Final Álgebra III: Hacia la clausura algebraica de $\mathbb{F}_2$

¡Los ordinales son útiles!

Guillermo Mosse

¿Qué son los ordinales?

$$0 = \varnothing$$

¿Qué son los ordinales?

$$0 = \varnothing$$

$$1 = \{0\}$$

¿Qué son los ordinales?

$$0 = \varnothing$$

$$1 = \{0\}$$

$$2 = \{0, 1\} \quad = 1 \cup \{1\}$$

¿Qué son los ordinales?

$$0 = \varnothing$$

$$1 = \{0\}$$

$$2 = \{0, 1\} \quad = 1 \cup \{1\}$$

$$3 = \{0, 1, 2\} = 2 \cup \{2\}$$

$$4 = \{0, 1, 2, 3\} = 3 \cup \{3\}$$

$$\ldots$$

Más ordinales

$$5 = \{0, 1, 2, 3, 4\} = 4 \cup \{4\}$$

$$6 = \{0, 1, 2, 3, 4, 5\} = 5 \cup \{5\}$$

Más ordinales

$$5 = \{0, 1, 2, 3, 4\} = 4 \cup \{4\}$$

$$6 = \{0, 1, 2, 3, 4, 5\} = 5 \cup \{5\}$$

$$\omega = \{0, 1, 2, 3, ...\} \leftarrow \text{ es un ordinal límite}$$

Más ordinales

$$5 = \{0, 1, 2, 3, 4\} = 4 \cup \{4\}$$

$$6 = \{0, 1, 2, 3, 4, 5\} = 5 \cup \{5\}$$

$$\omega = \{0, 1, 2, 3, ...\} \leftarrow \text{ es un ordinal límite}$$

$$\omega + 1 = \{0, 1, ..., \omega\} = \omega \cup \{\omega\}$$

$$\omega + 2 = \{0, 1, ..., \omega, \omega + 1\} = \omega + 1 \cup \{\omega + 1\}$$

$$...$$

Más ordinales

$$5 = \{0, 1, 2, 3, 4\} = 4 \cup \{4\}$$

$$6 = \{0, 1, 2, 3, 4, 5\} = 5 \cup \{5\}$$

$$\omega = \{0, 1, 2, 3, ...\} \leftarrow \text{ es un ordinal límite}$$

$$\omega + 1 = \{0, 1, ..., \omega\} = \omega \cup \{\omega\}$$

$$\omega + 2 = \{0, 1, ..., \omega, \omega + 1\} = \omega + 1 \cup \{\omega + 1\}$$

$$...$$

$$\omega + \omega = \omega \cdot 2 = \{0, 1, ..., \omega, \omega + 1, \omega + 2, ...\}$$

