Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática
Seminario Grupos Formales

Grupo asociado a un grupo formal
Francisco Gallardo
7 de septiembre, 2022

La mayoría de resultados en este documento provienen del libro de Silverman, [S] De momento, un grupo formal $F \in R[[X,Y]]$ es como una operación de grupo, pero sobre ningún conjunto. Veremos que cuando el anillo R es local y completo, es posible asignar un grupo (de toda la vida) a nuestro grupo formal F.

1. Preliminares

Definición 1. Un grupo formal sobre un anillo R es una $F \in R[[X,Y]]$ tal que

(a) $F(X,Y) = X + Y + \sum_{i,j\geq 1} a_{ij} X^i Y^j$.

(b) $F(F(X,Y),Z) = F(X,F(Y,Z))$.

F será conmutativo si además cumple

(c) $F(X,Y) = F(Y,X)$.

Definición 2. Sean $F, G \in R[[X,Y]]$ grupos formales. Un morfismo $f\colon F \to G$ es una serie $f(T) \in R[[T]]$ tal que

$$f(F(X,Y)) = G(f(X), f(Y)).$$

Proposición 1 (Teorema de la función inversa formal)**.** Sea $f(T) \in R[[T]]$ una serie formal de la forma

$$f(T) = aT + \sum_{j\geq 2} a_j T^j, \qquad a \in R^\times.$$

Luego existe un único $g(T) \in R[[T]]$ tal que

$$f(g(T)) = T.$$

Además, se satisface $g(f(T)) = T$.

Demostración. Construiremos una secuencia de polinomios $g_n(T) \in R[T]$ tales que

$$f(g_n(T)) \equiv T \pmod{T^{n+1}} \quad \text{y} \quad g_{n+1} \equiv g_n \pmod{T^{n+1}}.$$

Luego el límite $g(T) \in R[[T]]$ existe y satisface $f(g(T)) = T$.

La construcción será inductiva. La definición de g_1 es clara: $g_1(T) = a^{-1}T$. Ahora supongamos que g_{n-1} ha sido construido y cumple con las condiciones pedidas. Luego nuestro $g_n(T)$ debe cumplir

$$g_n(T) = g_{n-1}(T) + \lambda T^n$$

para algún $\lambda \in R$ que escogeremos de manera que $f(g_n(T)) \equiv T \pmod{T^{n+1}}$.

Para esto, usamos la hipótesis inductiva y calculamos

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}) + a\lambda T^n \pmod{T^{n+1}} \\ &\equiv T + bT^n + a\lambda T^n \pmod{T^{n+1}}, \quad b \in R. \end{aligned}$$

Es clara ahora la elección: $\lambda = a^{-1}b$. Esto completa la demostración de la existencia.

Ahora podemos aplicar el mismo proceso a nuestro $g(T) = a^{-1}T + \cdots \in R[[T]]$ para encontrar un $h(T) \in R[[T]]$ tal que $g(h(T)) = T$. Luego

$$g(f(T)) = g(f(g(h(T)))) = g(h(T)) = T.$$

Para la unicidad, supongamos que $G(T) \in R[[T]]$ es otra serie que satisface $f(G(T)) = T$. Luego $g(T) = g(f(G(T))) = G(T)$, mostrando que $g(T)$ es única. □

Proposición 2 (Existencia de inverso)**.** Sea $F \in R[[X, Y]]$ grupo formal. Luego existe una única serie $i(X) \in R[[X]]$ tal que $F(X, i(X)) = 0$.

Demostración. Consideremos la serie $H(X, Y) = X - F(X, Y) \in R[[X]][[Y]]$. Notemos que H no tiene término constante y el término que acompaña a Y es $-1 \in R[[X]]^\times$. Así, podemos usar la Proposición 1 para obtener $G(X, Y) \in R[[X]][[Y]]$ tal que $H(X, G(X, Y)) = Y$, o bien, $F(X, G(X, Y)) = X - Y$. Reemplazando Y por X obtenemos $F(X, G(X, X)) = 0$.

Definimos $i(X) \in R[[X]]$ por $i(X) = G(X, X)$. □

Es fácil ver que $i(T) = -T \pmod{T^2}$ y que $i\colon F \to F$ es morfismo.

