VARIEDADES ABELIANAS, MULTIPLICACIÓN COMPLEJA Y FORMAS MODULARES

CARLOS EDUARDO MARTÍNEZ AGUILAR

Capítulo 1

Variedades Abelianas

Definición 1.1 *Entenderemos por una variedad grupo como una variedad no singular (afín, proyectiva, analítica o abstracta) G con una estructura de grupo tales que los mapeos que la definen*

$$m : G \times G \to G \ \ (x, y) \mapsto xy, \quad i : G \to G \ \ x \mapsto x^{-1}$$

están definidos en todo G y racionales. Diremos que la variedad grupo G esta definida sobre un campo K si (G, m, i) están definios sobre K. Nosotros diremos que G es una variedad abeliana si G es una variedad proyectiva.

Es posible demostrar que toda variedad abeliana es conmutativa con su producto, por lo que utilizaremos notación aditiva para estas. Toda subvariedad de una variedad abeliana que herede la estructura de grupo tiene una estructura de variedad abeliana propia y por lo tanto diremos que es una subvariedad abeliana. Diremos que una variedad abeliana es *simple* si la unica subvariedad abeliana que tiene es $\{0\}$.

Si G y H son variedades abelianas, un *homomorfimo* de variedades abelianas es un mapeo racional $\varphi : G \to H$ que sea a su vez morfismo de grupos, es decir

$$\varphi(x + y) = \varphi(x) + \varphi(y) \ \ \forall\{x, y\}.$$

Denotamos por $Hom(G, H)$ al conjunto de homomorfimos entre dos variedades abelianas y llamaremos *grupo de endomorfismos* a $End(G) = Hom(G, G)$, es un resultado básico que $Hom(G, H)$ es un grupo abeliano libre de rango finito y que si G y H están definidos sobre K, entonces $Hom(G, H)$ esta definido sobre una extensión separable de $\mathbb{Q}$. Así definimos

$$Hom_{\mathbb{Q}}(G.H) := Hom(G, H) \otimes_{\mathbb{Z}} \mathbb{Q}, \qquad End_{\mathbb{Q}} := End \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Claramente $End(G)_{\mathbb{Q}}$ tiene una estructura de algebra sobre $\mathbb{Q}$ con una unidad dada por Id_G.

Para dos variedades abelianas A y B de la misma dirección existe un homomorfismo $A \to B$ si y sólo si existe uno $B \to A$, en cuyo caso decimos que A y B son *isogeneos* y cuales quiera de los morfimos mencionados se les llama una *isogenía*. Dada $\lambda \in Hom(A,B)$ con A y B de la misma dimensión, K el campo de definición de A y B, y x un punto genérico de A sobre K y λ una isogenía, definimos

$$\nu(\lambda) = [K(x) : K(\lambda\, x)],$$
$$\nu_s(\lambda) = [K(x) : K(\lambda\, x)]_s, \;\; \nu_i(\lambda) = [K(x) : K(\lambda\, x)],$$

de otra forma definimos $\nu(\lambda) = \nu_s(\lambda) = \nu_i(\lambda) = 0$. Estos número no dependen de la elección de K y x. Si λ es una isogenía entonces $\nu_s(\lambda)$ es el orden de $Ker(\lambda)$. Para cada isogenía $\lambda : A \to B$ existe un único elemento λ' de $Hom_{\mathbb{Q}}(B,A)$ tal que

$$\lambda\, \lambda' = Id_A \;\text{ y también} \lambda'\, \lambda = Id_B,$$

es decir que λ es un isomorfismo y $\lambda' = \lambda^{-1}$.

