0.1. Suma y Producto: números finitos y transfinitos

Observación 1. *Prima cumple Leibnitz con la suma.*

Definición 2 (Suma)**.** $\alpha + \beta = min\{\gamma : \gamma \neq \alpha' + \beta, \alpha + \beta' \forall \alpha' < \alpha, \beta' < \beta\}$

Teorema 3 (Los ordinales forman un grupo abeliano)**.**

- $\alpha + \beta = \beta + \alpha$
- $\alpha + \beta = \alpha + \gamma \Leftrightarrow \beta = \gamma$
- $\alpha + \beta = 0 \Leftrightarrow \alpha = \beta$
- $\alpha + 0 = \alpha, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \alpha + \alpha = 0, -\alpha = \alpha$

Demostración. Llamemos α' a un ordinal variable que puede ser cualquier ordinal menor que α, y si $\alpha = mex(S)$, llamemos $\alpha*$ a un ordinal que puede tomar un valor de S, un 'excluyente'. En ese sentido $\alpha*$ debe tomar todos los valores menores que α y puede tomar valores más grandes que α. Esto es porque no cambiaría la definición de $\alpha = mex\{\alpha*\}$. Justamente S puede tener huecos, como los conjuntos y las funciones de Bachmann-Howard.

- La conmutatividad sale directo de la definición; la asociatividad es medio aburrida de probar.
- Veamos que $\alpha + \beta = \alpha + \gamma \Leftrightarrow \beta = \gamma$:

  $\Leftarrow$): trivial

  $\Rightarrow$): SPG, supongamos que $\gamma < \beta$. Entonces por la definición de suma, $\alpha + \gamma$ es un 'excluyente' en la definición de $\alpha + \beta$, es decir, pertenece a $mex\{\alpha' + \beta, \alpha + \beta'\}$ y por lo tanto es distinto a $\alpha + \beta$.

  Además, $\alpha + \beta = mex\{\alpha * + \beta, \alpha + \beta *\}$. En efecto, todos los ordinales de la pinta $\alpha' + \beta, \alpha + \beta'$ son excluyentes, y cualquier otro ordinal de esa pinta que es excluyente, por lo visto recién, es distinto a $\alpha + \beta$.
- $\alpha + 0 = mex\{\alpha * + 0, \alpha + 0*\}$. Como no hay ordinales menores que cero, tenemos que $\alpha + 0 = mex\{\alpha * + 0\}$, y por inducción transfinita se ve que esto es igual a α.
- $\alpha + \beta = 0 \Leftrightarrow \alpha = \beta$:

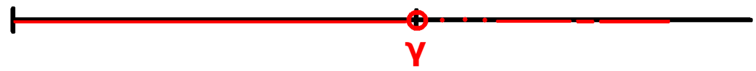
  $\Leftarrow$) : Por inducción en α. Si $\alpha = 0$ es trivial. Supongamos $\alpha > 0$. Entonces $\alpha + \alpha = mex\{\alpha' + \alpha\} = 0$ porque como $\alpha' + \alpha' = 0$ no puede ser $\alpha' + \alpha = 0$ porque sino, por cancelación a izquierda tendríamos $\alpha = \alpha'$.

  $\Rightarrow$) : Como $\alpha + \alpha = 0$ y $\alpha + \beta = 0$, nuevamente por cancelación a izquierda tenemos que $\alpha = \beta$.
- Es asociativa, por inducción en $\alpha + \beta$.

  Si $\alpha + \beta = 0$, entonces tenemos que $\alpha = \beta$. Si $\alpha = 0$ es trivial, así que supongamos $\alpha > 0$.

Probemos que $(\alpha+\alpha)+\gamma = \alpha+(\alpha+\gamma)$ por inducción en γ, para todo α. Si $\gamma = 0$ es trivial así que supongamos $\gamma > 0$.

Luego $(\alpha+\alpha)+\gamma = 0+\gamma = \gamma$. Por otro lado, $\alpha+(\alpha+\gamma) = \{\alpha * +(\alpha+\gamma), \alpha+(\alpha+\gamma)*\} = \{\alpha'+(\alpha+\gamma), \alpha+(\alpha'+\gamma), \alpha+(\alpha+\gamma')\}$. Como $\gamma' < \gamma'$ por H.I. en γ tenemos que $\alpha+(\alpha+\gamma') = (\alpha+\alpha)+\gamma' = \gamma'$, luego en el conjunto están todos los ordinales menores que γ'. Falta ver que no está γ en el conjunto. La imagen mental puede ser esta, lo rojo representando elementos del conjunto:



Supongamos que $\alpha+(\alpha+\gamma') = \gamma$ para cierto γ'. Entonces sumando a izquierda a ambos lados α y usando que $\alpha+\alpha = 0$ obtenemos que $\alpha+\gamma' = \alpha+\gamma$, lo cuál es absurdo por la definición de la suma. Análogamente, si $\alpha'+(\alpha+\gamma) = \gamma$, sumando a ambos lados a izquierda γ' obtenemos $\alpha+\gamma = \alpha'+\gamma$, nuevamente absurdo. Luego $\{\alpha * +(\alpha+\gamma), \alpha+(\alpha+\gamma)*\} = \{\alpha'+(\alpha+\gamma), \alpha+(\alpha'+\gamma), \alpha+(\alpha+\gamma')\} = \gamma$ como queríamos ver.

Esto prueba el caso $\alpha+\beta = 0 \forall \gamma$.

Supongamos ahora que $\alpha+\beta > 0$.

