g^{-1} = \bigcap_{\substack{M \leq H \\ M \text{ maximal}}} gMg^{-1} = \bigcap_{\substack{M \leq H \\ M \text{ maximal}}} M = \phi(H)$$

pues es solo aplicar la acción de conjugación sobre los subgrupos maximales de H.

Ahora usaremos el siguiente resultado bien conocido:

Teorema 3.6.3 (Burnside basis Theorem). *Sea H un $p-$grupo finito. Un subconjunto de H es un conjunto de generadores para H si y solo si su imagen en $H/\phi(H)$ es un conjunto de generadores para $H/\phi(H)$.*

Considere $H/\phi(H)$, como $\phi(H)$ es normal en G y $H/\phi(H)$ es abeliano la siguiente función es un $\mathbb{Z}/p\mathbb{Z}-$isomorfismo lineal:

$$\begin{array}{rccc} f: & H/\phi(H) & \to & H/\phi(H) \\ & h\phi(H) & \to & ghg^{-1}\phi(H). \end{array}$$

En efecto, la función f esta bien definida y es inyectiva pues, si

$$\begin{array}{rccc} & f(h\phi(H)) & = & f(t\phi(H)) \\ \iff & ghg^{-1}\phi(H) & = & gtg^{-1}\phi(H) \\ \iff & hg^{-1}\phi(H) & = & tg^{-1}\phi(H) \\ \iff & gt^{-1}hg^{-1}\phi(H) & = & \phi(H) \\ \iff & (t^{-1}h)g^{-1}\phi(H) & = & g^{-1}\phi(H) \\ \iff & (t^{-1}h)\phi(H)g^{-1} & = & g^{-1}\phi(H) \\ \iff & t^{-1}h\phi(H) & = & g^{-1}\phi(H)g \\ \iff & t^{-1}h\phi(H) & = & \phi(H) \\ \iff & h\phi(H) & = & t\phi(H). \end{array}$$

Además, la función f es sobreyectiva pues para cada $h\phi(H) \in H/\phi(H)$ existe $g^{-1}hg\phi(H)$ preimagen tal que $f(g^{-1}hg\phi(H)) = h\phi(H)$. Sea $\lambda \in \mathbb{Z}/p\mathbb{Z}$ entonces

$$f((h\phi(H))^\lambda) = f(h^\lambda\phi(H)) = gh^\lambda g^{-1}\phi(H) = (ghg^{-1})^\lambda\phi(H) = f(h\phi(H))^\lambda \quad .$$

De esta forma, f es un $\mathbb{Z}/p\mathbb{Z}$ isomorfismo lineal.

Por hipótesis g tiene orden que divide a $p-1$ entonces el orden de f también divide a $p-1$ y f es diagonalizable en el $\mathbb{Z}/p\mathbb{Z}-$espacio vectorial $H/\phi(H)$. Entonces existen $v_1, v_2, ..., v_k \in H$ tales que $\{v_i\phi(H) : 1 \leq i \leq k\}$ es una $\mathbb{Z}/p\mathbb{Z}-$base de $H/\phi(H)$ y existen $\lambda_i \in \mathbb{Z}$ tales que $gv_ig^{-1}\phi(H) = v_i^{\lambda_i}\phi(H)$.

Supongamos que $k = 1$ entonces $H/\phi(H)$ tiene un único generador $v_1\phi(H)$. Por el Teorema 3.6.3, H es generado por v_1 y es cíclico. Como H es normal en G tenemos que $gv_1g^{-1} = v_1^\lambda$ para $\lambda \in \mathbb{Z}$, que es la tesis. Ahora supongamos que $\lambda > 1$, consideremos los subgrupos $H_1, H_2 \subseteq H$ tales que

$$H_1 = \langle v_1, \phi(H)\rangle \qquad H_2 = \langle v_2, ..., v_k, \phi(H)\rangle \quad .$$

Entonces los conjuntos $\Gamma_1 = \langle g, H_1\rangle$ y $\Gamma_2 = \langle g, H_2\rangle$ son subgrupos de G. Declaramos que H_i es normal en Γ_i para $i = 1, 2$. En efecto, todo elemento de H_1 es de la forma $v_1^b h$ con $h \in \phi(H)$ entonces $gv_1^b hg^{-1} = (gv_1^b g^{-1})(ghg^{-1}) = v_1^\mu t$, con $t \in \phi(H)$, donde se utilizó que $gv_1g^{-1} = v_1^\lambda$ y que $\phi(H)$ es normal en G. De forma análoga se prueba que Γ_2 es normal en H_2.