1.0.1. Representación l-ádica de homorfismos

Dada una variedad abeliana A y un primo racional $l \in \mathbb{Z}$ definimos

$$\mathfrak{g}_l(A) = \bigcup_{\alpha=1}^{\infty} Ker(l^{\alpha} Id_A). \tag{1.1}$$

Si A es de dimensión n y l no es la característica del campo de definición de A, entonces $\mathfrak{g}_l(A)$ es isomorfo a $\mathfrak{M}$, el cual consiste de la suma directa de $2n$ copias de $\mathbb{Q}_l/\mathbb{Z}_l$. Llamamos a cualquier isomorfismo entre $\mathfrak{g}_l(A)$ y $\mathfrak{M}$ un sistema de coordenadas l-ádicas de $\mathfrak{g}_l(A)$. Pensaremos a un elemento de $\mathfrak{M}$ como un vector columna. Así si B es otra variedad abelliana de dimensión m y $\lambda : A \to B$ es un homomorfismo, entonces existe una matriz $M(\lambda) \in \mathcal{M}(2n \times 2m, \mathbb{Z})$ que representa un morfismo $M(\lambda) : \mathfrak{g}_l(A) \to \mathfrak{g}_l(B)$ dado por

$$\begin{array}{ccc} \mathfrak{g}_l(A) & \xrightarrow{\lambda} & \mathfrak{g}_l(A) \\ \downarrow{\scriptstyle \mathfrak{m}_A} & & \downarrow{\scriptstyle \mathfrak{m}_B} \\ \mathfrak{M}_A & \xrightarrow{M(\lambda)} & \mathfrak{M}_B \end{array}$$

donde $\mathfrak{m}_A$ y $\mathfrak{m}_B$ son los isomorfismos entre $\mathfrak{g}_l(A)$ y $\mathfrak{M}_A$ y $\mathfrak{g}_l(B)$ y $\mathfrak{M}_B$ respectivamente. Así si fijamos los isomrfismos, tenemos una correspondencia $\lambda \mapsto M(\lambda)$, que puede extenderse a un único mapeo $\mathbb{Q}$- lineal de $Hom_{\mathbb{Q}}(A,B)$ en $M(2n \times 2m, \mathbb{Q}_l)$, la cual llamamos la representación l-ádica de $Hom_{\mathbb{Q}}(A,B)$ con respecto de $\mathfrak{m}_A$ y $\mathfrak{m}_B$. En particular si $A = B$, tenemos un morfismo de anilllos entre $End_{\mathbb{Q}}(A)$ y $M(4n^2, \mathbb{Q}_l)$.
Si denotamos por M_l a la representación l-ádica de $End_{\mathbb{Q}}(A)$ y tomamos $\xi \in End_{\mathbb{Q}}(A)$, entonces definimos el polinomio característico de ξ como el polinomio

caracteístico de $M_l(\xi)$, resulta que éste no depende de las coordenadas l-ádicas escogidas. Si escribimos el polinomio característico de $\xi \in End_{\mathbb{Q}}(A)$ como

$$P(X) = X^{2n} + a_1 X^{2n-1} + \cdots + a_{2n},$$

entonces $a_i \in \mathbb{Q} \forall\, 1 \leq i \leq 2n$, además resulta que

$$P(\xi) = \xi^{2n} + a_1 \xi^{2n-1} + \cdots + a_{2n} Id_A = 0.$$

Más aún si $\xi \in End(A)$, entonces $a_i \in \mathbb{Z}$. Con esto también podemos definir la traza y el determinante de ξ como

$$tr(\xi) = tr(M_l(\xi)), \quad \nu(\xi) = det(M_l(\xi)),$$

respectivamente.

Teoría analítica de variedades abelianas

Funciones theta y formas de Riemann (o de polarización)

Sea $D \subset \mathbb{C}^n$ un subgrupo discreto aditivo de rango $2n$, entonces $\mathbb{C}^n/D$ es un toro complejo.

Definición 1.2 *Decimos que una función meromorfa $f : \mathbb{C}^n \to \mathbb{C}$ es una función theta en $\mathbb{C}^n$ si se cumple*

$$f(z+d) = f(z) \exp[l_d(z) + c_d], \;\; \forall d \in D, \tag{1.2}$$

donde $l_d : \mathbb{C}^n \to \mathbb{C}$ es una forma $\mathbb{C}$-linear y $c_d \in \mathbb{C}$, ambos dependen de d.

Para determinar los valores de l_d y c_d de la definición, hacemos uso de las formas de Riemann, también llamadas formas de polarización.

