Divulgaciones Matemáticas Vol. 7 No. 2 (1999), pp. 187–192

El Grupo de los Enteros p-ádicos

The Group of p-adic Integers

Edixo Rosales (erosales@hydra.math.luz.ve)
Departamento de Matemática y Computación
Facultad Experimental de Ciencias
La Universidad del Zulia
Maracaibo, Venezuela

Resumen

En este artículo se estudia el grupo aditivo del anillo de los números p-ádicos O^+ y se muestra que el mismo es un grupo topológico compacto y de Hausdorff, para lo cual presentamos una prueba usando la teoría de los límites proyectivos. Al final del trabajo se señala la importancia del problema inverso de Galois y su relaciòn con O^+.
Palabras y frases clave: números p-ádicos, límites proyectivos

Abstract

In this paper the additive group O^+ of the ring of p-adic numbers is studied, showing that it is a compact Hausdorff topological group. A proof using the theory of projective limits is presented. At the end of the article we point out the importance of the inverse Galois problem and its relation with O^+.
Key words and phrases: p-adic numbers, projective limits

Introducción

Este trabajo es fundamentalmente de tipo divulgativo. En el mismo estudiamos el grupo O^+ de los enteros p-ádicos y su conocida propiedad de grupo topológico compacto. El excelente texto de Paul J. MacCarty [1], en su ápendice 2, presenta de manera sintética lo que nosotros en este artículo desarrollamos, sobre todo el problema inverso de Galois, resuelto para O^+. Nuestro estudio en la segunda parte del trabajo permite ver el grupo O^+ como grupo topológico compacto vía el límite proyectivo de grupos topológicos

Recibido 1998/11/06. Revisado 1999/03/01. Aceptado 1999/05/20.
MSC (1991): Primary 22-01, 22C05; Secondary 11S20.

discretos. Nuestro interés es mostrar la hermosa herramienta proporcionada por los límites proyectivos y la elegancia de las pruebas en algunos tópicos de la teoría de los cuerpos.

1 Preliminares

Supondremos que el lector está familiarizado con los conceptos básicos de grupos topológicos, los cuales puede consultar en [2, pág. 125–129]. Comenzaremos nuestro estudio con los límites inversos.

Sea $(S, \leq)$ un conjunto dirigido (es decir $\leq$ es un orden parcial sobre S y si $\alpha, \beta \in S$ entonces existe $\gamma \in S$ tal que $\alpha \leq \gamma$ y $\beta \leq \gamma$).

Consideremos una familia de grupos topológicos $(G_\alpha)_{\alpha \in S}$ y supongamos que para cada par $(\alpha, \beta) \in S \times S$ con $\alpha \leq \beta$ existe un morfismo continuo $\Phi_{\beta\alpha} : G_\beta \to G_\alpha$. Se adiciona que $\Phi_{\alpha\alpha} = i_{G_\alpha}$ y si $\alpha \leq \beta$, $\beta \leq \gamma$, luego $\Phi_{\gamma\alpha} = \Phi_{\beta\alpha}\Phi_{\gamma\beta}$. Con estas propiedades se dice que la terna $(S, \{G_\alpha\}, \{\Phi_{\beta\alpha}\})$ es un *sistema inverso*.

Ahora consideremos el producto directo de grupos $\prod_{\alpha \in S} G_a$ y el subconjunto de este producto $G = \{(x_\alpha)_{\alpha \in S} : \text{ si } \alpha \leq \beta \text{ entonces } \Phi_{\beta\alpha}(x_\beta) = x_\alpha\}$. Notemos que $G \neq \varnothing$ ya que si $x_\alpha = 1$ luego $(x_\alpha)_{\alpha \in S} \in G$. A G se le llama el *límite inverso* o *proyectivo* de los G_α y se denota por $G = \varprojlim G_\alpha$.