Demostraremos que Γ_1, Γ_2 no son G. Como H_1 y H_2 son normales a Γ_1 y Γ_2 respectivamente y Γ_1, Γ_2 son grupos generados por el elemento g que no es divisible por p y por los subgrupos H_1, H_2 tenemos que H_1 es el único p-Sylow de Γ_1 y H_2 es el único $p-$Sylow de Γ_2. Como H_1, H_2 estan contenidos de forma propia en H entonces Γ_1, Γ_2 estan contenidos de forma propia en G, de esta forma podemos aplicar la hipótesis de inducción sobre Γ_1 y Γ_2. Como H es generado por H_1 y H_2 la unión del conjunto de generadores de H_1 con el conjunto de generadores de H_2 nos da un conjunto de generadores para H, lo que concluye la demostración. □

Demostración. (Proposición 3.4) Considere las dos restricciones (Definición 1.10)

$$H^1(G, V_{n,d}) \overset{res}{\to} H^1(\langle g, H\rangle, V_{n,d}) \overset{res}{\to} H^1(H, V_{n,d})$$

Notar que $res : H^1(G, V_{n,d}) \to H^1(H, V_{n,d})$ es un homomorfismo inyectivo pues $V_{n,d}$ es un p-grupo y H es el $p-$Sylow subgrupo de G [14, Corollary 1.33]. Entonces deducimos que $res : H^1(G, V_{n,d}) \to H^1(\langle g, H\rangle, V_{n,d})$ es también inyectivo. Más aún, los homomorfismos restricción anteriores inducen un mapeo sobre los primeros grupos de cohomología local. Entonces, el homomorfismo $res : H^1_{\text{loc}}(G, V_{n,d}) \to H^1_{\text{loc}}(\langle g, H\rangle, V_{n,d})$ es también inyectivo.

Para probar la proposición es suficiente probar que $H^1_{\text{loc}}(\langle g, H\rangle, V_{n,d}) = 0$. Aplicaremos la Proposición 3.6 al grupo $\langle g, H\rangle$. Entonces existe $r \in \mathbb{N}$ y generadores $h_1, h_2, ...h_r$ en H tales que para todo $1 \leq i \leq r$ se cumple que $gh_ig^{-1} = h_i^{\lambda_i}$ para algún $\lambda_i \in \mathbb{Z}$. Entonces, para todo $1 \leq i \leq r$, consideremos $\Gamma_i = \langle g, h_i\rangle$ y $H_i = \langle h_i\rangle$. Para todo i de 1 a r tenemos que H_i es el p-Sylow de Γ_i, usando [14, Corollary 1.33] tenemos que $H^1_{\text{loc}}(\Gamma_i, V_{n,d}) \to H^1_{\text{loc}}(H_i, V_{n,d})$ es inyectiva. Como H_i es cíclico, se cumple que $H^1_{\text{loc}}(H_i, V_{n,d}) = 0$ entonces $H^1_{\text{loc}}(\Gamma_i, V_{n,d}) = 0, \forall i = \{1, ..., r\}$. Sea Z un cociclo de $\langle g, H\rangle$ que satisface la condición local [ver sección 2.2] entonces para todo $1 \leq i \leq r$, Z es un coborde sobre Γ_i, es decir, existe $\gamma_i \in \Gamma_i$ y existe $v_i \in V_{n,d}$ tal que $Z_{\gamma_i} = \gamma_i(v_i) - \gamma_i$. Como $g \in \Gamma_i$ para todo $1 \leq i, j \leq r$, tenemos que $Z_g = g(v_i) - v_i = g(v_j) - v_j$ lo que es equivalente a $(g - Id)(v_i) = (g - Id)(v_j)$. Por hipótesis la función $g - Id$ es biyectiva entonces $v_i = v_j, \forall i, j$. Como $g, h_1, ...h_r$ generan a $\langle g, H\rangle$ tenemos que Z es un coborde sobre $\langle g, H\rangle$,es decir , $H^1_{\text{loc}}(\langle g, H\rangle, V_{n,d}) = 0$ lo que implica que $H^1_{\text{loc}}(G, V_{n,d}) = 0$, lo que concluye la demostración. □

Lema 3.7. *Sea G un grupo, sea N un subgrupo normal de G y sea H el $p-$Sylow subgrupo de G. Sea g un elemento de G tal que su clase en G/N esta en el normalizador del $p-$Sylow subgrupo HN/N de G/N. Entonces existe un elemento de la clase gN que esta en el normalizador de H.*