Definición 1.3 *Decimos que una forma $\mathbb{R}$-bilinear $E(x,y)$ en $\mathbb{C}^n$ con valores reales, es una forma de Riemann en $\mathbb{C}^n/D$ si satisface las siguientes condiciones:*

i) $E(x,y) \in \mathbb{Z}$ *para todo* $\{x,y\} \subset D$.

ii) $E(x,y) = -E(y,x)$.

iii) La forma bilineal $(x,y) \mapsto E(x,iy)$ es simétrica, postitiva definida pero no necesariamente no degenerada.

Es posible demostrar que existen dos $\mathbb{R}$-formas bilineales con valores en $\mathbb{C}$, H y H_0 y una forma bilinearcon valores en $\mathbb{R}$, β todas definidas en $\mathbb{C}^n$ y que se relacionan con la función theta f de la siguiente forma

$$f(z+d) = f(z) \exp\big\{2\pi i\big[H(d,z) + \frac{1}{2}H_0(d,d) + \beta(d)\big]\big\}. \tag{1.3}$$

Donde

$$H_0(u,v) = H_0(v,u) \quad \forall\{u,v\} \subset \mathbb{C}^n \tag{1.4}$$

$$H(d_1,d_2) \equiv H_0(d_1,d_2) \quad \text{mód } \mathbb{Z} \quad \forall\{d_1,d_2\} \subset D. \tag{1.5}$$

Así definimos

$$E(x,y) = H(x,y) - H(y,x),$$

la cual llamaremos la forma de polarización definida por f. Si f es holomorfa, entonces E es una forma de Riemann en $\mathbb{C}^n/D$ y llamamos a E como la forma de Riemann definida por f. Decimos que una función theta es *normalizada* si H es semi-hermiteana y β es real valuada, en cuyo caso

$$H(x,y) = \frac{1}{2}\big[E(x,y) - iE(x,iy)\big]. \tag{1.6}$$

Por otro lado si $E(x,y)$ es una forma de Riemann en $\mathbb{C}^n/D$, entonces existe una función theta holomorfa en $\mathbb{C}^n/D$ tal que E es su forma de Riemann asociada.

Si f es una dunción theta en $\mathbb{C}^n/D$, entonces el divisor de f, $div(f)$ es un divisor analítico en $\mathbb{C}^n/D$. De la misma manera en que hay una correspondencia entre funciones theta y formas de Riemann, hay una correxpondencia entre funciones theta y divisores. Si X es un divisor anaítico de $\mathbb{C}^n/D$, entonces existe una función theta f tal que $X = div(f)$. Así un divisor X define a su vez una forma de Riemann, la cual denortaremos por $E(X)$.

Existe un resultado básico de variedades abelianas que dice que $\mathbb{C}^n/D$ es una variedad abeliana si y sólo si existe una forma de Riemann no degenerada en $\mathbb{C}^n/D$.

Dada una variedad abeliana sobre $\mathbb{C}$ A, existe un isomorfismo analítico θ entre A y un toro complejo $\mathbb{C}^n/D$. Llamamos $(\mathbb{C}^n, \theta)$ un sistema de coordenadas analítico para A. Si X es un divisor analitico de A entonces $\theta(X)$ es un divisor analítico de $\mathbb{C}^n/D$, llamaremos $E(X) = E(\theta(X))$ la forma de Riemann definida por X. Resulta que $E(X) = E(Y)$ si y sólo si X y Y son algebraicamente equivalentes.