Proposición 1. *G con la topología inducida de la topología producto es un grupo topológico.*

Demostración. Hay que ver que G es un subgrupo de $\prod_{\alpha \in S} G_a$. En efecto, como $(x_\alpha)_{\alpha \in S}.(y_\alpha)_{\alpha \in S} = (x_\alpha.y_\alpha)_{\alpha \in S}$ y $\Phi_{\beta\alpha}(x_\beta.y_\beta) = \Phi_{\beta\alpha}(x_\beta).\Phi_{\beta\alpha}(y_\beta) = x_\alpha.y_\alpha$, se deduce que G es cerrado con respecto al producto. Supongamos que $(x_\alpha)_{\alpha \in S} \in G$, luego $\Phi_{\beta\alpha}(x_\beta^{-1}) = \Phi_{\beta\alpha}(x_\beta)^{-1} = x_\alpha^{-1} \Longrightarrow (x_\alpha)_{\alpha \in S}^{-1} \in G$. □

Proposición 2. *Si cada G_α es de Hausdorff entonces G es un subespacio cerrado de $\prod_{\alpha \in S} G_a$.*

Demostración. Sea $(x_\alpha)_{\alpha \in S} \notin G$. Entonces existe $\alpha \leq \beta$ tal que $\Phi_{\beta\alpha}(x_\beta) \neq x_\alpha$. Como cada G_γ es de Hausdorff, existen entornos $U_\alpha \in U_{x_\alpha}$ y $V_\alpha \in U_{\Phi_{\beta\alpha}(x_\beta)}$, con $U_\alpha \cap V_\alpha = \varnothing$. Sea el abierto básico $\prod_{\gamma \in S} A_\gamma$, con $A_\alpha = U_\alpha$, $A_\beta = \Phi_{\beta\alpha}^{-1}(V_\alpha)$, $A_\gamma = G_\gamma$, para todo $\gamma \neq \alpha, \beta$. Si $(y_\alpha)_{\alpha \in S} \in \prod_{\gamma \in S} A_\gamma \cap G \Rightarrow y_\beta \in A_\beta$, $y_\alpha \in U_\alpha$, y $\Phi_{\beta\alpha}(y_\beta) = y_\alpha \in U_\alpha$. Se concluye que $\Phi_{\beta\alpha}(y_\beta) \in V_\alpha \cap U_\alpha$. Esto es un absurdo. □

Proposición 3. *Si cada G_α es compacto y de Hausdorff entonces G es compacto y de Hausdorff.*

Demostración. Como $\prod_{\alpha\in S} G_a$ es compacto y de Hausdorff y G es de Hausdorff y cerrado, se deduce que G es compacto. □

Teorema 4. *Sean G un grupo topológico de Hausdorff compacto y (S, $\{G_\alpha\}$, $\{\phi_{\beta\alpha}\}$) un sistema inverso de grupos topológicos, donde cada G_α es compacto y de Hausdorff. Supongamos que para cada $\beta \in S$ existe un morfismo continuo sobreyectivo $\psi_\beta : G \to G_\beta$ tal que si $\beta \leq \gamma$ luego $\phi_{\gamma\beta} \circ \psi_\gamma = \psi_\beta$ y que la familia $\{\psi_\beta\}$ separa puntos en G. Es decir dados $a \neq b$ en G, existe un ψ_β tal que $\psi_\beta(a) \neq \psi_\beta(b)$. Entonces $G \simeq \varprojlim G_\alpha$ como isomorfismo de grupos topológicos.*