Operaciones

Suma y Producto de **ordinales** $\approx$ Suma y producto de **cardinales**

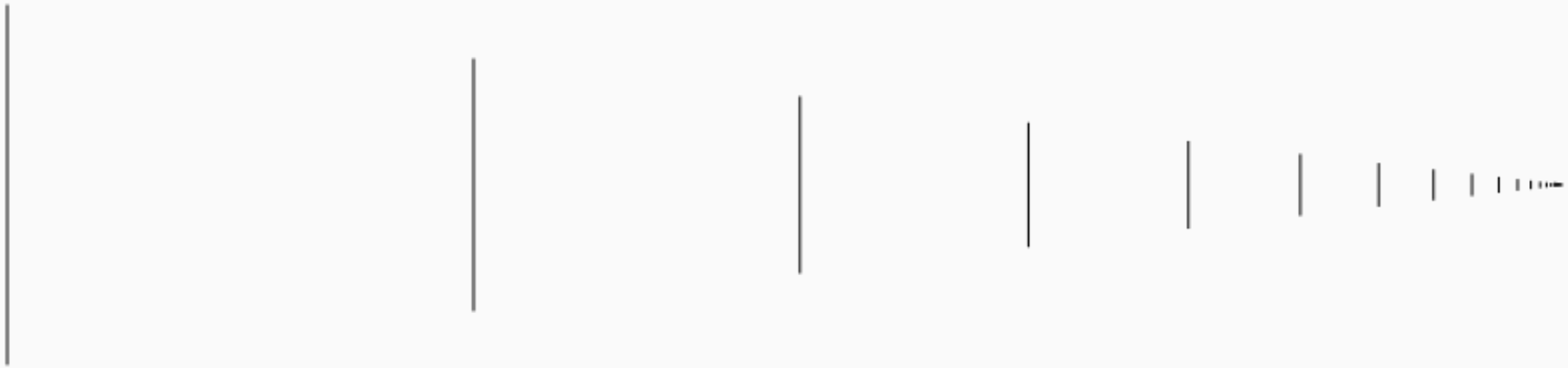
Operaciones

Suma y Producto de **ordinales** $\approx$ Suma y producto de **cardinales**

¡La exponenciación es distinta!

- $\alpha^0 := 1$
- $\alpha^{\beta+1} := \alpha^\beta \cdot \alpha$
- Si β es límite, $\alpha^\beta = \bigcup_{\lambda<\beta} \alpha^\lambda$.