Tenemos que $(\alpha+\beta)+\gamma = mex\{(\alpha+\beta)*+\gamma, (\alpha+\beta)+\gamma*\} = mex\{(\alpha'+\beta)+\gamma, (\alpha+\beta')+\gamma, (\alpha+\beta)+\gamma'\}$. Hay 3 tipos de ordinales en ese conjunto..

Por acá no sale.

Pero si hacemos inducción en n donde n es igual a la suma usual ordenados de mayor a menor de α, β, γ, ganamos. Tenemos que ordenarlos de mayor a menor para poder usar la H.I.

Si no los ordenáramos antes de sumar podría pasar que $\alpha'+\beta+\gamma = \alpha+\beta+\gamma$. Tomar por ejemplo $\alpha = 1, \beta = \gamma = \omega$.

porque en ese caso arriba podemos aplicar hipótesis inductiva en todos lados y listo. (puedo aplicar H.I. para cada término)

Faltaría probar el caso base $[\alpha+\beta+\gamma] = 0$ pero en este caso es trivial porque los 3 son cero (recordemos que si hay corchete se trata de la suma usual).

$\square$

Teorema 4. *Asumiendo que vale la distributiva y que los elementos distintos de* 0 *tienen inverso, estamos trabajando sobre un dominio íntegro.*

Demostración. Supongamos $xy = 0$. Entonces $xy + x = x \Rightarrow x(y+1) = x$. Supongamos que $x \neq 0$. Quiero ver que $y = 0$. Como $x \neq 0$ podemos dividir por x a ambos lados obteniendo $y+1 = 1 \Rightarrow y = 0$. $\square$

Teorema 5. *Dividir funciona*

Demostración. Basta ver que $\forall\alpha \neq 0 exists\beta$ tal que $\alpha\beta = 1$. La unicidad sale automáticamente de que es dominio íntegro: si $\alpha \hat{beta} = 1 \Rightarrow \alpha\hat{\beta} - \alpha\beta = \alpha(\hat{\beta} - \beta) = 0$ y por lo tanto $\hat{\beta} = \beta$. Construimos los inversos inductivamente. Si ya existe $\frac{1}{\alpha'} \forall 0 < \alpha' < \alpha$, entonces:

Dado $\alpha, \beta = \frac{1}{\alpha} := mex\{0, \frac{1+(\alpha'-\alpha)\beta'}{\alpha'} : \alpha' \neq 0\}$ donde β' indica un elemento que ya "metimos.en" el conjunto. Esta idea se repite en la construcción de la función de Bachmann: 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 $\frac{1+(\alpha'-\alpha)\beta'}{\alpha'}$.

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

Multiplicando por α a ambos lados y luego componiendo con la función $1-x$ obtenemos $1 - \alpha\beta'' = 1 - \alpha\frac{1+\alpha'\beta'-\alpha\beta'}{\alpha'} = 1 - \frac{\alpha+\alpha\alpha'\beta'-\alpha^2\beta'}{\alpha'} = \frac{\alpha'-\alpha-\alpha\alpha'\beta'+\alpha^2\beta'}{\alpha'}$. Analicemos la expresión $\alpha' - \alpha - \alpha\alpha'\beta' + \alpha^2\beta'$. La podemos agrupar de modo que quede $\alpha' - \alpha\alpha'\beta' + \alpha^2\beta' - \alpha$, y sacando factor común obtenemos $\alpha'(1 - \alpha\beta') - \alpha(1 - \alpha\beta') = (1 - \alpha\beta')(\alpha' - \alpha)$.

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

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

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

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

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

Además, si $\beta' = 0 \Rightarrow \beta'' = \frac{1}{\alpha}$ 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. □

0.2. "Por qué" no conocemos bien a $\bar{F}_2$ (pero a ω^{ω^ω} sí)

Conway polinomials, aplicaciones en criptografía

0.3. ¿Cómo son los inversos?

0.4. Primero construir ω^{ω^ω} a la manera usual

0.5. Ejemplos en sage?

Note that, in an additive group, a + b cannot be equal to either a' + b or a + b' unless a' = a or b' = b. Therefore, the above definition is the "simplest"possible definition of addition in some sense.

Likewise, in a field, a b can't be equal to a' b + a b' - a' b'. Otherwise, (a-a') (b-b') would be a zero product of nonzero factors.

0.6. Entonces ω^{ω^ω} te permite demostrar la existencia de $\bar{F}_2$. Vale la recíproca? (Reverse Mathematics) Ver cobb.pdf de la tesis

Me parece que para probar asociatividad de la suma tuve que hacer inducción hasta $\omega^{\omega^\omega}3$ pero si ω^{ω^ω} está bien definido entonces el otro también (claim) porque si hubiera una secuencia infinita decreciente en este habría una en alguna de las 3 copias.

0.7. che, pero esto permite operar con elementos en Fp?

Creo que sí, pero no hay una traducción obvia.

¿Cómo será la traducción? De esto estaría bueno hablar!!!

0.8. Tecnicismos

Conway afirma que la abelianidad permite hacer las cosas de a pasos `https://math.stackexchange.com/questions/2627213/prove-that-this-quadratically-closed-extension-`

$\bar{F}_p$ tiene Gal abeliano: `https://math.stackexchange.com/questions/2594693/galois-group-of-algebraic-closure-of-a-finite-field-is-abelian?noredirect=1&lq=1`

Si agarrás dos morfismos de la clausura algebraica que no conmutan, tenemos por ejemplo $\sigma_1(\alpha)\sigma_2(\alpha) \neq \sigma_2(\alpha)\sigma_1(\alpha)$ para algún α.