Demostración. Sea $K = \varprojlim G_\alpha$. Si $a \in G$, se define $\Psi(a) = (\Psi_\alpha(a))_{\alpha\in S}$. Hay que demostrar que $\Psi(a) \in K$. Si $\beta \leq \gamma \Rightarrow \Phi_{\gamma\beta}(\Psi_\gamma(a)) = \Psi_\beta(a)$, esto dice que Ψ está bien definido. Por otro lado si $a \neq b$, existe un $\gamma \in S$, tal que $\Psi_\gamma(a) \neq \Psi_\gamma(b)$. Por lo tanto Ψ es inyectiva. Supongamos que $(x_\alpha)_{\alpha\in S} \in K$, luego $\psi_\beta^{-1}(\{x_\beta\}) = F_\beta$ es cerrado. Es claro que cada $F_\beta \neq \varnothing$. Veamos que la familia $\{F_\beta\}$ cumple la propiedad de intersección finita. En efecto $\bigcap_{k=1}^n F_\beta = \bigcap_{k=1}^n \psi_\beta^{-1}(\{x_\beta\})$. Si $\beta_k \leq \gamma \forall\ k = 1, ..., n$, tenemos que existe $a \in G$, con $\Psi_\gamma(a) = x_\gamma$. Veamos que $a \in \bigcap_{k=1}^n F_\beta$. Note que $\Psi_{\beta_k}(a) = \phi_{\gamma\beta_k} \circ \psi_\gamma(a) = \phi_{\gamma\beta_k}(x_\gamma) = x_{\beta_k}$. Como G es compacto y de Hausdorff, se deduce que $\bigcap_{\beta\in S} F_\beta \neq \varnothing$.

Veamos que Ψ es continuo. Sea el abierto básico $\prod_{\gamma\in S} A_\gamma$ en la topología producto, con $A_\gamma = G_\gamma$, salvo a lo sumo para los abiertos A_{γ_i} de G_{γ_i}, con $i = 1, ..., n$. Entonces $\Psi^{-1}(\prod_{\alpha\in S} A_\alpha) = \bigcap_{\alpha\in S} \psi_\alpha^{-1}(A_\alpha) = \psi_{\alpha_1}^{-1}(A_{\alpha_1}) \cap .... \cap \psi_{\alpha_n}^{-1}(A_{\alpha_n})$ es un abierto de G. Finalmente como G es de Hausdorff y compacto, K es de Hausdorff y compacto , Ψ es una biyección y continua, luego Ψ es un homeomorfismo. Esto prueba lo pedido. □

Corolario 5. *Sean G un grupo topológico compacto y T_2 y $\{H_\alpha\}_{\alpha\in S}$ familia de subgrupos normales y cerrados. Supongamos que si α y β están en S, existe un $\gamma \in S$ tal que $H_\gamma \subseteq H_\alpha \cap H_\beta$ y que $\bigcap_{\alpha\in S} H_\alpha = \{1\}$. Para cada α consideramos $G_\alpha = G/H_\alpha$. Si $H_\beta \subseteq H_\alpha$ se define $\phi_{\beta\alpha} : G_\beta \longrightarrow G_\alpha$ por $\phi_{\beta\alpha}(a.H_\beta = a.H_\alpha$. Entonces S puede ser parcialmente ordenado de tal forma que $(S, \{G_\alpha\}, \{\phi_{\beta\alpha}\})$ forman un sistema inverso y $G \simeq \varprojlim G_\alpha$.*

Demostración. Se define $\alpha \leq \beta$ sii $H_\beta \subseteq H_\alpha$. Esto define un orden parcial en S. Si $\alpha, \beta \in S$, existe un $\gamma \in S$ tal que $H_\gamma \subseteq H_\alpha \cap H_\beta$ entonces $\alpha \leq \gamma$ y $\beta \leq \gamma$. Esto dice que S es dirigido. Veamos que cada H_α es compacto y T_2. Se supone que G_α tiene la topología cociente inducida por el morfismo proyección. Sabemos que G_α es un grupo topológico. Además el morfismo

proyección $\psi_\alpha : G \longrightarrow G_\alpha$ definida por $\psi_\alpha(a) = a.H_\alpha$ es morfismo continuo y abierto.