Para un grupo formal $F \in R[[X, Y]]$, definimos inductivamente para cada $m \in \mathbb{Z}$:

$$[0](T) = 0, \qquad [m+1][T] = F([m](T), T), \quad \text{y} \quad [m-1][T] = F([m](T), i(T)).$$

Proposición 3. Sea $F \in R[[X, Y]]$ grupo formal.

(a) $[m]\colon F \to F$ son morfismos para todo $m \in \mathbb{Z}$.

(b) $[m](T) \equiv mT \pmod{T^2}$.

(c) Si $m \in R^\times$, entonces $[m]$ es isomorfismo.

Demostración. Notemos primero que como F es conmutativo, entonces

$$\begin{aligned} F(F(A, B), F(C, D)) &= F(A, F(B, F(C, D))) \\ &= F(A, F(B, F(D, C))) \\ &= F(A, F(F(B, D), C)) \\ &= F(A, F(C, F(B, D))) \\ &= F(F(A, C), F(B, D)). \end{aligned}$$

(a) Por inducción. El primero caso es simple:

$$[0](F(X, Y)) = 0 = F(0, 0) = F([0](X), [0](Y)).$$

Supongamos que $[m]\colon F \to F$ es morfismo. Luego

$$\begin{aligned}[m+1](F(X,Y)) &= F([m](F(X,Y)), F(X,Y)) \\ &= F(F([m](X),[m](Y)), F(X,Y)) \\ &= F(F([m](X),X), F([m](Y),Y)) \\ &= F([m+1](X),[m+1](Y)).\end{aligned}$$

El cálculo para $[m-1]$ es similar y hay que usar que $i\colon F \to F$ es morfismo (inversión).

(b) Nuevamente el resultado sigue por inducción. Para $m = 0$ es claro. Supongamos ahora que $[m](T) \equiv mT \pmod{T^2}$. Luego

$$[m+1](T) \equiv F([m](T), T) \equiv [m]T + T \equiv (m+1)T \pmod{T^2}.$$

Para $[m-1]$ es similar usando que $i(T) \equiv -T \pmod{T^2}$.

(c) Usando la Proposición 1, para cada entero m encontramos una serie $[m]^* \in R[[T]]$ tal que $[m]([m]^*(T)) = T$. Es fácil probar que $[m]^* : F \to F$ es morfismo y es inverso de $[m]$.

□

2. Convergencia y ley de grupo

Recordemos que un anillo local $(R, \mathfrak{m})$ es un anillo R que tiene un único ideal maximal, $\mathfrak{m}$. El campo residual de $(R, \mathfrak{m})$ es $k := R/\mathfrak{m}$. Un anillo local completo será un anillo local $(R, \mathfrak{m})$ completo con respecto a la topología $\mathfrak{m}$-ádica.

Sea

$$F = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j \in R[[X, Y]]$$

un grupo formal y R un anillo local completo. Definimos sumas parciales

$$F_n(X,Y) = X + Y + \sum_{\substack{i+j \leq n \\ i,j \geq 1}} a_{ij} X^i Y^j, \quad n \geq 1$$

y decimos que F converge en un punto $(a, b) \in R^2$ si $F_n(a, b)$ converge cuando n tiende a infinito. Como R es completo, la secuencia $F_n(a, b)$ converge si y solo si $F_n(a, b)$ es Cauchy.

Proposición 4. Si $a, b \in \mathfrak{m}$, entonces $F(a, b)$ converge a un elemento en $\mathfrak{m}$. Lo mismo vale para $\mathfrak{m}^n$, $n \geq 2$.

Demostración. Sean $a, b \in \mathfrak{m}$ y sea $k \geq 1$. Luego, si $m > n \geq k$, $\sum_{\substack{n \leq i+j \leq m \\ i,j \geq 1}} a_{ij} a^i b^j \in \mathfrak{m}^k$. Ciertamente, si $i + j \geq n \geq k$, $a^i b^j \in \mathfrak{m}^{i+j} \leq \mathfrak{m}^k$ y luego $a_{ij} a^i b^j \in \mathfrak{m}^k$. Además, estamos sumando finitos términos pues $n \leq i + j \leq m$, de manera que su suma sigue estando en el ideal. Esto muestra que la secuencia $F_n(a, b)$ es Cauchy y la completitud de R nos da su convergencia a un elemento en R.