Representaciones analíticas y racionales

Sean A_1 y A_2 variedades abelianas definidas sobre $\mathbb{C}$, sean $(\mathbb{C}^n/D_1, \theta_1)$ y $(\mathbb{C}^m/D_2, \theta_2)$ sistemas de coordenadas anaíticas para A_1 y A_2 respectivamente. Consideramos un homomorfismo $\lambda : A_1 \to A_2$. Asi existe un mapeo lineal $\Lambda : \mathbb{C}^n \to \mathbb{C}^m$ tal que

$$\theta_2 \circ \lambda = \Lambda \circ \theta_1,$$

esto quiere decir que Λ satisface que $\Lambda(D_1) \subset D_2$. Similarmente cualquier mapeo lineal de $\mathbb{C}^n$ en $\mathbb{C}^m$ que mande D_1 dentro de D_2 define un homomorfismo de A_1 en A_2. Con respecto al sistema de coordendas $(z_1, \cdots, z_n)$ y $(w_1, \cdots, w_m)$, Λ se representa con una matriz con ceficientes complejos de $m \times n$ dimensiones, $S = (s_{ij})$, si pensamos a las coordenadas como funciones tenemos que

$$w_i \circ \Lambda = \sum_{j=1}^{n} s_{ij} z_j \;\; \forall\, 1 \leq i \leq m.$$

El mapeo $\lambda \mapsto \Lambda$ se puede extender de manera única a una representación en $Hom_{\mathbb{Q}}(A_1, A_2)$ la cual llamamos *representación analítica* con respecto a los sistemas analíticos de coordenadas θ_1 y θ_2.

Ahora sea:

$$\omega_j = d\, z_j \circ \theta_1, \;\; \eta_i = d\, w_i \circ \theta_2.$$

Podemos ver facilmente que $\{\omega_1, \cdots, \omega_n\}$ es una base de $\mathfrak{D}_0(A_1)$ el espacio de las 1-formas invariantes a la izquierda en A_1, tambíen es claro que $\{\eta_1, \cdots, \eta_m\}$ es una base de $\mathfrak{D}_0(A_2)$, claramente

$$\delta\lambda(\eta_i) = \sum_{j=1}^{n} s_{ij}\omega_j \;\; \forall\, 1 \leq i \leq m.$$

Esto muestra que S es la matriz transpuesta a $\delta\lambda$ con respecto a las bases $\{\omega_j\}$ y $\{\eta_i\}$. Sean $\{u_i, \cdots, u_{2n}\}$ y $\{v_1, \cdots, v_{2m}\}$ bases de D_1 y D_2 respectivamente (como $\mathbb{Z}$-módulos libres), Λ es un morfismo entre D_1 y D_2, entonces existe una matriz $M = (a_{ij}) \in M(2n \times 2m, \mathbb{Z})$ tal que

$$\Lambda(u_j) = \sum_{i=1}^{2m} a_{ij} v_i \;\; \forall\, 1 \leq j \leq 2n.$$

Igual que antes las correspondencia $\lambda \mapsto M$ se extiende de manera única a una representación de $Hom_{\mathbb{Q}}(A_1, A_2)$, la cual llamamos la representación racional de $Hom_{\mathbb{Q}}(A_1, A_2)$ con respecto a $\{u_j\}$ y $\{v_i\}$. Se puede verificar que la representación l-ádica es equivalente a la representación racional de $End_{\mathbb{Q}}(A)$. Sea U la matriz de $n \times 2n$ cuyos vectores columna son $\{u_j\}$ y sea V la matriz con vectores columna $\{v_i\}$,entonces con la notación anterior:

$$SU = VM,$$

así sucede que

$$\begin{pmatrix} S & 0 \\ 0 & \overline{S} \end{pmatrix} \begin{pmatrix} U \\ \overline{U} \end{pmatrix} = \begin{pmatrix} V \\ \overline{V} \end{pmatrix} M, \tag{1.7}$$

donde la línea significa conjugación compleja, así si $A_1 = A_2$, $D_1 = D_2$, $\theta_1 = \theta 2$ y $U = V$, entonces como la matriz $\begin{pmatrix} U \\ \overline{U} \end{pmatrix}$, es invertible, entonces M es equivallente a la suma directa de S y $\overline{S}$.