Demostración. Sea g' la clase de g módulo N, por hipótesis g' pertenece al normalizador de HN/N, es decir, $g'(HN/N)g'^{-1} = HN/N$. Observemos el siguiente conjunto

$$\begin{aligned} g'(HN/N)g'^{-1} &= \{gN(hnN)g^{-1}N : h \in H, n \in N\} \text{ en GN/N} \\ &= \{ghNnNg^{-1}N : h \in H, n \in N\} \\ &= \{ghn'g^{-1}N : h \in H, n' \in N\} \\ &= (gHNg^{-1})/N. \end{aligned}$$

Entonces $gHNg^{-1}/N = HN/N$ que implica que $gHNg^{-1} = HN$ y como N es normal en G, tenemos que $gHg^{-1}N = HN$. Observar que por la normalidad de N en G se cumple que N es normal en H, entonces $HN = NH$. Como gHg^{-1} y H son dos subgrupos de $p-$Sylow de HN, entonces ellos son conjugados entre sí, es decir, existe $x \in HN$ y existen $h \in H, n \in N$ tal que $x = nh$ y se cumple que

$$\begin{aligned} & gHg^{-1} = xHx^{-1} \\ \iff & gHg^{-1} = (nh)H(nh)^{-1} \\ \iff & H = g^{-1}nHn^{-1}g \\ \iff & (n^{-1}g)H = H(n^{-1}g). \end{aligned}$$

Entonces $n^{-1}g$ pertenece al normalizador de H y $n^{-1}g \in Ng$ que es la misma clase que gN, pues N es normal en G, esto concluye la demostración. □

Observación 3.8. *Sea N el subgrupo normal de G que consiste en los elementos congruentes a la identidad módulo p. Si existe $g' \in G_1 = G/N$ tal que g' esta en el normalizador del $p-$Sylow de G_1, g' tiene orden que divide a $p-1$ y $g' - I_2$ es biyectiva, entonces por el Lema 3.7 existe $g \in G$ tal que g esta en el normalizador del $p-$Sylow subgrupo de G, tiene orden que divide a $p-1$ y $g - I$ es biyectiva.*

3.3. Criterio

Criterio 3.9. *Sea p un número primo. Sea k un cuerpo de números que no contiene a $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Sea E una curva elíptica definida sobre k tal que para toda E' curva elíptica definida sobre k, k-isogena a E, tal que $E'[p] \cap E'(k) = \{0\}$. Entonces, para todo $n \in \mathbb{N}$*

$$H^1_{\text{loc}}(\text{Gal(k(E[p}^{\text{n}}\text{])/k)}, \text{E[p}^{\text{n}}\text{]}) = 0.$$

Demostración. Sea G_1 subgrupo de Gal(k(E[p])/k). Analizaremos los casos en que G_1 está contenido en un subgrupo de Borel, pues los otros casos se encuentran en la demostración del Teorema 3.1. Por Lema 3.2 tenemos que $G_1 \leq \langle \sigma, \tau \rangle$ con $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y

$\tau = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, $\lambda_1, \lambda_2 \in (\mathbb{Z}/p\mathbb{Z})^*$.

Consideremos $H = \langle \sigma \rangle$ es un $p-$grupo, más aún es el $p-$Sylow subgrupo de G_1. El orden de τ divide a $p-1$, pues el orden de λ_1, λ_2 lo hacen, además τ pertenece al normalizador del grupo H y $\tau - I_2$ es una función biyectiva si y solo si $\lambda_1 \neq 1$ y $\lambda_2 \neq 1$. Estas son las hipótesis de la Proposición 3.4 entonces $H^1_{\text{loc}}(G_1, E[p]) = 0$, lo que implica que se tiene respuesta positiva al problema de divisibilidad local-global y al problema de Cassels.

Ahora probaremos que $G_n = \text{Gal}(\text{k}(\text{E}[\text{p}^\text{n}])/\text{k}, \text{E}[\text{p}^\text{n}])$ cumple todas las hipótesis de la Proposición 3.4. Para esto, recordar que las extensiones $k(E[p^n])/k$ y $k(E[p])/k$ son de Galois, por lo tanto se cumple que

$$G_1 \simeq G_n/(\text{Gal}(\text{k}(\text{E}[\text{p}^\text{n}])/\text{k}(\text{E}[\text{p}]))) \quad .$$