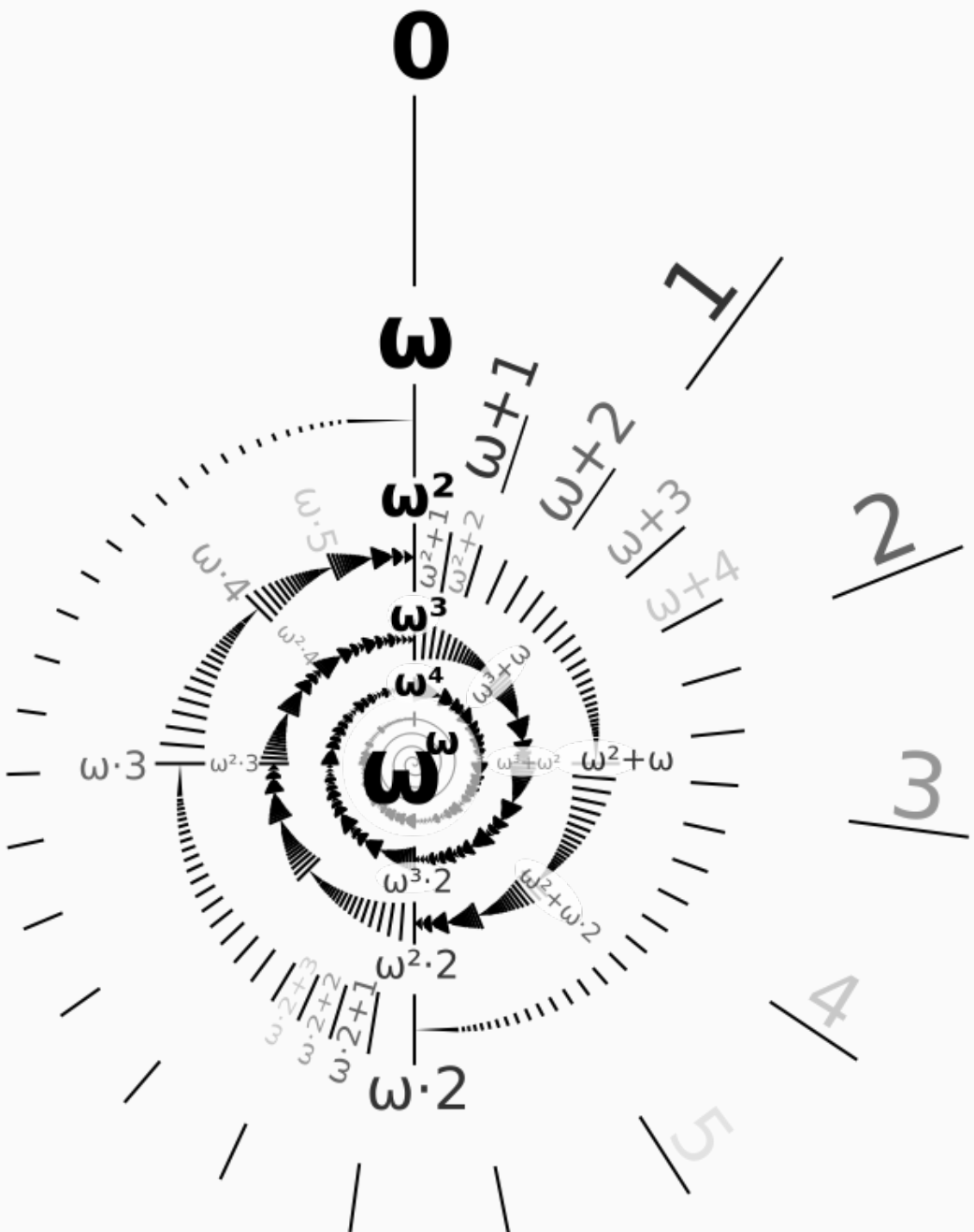
Matchsticks: ω



ω^2

ωω

Una representación gráfica hasta ω^ω



ωωω (¡INENTENDIBLE!)

Los ordinales como algo efectivo

Los ordinales como algo efectivo

Toda secuencia descendente de ordinales eventualmente termina.

Equivalentemente, todo conjunto tiene un mínimo. Esto nos permite usar un esquema inductivo para probar propiedades sobre los ordinales.

Forma normal de Cantor

Todo ordinal $0 \neq \beta$ que nos va a interesar (o sea, no muy grande) admite una expresión de la siguiente forma:

$$\beta = \omega^{\alpha_1} \cdot m_1 + ... + \omega^{\alpha_k} \cdot m_k$$

con $\beta > \alpha_1 > ... > \alpha_k$, y $m_i \in \mathbb{N}$

Esto es una descomposición de β en ordinales más chicos que él.

Forma normal de Cantor

Todo ordinal $0 \neq \beta$ que nos va a interesar (o sea, no muy grande) admite una expresión de la siguiente forma:

$$\beta = \omega^{\alpha_1} \cdot m_1 + ... + \omega^{\alpha_k} \cdot m_k$$

con $\beta > \alpha_1 > ... > \alpha_k$, y $m_i \in \mathbb{N}$

Esto es una descomposición de β en ordinales más chicos que él.

Además, uno puede hacer lo mismo con los α_i...

Forma normal de Cantor

Todo ordinal $0 \neq \beta$ que nos va a interesar (o sea, no muy grande) admite una expresión de la siguiente forma:

$$\beta = \omega^{\alpha_1} \cdot m_1 + ... + \omega^{\alpha_k} \cdot m_k$$

con $\beta > \alpha_1 > ... > \alpha_k$, y $m_i \in \mathbb{N}$

Esto es una descomposición de β en ordinales más chicos que él.

Además, uno puede hacer lo mismo con los α_i...

Algunos ejemplos:

ω, $\omega^\omega \cdot 2$, $\omega^{\omega^2} + \omega^\omega + 4$, $\omega^{\omega^{\omega^2}+2}$

El producto no es conmutativo

El producto no es conmutativo

$2 \cdot \omega$ es así:

, y ω es así:

El producto no es conmutativo (Cont)

Mientras que: $\omega \cdot 2$ es así:

Las operaciones naturales de Conway

⊕	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Producto

$\odot$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	3	1	8	10	11	9	12	14	15	13	4	6	7	5
3	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
4	0	4	8	12	6	2	14	10	11	15	3	7	13	9	5	1
5	0	5	10	15	2	7	8	13	3	6	9	12	1	4	11	14
6	0	6	11	13	14	8	5	3	7	1	12	10	9	15	2	4
7	0	7	9	14	10	13	3	4	15	8	6	1	5	2	12	11
8	0	8	12	4	11	3	7	15	13	5	1	9	6	14	10	2
9	0	9	14	7	15	6	1	8	5	12	11	2	10	3	4	13
10	0	10	15	5	3	9	12	6	1	11	14	4	2	8	13	7
11	0	11	13	6	7	12	10	1	9	2	4	15	14	5	3	8
12	0	12	4	8	13	1	9	5	6	10	2	14	11	7	15	3
13	0	13	6	11	9	4	15	2	14	3	8	5	7	10	1	12
14	0	14	7	9	5	11	2	12	10	4	13	3	15	1	8	6
15	0	15	5	10	1	14	4	11	2	13	7	8	3	12	6	9

