MAT240
Dror Bar-Natan ~~Agenda: Uno~~

Sept. 12, 2006.

The real numbers: Set $\mathbb{R}$ with two binary operations + (plus) and $\cdot, \times$ (times) and two ~~special~~ distinct elements called 0 (zero) and 1 (one) such that

F1 $\mathbb{R}1$: Whenever a and b are in F real numbers, $(\forall a,b)$
$a+b=b+a \qquad a\cdot b = b\cdot a$
(The commutative laws)

F2 $\mathbb{R}2$: $\forall a,b,c^{\in F}\ (a+b)+c = a+(b+c)$ and $(a\cdot b)c = a(bc)$
(Associative law)

F3 $\mathbb{R}3$: "0 is an additive unit" (identity)
$\forall a^{\in F}\ a+0=a \ (=0+a)$ [$\mathbb{R}1$]
"1 is an ~~additive~~ multiplicative unit (identity)"
$\forall a^{\in F}\ 1\cdot a = a$

F4 $\mathbb{R}4$: For every a there is a b s.t. $a+b=0$
For every $a\neq 0$ there is a b s.t. $a\cdot b=1$
$\forall a\ \exists b$ s.t. $a+b=0$
$\forall a\neq 0\ \exists b\ a\cdot b = 1$ (Existence of negatives & inverses

F5 $\mathbb{R}5$: $\forall a,b,c \quad (a+b)\cdot c = a\cdot c + b\cdot c$
(Distributive law)

Much of algebra follows:
Follows: $(a+b)(a-b) = \underbrace{a^2}_{a\cdot a} - \underbrace{b^2}_{b\cdot b}$ $\qquad [- = +(-1)]$

Doesn't follow:
$\forall a\ \exists x$ s.t. $a=x^2$ or $-a=x^2$
↳ Every positive number has a square root.
eg. $9=3^2$

But this doesn't follow from our axioms & we don't need it.

eg Take $a=2$ No. x s.t. $2=x^2$ or $-2=x^2$ in $\mathbb{Q}$
↳ there is no number x that satisfies this that can be expressed as a fraction.

<u>Def'n</u>: A "field" is a set F with two binary operations $+$ (plus) and $\cdot, \times$ (times) and two distinct special elements 0 (zero) and 1 (one) s.t.

F1 (over):

<u>Examples.</u>

curly brackets - set

Set of things on left which satisfy set of things on right

1. Take $F = \mathbb{R}$, $0, 1, +, \times$ the usual ones.
2. Take $F = \mathbb{Q} = \{\text{the rational numbers}\} = \{\frac{m}{n} : m, n \text{ are integers}, n \neq 0\}$

$= \{\frac{0}{1} = 0, \frac{1}{1} = 1, \frac{240}{1} = 240, \frac{2}{7}, \frac{-2}{7} = -\frac{2}{7}, \dots\}$

Check: $0 = \frac{0}{1}$ $\quad 1 = \frac{1}{1}$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \dots$$

3. $F = \mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3\}$ = integers
all axioms work except for F4 part b.: no inverses.

No. Take $a = 3 \in \mathbb{Z}$, there is no $b \in \mathbb{Z}$ s.t. $a \cdot b = 1$
Indeed, in $\mathbb{R}$ $b = \frac{1}{3}$ but $\frac{1}{3} \notin \mathbb{Z}$

4. Tiny example. $F = \{0, 1\}$.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

In example, <u>you</u> set the rules and then show that it's true

$a + b = b + a$ $\quad$ check $\begin{cases} a = 0 & b = 0 \\ a = 0 & b = 1 \\ a = 1 & b = 0 \\ a = 1 & b = 1 \end{cases}$ $\quad$ check: $0 + 1 \overset{\shortparallel}{1} = 1 \overset{\shortparallel}{+} 0$ $\quad$ [F1a]✓

for all examples.

Check $a+(b+c)=(a+b)+c$ ... check for all.

$\forall a^{\neq 0} \exists b \ ab = 1$ [F4b]

a	b
0	X
1	1

don't need to check, according to axiom.
indeed, $\underset{a}{1} \cdot \underset{b}{1} = 1$

5. $\mathbb{C} = \{\text{Complex numbers}\} = \{a+bi : a, b \in \mathbb{R}\}$
↳ very useful for describing waves.

example to show how to work w/ axioms.

• Every theorem that we prove in class depends only on F1–F5 and ∴ holds true for $\mathbb{C}, \mathbb{Z}, \{0,1\}, \mathbb{R}$

Thm. $\forall a, b \in F$
$(a+b)(a-b) = a^2 - b^2$

$-$ is not yet formally defined.

Lemma: (Little theorem you prove on way to something else)
(I) Every $a \in F$ has a unique negative.
(II) Every $a \neq 0 \in F$ has unique inverse.

Precisely: (I) $a + b_1 = 0$, $a + b_2 = 0 \Rightarrow b_1 = b_2$
→ need to prove this! (Implication)
(II) $a \neq 0$, $ab_1 = 1$, $ab_2 = 1 \Rightarrow b_1 = b_2$

Try proving (I)

Proof: (II) Suppose $a \neq 0$, $ab_1 = 1 = ab_2$
Take any c s.t. $ca = 1$. (exists by F4b)
$c(ab_1) = c(ab_2)$
$(ca)b_1 = (ca)b_2$ (by F2)
$1b_1 = 1b_2$ (by choice of c)
$b_1 = b_2$ (by F3)

Lemma proved it's unique.

$\boxed{a + (-a) = 0}$

Def'n: For any $a \in F$ define $(-a)$ to be the b for which $a + b = 0$
Likewise, for any $a \neq 0$, define a^{-1} to be the b for which $ab = 1$. $\boxed{aa^{-1} = 1}$

hereby defined to be

Def'n: $a - b := a + (-b)$

$\frac{a}{b} := a \cdot (b^{-1})$ provided $b \neq 0$.

Silly def'n: $a^2 := a \cdot a$.

Now, everything that appears in theorem finally makes sense.

i.e. $(a+b)(a-b) = a^2 - b^2$ makes sense.

Proof of main theorem: (start w/ LHS and try to get to RHS)

$$
\begin{aligned}
(a+b)(a-b) &\overset{\text{def}}{=} (a+b)(a+(-b)) \overset{F5}{=} \\
&= (a+b)a + (a+b)(-b) \\
&\overset{F5}{=} aa + ba + a(-b) + b(-b) \\
&\overset{\text{Lemma}}{=} aa + ba + -(ab) + (-bb) \\
&= \\
&\vdots
\end{aligned}
$$

Lemma $a(-b) = -ab$.

Proof: exercise.