Debido al isomorfismo anterior, como $\tau \in G_1$ y cumple todas las hipótesis de la Proposición 3.4 vía isomorfismo existe $\overline{\tau_n} \in G_n/(\text{Gal}(\text{k}(\text{E}[\text{p}^\text{n}])/\text{k}(\text{E}[\text{p}])))$, tal que su orden divide a $p-1$, pertenece al normalizador del $p-$Sylow de $G_n/(\text{Gal}(\text{k}(\text{E}[\text{p}^\text{n}])/\text{k}(\text{E}[\text{p}])))$ y cumple $\overline{\tau_n} - I_2$ es biyectiva, para todo $n \in \mathbb{N}^*$. Luego, aplicando la Observación 3.8 a $\overline{\tau_n}$ tenemos que existe $\tau_n \in G_n$ que satisface todas las hipótesis de la Proposición 3.4, entonces $H^1_{\text{loc}}(G_n, E[p^n]) = 0$, para todo $n \in \mathbb{N}^*$ lo que implica que se tiene respuesta positiva al problema de divisibilidad local-global y al problema de Cassels.

Ahora debemos analizar el caso en que $\tau - I_2$ no es biyectiva, lo cual sucede cuando $\lambda_1 = 1$ ó $\lambda_2 = 1$. Comencemos con el caso en que $\lambda_1 = 1$, entonces

$$G_1 \leq \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \lambda_2 \end{pmatrix} : \lambda_2 \in (\mathbb{Z}/p\mathbb{Z})^* - \{1\} \right\rangle$$

Notar que $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $\tau = \begin{pmatrix} 1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ fijan al elemento $(1,0) \in (\mathbb{Z}/p\mathbb{Z})^2$ entonces el grupo G_1 fija a $(1,0)$. Como $E[p] \simeq (\mathbb{Z}/p\mathbb{Z})^2$ existe P punto de $p-$torsión de la curva elíptica E definida sobre el cuerpo k.

Supongamos que $G_1 \leq \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \lambda_1 & 0 \\ 0 & 1 \end{pmatrix} : \lambda_1 \in (\mathbb{Z}/p\mathbb{Z})^* - \{1\} \right\rangle$, probaremos que existe E' curva elíptica definida sobre k, tal que es $k-$isogenia a E y E' tiene un punto de $p-$torsión sobre k. Sea P el punto $(1,0)$ vía isomorfismo, se cumple que $\langle P \rangle$ es un G_1-módulo pues si $\gamma \in G_1$ tenemos que $\gamma(1,0)$ es un múltiplo de $(1,0)$. Entonces, por [21, Proposition 4.12 and Remark 4.13.2] existe una curva elíptica E' definida sobre k que es $k-$isogenia a E y el kernel de esta isogenia $\phi : E \to E'$ es

$\langle P\rangle$. Como las isogenias no constantes son sobreyectivas aplicando el primer teorema de homomorfismo de grupos tenemos que

$$E' = E/ker(\phi) \quad .$$

Consideremos $\phi(Q)$ con Q el punto $(0,1)$ vía isomorfismo. Observamos que $\tau(Q) = Q$ pero $\sigma(Q) \neq (0,1)$ y que $\phi(Q)$ tiene orden p pues $Q \notin Ker(\phi)$ y Q tiene orden p. Sea $\gamma \in G_k$, para todo T punto de torsión de orden una potencia de p en $E(\overline{k})$ se cumple lo siguiente:

$$\gamma\phi(T) = \phi(\gamma T) \quad .$$

Entonces $\gamma\phi(Q) = \phi(\gamma Q)$, como Q tiene orden p basta ver la restricción de γ a G_1. Todo elemento de G_1 es de la forma $\begin{pmatrix} \lambda_1^b & c \\ 0 & 1 \end{pmatrix}$ con $b \in \mathbb{Z}, c \in \mathbb{Z}/p\mathbb{Z}$. Entonces

$$\begin{aligned} \phi\Big(\begin{pmatrix} \lambda_1^b & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\Big) &= \phi(c,1) \\ &= \phi((c,0)+(0,1)) \\ &= \phi(c,0)+\phi(0,1) \\ &= c\phi(P)+\phi(Q) \\ &= \phi(Q). \end{aligned}$$

Por lo tanto, $\gamma\phi(Q) = \phi(Q)$, es decir, $\phi(Q)$ es un punto de $p-$torsión y es dejado fijo por G_1.

□

A continuación, presentaremos un teorema de Merel sobre curvas elípticas, el cual nos permitirá demostrar que fuera de un conjunto finito de primos, el problema de Grunwald-Wang y el problema de Cassels tienen respuesta positiva.