1.1. Variedades abelianas con multiplicación compleja

Sea R una $\mathbb{Q}$-álgebra simple y Z su centro, supongamos que $[R : Z] = f^2$, además supongamos que $[Z : \mathbb{Q}] = d$, entonces R tiene d representaciones irreducibles no equivalentes en la cerradura de $\mathbb{Q}$ que son de grado f. Diremos que una representación S de R en una extensión de $\mathbb{Q}$ es una *reprecentación reducida* si es equivalente a la suma direcra de dichas d representaciones irreducibles. Si S es una representación reducida, el polinomio característico de $S(\alpha)$ tiene coeficientes racionales para toda $\alpha \in R$. Definimos para $\alpha \in R$

$$N(\alpha) = det\, S(\alpha), \;\; Tr(\alpha) = tr\, S(\alpha), \tag{1.8}$$

la *norma reducida* y *traza reducida* respectivamente, éstas son independientes de la elección de S.

Lema 1.1 *Sea R un álgebra simple sobre $\mathbb{Q}$ y S una representación de R en una extensión de $\mathbb{Q}$. Supongamos que para cada α, el polinomio característico de $S(\alpha)$ tiene coeficientes racionales, entonces S es equivalente a la suma de múltiples representaciones reducidas de R y una 0-representación.*

Demostración. Sean $\{S_i\}$, $1 \leq i \leq d$ las representaciones irreducibles no equivalentes de R en la cerradura algebraica L de $\mathbb{Q}$ en la extensión. Así S es equivalente a la suma directa de las representaciones $m_i S_i$ más una 0- representación, donde los m_i denotan las mulltiplicidades. Sean σ_i $1 \leq i \leq d$ los isomorfismos del centro de R, Z en L, entonces tras reordenamiento (si es necesario) $S_i(\alpha)$ es una matriz diagonal $\alpha^{\sigma_i} Id_f$ para $\alpha \in Z$ $\forall 1 \leq i \leq d$. Por lo tanto el polinomio caracteríoco de $S(\alpha)$ es de la forma

$$p(x) = \prod_{i=1}^{d} (x - \alpha^{\sigma_i})^{m_i f}.$$

Por nuestras hipótesis los m_i son iguales y tenemos el resultado. ■

Proposición 1.2 *Sea A una variedad abeliana de dimensión n y $\mathfrak{S} \subset End_{\mathbb{Q}}(A)$ una subálgebra conmutativa y semi simple, entonces tenemos que*

$$[\mathfrak{S} : \mathbb{Q}] \leq 2n.$$

Si $[\mathfrak{S} : \mathbb{Q}] = 2n$, entonces el conmutador de $\mathfrak{S}$ en $End_{\mathbb{Q}}(A)$ coincide con $\mathfrak{S}$.

Demostración. Sean K_i las componentes simples de $\mathfrak{S}$. Como $\mathfrak{S}$ es conmutativo, cada K_i es un campo. Sean $d_i = [K_i : \mathbb{Q}]$ y sea S_i una representación reducida para K_i, sea l un primo distinto a la característica del campo que define A y consideremos M_l una representación l-ádica de $End_{\mathbb{Q}}(A)$. Por 1.1, la restricción de M_l a K_i es equivalente a la suma directa $m_i S_i$ y una 0-representación. Similarmente la restricción de M_l en $\mathfrak{S}$ es equivalente la suma de $m_i S_i$ y una

0-representación. Como M_l es una representación fiel, entonces los m_i son positivos. Por lo tanto

$$2n \geq \sum_i m_i d_i \geq \sum_i d_i = [\mathfrak{S} : \mathbb{Q}].$$

Ahora supongamos que $2n = [\mathfrak{S} : \mathbb{Q}]$ y supongamos que $\mathfrak{S}'$ es el conmutador de $\mathfrak{S}$ en $End_{\mathbb{Q}}(A)$. Así es posible encontrar una matríz P con coeficientes en la cerradura algbraica de $\mathbb{Q}_l$ tal que $PM_l(\xi)P^{-1}$ es una matriz diagonal para cada $\xi \in \mathfrak{S}$. Como $[\mathfrak{S} : \mathbb{Q}] = 2n$, existe un elemento $\alpha \in \mathfrak{S}$ tal que los componente diagonales de $PM_l(\alpha)P^{-1}$ sean distintos. Como para toda $\eta \in \mathfrak{S}'$, $PM_l(\eta)P^{-1}$ conmuta con $PM_l(\alpha)P^{-1}$, entonces $PM_l(\eta)P^{-1}$ es una matriz diagonal para toda $\eta \in \mathfrak{S}'$, esto implica que $\mathfrak{S}'$ es un álgebra conmutativa semi simple. entonces lo que acabamos de probar muestra que $[\mathfrak{S} : \mathbb{Q}] \leq 2n$, por lo tanto $\mathfrak{S} = \mathfrak{S}'$. ■

