9/7/11 First: When does $a+x=b$ have a sol?

407

$2+x=3$
$2+x=1$
$2(1-3x)=3(1-2x)$
$2(6-3x)=3(4-2x)$
$3x=2$, $2-3x=3$
in: integers, pos. ints, even integers, reals, pos. reals

1

Recall our analogy

$$(\mathbb{R},+) \longleftrightarrow (\mathbb{R}_{>0}, \times)$$

$$a+b \longleftrightarrow p\cdot q$$

Via this correspondence,

same letters, to ~~strengthen~~ analogy

$$a+x=b \longleftrightarrow ax=b$$

So both eqns are of the form

$$a * x = b \quad \text{for } * = \begin{cases} + \\ \times \end{cases} \text{ or}$$

How to solve equations of this type (slo-mo):

For $a,b \in S =$ any set (e.g. reals, integers, ...)

$+$	$\times$	$*$	property used
$a+x=b$	$ax=b$	$a*x=b$	
$-a+(a+x)=-a+b$	$\frac{1}{a}(ax)=\frac{1}{a}\cdot b$	$a^{-1}*(a*x)=a^{-1}*b$	Existence of inverses; apply same op to both sides
$(-a+a)+x=-a+b$	$(\frac{1}{a}\cdot a)x=\frac{1}{a}\cdot b$	$(a^{-1}*a)*x=a^{-1}*b$	assoc. property
$0+x=-a+b$	$1\cdot x=\frac{1}{a}\cdot b$	$I*x=a^{-1}*b$	existence of inverses
$x=-a+b$	$x=\frac{1}{a}\cdot b$	$x=a^{-1}*b$	property of identity

<u>So</u>: Given a set S with a binary operation $*$ ~~(e.g~~, what properties must $*$ have in order to solve equations like $a * x = b$ in S?? (e.g. $(S,*) = (\mathbb{R},+)$ or $(\mathbb{R}_{>0}, \times)$ or ...)

→ Come to board / write up suggestions.

<u>End Goal</u>

1) S is closed under $*$ (closure)
2) $*$ is assoc.
3) $\exists\ I \in S$ s.t. $I * a = a * I = a \quad \forall\ a \in S$ (identity)
4) $\forall\ a \in S$, $\exists\ a^{-1} \in S$ s.t. $a^{-1} * a = a * a^{-1} = I$.

<u>Def</u>: $(S,*)$ is called a <u>group</u> if it satisfies 1–4

<u>Examples</u>

$S = \mathbb{R}$, $* = +$

$S = \mathbb{Z}$, $* = +$

$S = \mathbb{R} \setminus \{0\}$, $* = \times$

$S = \mathbb{R}_{>0}$, $* = \times$

$S = 2\mathbb{Z}$, $* = +$

<u>Non-Examples</u>

$S = \mathbb{R}_{<0}$, $* = \times$

$S = \mathbb{R}_{>0}$, $* = +$

$S = \mathbb{Z} \setminus 0$, $* = \times$

$S = 1 + 2\mathbb{Z}$, $* = +$

More examples

- $S = \{0\}$, with $*$ defined by $0 * 0 = 0$.

$$0 = I$$
$$0^{-1} = 0$$

- $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ using $+$

$\bar{a} + \bar{b} = \overline{a+b} :=$ remainder upon dividing $a+b$ by n.

$\mathbb{Z}/3\mathbb{Z}$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

what is I?
what is $-\bar{2}$ = inverse of $\bar{2}$?

$\mathbb{Z}/2\mathbb{Z}$:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

So $\bar{1} + \bar{1} = \bar{0}$. (!)

Linear equations

$ax + b = cx + d$, either $a \neq 0$ or $c \neq 0$

$a, b, c, d \in S$ = a set, equipped w/ $+, \times$

$$ax + b = cx + d$$

$-cx + (ax+b) = -cx + (cx+d)$: existence of additive inverses

$(-cx + ax) + b = (-cx + cx) + d$: + is assoc

$(-cx + ax) + b = 0 + d$: property of additive inverses

$(-cx + ax) + b = d$: additive identity

$(-c+a)x + b = d$: $\times$ distributes over +

$((-c+a)x + b) + -b = d + -b$: existence of add inv.

$(-c+a)x + (b + -b) = d + -b$: assoc of +

$(-c+a)x + 0 = d + -b$: prop. of + inverses

$(-c+a)x = d + -b$: additive iden

<u>CASE 1</u> $a = c$: no solutions if $d \neq b$
infinitely many sols if $d = b$

<u>CASE 2</u> $a \neq c$

$\frac{1}{a-c}\left((a-c)x\right) = \frac{1}{a-c}(d-b)$: existence of mult inverses

$\left(\left(\frac{1}{a-c}\right)(a-c)\right)x = \frac{d-b}{a-c}$: $\times$ is assoc

$1 \cdot x = \frac{d-b}{a-c}$: prop of $\times$-inverses

$x = (d-b)/(a-c)$: mult iden

$(S, +, *)$ must satisfy:

1) $(S, +)$ is a group
2) $\times$ distributes over $+$
3) $(S - \{0\}, \times)$ is a group.

Any triple $(S, +, \times)$ satisfying 1–3 is called a <u>FIELD</u>.

<u>Examples</u>: $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$

<u>Non-examples</u>. $(\mathbb{Z}, +, \times)$, $(\mathbb{R}_{\geq 0}, +, \times)$

More examples

$\mathbb{Z}/2\mathbb{Z} := \{\bar{0}, \bar{1}\}$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Q: Is $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ a field?

Matrix Groups

Let F be a field (e.g. $F = \mathbb{R}$)

$$M_2(F) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in F \right\}$$

We say $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ iff $a = a'$, $b = b'$, $c = c'$, $d = d'$

We define.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}$$

Q: When does $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$?

$\longrightarrow$ iff $w = z = 1$, $x = y = 0$

$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Check. $I \cdot A = A \cdot I = A$

Solve $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$\rightsquigarrow GL_2(F)$ is a group under $\times$