Teorema 3.10 (Teorema de Merel)**.** *Para todo $d \in \mathbb{N}$, tal que $d \geq 1$ existe una constante $C(d)$ que depende de d, tal que para todo cuerpo de números k que cumple $[k:\mathbb{Q}] \leq d$, para toda curva elípitica definida sobre k y para todo número primo $p > C(d)$. Entonces, se sostiene que $E[p] \cap E(k) = \{0\}$.*

El teorema de Merel nos permite demostrar el siguiente corolario:

Corolario 3.11. *Para todo $d \in \mathbb{N}$ con $d \geq 1$, existe una constante $C(d)$ que depende solo de d tal que para todo cuerpo de números k que cumple $[k:\mathbb{Q}] \leq d$, para toda curva elíptica definida sobre k y para todo número primo p. Entonces, para todo $n \in \mathbb{N}$*

$$H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) = 0.$$

Demostración. Sea k cuerpo de números tal que $[k : \mathbb{Q}] \leq d$ y sea $p > C(d)$. Entonces para toda curva elíptica definida sobre el cuerpo k, por teorema de Merel se cumple que $E[p] \cap E(k) = \{0\}$. Usando el Criterio 3.9 concluimos que

$$H^1_{\mathrm{loc}}(\mathrm{Gal(k(E[p^n])/k)}, \mathrm{E[p^n]}) = 0.$$

□

Capítulo 4

Definición de $\mathbf{H}^r$ vía Funtores Derivados

En esta sección, definiremos los grupos de cohomología vía funtores derivados utilizando resoluciones inyectivas. Para lograr este objetivo, es necesario recordar algunas definiciones y propiedades de la categoría de los $G-$módulos y de los funtores derivados. Como se mencionó en el primer capítulo esta definición es equivalente a la por cadenas no homogéneas [14].

Definición 4.1. *Sea M un $G-$módulo se define M^G como el conjunto de todos los elementos de M dejados fijos por la acción de G,es decir,*

$$M^G = \{m \in M : g \bullet m = m, \forall g \in G\}.$$

Sea Mod_G la categoría de los $G-$módulos y sea Ab la categoría de los grupos abelianos. Definiremos el siguiente funtor covariante [11, Definition 1.2]

$$\begin{array}{rccc} F & : & Mod_G & \to & Ab \\ & & M & \to & M^G \end{array}$$

Si $f : M \to N$ homomorfismo de $G-$módulos se define

$$\begin{array}{rccc} F(f) & : & M^G & \to & N^G \\ & & m & \to & F(f)(m) = f(m) \end{array}$$

Se cumple que $F(f)$ es un homomorfismo de grupos bien definido, pues si consideramos $m \in M^G$ y $g \in G$ se cumple que

$$g \bullet f(m) = f(g \bullet m) = f(m).$$

Por lo tanto, $$f(m) \in N^G.$$

Además, se cumplen las siguientes dos condiciones:

a) $F(Id_M) = Id_{F(M)}$ para todo $M \in \mathrm{Obj}(\mathrm{Mod_G})$.

b) Si $f \in \mathrm{Hom_G(M, N)}$ y $h \in \mathrm{Hom_G(N, T)}$ entonces $F(h \circ f) = F(h) \circ F(f)$.

Consideremos la siguiente sucesión exacta corta de G-módulos

$$0 \to M' \xrightarrow{f} M \xrightarrow{h} M'' \to 0 \tag{4.1}$$

se cumple que

$$0 \to (M')^G \xrightarrow{F(f)} M^G \xrightarrow{F(h)} (M'')^G \tag{4.2}$$

es una sucesión exacta corta. En efecto, como f es un homomorfismo inyectivo tenemos que $F(f)$ también lo es, ya que es simplemente la restricción de f a M'^G. Debemos probar también que $\mathrm{Im(F(}f\,\mathrm{))} = \mathrm{Ker(F(}h\,\mathrm{))}$, para ello consideremos $m \in \mathrm{Ker(F(}h\,\mathrm{))}$, es decir, $m \in M^G$ y $F(h)(m) = h(m) = 0$, como la primera sucesión es exacta existe $m' \in M'$ tal que $f(m') = m$, debemos probar que $m' \in M'^G$. Para esto consideremos $g \in G$, se cumple que

$$f(g \bullet m') = g \bullet f(m') = g \bullet m = m$$

entonces $f(g \bullet m') = f(m')$ para todo $g \in G$ como f es inyectiva tenemos que $g \bullet m' = m'$, es decir, $m' \in M'^G$. Para la otra inclusión consideremos $m \in \mathrm{Im(F(}f\,\mathrm{))}$, es decir, $m \in M^G$ y existe $m' \in M'^G$ tal que $f(m') = m$, por la exactitud de la primera sucesión se cumple que $h(m) = 0$ entonces $m \in \mathrm{Ker(F}(h))$. Lo anterior demuestra que el funtor F es exacto izquierdo.