Proposición 1.3 *Sea A una variedad abeliana de dimensión n, y sea R una subálgebra simple de $End_{\mathbb{Q}}(A)$ y Z el centro de R con*

$$[R : Z] = f^2, \quad [Z : \mathbb{Q}] = d.$$

Supongase que R contiene a la identidad. Entonces $fd|2n$ y si escribimos $2n = fdm$, tenemos que para cada $\alpha \in R$ se cumple

$$\nu(\alpha) = N(\alpha)^m, \quad tr(\alpha) = mTr(\alpha).$$

Demostración. Sea S una representación reducida de R y sea l primo distinto a la característica del campo de definición de A, sea M_l representación l-ádica de $End(A)_l$. Por 1.1 la restricción de M_l a R es equivalente a un múltiplo mS con $m \in \mathbb{Z}$, así $2n = fdm$ y el polinomio característico de $M_l(\alpha)$ es la m-ésima potencia de el se $S(\alpha)$. ■

Proposición 1.4 *Sea A variedad abeliana de dimensión n. Si $End_{\mathbb{Q}}(A)$ contiene un campo F de grado $2n$ sobre $\mathbb{Q}$, entonces A es isogéneo a un producto $B \times \cdots \times B$ con B variedad abeliana simple. El conmutador de F en $End_{\mathbb{Q}}(A)$ coincida con F y además*

$$\nu(\alpha) = N_{F/\mathbb{Q}}(\alpha), \quad tr(\alpha) = Tr_F/\mathbb{Q}(\alpha).$$

Véase [3][p. 37]

Proposición 1.5 *Sean A, B y F como en la proposición anterior, sea m la dimensión de B y h el número de veces que aparece B en el producto isogeneo a A. Sea K el centro de $End_{\mathbb{Q}}(B)$, entonces K es un subcampo de F y si*

$$[K : \mathbb{Q}] = f, \quad [End_{\mathbb{Q}}(B) : K] = g^2,$$

entonces sucede que $2n = fgh$, $2m = fg$.

De lo anterios se y el el siguente resultado, podremos saber mucho sobre la estructura de las variedades abelianas

Proposición 1.6 *Sea B una variedad abeliana simple y K el centro de $End_{\mathbb{Q}}(B)$, entonces K es un campo totalmente real o una extensión totalmente imaginaria cuadrática de un campo totalmente real.*

Corolario 1.7 *Si seguimos la notación de la proposicón 1.5 y suponemos que la característica del campo que define a A es cero, entonces $End_{\mathbb{Q}}(B) = K$.*

Demostración. Si la característica es 0, consideramos una representación racional de $End_{\mathbb{Q}}(B)$ de grado $2m$ (la dimensión de B). Como $End_{\mathbb{Q}}(B)$ es un álgebra con divisón, el grado cualquier representación de $End_{\mathbb{Q}}(B)$ es divisble por $[End_{\mathbb{Q}}(B) : \mathbb{Q}] = fg^2$, así como $2m = fg$, entonces $g = 1$ y $End_{\mathbb{Q}}(B) = K$. ■

Tipos CM

Definición 1.4 *Sea R un álgebra sobre $\mathbb{Q}$ con unidad 1, definimos una variedad abeliana de tipo (R) como el par (A, ι), donde A es una variedad abeliana y $\iota : R \to End_{\mathbb{Q}}(A)$ es un isomorfismo de álgebras. Frecuentemente usaremos sólo A en lugar de (A, ι).*