Para ver que G_α es T_2 , sea $R = \{(a,b) : ab^{-1} \in H_\alpha\}$. Consideremos una red $(a_d, b_d) \to (a,b)$ en la topología producto, luego $a_d \to a$ y $b_d \to b$, por lo tanto $a_d b_d^{-1} \to ab^{-1}$ y como $a_d b_d^{-1} \in H_\alpha$ luego $a_d b_d^{-1} \in \overline{H_\alpha} = H_\alpha$. Se deduce lo pedido.

Como $\psi_\alpha(G) = G/H_\alpha$ y G es compacto luego G_α es compacto .

Veamos que la familia $\{\psi_\alpha\}$ separa puntos. En efecto si $a \neq b$ en G luego $ab^{-1} \notin \bigcap_{\alpha\in S} H_\alpha$. Se tiene que $ab^{-1} \notin H_\alpha$ para algún α. Se deduce que $a \notin \psi_\alpha(b)$ y por tanto $\psi_\alpha(a) \neq \psi_\alpha(b)$.

Finalmente $\phi_{\beta\alpha}\psi_\beta(a) = \phi_{\beta\alpha}(aH_\alpha) = aH_\alpha = \psi_\alpha(a)$,cuando $\alpha \leq \beta$. Aplicando el Teorema 4 se deduce $G \simeq \varprojlim G_\alpha$.

□

2 El grupo O^+ de los enteros p-ádicos

Sean Q el conjunto de los números racionales con la valuación $p-$ádica $|\ |_p$ y Q_p su completación. Sea O_p el anillo de valuación asociado a Q_p. Denotamos por Q_p^+ a $(Q_p, +)$.

Se quiere ver que Q_p^+ es un grupo topológico compacto.

Lema 6. *Sea $x \in O^+$. Entonces existe una única sucesión $x_n \in Z$, $0 \leq x_n \leq p^n - 1$, tal que $x_n \equiv x_{n+1} \pmod{p^n}$ con $x_n \longrightarrow x$ en la valuación $p-$ádica.*

Se define $\phi_{nm} : Z/(p^n) \to Z/(p^m)$ con $m \leq n$ por $\phi_{nm}(\pmod{p^n}) = x \pmod{p^m}$. Se tiene que $(\{Z/(p^n)\}, \{\phi_{nm}\}, N)$ es un sistema inverso y $A = \varprojlim Z/(p^n)$ es compacto.

Teorema 7. $O^+ \simeq \varprojlim Z/(p^n)$ *como isomorfismo topológico.*

Demostración. Usando el Lema 6, dado $x \in O^+$ existe $x_n \to x$ en la valuación $p-$ádica tal que $x_n \equiv x_{n+1} \pmod{p^n}$ y $(x_n)_{n\in N}$ es la única sucesiòn con esta propiedad. Se define $\gamma : O^+ \to A$ por $\gamma(x) = (x_n \pmod{p^n})$. Veamos que γ está realmente bien definida. Note que si $m \leqq n$ luego $x_m \equiv x_{m+1} \pmod{p^m}, ..., x_{n-1} \equiv x_n \pmod{p^{n-1}}$. Como $x_n - x_m = (x_n - x_{n-1}) + (x_{n-1-}x_{n-2}) + ... + (x_{m+1-}x_m) = a_1 p^{n-1} + ... + a_m p^m = p^m b$, se concluye que $x_n \equiv x_m \pmod{p^m}$.

Dado $(x_n \pmod{p^n}) \in A$, se tiene que $x_{n+1} \equiv x_n \pmod{p^n}$. Podemos elegir $0 \leq x_n \leq p^{n-1}$. Como $|x_n - x_m|_p \leq \max(|x_i - x_{i-1}|_p)_{m\leq i\leq n} \leq 1/p^n$, se deduce que (x_n) es de Cauchy en O_p y por tanto $x_n \to x$ en la valuación p-ádica. Además $|x_n|_p \leq 1$ luego $|x|_p \leq 1$. Esto dice que $x \in O^+$. Se define