A continuación presentaremos dos definiciones que pueden ser consultadas en [3, Capitule 6] y [14, page 72] respectivamente.

Definición 4.2. *Sea $\mathcal{C}$ una categoría abeliana* [3, Section 5] *y Q un objeto de $\mathcal{C}$. Diremos que Q es inyectivo si para todo monomorfismo $\alpha : A' \to A$ y para todo morfismo $u : A' \to Q$ existe un morfismo $v : A \to Q$ tal que $v\alpha = u$.*

Definición 4.3. *Sea $\mathcal{C}$ una categoría abeliana. Sea M un objeto de $\mathcal{C}$. Una resolución de M es una sucesión exacta larga*

$$0 \to M \to I^0 \to I^1 \to ... \to I^r \to ...$$

Si I^r son objetos inyectivos de $\mathcal{C}, \forall r \in \mathbb{N}$, diremos que es una resolución inyectiva de M.

La categoría de G-módulos y la categoría de Grupos abelianos son categorías abelianas [3, Capitule 5] y la categoría de los $G-$módulos tiene suficientes objetos inyectivos.

Esto significa que dado un $G-$módulo M podemos elegir una resolución inyectiva I° de M, la cual es una sucesión exacta larga formada por objetos inyectivos:

$$0 \to M \xrightarrow{i} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} ... \xrightarrow{d^{r-1}} I^r \xrightarrow{d^r} I^{r+1} \to ...$$

A cada uno de los objetos anteriores le podemos aplicar el funtor F definido anteriormente, donde obtenemos el siguiente complejo

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \xrightarrow{d^2} ... \xrightarrow{d^{r-1}} (I^r)^G \xrightarrow{d^r} (I^{r+1})^G \to ... \tag{4.3}$$

que no es una sucesión exacta larga pues el funtor aplicado es sólo exacto izquierdo.

Por lo tanto, se construyó una secuencia de funtores covariantes de la categoría de los $G-$módulos a la categoría de los grupos abelianos, los cuales son $R^0F, R^1F, R^2F, ...$ llamados funtores derivados derechos de F, que se definen por

$$(R^rF)(M) = H^r(G, M) := \frac{Ker(d^r)}{Im(d^{r-1})} \quad .$$

La definición anterior se conoce como el $r-$ésimo Grupo de Cohomología de G con coeficientes en M. Y es importante mencionar, que esta definición es equivalente a la dada en el capítulo 1 [14, Proposition 1.17].

Explicitaremos, como los funtores anteriores actúan sobre las flechas de la categoría de los $G-$módulos. Para esto considere $f \in \mathrm{Hom_G(M, N)}$ se define $(R^rF)(f) : (R^rF)(M) \to (R^rF)(N)$ que es un funtor covariante para todo $r \in \mathbb{N}$.

A continuación se presentarán algunas de las propiedades más importantes de los grupos de cohomología:

Propiedades 4.4.

a) El grupo de cohomología $H^0(G, M) = M^G$.

Demostración. Por definición

$$H^0(G, M) := \frac{\mathrm{Ker(d^0)}}{\mathrm{Im(d^{r-1})}} = \frac{\mathrm{Ker(d^0)}}{0} = \mathrm{Ker(d^0)}.$$

Por otro lado, al considerar una resolución inyectiva I° de M y aplicar el funtor F se obtiene que

$$0 \to M^G \xrightarrow{i} (I^0)^G \xrightarrow{d^0} (I^1)^G$$

es exacta. Es decir, $\mathrm{Ker(d^0) = Im(i) = M^G}$. Por lo tanto, $H^0(G, M) = M^G$. □

b) Si I es un $G-$módulo inyectivo entonces $H^r(G, I) = 0, \forall r > 0$.

Demostración. Dado I un $G-$módulo inyectivo su resolución inyectiva es la siguiente:

$$0 \to I \xrightarrow{i} I \xrightarrow{d^0} 0 \xrightarrow{d^1} I \to I \to ...$$

Entonces, $H^r(G, I) = 0, \forall r > 0$. □

c) Para cualquier homomorfismo de $G-$módulos $\alpha : M \to N$ y cualquieras resoluciones inyectivas I° de M y J° de N, α se puede extender a una función de complejos

$$\begin{array}{ccc} M & \longrightarrow & I \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\overline{\alpha}} \\ N & \longrightarrow & J \end{array}$$

y a un homomorfismo $H^r(\overline{\alpha}) : H^r(I^\circ) \to H^r(J^\circ)$.