Formalización de la definición de las operaciones

Definición (Suma)

$\alpha \oplus \beta = min\{\gamma : \gamma \neq \alpha' \oplus \beta, \alpha \oplus \beta' \ \forall \ \alpha' < \alpha, \beta' < \beta\}$

O, de manera más compacta:

$\alpha \oplus \beta = mex\{\alpha' \oplus \beta, \alpha \oplus \beta'\}$

Definición (Producto)

$\alpha \odot \beta = mex\{(\alpha' \odot \beta) \oplus (\alpha \odot \beta') \ominus (\alpha' \odot \beta')\}$

Simplest Extension Theorem

(Notación: si γ es un ordinal, escribimos P_γ si lo queremos ver como conjunto)

Sea γ un ordinal.

- Si $(P_\gamma, \oplus)$ no es un grupo, entonces $\gamma = \alpha \oplus \beta$, donde (α, β) es el par de ordinales más chico (en el orden lexicográfico) con $\alpha \oplus \beta \notin P_\gamma$
- Si $(P_\gamma, \oplus, \odot)$ es un grupo pero no es un anillo, entonces $\gamma = \alpha \odot \beta$, donde (α, β) es el par de ordinales más chico (en el orden lexicográfico) con $\alpha \odot \beta \notin P_\gamma$
- Si $(P_\gamma, \oplus, \odot)$ es un anillo pero no un cuerpo, entonces $\gamma \odot \alpha = 1$, donde α es el ordinal más chico de P_γ sin inverso en el conjunto.
- Si $(P_\gamma, \oplus, \odot)$ es un cuerpo pero no es algebraicamente cerrado, entonces γ es una raíz del polinomio más chico en el orden lexicográfico con ninguna raíz en P_γ
- Si $(P_\gamma, \oplus, \odot)$ es un cuerpo algebraicamente cerrado, entonces γ es el primer elemento trascendente sobre P_γ.

Simplest extension theorem, parte 2

Sea γ un ordinal.

- Supongamos que P_γ es un grupo. Entonces $\gamma \oplus \alpha = \gamma + \alpha \ \forall \ \alpha \in P_\gamma$
- Supongamos que P_γ es un anillo y $\exists \delta \leqslant \gamma$ con P_δ un grupo tal que todo $\alpha \in \delta$ tiene inverso multiplicativo en P_γ entonces: $\gamma \odot \alpha = \gamma \cdot \alpha \forall \alpha < \delta$
- Si P_γ es un cuerpo y todo polinomio de grado $\leqslant n$ tiene raíz en P_γ entonces $\bigoplus_{i=0}^{n}(\gamma^{\boxed{i}} \odot \alpha_i) = \sum_{i=0}^{n} \gamma^i \cdot \alpha_i, \ \forall \alpha_0, ..., \alpha_n < \gamma$

Proof. It follows from well-known theorems about ordinals that each ordinal has a unique expression $[2^{\alpha_0} + 2^{\alpha_1} + \ldots + 2^{\alpha_{n-1}}]$, where n is finite and $\alpha_0 > \alpha_1 > \ldots > \alpha_{n-1}$. That this is the same as $[2^{\alpha_0}] + \ldots + [2^{\alpha_{n-1}}]$ then follows from Theorem 40.

This justifies the normal rule for finding Nim-sums.

