Notes on "Finite-Dimensional Vector Spaces" by Paul R. Halmos

September 26, 2022

Each `\section` corresponds to the scope of one member's assignment, and each `\subsection` corresponds to one theorem or exercise in the textbook, specified in the format $m.n$ where m is the section number and n is the theorem/exercise number. If n is not given, we use $n = 1$ instead.

1 Toga (2022/09/19)

1.1 Exercise 1.1

(a) Since addition is commutative, $0+\alpha = \alpha+0$ holds. We also have $\alpha+0 = \alpha$ by definition, hence $0 + \alpha = \alpha$.

2 Mohehe

2.1 Exercise 1.1

(b) We have $(\alpha+\beta)+(-\alpha) = (\beta+\alpha)+(-\alpha) = \beta+(\alpha+(-\alpha)) = \beta+0 = \beta$ by definition. We also have $(\alpha+\beta)+(-\alpha) = (\alpha+\gamma)+(-\alpha) = (\gamma+\alpha)+(-\alpha) = \gamma + (\alpha + (-\alpha)) = \gamma + 0 = \gamma$ by definition. Therefore, $\beta = \gamma$ holds.

If $\alpha + \beta = \alpha + \gamma$, we have $\beta = \beta + 0 = 0 + \beta = (\alpha + (-\alpha)) + \beta = (-\alpha + \alpha) + \beta = -\alpha + (\alpha + \beta) = -\alpha + (\alpha + \gamma) = (-\alpha + \alpha) + \gamma = (\alpha + (-\alpha)) + \gamma = 0 + \gamma = \gamma + 0 = \gamma$ by definition.

(c) We have $\alpha+(\beta-\alpha) = \alpha+(\beta+(-\alpha)) = \alpha+((-\alpha)+\beta) = (\alpha+(-\alpha))+\beta = 0 + \beta = \beta + 0 = \beta$ by definition.

We have $\alpha+(\beta-\alpha) = (\beta-\alpha)+\alpha = \beta+(-\alpha+\alpha) = \beta+(\alpha-\alpha) = \beta+0 = \beta$ by definition.

(d) We have $0 \cdot \alpha = \alpha \cdot 0 = \alpha(1 + (-1)) = \alpha 1 + \alpha(-1) = \alpha + (-1)\alpha = \alpha + (-\alpha) = 0$ by definition and Exercise 1(e), hence $\alpha \cdot 0 = 0 \cdot \alpha = 0$.

We have $\alpha 0 + \alpha 0 = \alpha(0 + 0) = \alpha 0 = \alpha 0 + 0$ by definition, hence $\alpha 0 = 0$ by Exercise 1(b). Note that $0\alpha = \alpha 0$ by definition.

(e) We have $\alpha+(-1)\alpha = 1\alpha+(-1)\alpha = (1+(-1))\alpha = 0\alpha = 0$ by definition and Exercise 1(d). Since the additive inverse is unique, we obtain $(-1)\alpha = -\alpha$.

(f) We have $(-\alpha)(-\beta) = ((-1)\alpha)((-1)\beta) = (\alpha(-1))((-1)\beta) = \alpha((-1)((-1)\beta)) = \alpha((-1)(-1)\beta)$ by Exercise 1(e) and definition. We also have $(-1)(-1) = 0 + (-1)(-1) = (1 + (-1)) + (-1)(-1) = 1 + (-1) + (-1)(-1) = 1 + (-1)((-1) + 1) = 1 + (-1)(1 + (-1)) = 1 + (-1)0 = 1 + 0 = 1$ by definition. By it and definition, $\alpha((-1)(-1)\beta) = \alpha(1\beta) = \alpha(\beta 1) = \alpha\beta$ holds. Therefore, $(-\alpha)(-\beta) = \alpha\beta$ holds.

(g) If $\alpha\beta = 0$, suppose $\alpha \neq 0$ and $\beta \neq 0$ hold. By supposition and definition, we have $0 = \alpha^{-1}0 = \alpha^{-1}(\alpha\beta) = (\alpha^{-1}\alpha)\beta = (\alpha\alpha^{-1})\beta = 1\beta = \beta 1 = \beta$, hence $\beta = 0$. However, this result contradicts supposition, "$\alpha \neq 0$ and $\beta \neq 0$". Therefore, if $\alpha\beta = 0$, then either $\alpha = 0$ or $\beta = 0$ (or both).

3 Joh (2022/09/19)

3.1 Exercise 1.2

(a) The set of positive integers is not a field since there is no additive inverse for 1.

(b) The set of integers is not a field since there is no multiplicative inverse for 2.

(c) There exists a bijective map φ from $\mathbb{N}$ (or $\mathbb{Z}$) to $\mathbb{Q}$ [1], where $\mathbb{Q}$ is a field [2]. We can make $\mathbb{N}$ a field by re-defining (i) addition by $a \oplus b = \varphi^{-1}(\varphi(a) + \varphi(b))$ and (ii) multiplication by $a \otimes b = \varphi^{-1}(\varphi(a)\varphi(b))$ for each $a, b \in \mathbb{N}$. Note that the additive and multiplicative identities become $\varphi^{-1}(0)$ and $\varphi^{-1}(1)$, respectively. For each $\alpha \in \mathbb{N}$, the additive inverse becomes $\varphi^{-1}(-\varphi(\alpha))$, and the multiplicative inverse becomes $\varphi^{-1}(1/\varphi(\alpha))$ if $\alpha \neq \varphi^{-1}(0)$.