$\varphi : A \to O^+$ por $\varphi((x_n \pmod{p^n})) = x$. Note que $\varphi(A) = O^+$ y como φ es continua luego O^+ es compacto. □

Consideremos los subgrupos cerrados $A_n = p^n O^+$ de O^+. Veamos que $\bigcap_{n\geq 1} p^n O^+ = 0$. En efecto si $x \in \bigcap_{n\geq 1} p^n O^+$ luego $x = p^n a_n \Longrightarrow |x|_p \leq 1/p^n \Longrightarrow x = 0$. Si $m \leq n$ se define $\phi_{nm} : O^+/p^n O^+ \to O^+$ por $\phi_{nm}(a + p^n O^+) = b + p^m O^+$. Es claro que $(\{O^+/p^n O^+\}, \{\phi_{nm}\}, N)$ es un sistema inverso. Usando el *corolario*5 se tiene que $\mathrm{O}^+ \simeq \varprojlim O^+/p^n O^+$.

Corolario 8. $O^+ \simeq \varprojlim O^+/p^n O^+ \simeq \varprojlim Z/(p^n)$.

3 Comentarios finales

Dado un cuerpo finito k, sabemos que k es el cuerpo descomposición del polinomio $x^{p^n} - x \in F_p[x]$, donde F_p es el subcuerpo primo de k y $[k : F_p] = n$.

Se puede construir inductivamente una torre de subcuerpos k_n de la clausura algebraica $\overline{F_p}$ de F_p, tal que $k_n \mid k_{n-1}$ y $[k_n : k_{n-1}] = p^n$.

Sea $\tau : k_n \to k_n$ por $\tau(a) = a^p$ el morfismo de Frobenius. Sabemos que τ es un generador cíclico del grupo $\mathrm{Aut}_{F_p} k_n$. Si $\tau(a) = a^p = a$, luego $a \in F_p$. Esto dice que el cuerpo fijo $k_n^{\mathrm{Aut}_{F_p} k_n} = F_p$, por lo tanto k_n es de Galois.

Definimos $K = \bigcup_{n\geq 1} k_n$. Sabemos que K es una extensión normal y separable de F_p y por tanto de Galois.

Sea $F = \{L \mid F_p : L \subset K \text{ normal y finita}\}$. Es claro que cada $k_n \in F$. Sea $L \in F$ luego $L = k(a)$ con $a \in L$. Se tiene que $a \in k_n$, donde elegimos n como el primer índice que tiene esta propiedad. Como $k_n \mid F_p$ es de Galois y $L \mid F_p$ es normal tenemos que $\mathrm{Aut}_L k_n$ es un subgrupo normal de $\mathrm{Aut}_{F_p} k_n$. Se deduce que $|\mathrm{Aut}_L k_n| = p^{n-s}$. Además $\mathrm{Aut}_L k_n$ es el único subgrupo de $\mathrm{Aut}_{F_p} k_n$ que tiene este orden. Como $|\mathrm{Aut}_{k_s} k_n| = p^{n-s}$ se tiene que $\mathrm{Aut}_L k_n = \mathrm{Aut}_{k_s} k_n \Longrightarrow L = k_s$.

Es obvio el resultado:

Corolario 9. $\mathrm{Aut}_{F_p} K \simeq \varprojlim \mathrm{Aut}_{F_p} k_n \simeq \varprojlim Z/(p^n) \simeq O^+$.

Referencias

[1] McCarthy, P. *Algebraic Extensions of Fields*, Blaisdell, 1966.

[2] Kelley, J. *Topología General*, Editorial Universitaria de Buenos Aires, Buenos Aires, 1962.

[3] Morandi, P. *Fields and Galois Theory*, Springer, Berlin, 1996.

[4] Quadros, F. *Primeiros Passos p-ádicos*, 17^o Coloquio Brasileiro de Matemática, IMPA, Rio de Janeiro, 1989.