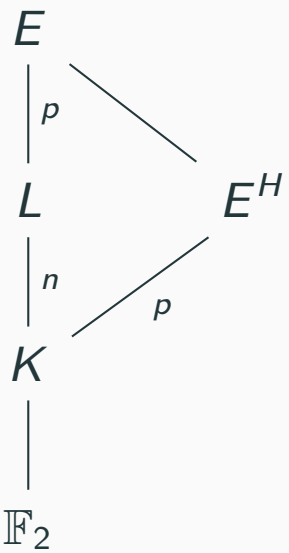
Now the ordinals below the first transcendental are algebraic over previous ones, and so by induction algebraic over the field 2 whose only elements are 0 and 1. It follows that any finite number of such ordinals generate a finite field. Each of these ordinals $\triangle$ which is itself a field defines an algebraic extension of itself. Since these extensions are taken in order of degree where

possible, the first extensions will be quadratic, and then when the field is quadratically closed we shall take cubic extensions, then quintic ones, etc. [Since the Galois group of every finite field is abelian, the quadratically closed field remains quadratically closed after taking cubic extensions, etc.]

Moreover, the quadratic extensions will all be by equations of the form $x^2 + x = \alpha$, since the only lexicographically earlier quadratics are $x^2 = \alpha$, and every element of a finite field of characteristic 2 already has a square root

Demostración

Sea E tal que no tiene polinomios irreducibles de grado p y sea L/E una extensión algebraica de E. Sea $f \in L[X]$ un polinomio de grado p y supongamos que es irreducible. SPG, podemos suponer que $[L : K] < \infty$ porque de última lo cambiamos por K[coef/raíces de f] Sea $E = L(\alpha)$ con α una raíz de f. Luego $[E : L] = p$ y por lo tanto p divide a $[E : K]$. Ahora bien, E/K tiene Galois abeliano, y por el teorema de estructura para grupos abelianos, podemos obtener un subgrupo $H \subset (E/K)$ de índice p. Luego E^H es una extensión de grado p. Pero esto era imposible, por como era K.



Factorización de polinomios

Analicemos el polinomio $x^3 - 2$. No se factoriza en F_2.

Afirmo que ω es raíz. En efecto, ω es la clausura cuadrática de 2, así que es la solución del polinomio más simple que no tiene raíces en ω. Ese polinomio es $x^3 - 2$, porque x^3 y $x^3 - 1$ se factorizan linealmente en ω, y porque 2 no tiene raíz cúbica en ω. Veamos esta última afirmación:

$2 \odot 2 \odot 2 = 1$ así que si α es raíz cúbica de 2 entonces tiene orden multiplicativo igual a 9, y si $\alpha \in \omega \Rightarrow \alpha \in F_{2^{2^n}}$ para algún n. Pero el subgrupo multiplicativo de $F_{2^{2^n}}$ tiene índice $2^{2^n} - 1$ y por inducción se ve que $0 \ |2^{2^n} - 1 \forall n$. Luego $\alpha \notin \omega$, entonces debe ser ω.

Ahora, si uno hace Ruffini, obtiene $x^3 - 2 = (x - \omega)(x^2 + \omega x + \omega^2)$

Analicemos $q(x) = x^2 + \omega x + \omega^2$.

Después de mucho pensar, intuí que una raíz debe 'estar cerca' de ω y propuse como solución $\omega \odot n$.

Enchufándolo en la ecuación y sacando factor común ω^2 obtenemos que $q(x) = 0 \Leftrightarrow n^2 + n + 1 = 0$.

¡Y esta última ecuación es bien conocida! Es la que genera $F_{2^2} = 4$. Luego buscamos las raíces ahí y resulta que 2 y 3 son raíces.