Let $\alpha, \beta, \gamma, \alpha', \beta' \in \mathbb{N}$. Note that
1) $\alpha \oplus \beta = \varphi^{-1}(\varphi(\alpha)+\varphi(\beta)) = \varphi^{-1}(\varphi(\beta)+\varphi(\alpha)) = \beta \oplus \alpha$ holds.(addition is commutative)
(from here, mohehe)
2) $\alpha \oplus (\beta \oplus \gamma) = \alpha \oplus (\varphi^{-1}(\varphi(\beta) + \varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha) + \varphi(\varphi^{-1}(\varphi(\beta) + \varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha) + (\varphi(\beta) + \varphi(\gamma))) = \varphi^{-1}((\varphi(\alpha) + \varphi(\beta)) + \varphi(\gamma)) = \varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha) + \varphi(\beta))) + \varphi(\gamma)) = \varphi^{-1}(\varphi(\alpha) + \varphi(\beta)) \oplus \gamma = (\alpha \oplus \beta) \oplus \gamma$ holds.(addition is associative)
3) $\alpha \oplus \varphi^{-1}(0) = \varphi^{-1}(\varphi(\alpha)+\varphi(\varphi^{-1}(0))) = \varphi^{-1}(\varphi(\alpha)+0) = \varphi^{-1}(\varphi(\alpha)) = \alpha$ holds.(there exists additive identity, $\varphi^{-1}(0)$) If α' and β' are additive identity, we have $\alpha' = \alpha' \oplus \beta' = \beta' \oplus \alpha' = \beta'$ by 1) and the definition of additive identity.(additive identity is unique)
4) $-\varphi(\alpha) \in \mathbb{Q}$ holds by definition, so $\varphi^{-1}(-\varphi(\alpha)) \in \mathbb{N}$ holds. Therefore,

$\alpha \oplus \varphi^{-1}(-\varphi(\alpha)) = \varphi^{-1}(\varphi(\alpha)+\varphi(\varphi^{-1}(-\varphi(\alpha)))) = \varphi^{-1}(\varphi(\alpha)+(-\varphi(\alpha))) = \varphi^{-1}(0)$ holds.(for each α ($\alpha \in \mathbb{N}$), there exists additive inverse) For each α, if α' and β' are additive inverse, we have $\alpha' = \alpha' \oplus \varphi^{-1}(0) = \alpha' \oplus (\alpha \oplus \beta') = (\alpha' \oplus \alpha) \oplus \beta' = (\alpha \oplus \alpha') \oplus \beta' = \varphi^{-1}(0) \oplus \beta' = \beta \oplus \varphi^{-1}(0) = \beta'$ by 1), 2), 3) and the definition of additive inverse.(additive inverse is unique)
5) $\alpha \otimes \beta = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)) = \varphi^{-1}(\varphi(\beta)\varphi(\alpha)) = \beta \otimes \alpha$ holds.(multiplication is commutative)
6) $\alpha \otimes (\beta \otimes \gamma) = \alpha \otimes (\varphi^{-1}(\varphi(\beta)\varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(\varphi(\beta)\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)\varphi(\gamma)) = \varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\beta)))\varphi(\gamma)) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)) \otimes \gamma = (\alpha \otimes \beta) \otimes \gamma$ holds.(multiplication is associative)
7) $\alpha \otimes \varphi^{-1}(1) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(1))) = \varphi^{-1}(\varphi(\alpha) \cdot 1) = \alpha$ holds.(there exists additive identity, $\varphi^{-1}(1)$) If α' and β' are additive identity, we have $\alpha' = \alpha' \otimes \beta' = \beta' \otimes \alpha' = \beta'$ by 5) and definition of multiplicative identity.(multiplicative identity is unique)
8) For each α ($\alpha \neq \varphi^{-1}(0)$), $(1/\varphi(\alpha)) \in \mathbb{Q}$ holds by definition, so $\varphi^{-1}(1/\varphi(\alpha)) \in \mathbb{N}$ holds. Therefore, $\alpha \otimes \varphi^{-1}(1/\varphi(\alpha)) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(1/\varphi(\alpha)))) = \varphi^{-1}(\varphi(\alpha)(1/\varphi(\alpha))) = \varphi^{-1}(1)$ holds.(for each α ($\alpha \in \mathbb{N}$), there exists multiplicative inverse) For each α ($\alpha \neq \varphi^{-1}(0)$), if α' and β' are multiplicative inverse, we have $\alpha' = \alpha' \otimes \varphi^{-1}(1) = \alpha' \otimes (\alpha \otimes \beta') = (\alpha' \otimes \alpha) \otimes \beta' = (\alpha \otimes \alpha') \otimes \beta' = \varphi^{-1}(1) \otimes \beta' = \beta' \otimes \varphi^{-1}(1) = \beta'$ by 5), 6), 7) and the definition of multiplicative inverse.(multiplicative inverse is unique)
9) $\alpha \otimes (\beta \oplus \gamma) = \alpha \otimes (\varphi^{-1}(\varphi(\beta)+\varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(\varphi(\beta)+\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha)(\varphi(\beta)+\varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)+\varphi(\alpha)\varphi(\gamma)) = \varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\beta)))+\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha \otimes \beta)+\varphi(\alpha \otimes \gamma)) = \alpha \otimes \beta \oplus \alpha \otimes \gamma$ holds.(distributive law stands)

References

[1] https://proofwiki.org/wiki/Rational_Numbers_are_Countably_Infinite

[2] https://proofwiki.org/wiki/Rational_Numbers_form_Field