Definibilidad de $\mathbb{N}$ en $(\mathbb{Q}, +, *, 0, 1)$

Enrique Acosta Jaramillo

Teorema (Julia Robinson, 1949)**.** $\mathbb{N}$ es definible en $\mathcal{Q} = (\mathbb{Q}, +, *, 0, 1)$, es decir:

existe una fórmula $\phi(x)$ de primer orden con una variable libre sobre el lenguaje $L = \{+, *, 0, 1\}$ tal que

$$\mathcal{Q} \models \phi[r] \Leftrightarrow r \in \mathbb{N}$$

Decidibilidad

Son decidibles:

- La teoría de campos algebraicamente cerrados de característica de una característica fija.
- $Th(\mathbb{C}, +, *, 0, 1) = \{\phi \mid \mathbb{C} \models \phi\}$
- $Th(\mathbb{R}, +, *, 0, 1)$

Son indecidibles:

- Teoría de Grupos
- La teoría vacía (el cálculo de predicados) sobre el lenguaje de la aritmética.
- $Th(\mathbb{C}, +, *, 0, 1, exp)$
- AP^1 (Axiomática de Peano de primer orden)
- Cualquier teoría que extienda a AP^1
- $Th(\mathcal{N})$, la teoría de los naturales $\mathcal{N} = (\mathbb{N}, +, *, 0, 1)$.

Se desconoce la decidibilidad de:

- $Th(\mathbb{R}, +, *, 0, 1, exp)$ (Propuesto por Tarski 19..)

Indecidibilidad de $Th(\mathcal{N})$

Axiomática de Peano

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + 0 = x$
- $x * (y + z) = (x * y) + (x * z)$
- $x * y = y * x$
- $x * 1 = x$
- $(x + z = y + z) \longrightarrow x = y$
- $\neg(0 = x + 1)$
- Inducción: Para toda $\phi(x, \overline{y})$ el axioma

$\forall \overline{y}\{\phi(0, \overline{y}) \wedge \forall x[\phi(x, \overline{y}) \rightarrow \phi(x + 1, \overline{y})] \longrightarrow \forall x \phi(x, \overline{y})\}$

Teorema. Toda extensión consistente de AP^1 es indecidible.

Consecuencias

- Incompletitud de Gödel: Toda extensión consistente y recursivamente axiomatizable de AP^1 es incompleta.
- AP^1 es indecidible y incompleta.
- $Th(\mathcal{N})$ es indecidible.
- $Th(\mathcal{N})$ no es recursivamente axiomatizable.

Consecuencias de la indecidibilidad de $Th(\mathcal{N})$

Teorema

Sea $\mathcal{M}$ una estructura en el lenguaje de la aritmética con $\mathcal{N} \leq \mathcal{M}$. Si $\mathbb{N}$ es definible en $\mathcal{M}$ entonces $Th(\mathcal{M})$ es indecidible.

Demostración. Sea $\phi(x)$ la fórmula que define $\mathbb{N}$ en $\mathcal{M}$. Para cada sentencia θ sobre L sea $\theta^{\phi(x)}$ su relativización. Entonces,

$$\mathcal{N} \models \theta \Leftrightarrow \mathcal{M} \models \theta^{\phi(x)}$$

luego si $Th(\mathcal{M})$ fuera decidible, $Th(\mathcal{N})$ sería decidible. □

Consecuencias:

- Si $\mathbb{N}$ es definible en $\mathcal{Q} = (\mathbb{Q}, +, *, 0, 1)$ entonces $Th(\mathcal{Q})$ es indecidible y no es recursivamente axiomatizable.
- $Th(\mathbb{Z}, +, *, 0, 1)$ es indecidible.
- $\mathbb{N}$ y $\mathbb{Z}$ no son definibles en $(\mathbb{C}, +, *, 0, 1)$ ni en $(\mathbb{R}, +, ., 0, 1)$.
- $Th(\mathbb{C}, +, *, 0, 1, exp)$ es indecidible.

Motivación

La fórmula $\phi(x)$ buscada debe cumplir que si $\mathcal{Q} \models \phi[n/d]$ entonces $d = 1$.

El problema:
No hay forma aparente de extraer el nominador y denominador de un racional en primer orden. Inclusive si esto se puede hacer, no hay forma de hablar de primos si uno ni siquiera tiene a los naturales (eso es lo que se está tratando de hacer!).