Demostración. Para demostrar esta propiedad es necesario utilizar el siguiente lema:

Lema 4.5. *Una resolución inyectiva I° de M existe y si J° es otra resolución inyectiva de M existe un homomorfismo de I° a J° que hace que el siguiente diagrama conmute:*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & ... \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M & \longrightarrow & J^0 & \longrightarrow & J^1 & \longrightarrow & J^2 & \longrightarrow & ... \end{array}$$

Demostración. Sea M un $G-$módulo, como esta categoría tiene suficientes inyectivos existe I^0 elemento inyectivo de la categoría e i la inclusión, tales que

$$0 \to M \xrightarrow{i} I^0.$$

Consideremos B^1 como el cokernel de i, es decir, $B^1 = I^0/\mathrm{Im(i)}$ este es un objeto en la categoría entonces existe I^1 inyectivo e i la inclusión tales que

$$0 \to B^1 \xrightarrow{i} I^1.$$

Ahora, la siguiente sucesión es exacta

$$0 \to M \to I^0 \to I^1.$$

Sea $B^2 = \mathrm{Coker(B^1 \to I^1)}$ y continuamos de la misma manera.
El homomorfismo entre las resoluciones se construye paso a paso usando la definición de objeto inyectivo. □

Consideremos las resoluciones inyectivas de M y N, construidas como en el Lema anterior:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & M & \xrightarrow{i_0} & I^0 & \xrightarrow{\pi_0} & I^0/\mathrm{Im}(i_0) & \xrightarrow{i_1} & I^1 & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N & \xrightarrow{i'_0} & J^0 & \xrightarrow{\pi'_0} & J^0/\mathrm{Im}(i'_0) & \xrightarrow{i'_1} & J^1 & \longrightarrow & \ldots
\end{array}$$

Como i_0 es un homomorfismo inyectivo, $\alpha \circ i'_0$ es un homomorfismo cualquiera e J^0 es un objeto inyectivo entonces existe $\alpha_0 : I^0 \to J^0$ tal que $\alpha_0 \circ i_0 = \alpha \circ i'_0$. Como $\mathrm{Im}(i_0) \subseteq \mathrm{Ker}(\pi'_0 \circ \alpha_0)$ tenemos por teorema de homomorfismo que existe $\beta : I^0/\ \mathrm{Im}(i_0) \to J^0/\mathrm{Im}(i'_0)$, luego usando que J^1 es un objeto inyectivo podemos construir $\alpha_1 : I^1 \to J^1$ de la misma forma que antes.

Realizando lo anterior, tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \\
0 & \longrightarrow & N & \longrightarrow & J^0 & \longrightarrow & J^1 & \longrightarrow & J^2 & \longrightarrow & \ldots
\end{array}$$

Aplicando el funtor F, obtenemos que

$$\begin{array}{ccccccccccc}
0 & \xrightarrow{d^{-1}} & (I^0)^G & \xrightarrow{d^0} & (I^1)^G & \xrightarrow{d^1} & (I^2)^G & \xrightarrow{d^2} & \ldots \\
 & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \\
0 & \xrightarrow{d^{-1}} & (J^0)^G & \xrightarrow{d^0} & (J^1)^G & \xrightarrow{d^1} & (J^2)^G & \xrightarrow{d^2} & \ldots
\end{array}$$

donde se cumple que $\alpha_{r+1} \circ d^r = d^r \circ \alpha_r, \forall r \in \mathbb{N}$, es decir, el diagrama es conmutativo, entonces se define

$$\begin{array}{rcccc}
H^r(\overline{\alpha}) & : & H^r(G,M) & \to & H^r(G,N) \\
 & & [x] & \to & [\alpha_r(x)]
\end{array}$$

Para más detalles ver [14]. □

d) Dada una sucesión exacta de G-módulos

$$0 \to M' \to M \to M'' \to 0$$

se puede asociar una sucesión exacta larga de grupos de cohomología

$$0 \to H^0(G,M') \to \ldots \to H^r(G,M) \to H^r(G,M'') \xrightarrow{\delta_r} H^{r+1}(G,M') \to \ldots$$

