Lec 8/24

Wednesday, August 24, 2016 9:06 AM

Proofs about fields

Field $\mathbb{F}$ - a set with two binary operations, $+, \cdot$, satisfying P1-P9

examples: $\mathbb{R}, \mathbb{Q}, \mathbb{C}$

Proposition 1 $-(-a) = a \quad \forall a \in \mathbb{F}$

Justification

Proof $(a + (-a)) + (-(-a)) = a + ((-a) + (-(-a)))$ P1

$0 + (-(-a)) = a + 0$ P3

$-(-a) = a$ P2

Proposition 2 $(a^{-1})^{-1} = a \quad \forall a \in \mathbb{F} \setminus \{0\}$

Proof

lemma 1 $a \in \mathbb{F}\setminus\{0\} \Rightarrow a^{-1} \in \mathbb{F}\setminus\{0\}$

Proof by contradiction:

assume $a^{-1} = 0$ for contradiction

$a \cdot a^{-1} = a \cdot 0$

$1 = 0$ P7, $0 \cdot a = 0$ (proved)

This contradicts P5, $1 \neq 0$

so $a^{-1} \neq 0$

Global substitution: $+ \longrightarrow \cdot$

$0 \longrightarrow 1$

$-(\,) \longrightarrow (\,)^{-1}$

from proposition 1.

Proposition 3 $a(-b) = -(ab) \quad \forall a, b \in \mathbb{F}$

Proof $a(b + (-b)) = a \cdot 0$

$ab + a(-b) = 0$ P9, and $a \cdot 0 = 0$ proved

$-(ab) + (ab + a(-b)) = -(ab) + 0$ P3, addition well-defined

$(-(ab) + ab) + a(-b) = -(ab) + 0$ P1

$0 + a(-b) = -(ab) + 0$ P3

$a(-b) = -(ab)$ P2

Corollary (of Prop 1 and Prop 3) $(-a)(-b) = ab$

Corollary (of Prop 1 and prop 3) $(-a)(-b) = ab$

Proof

$(-a)(-b) = -((-a)b)$	Prop 3
$(-a)(-b) = -(b(-a))$	P8
$(-a)(-b) = -(-(ba))$	Prop 3
$(-a)(-b) = ba$	prop 1
$(-a)(-b) = ab$	P8

"Proposition" → from homework assignment. $a-b = b-a \Rightarrow a=b$

"Proof"

$a-b=b-a$	hypothesis
$(a-b)+b = (b-a)+b = b+(b-a)$	P4
$a+(-b+b) = (b+b)+(-a)$	P1
$a = a+0 = (b+b)+(-a)$	P3, P2
$a+a = ((b+b)+(-a))+a$	addition
$a+a = (b+b)+(-a+a)$	P1
$a+a = b+b+0 = b+b$	P3, P2
$a(1+1) = b(1+1)$	P9
$a=b$	P8??? if $1+1 \neq 0$ we can multiply both the sides by $(1+1)^{-1}$

$\mathbb{Z}_2$

Problem 1.25: a field of 2 elements, $\mathbb{Z}_2$ or $\mathbb{F}_2$
$\mathbb{F}_2 = \{0, 1\}$

with the following + and · tables:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

remark: for any prime p, there is a field $\mathbb{F}_p = \{0, 1, \ldots p-1\}$

where $\forall a,b \in \mathbb{F}_p$ $a+b = \text{mod}(a+b, p)$ (remainder after division of $\frac{a+b}{p}$)
$a \cdot b = \text{mod}(a \cdot b, p)$

$\mathbb{F}_6$ is not a field $2 \neq 0$, $3 \neq 0$, but $2 \cdot 3 \bmod 6 = 0$
↳ non prime

More axioms for real numbers which exclude these fields

[illegible]

More axioms for real numbers which exclude these fields

an ordered field $\mathbb{F}$ contains a distinguished subset $P \subseteq \mathbb{F} \setminus \{0\}$ which satisfy 3 additional axioms

P10: Trichotomy: $\forall a \in \mathbb{F}$, exactly one of the following holds:

(1) $a = 0$
(2) $a \in P$
(3) $-a \in P$

P11: $a, b \in P \Rightarrow a+b \in P$

P12: $a, b \in P \Rightarrow ab \in P$

Observation: $\mathbb{C}$ is not an ordered field.

Proof by contradiction. suppose we could find a set $P \subseteq \mathbb{C} \setminus \{0\}$ satisfying P10 - P12

$$i = \sqrt{-1} \neq 0$$

so either $i \in P$ or $-i \in P$

if $i \in P$, then $i \cdot i = -1 \in P$ P12

so $-1 \cdot i = -i \in P$. but this is a contradiction of P10

if $-i \in P$, then $(-i) \cdot (-i) \cdot (-i) = -i \cdot (-1) = i \in P$
same contradiction.

Note: if $\mathbb{F}$ is an ordered field, then we can define

$a < b \iff b - a \in P$

$a \leq b \iff b - a \in P \cup \{0\}$