Sea F un campo numérico algebraico y (A, ι) una variedad abeliana de dimensión n de tipo (F). Como sabemos por la proposición 1.3 $[F : \mathbb{Q}]$ divide a $2n$, entonces investigamos cuando $[F : \mathbb{Q}] = 2n$, además asumiremos que la característica de F es 0. En dado caso A es isomorfo a un toro complejo y así tenemos una representación racional de A, M y una representación analítica S de $End_{\mathbb{Q}}(A)$ proveniente de el sistema de coordenadas analíticas. M es de grado $2n$, y S es de grado n, además $M \cong S \oplus \overline{S}$. Sean $\{\varphi_1, \cdots, \varphi_{2n}\}$ los isomorfismos de F en $\mathbb{C}$, entonces por el lema 1.1, la representación M restringida a F es equivalente a la suma directa de φ_i, así podemos reordenar a los φ_i de tal forma que S sea la suma directa de $\{\varphi_1, \cdots, \varphi_n\}$ y $\overline{S}$ es equivalente a la suma directa de $\{\varphi_{n+1}, \cdots, \varphi_{2n}\}$ y por lo tanto éste ultimo conjunto es igual a $\{\overline{\varphi_1}, \cdots, \overline{\varphi_n}\}$. Más aún observamos que F es totalmente imaginario, así decimos que (A, ι) es de tipo $(F; \{\varphi_1, \cdots, \varphi_n\})$. Ahora S es equivalente a representación de $End_{\mathbb{Q}}(A)$ por formas diferenciales invariantes, por lo que podemos encontrar n 1-formas difereneciales invariantes en A tales que para cada $\alpha \in F$,

$$\delta_\iota(\alpha) = \alpha^{\varphi_i}\omega_i \ \ \forall\, 1 \leq i \leq n.$$

Por otra lado, dadas dichas ω_i, entonces (A, ι) es de tipo $(F : \{\varphi_i\})$ y las ω_i forman una base para $\mathfrak{D}_0$.

Ahora consideremos K el centro de $End_{\mathbb{Q}}(A)$ que también es el centro de $End_{\mathbb{Q}}(B)$, donde B es una subvariedad abeliana de A determinada en la misma forma que en la proposición 1.4. Por la proposición 1.6 K es totalmente real o una extensión cuadrática imaginaria de un campo totalmente real, además por

la proposiciones 1.5 y el corolario de 1.6, tenemos que $[K : \mathbb{Q}] = 2\dim(B)$, lo que significa que podemos aplicar a B y K lo que hemos hecho con A y F, lo que significa que K tiene que ser totalmente imaginario. Sea S' una representación analítica de $End_{\mathbb{Q}}(B)$, entonces A es isogenea al producto de h copias de B y la restricción de S a K es equivallente al producto de h copias de S'. Por lo tanto la restricción de $\{\varphi_1, \cdots, \varphi_n\}$ a K nos dan $f/2$ isomorfismos $\{\psi_1, \cdots, \psi_{f/2}\}$ de K a un subcampo de $\mathbb{C}$, cada uno repetido h veces, donde $f = [K : \mathbb{Q}]$, además S' es equivalente a las suma directa de los ψ_j y éstos no son conjudagos complejos uno de los demás.

Definición 1.5 *Dado un campo numérico algebraico F de grado $2n$ y n distintos isomorfismos $\{\varphi_1, \cdots, \varphi_n\}$ de F en $\mathbb{C}$, decimos que el par $(F; \{\varphi_1, \cdots, \varphi_n\})$ es de tipo CM (complex multiplication) si existe una variedad abeliana de dimensión n de tipo $(F : \{\varphi_i\})$.*

Teorema 1.8 *El par $(F; \{\varphi_i\})$ es de tipo CM si y solo sí F contiene a dos campos K y K_0 que satisfacen las siguientes condiciones:*

(CM 1) K_0 es totalmente real y K es una extensión cuadrática totalmente imaginaria de K_0

(CM 2) Ninguno de los isomorfismos φ_i son conjugados complejos entre ellos.

El reflex de un tipo CM

A partir de ahora todos los campos que aparezcan son subcampos de $\mathbb{C}$.

