Probar a partir de los axiomas de grupo el inverso de ab

$$(ab)^{-1} = b^{-1}a^{-1}$$

$$ab\,\underbrace{(ab)^{-1}} = e$$

son únicos

axioma del inverso

$$b\,\underbrace{b^{-1}} = e \quad , \quad a\,\underbrace{a^{-1}} = e$$

¿cómo puedo probar esto?

Alcanza con probar que $b^{-1}a^{-1}$ cumple las condiciones de ser el inverso de ab

El inverso de ab es el único que cumple

$ab(ab)^{-1} = e$, $(ab)^{-1}ab = e$

Alcanza con sustituir $(ab)^{-1}$

por $b^{-1}a^{-1}$ y ver si se verifican

Vamos a ver si $(ab)(b^{-1}a^{-1}) = e$

Podemos calcular esto ↲ y ver si da e

$(ab)(b^{-1}a^{-1})$

podemos mostrar dónde usamos asociatividad

en cada caso. o no

Primero no nos fijamos donde estamos usando la asociatividad.

$$a b b^{-1} a^{-1} = a(b b^{-1})a^{-1} = a e a^{-1} = a a^{-1}$$
$$= e$$

Cómo sería formalmente (con todos los paréntesis)

por def.

$$abc := a(bc)$$

que es $= (ab)c$

$$abcd = a(b(cd)) = a$$

salimos de

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1}))$$

As con $a, b, b^{-1}a^{-1}$

$$= a((bb^{-1})a^{-1}) = a(e \cdot a^{-1}) = a(a^{-1})$$

As con b, b^{-1}, a^{-1}

Inv de b

Ne

llegamos a $= e$

Inv de a

análogamente salimos

$(b^{-1}a^{-1})(ab)$ y llegamos a e

Con estas dos igualdades

concluimos que $b^{-1}a^{-1}$ es el inverso de ab

$$(a^n)^{-1} = (a^{-1})^n$$

Una vez que sepamos que son el mismo elemento, podemos llamarlo a^{-n}

Formalmente podemos probarlo por inducción usando la propiedad anterior

PB: $n=0$ $(a^0)^{-1} = e^{-1} = e$, $(a^{-1})^0 = e$.

Si no: $n=1$ $(a^1)^{-1} = a^{-1}$, $(a^{-1})^1 = a^{-1}$

Si no: $n=2$ $(a^2)^{-1} = (a \cdot a)^{-1} = a^{-1} a^{-1} = a^{-2}$

parte anterior

P.I: $(a^n)^{-1} \overset{df}{=} (a \cdot a^{n-1})^{-1} = (a^{n-1})^{-1} a^{-1} =$

H.I $= (a^{-1})^{n-1} a^{-1} \overset{df}{=} (a^{-1})^n$

Si $gx = hx \Rightarrow g = h$

multiplicamos la igualdad por x^{-1} a la derecha

$$gxx^{-1} = hxx^{-1}$$
$$ge = he$$
$$g = h$$

Formalmente (con paréntesis)

$$(gx)x^{-1} = (hx)x^{-1}$$
$$g(xx^{-1}) = h(xx^{-1})$$
$$ge = he$$
$$g = h$$

$G = (\mathbb{Z}, +)$

↳ ojo la notación

$H = m\mathbb{Z} = \{\text{enteros múltiplos de } m\}$

$= \{mk \text{ con } k \in \mathbb{Z}\}$

terminarlo

2) y 3)

1) H es cerrado por $+$

2) el neutro $0 \in H$

3) Si $n \in H \Rightarrow -n$ está en H

1) Si $a \in H$ y $B \in H \Rightarrow a+b \in H$

$a = mk$, $b = mk' \Rightarrow a+b = mk + mk' = m(\underbrace{k+k'}_{\mathbb{Z}}) \in H$