Llamemos L al límite. Como $F_n(a, b)$ converge a L, existe un k tal que $F_k(a, b) - L \in \mathfrak{m}$. Por último, $F_k(a, b) \in \mathfrak{m}$ implica $L = F_k(a, b) - (F_k(a, b) - L) \in \mathfrak{m}$. De manera similar, podemos ver que si $a, b \in \mathfrak{m}^n$, entonces el límite también estará en $\mathfrak{m}^n$. □

La convergencia nos permite ver a F como una función $F\colon \mathfrak{m}^n \times \mathfrak{m}^n \to \mathfrak{m}^n$, $n \geq 1$. A partir de esta función creamos el grupo $F(\mathfrak{m}^n) = (\mathfrak{m}^n, \oplus_F)$, donde $\oplus_F$ se define por

$$a \oplus_F b := F(a, b).$$

El hecho de que $\oplus_F$ sea operación de grupo viene de que F es un grupo formal. Notamos inmediatamente que $F(\mathfrak{m}^n)$ es subgrupo de $F(\mathfrak{m}^k)$ siempre que $m \geq k$.

Ejemplo 1. El grupo aditivo $\hat{\mathbb{G}}_a(\mathfrak{m})$ es simplemente $(\mathfrak{m}, +)$. Notemos la secuencia exacta

$$0 \longrightarrow \hat{\mathbb{G}}_a(\mathfrak{m}) \longrightarrow R \longrightarrow R/\mathfrak{m} \longrightarrow 0.$$

Ejemplo 2. El grupo $\hat{\mathbb{G}}_m(\mathfrak{m})$ es isomorfo a $1 + \mathfrak{m}$ con multiplicación. El morfismo $f\colon \hat{\mathbb{G}}_m(\mathfrak{m}) \to 1 + \mathfrak{m}$, $z \mapsto 1 + z$ es isomorfismo. Ciertamente,

$$f(x \oplus_{\hat{\mathbb{G}}_m} y) = f(x + y + xy) = x + y + xy + 1 = (x + 1)(y + 1) = f(x)f(y),$$

y f es claramente inyectivo y sobreyectivo.

Nuevamente tenemos una secuencia exacta

$$0 \longrightarrow \hat{\mathbb{G}}_m(\mathfrak{m}) \longrightarrow R^\times \longrightarrow (R/\mathfrak{m})^\times \longrightarrow 1.$$

Terminaremos con la siguiente proposición, que nos habla acerca de los puntos de torsión del grupo.

Proposición 5. Sea $F \in R[[X, Y]]$ un grupo formal con R anillo local completo. Luego

(a) Para cada $n \geq 1$, el mapa
$$\frac{F(\mathfrak{m}^n)}{F(\mathfrak{m}^{n+1})} \to \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}$$
inducido por la identidad en conjuntos es isomorfismo de grupos.

(b) Si p la característica del campo residual $k = R/\mathfrak{m}$, entonces $F(\mathfrak{m})^{\text{tors}}$ es un p-grupo (si $p = 0$, entonces $F(\mathfrak{m})$ es libre de torsión).

Demostración. (a) Como el mapa es biyectivo solo hay que ver que es un morfismo de grupos. Pero esto es claro ya que para $x, y \in \mathfrak{m}^n$

$$x \oplus_F y = F(x, y) = x + y + xy \cdot (\text{algo no nulo}) \equiv x + y \pmod{\mathfrak{m}^{2n}}.$$

Como $2n \geq n + 1$ para todo $n \geq 1$, $x \oplus_F y \equiv x + y \pmod{\mathfrak{m}^{n+1}}$.

(b) Sea x no nulo y de torsión, con orden $m = p^k n$, $(n, p) = 1$. Sea $y = [p^k]x$. Como $p \nmid n$, $n \neq 0 \in k$ y así $n \in \mathfrak{m}^c = R^\times$. La Proposición 3 nos dice entonces que $[n]\colon F \to F$ es isomorfismo. Esto junto con $[n](y) = 0$ muestra que $y = [p^k]x = 0$. Por lo tanto $p^k n \mid p^k$, lo cual ocurre si y solo si $n = 1$.

Por ende, todo elemento de torsión tiene orden una potencia de p.

□

Bibliografía

[S] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094