MAT157 Lecture 6 Notes

Anatoly Zavyalov

September 23, 2020

1 Consequences of the field axioms P1-P9

Let F be a field, and $a, b, c, ... \in F$.

1.1 Proposition

- For $a, b \in F$, there is a unique $x \in F$ s.t.

$$a + x = b$$

- for $a, b, \in F$ with $a \neq 0$, there is a unique $x \in F$ with

$$a \cdot x = b.$$

Proof. Given $a, b \in F$, by P3 (additive inverse) there is $-a \in F$ with $a + (-a) = 0$. The calculation

$$\begin{aligned} a + ((-a) + b) &= (a + (-a)) + b && \text{By P1} \\ &= 0 + b && \text{By P3} \\ &= b && \text{By P2} \end{aligned}$$

So $x = (-a) + b$ is a solution to $a + x = b$.

Conversely, if x is **any** solution then

$$\begin{aligned} x &= 0 + x && \text{By P2} \\ &= ((-a) + a) + x && \text{By P3} \\ &= (-a) + (a + x) && \text{By P1} \\ &= (-a) + b && \text{by assumption} \end{aligned}$$

So, $x = (-a) + b$.

The second part is very similar (left as an exercise). $\square$

1.2 Special Cases

- If $a + x = a$, then $x = \mathbf{0}$ (uniqueness of additive neutral element).
- If $a + x = \mathbf{0}$, then $x = -a$ (uniqueness of additive inverse).
- If $a \neq 0, ax = a$, then $x = \mathbf{1}$ (uniqueness of multiplicative neutral element).
- If $a \neq 0, ax = 1$ then $x = a^{-1}$ (uniqueness of multiplicative inverse).

1.3 Proposition

For all $a \in F$,

$$a \cdot 0 = 0 = 0 \cdot a$$

Proof.

$$\begin{aligned} a \cdot 0 = 0 \cdot a & & \text{By P8} \\ &= a \cdot (0 + 0) & \text{By P2} \\ &= a \cdot 0 + a \cdot 0 \end{aligned}$$

So, $x = a \cdot 0$ solves $a \cdot 0 + x = a \cdot 0$, but so does $x = 0$. So $a \cdot 0 = 0$. □

1.4 Proposition

For $a, b, c \in F$:

$$\begin{aligned} -(-a) &= a \\ (-a) + (-b) &= -(a + b) \\ (a^{-1})^{-1} &= a & \text{(if } a \neq 0\text{)} \\ a^{-1} \cdot b^{-1} &= (a \cdot b)^{-1} & \text{if } a, b \neq 0 \\ (-a) \cdot (-b) &= a \cdot b \\ a \cdot (-b) &= -(a \cdot b) \end{aligned}$$

Proof. We show both sides solve $a \cdot b + x = 0$.

$$\begin{aligned}
a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) & & \text{By P9} \\
= a \cdot 0 & & \text{By P3} \\
= 0 & & \text{by proposition} \\
a \cdot b + (-(a \cdot b)) = 0 & & \text{By P3}
\end{aligned}$$

So, $a \cdot (-b) = -a \cdot b$. □

1.5 Proposition

A product is equal to **0** if an only if one of the factors is **0**, that is

$$(a \cdot b = \mathbf{0}) \Leftrightarrow (a = 0 \text{ or } b = \mathbf{0}).$$

Proof. We prove both directions.
$(\Longleftarrow)$

If $a = 0$, then $a \cdot b = 0 \cdot b = 0$. Similarly, for $b = 0$.
$(\Longrightarrow)$

Suppose $a \cdot b = 0$. If $a = 0$, then we're done (nothing to prove). If $a \neq 0$, then a^{-1} is defined by P6 (?).

$$\begin{aligned}
a \cdot b = 0 &\implies a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0 \\
&\implies (a^{-1} \cdot a) \cdot b = 0 \\
&\implies \mathbf{1} \cdot b = 0 \\
&\implies b = 0.
\end{aligned}$$

□

2 Notational conventions

- Omitting dots: $ab = a \cdot b$
- Omitting parentheses: $a + b + c = (a + b) + c = a + (b + c)$, $abc = (ab)c = a(bc)$
- Multiplication comes before addition: $ab + c = (a \cdot b) + c$
- $a - b = a + (-b)$
- $\frac{a}{b} = ab^{-1}$
- $a^2 = a \cdot a, a^3 = a \cdot a^2$, etc.

You're used to this for real numbers, but we'll use the conventions for **any** field. E.g. $\mathbb{Z}_7$. Something like

$$\frac{[2]_7}{[5]_7} = [2]_7 \cdot ([5]_7)^{-1} = [2]_7 \cdot [3]_7 = [6]_7$$

$[3]_7$ is the multiplicative inverse of $[5]_7$ because

$$\begin{aligned} [5]_7 \cdot [3]_7 = [15]_7 \\ &= [1]_7 \\ &= \mathbf{1} \end{aligned}$$