Lema 1.9 *Sea L una extensión de Galois de $\mathbb{Q}$ y G el grupo de Galois de dicha extensíon, sea también $\rho \in G$ el elemento que manda a cada $\xi \in L$ a su conjugado complejo, es decir $\xi^\rho = \overline{\xi}$. Sean K y K_0 subcampos de L tales que $[K : K_0] = 2$, y H, H_0 los subgrupos de G correspondientes, entonces las siguientes condiciones son equivalentes*

i) K_0 es un campo totalmente real y K es totalmente imaginario

ii) $H_0 = H \cup \sigma\rho\sigma^{-1}$ para toda $\sigma \in G$.

si estas condiciones se satisfacen, entonces se tiene que

$$\rho H\tau = H\tau\rho = \sigma\rho\sigma - 1H\tau = H\tau\sigma\rho\sigma^{-1}, \quad \forall\, \{\sigma, \tau\} \subset G.$$

Véase [3][p.60]

Proposición 1.10 *Sea F una extensión de $\mathbb{Q}$ de grado n y $\{\varphi_1, \cdots, \varphi_n\}$ un conjunto de n isomorfismos de F a $\mathbb{C}$ distintos. Sea L una extensión de Galois de $\mathbb{Q}$ que contiene a F y G el grupo de galois de $L/\mathbb{Q}$. Denotamos por ρ al elemento de G correspondiente a la conjugación compleja como antes y consideramos S el conjunto de todos los elementos de G que inducen algún φ_i en F. Entonces $(F; \{\varphi_i\})$ es un tipo CM si y sólo si tenemos*

$$G = S \cup S\sigma\rho\sigma^{-1}, \;\; S\sigma\rho\sigma^{-1} = \sigma\rho\sigma^{-1}S \quad \forall\, \sigma \in G.$$

Como podemos apreciar la proposición anterio junto com el lema 1.9 son una forma de recontextualizar el teorema 1.8.

Tipos CM primitivos

Diremos que un tipo CM es primitivo si la variedad abeliana de dicho tipo es simple (recordemos que las variedades abelianas del mismo tipo CM son isogéneas). El siguiente resultado es un criterio para la primitividad de un tipo CM

Proposición 1.11 *Dado un tipo CM $(F;\{\varphi_i\})$, sean L, G, ρ, S como en la proposición anterior y H_1 el subgrupo de G que corresponde a F. Sea*

$$H := \{\gamma \in G \,\big|\, \gamma S = S\}.$$

Entonces $(F;\{\varphi_i\})$ es primitivo si y sólo si $H_1 = H'$

La siguiente proposición es a su vez la definición de el campo reflex de un tipo CM y la afirmación de que éste es primitivo, junto con una descripcíon del mismo

Proposición 1.12 *Sean $(F;\{\varphi_i\})$, L, G, ρ, S como en la proposición anterior, definimos*

$$S^* := \{\sigma^{-1} \,\big|\, \sigma \in S\}, \quad H^* := \{\gamma \,\big|\, \gamma \in G,\, \gamma S^* = S^*\}. \tag{1.9}$$

Sea K^* el subcampo de L correspondiente al subgrupo H^* y $\{\psi_j\}$ el conjunto de los isomorfimos de K^* a $\mathbb{C}$ correspondientes a elementos de S^*. Entonces $(K^*;\{\psi_j\})$ es un tipo CM primitivo y

$$K^* = \mathbb{Q}\Big(\sum_i \xi^{\varphi_i} \,|\, \xi \in F\Big). \tag{1.10}$$

$(K^*;\{\psi_j\})$ esta deteminado únicamente por $(K;\{\varphi\})$ y es independiente de la elección de L. A $(K^*;\{\psi_j\})$ le llamamos el campo reflex de $(K;\{\varphi\})$.

Bibliografía

[1] Stein, W., *Algebraic Number Theory a Computaional Approach*

[2] Weil, A., *Foundations of Algebraic Geometry*

[3] Shimura, G.,*Abelian Varieties with Complex Multiplication and Modular Functions, Princeton University Press*