Teorema (Julia Robinson)**.** La fórmula

$$\phi(x) : \exists x_1 \exists x_2 \exists x_3 (7x^2 + 2 = x_1^2 + x_2^2 + x_3^2)$$

define en $\mathcal{Q}$ a los racionales cuyo denominador exacto no es divisible por 2, es decir, para $r \in \mathbb{Q}$, $r = n/d$ con $mcd(n, d) = 1$

$$\mathcal{Q} \models \phi[r] \Leftrightarrow 2 \not| \ d.$$

Teorema (Gauss-Legendre)**.** $n \in \mathbb{N}$ es suma de tres cuadrados racionales si y solo si n NO es de la forma $4^m(8k + 7)$ $m, k \in \mathbb{N}$.

$$\phi(x) : \exists x_1 \exists x_2 \exists x_3 (7x^2 + 2 = x_1^2 + x_2^2 + x_3^2)$$

Demostración. $\mathcal{Q} \models \phi[n/d]$ si y solo si existen $x_1, x_2, x_3 \in \mathbb{Q}$ tales que

$$7(n/d)^2 + 2 = x_1^2 + x_2^2 + x_3^2$$

si y solo si existen $x_1, x_2, x_3 \in \mathbb{Q}$ tales que

$$7n^2 + 2d^2 = x_1^2 + x_2^2 + x_3^2,$$

luego es suficiente ver que $7n^2 + 2d^2$ es suma de cuarto cuadrados racionales si y solo si d es impar.

- Si d es impar,

$$7n^2 + 2d^2 \equiv (\text{mod } 8) \begin{cases} 1 & n \text{ impar} \\ 2, 6 & n \text{ par} \end{cases}$$

  en ambos casos n no es de la forma $4^m(8k + 7)$ pues todo entero de la forma $4^m(8k + 7) \equiv 7, 0, 4(\text{mod } 8)$ luego es suma de tres cuadrados racionales.

- Si d es par,

  $4 \not| 7n^2 + 2d^2$ y además $7n^2 + 2d^2 \equiv 7(\text{mod } 8)$ luego no es suma de cuatro cuadrados racionales.

□

Formas cuadráticas sobre $\mathbb{Q}$

Definición. Sea D un anillo, una *forma cuadrática sobre* D es una función de la forma

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j.$$

con $a_{ij} \in D$.

Teorema. Dada una forma cuadrática $f(x_1, \ldots, x_n)$ sobre un campo F de característica distinta de 2, la ecuación

$$f(x_1, \ldots, x_n) = a$$

tiene solución en F^n si y solo si tiene solución NO TRIVIAL en F^{n+1} la ecuación

$$f - a x_{n+1}^2 = 0.$$

Teorema (Hasse-Minkowski)**.** La ecuación

$$a_1 x_1^2 + \ldots + a_n x_n^2 = 0$$

con $a_1, \ldots, a_n \in \mathbb{Z}$ tiene solución no trivial en $\mathbb{Q}^n$ si y solo si tiene solución no trivial en $\mathbb{R}$ y tiene solución no trivial ni divisible por p en $\mathbb{Z}$ módulo p^n para todo primo p y todo $n \geq 1$.

El principio de Hasse

Teorema (Hasse-Minkowski, enunciado de Hasse,1923)**.** Sea $f(x_1, \ldots, x_n)$ una forma cuadrática sobre $\mathbb{Q}$. La ecuación

$$f(x_1, \ldots, x_n) = 0$$

tiene solución no trivial en $\mathbb{Q}$ si y solo si tiene solución no trivial en $\mathbb{R}$ y en $\mathbb{Q}_p$ (el campo de los números p-ádicos) para todo primo p.

Teorema. Dada una forma cuadrática $f(x_1, \ldots, x_n)$ sobre $\mathbb{Q}_p$ con determinante $d \neq 0$, la ecuación

$$f(x_1, \ldots, x_n) = 0$$

tiene solución no trivial (en $\mathbb{Q}_p$) si y solo si

- $\diamond$ $n = 2 : -d$ es un cuadrado (en $\mathbb{Q}_p$).
- $\diamond$ $n = 3 : c_p(f) = 1$.
- $\diamond$ $n = 4 : c_p(f) = 1$ cuando d es un cuadrado.
- $\diamond$ $n \geq 5$.

Nota. Si $d = 0$, existe una solución no trivial.
$c_p(f)$ es una función de los coeficientes de f en $\{-1, 1\}$.