Demostración. Consideremos las resoluciones inyectivas $I'^{\circ}, I^{\circ}, I''^{\circ}$ de los $G-$módulos M', M, M'' respectivamente. Entonces obtenemos el siguiente diagrama

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^0 & \longrightarrow & I^0 & \longrightarrow & I''^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^1 & \longrightarrow & I^1 & \longrightarrow & I''^1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \cdots & & \cdots & & \cdots & &
\end{array}$$

Aplicando la propiedad anterior y la exactitud de las sucesiones del diagrama obtenemos la sucesión exacta larga buscada. Para mas detalles consultar [16]. □

e) Si las sucesiones son exactas y siguiente diagrama de G-módulos es conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0
\end{array}$$

entonces el diagrama siguiente

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & M'^G & \longrightarrow & M^G & \longrightarrow & M''^G & \longrightarrow & H^1(G,M') & \longrightarrow & \ldots & \longrightarrow & H^r(G,M) & \longrightarrow & \ldots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N'^G & \longrightarrow & N^G & \longrightarrow & N''^G & \longrightarrow & H^1(G,N') & \longrightarrow & \ldots & \longrightarrow & H^r(G,N) & \longrightarrow & \ldots
\end{array}$$

es conmutativo para todo $r \in \mathbb{N}$.

Demostración. Aplicar propiedad c) y d). [16, Proposition 1.3.3] □

Bibliografía

[1] Artin, Emil, and Tate John Torrence. *Class field theory*. Vol. 366. American Mathematical Soc., 1952.

[2] Aschbacher, Michael. *Finite group theory*. Vol. 10. Cambridge University Press, 2000.

[3] Bucur, Ion, and Deleanu Aristide. *Introduction to the Theory of Categories and Functors*. Vol. 19. John Wiley & Sons, 1968.

[4] Çiperiani, Mirela, and Stix Jakob. *Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels*. Journal für die reine und angewandte Mathematik (Crelles Journal)(2015), 175-207.

[5] Creutz, Brendan. *Locally trivial torsors that are not Weil–Châtelet divisible*. Bulletin of the London Mathematical Society 45.5 (2013), 935-942.

[6] Creutz, Brendan. *On the local-global principle for divisibility in the cohomology of elliptic curves*. arXiv preprint arXiv:1305.5881 (2013).

[7] Dummit, David Steven, and Foote Richard M. *Abstract algebra*. Vol. 3. Hoboken: Wiley, 2004.

[8] Dvornicich, Roberto, and Zannier Umberto. *Local-global divisibility of rational points in some commutative algebraic groups*. Bulletin de la Société mathématique de France 129.3 (2001), 317-338.

[9] Dvornicich, Roberto, and Zannier Umberto. *On a local-global principle for the divisibility of a rational point by a positive integer*. Bulletin of the London Mathematical Society 39.1 (2007): 27-34.

[10] Gillibert Florence, and Ranieri Gabriel. *On the local global divisibility over abelian varieties*. Annales de L'Institutut Fourier (2018): 847-873.

[11] Hungerford, Thomas W. *Algebra*. Volume 73 of graduate texts in mathematics. (1980).

[12] Lang, Serge.*Number theory. III. Diophantine geometry*. Encyclopaedia of Mathematical Sciences, 60.(1991).

[13] Merel, Loïc. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Inventiones mathematicae 124.1-3 (1996), 437-449.

[14] Milne, J. S.*Class field theory, Course notes*. (2013).

[15] Mumford, David.*Abelian varieties*. Volume 5 of Tata Institute of Fundamental Research Studies in Mathematics. Published for the Tata Institute of Fundamental Research, Bombay (2008).

[16] Neukirch, Jürgen, Schmidt Alexander, and Wingberg Kay. *Cohomology of number fields*. Vol. 323. Springer Science & Business Media. (2013).

[17] Paladino, Laura, Ranieri Gabriele, and Viada Evelina.*On local–global divisibility by pn in elliptic curves*. Bulletin of the London Mathematical Society 44.4 (2012), 789-802.

[18] Ranieri, Gabriele.*Counterexamples to the local–global divisibility over elliptic curves*. Annali di Matematica Pura ed Applicata (2017), 1-11.

[19] Sansuc, J-J. *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*. Journal für die reine und angewandte Mathematik 327 (1981), 12-80.

[20] Serre, J.P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math.15 (1972), 259-331.

[21] Silverman, Joseph H.*The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[22] Tate, John.*Duality theorems in Galois cohomology over number fields*. Proc. Internat. Congr. Mathematicians (Stockholm, 1962). 1962.