Luego las raíces del polinomio original son $\omega, \omega \odot 2, \omega \odot 3$

BIS, si me queda tiempo: dividir anda

Construimos los inversos inductivamente. Si ya existe $\frac{1}{\alpha'} \forall 0 < \alpha' < \alpha$, entonces:

Dado $\alpha, \beta = \frac{1}{\alpha} := mex\{0, \frac{1+(\alpha'-\alpha)\hat{beta}}{\alpha'} : \alpha' \neq 0\}$ donde $\hat{beta}$ indica un elemento que ya "metimos" en el conjunto. La idea es que tenés un "sitio de construcción" donde podés usar los elementos anteriores para obtener nuevos elementos. Otra manera de definir al conjunto es diciendo que es el menor conjunto que contiene a 0 y cerrado por $\frac{1+(\alpha'-\alpha)\hat{\beta}}{\alpha'}$.

Ahora bien, ¿qué pinta tienen estos elementos? Si $\hat{\beta}$ ya pertenece al conjunto, entonces un nuevo elemento $0 \neq \hat{\hat{\beta}} = \frac{1+(\alpha'-\alpha)\hat{\beta}}{\alpha'} = \frac{1+\alpha'\hat{\beta}-\alpha\hat{\beta}}{\alpha'}$

Multiplicando por α a ambos lados y luego componiendo con la función $1 - x$ obtenemos
$1 - \alpha\hat{\hat{\beta}} = 1 - \alpha\frac{1+\alpha'\hat{\beta}-\alpha\hat{\beta}}{\alpha'} = 1 - \frac{\alpha+\alpha\alpha'\hat{\beta}-\alpha^2\hat{\beta}}{\alpha'} = \frac{\alpha'-\alpha-\alpha\alpha'\hat{\beta}+\alpha^2\hat{\beta}}{\alpha'}$

Analicemos la expresión $\alpha' - \alpha - \alpha\alpha'\hat{\beta} + \alpha^2\hat{\beta}$. La podemos conmutar de modo que quede $\alpha' - \alpha\alpha'\hat{\beta} + \alpha^2\hat{\beta} - \alpha$, y sacando factor común obtenemos $\alpha'(1 - \alpha\hat{\beta}) - \alpha(1 - \alpha\hat{\beta}) = (1 - \alpha\hat{\beta})(\alpha' - \alpha)$.

Juntando todo hemos obtenido $1 - \alpha\hat{\hat{\beta}} = (1 - \alpha\hat{\beta})\frac{\alpha'-\alpha}{\alpha'}$. Como el conjunto se construye inductivamente y $1 - \alpha 0 = 1 \neq 0$, tenemos que todo elemento $\hat{\beta}'$ cumple $1 - \alpha\hat{\hat{\beta}} \neq 0$.

Ahora bien, aprovechando que $\hat{\hat{\beta}} = \frac{1+(\alpha'-\alpha)\hat{\beta}}{\alpha'}$, podemos hacer la siguiente cuenta:

Un excluyente para $\alpha\beta$ va a ser de la forma $\alpha'\beta + \alpha\hat{\beta} - \alpha'\hat{\beta}$, y sabemos que $\hat{\hat{\beta}}\alpha' = 1 + \alpha'\hat{\beta} - \alpha\hat{\beta} \Rightarrow \alpha\hat{\beta} - \alpha'\hat{\beta} = 1 - \hat{\beta}'\alpha'$.

Luego tenemos que el excluyente va a ser de la forma $\alpha'\beta + 1 - \hat{\beta}'\alpha' = \alpha'(\hat{\beta} - \hat{\beta}') + 1$.

Esta cuenta nos dice que los excluyentes de $\alpha\beta$ son todos $\neq 1$, ya que $\beta, (\hat{\beta} - \hat{\beta}') \neq 0$.

Además, si $\hat{\beta} = 0 \Rightarrow \hat{\hat{\beta}} = \frac{1}{\alpha'}$ por la definición, así que el excluyente queda 0.

Probamos que los ecluyentes de $\alpha\beta$ son todos distintos de 1 y además está 0, así que $\alpha\beta$ debe ser 1.

Bibliografía

- John H. Conway - On Numbers and Games (1976)
- Hendrik Lenstra - On the Algebraic Closure of Two (1977)
- [Graduate Studies in Mathematics] Aaron N. Siegel - Combinatorial Game Theory (2013, American Mathematical Society)