Formas cuadráticas módulo p^n

Definición. Sea $f(x_1, \ldots, x_n)$ una forma cuadrática sobre $\mathbb{Z}$. Se dice que f *representa cero módulo* p^n si

$$f(x_1, \ldots, x_n) = 0$$

tiene solución no trivial ni divisible por p en $\mathbb{Z}$ módulo p^n.

Teorema. Si p es un primo impar y $a, b, c, d \in \mathbb{Z}$ con $p \nmid abcd$ entonces

$\diamond$ $ax^2 + by^2 + cz^2$

representa cero módulo p^n para todo n y las siguientes representan cero módulo p^n para todo n si y solo si

- $\diamond$ $ax^2 + by^2$: $(-ab \,|\, p) = 1$.
- $\diamond$ $ax^2 + by^2 + pcz^2 + pdw^2$: $(-ab \,|\, p) = 1$ o $(-cd \,|\, p) = 1$.

Teorema. Si $a, b, c, d \in \mathbb{Z}$ son impares entonces

$\diamond$ $ax^2 + by^2 + cz^2 + 2dw^2$

representa cero módulo 2^n para todo n y las siguientes representan cero módulo 2^n para todo n excepto cuando

- $\diamond$ $ax^2 + by^2 + cz^2$: $a \equiv b \equiv c \,(\text{mod } 4)$.
- $\diamond$ $ax^2 + by^2 + cz^2 + dw^2$: $a \equiv b \equiv c \equiv d (\text{mod } 4)$ y $a + b + c + d \equiv 4 (\text{mod } 8)$.

Los lemmas de Julia Robinson

Lema. Sean $n \in \mathbb{N}$, $n \neq 0$ y p primo $p \equiv 3(\text{mod } 4)$.
Existen $x, y, z \in \mathbb{Q}$ tales que

$$x^2 + y^2 - pz^2 = n$$

si y solo si al escribir n en la forma $n = st^2$ con s
"squarefree" se cumplen las dos condiciones siguientes

a. $s \not\equiv p \pmod 8$

b. si $s = pk$ entonces $(k \,|\, p) = -1$.

Lema. Sean $n \in \mathbb{N}$, $n \neq 0$ y p, q primos impares con
$p \equiv 1(\text{mod } 4)$ y $(q \,|\, p) = -1$. Existen $x, y, z \in \mathbb{Q}$ tales que

$$x^2 + qy^2 - pz^2 = n$$

si y solo si al escribir n en la forma $n = st^2$ con s
"squarefree" se cumplen las dos condiciones siguientes

a. Si $s = pk$ entonces $(k \,|\, p) = 1$.

b. Si $s = qk$ entonces $(k \,|\, q) = 1$.

Los lemmas de Julia Robinson

Lema (Julia Robinson)**.** Sean $r \in \mathbb{Q}$ y p primo $p \equiv 3 (\text{mod } 4)$.

$$x^2 + y^2 - pz^2 = pr^2 + 2$$

tiene solución $(x, y, z) \in \mathbb{Q}^3$ si y solo si el denominador exacto de r no es divisible por 2 ni por p.

Lema (Julia Robinson)**.** Sean $r \in \mathbb{Q}$ y p, q primos impares con $p \equiv 1 (\text{mod } 4)$ y $(q \,|\, p) = -1$.

$$x^2 + qy^2 - pz^2 = qpr^2 + 2$$

tiene solución $(x, y, z) \in \mathbb{Q}^3$ si y solo si el denominador exacto de r no es divisible por p ni por q.

La fórmula $\phi(x)$

Definiendo

$$\sigma(q,p,x) : \exists y \exists z \exists w (y^2 + qz^2 = qpx^2 + pw^2 + 2)$$

las hipótesis de existencia de los lemas anteriores se pueden reescribir como

$$\mathcal{Q} \models \sigma[1,p,r] \quad y \quad \mathcal{Q} \models \sigma[q,p,r].$$

La fórmula:

$$\phi(x) : \forall p \forall q \Big\{ \Big[\sigma(q,p,0) \wedge \forall r \Big(\sigma(q,p,r) \rightarrow \sigma(q,p,r+1) \Big) \Big] \rightarrow \sigma(q,p,x) \Big\}$$

Teorema. $\phi(x)$ define a $\mathbb{Z}$ en $\mathcal{Q} = (\mathbb{Q}, +, *, 0, 1)$, es decir,

$$\mathcal{Q} \models \phi[r] \Leftrightarrow r \in \mathbb{Z}.$$

Corolario. $\mathbb{N}$ es definible en $\mathcal{Q}$ y por lo tanto $Th(\mathcal{Q})$ es indecidible.