

# Notes on “Finite-Dimensional Vector Spaces”

by Paul R. Halmos

September 24, 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) Since addition is commutative,  $(\alpha + \beta) + (-\alpha) = (\beta + \alpha) + (-\alpha)$  holds. We have  $(\beta + \alpha) + (-\alpha) = \beta + (\alpha + (-\alpha))$  because addition is associative. We obtain  $\beta + (\alpha + (-\alpha)) = \beta + 0$  by definition. We also have  $\beta + 0 = \beta$  because of definition, hence  $(\alpha + \beta) + (-\alpha) = \beta$ . Since addition is commutative,  $(\alpha + \gamma) + (-\alpha) = (\gamma + \alpha) + (-\alpha)$  holds. We have  $(\gamma + \alpha) + (-\alpha) = \gamma + (\alpha + (-\alpha))$  because addition is associative. We obtain  $\gamma + (\alpha + (-\alpha)) = \gamma + 0$  by definition. We also have  $\gamma + 0 = \gamma$  because of definition, thus  $(\alpha + \gamma) + (-\alpha) = \gamma$ . In addition, we have  $(\alpha + \beta) + (-\alpha) = (\alpha + \gamma) + (-\alpha)$ , therefore  $\beta = \gamma$ .

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 obtain  $\alpha + (\beta - \alpha) = \alpha + (\beta + (-\alpha))$  because of the sentence in the problems. Since addition is commutative,  $\alpha + (\beta + (-\alpha)) = (\beta + (-\alpha)) + \alpha$  holds. We have  $(\beta + (-\alpha)) + \alpha = \beta + ((-\alpha) + \alpha)$  because addition is associative. We obtain  $\beta + ((-\alpha) + \alpha) = \beta + (\alpha + (-\alpha))$  because addition

is commutative. In addition, the definition leads  $\beta + (\alpha + (-\alpha)) = \beta + 0$ . We also have  $\beta + 0 = \beta$ , hence  $\alpha + (\beta - \alpha) = \beta$ .

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

- (d) We have  $\alpha \cdot (\beta + (-\beta)) = \alpha \cdot 0$  by the definition of addition. We obtain  $\alpha \cdot 0 = 0 \cdot \alpha$  because multiplication is commutative. The definition of multiplication leads  $\alpha \cdot (\beta + (-\beta)) = \alpha\beta + \alpha(-\beta)$ . Since multiplication is commutative,  $\alpha\beta + \alpha(-\beta) = \beta\alpha + (-\beta)\alpha$ . We obtain  $\beta\alpha + (-\beta)\alpha = \beta\alpha + (-1)\beta\alpha$  by exercise 1.(e) We also have  $\beta\alpha + (-1)\beta\alpha = \beta\alpha + (-1)(\beta\alpha)$  because multiplication is associative. Exercise 1.(e) leads  $\beta\alpha + (-1)(\beta\alpha) = \beta\alpha + (-\beta\alpha)$ . We have  $\beta\alpha + (-\beta\alpha) = 0$  by the definition of addition, hence  $\alpha \cdot 0 = 0 \cdot \alpha = 0$  holds.

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  $(-1)\alpha = (-\alpha\alpha^{-1})\alpha$  by the definition of multiplication. Since multiplication is associative,  $(-\alpha\alpha^{-1})\alpha = (-\alpha)(\alpha^{-1}\alpha)$ . We obtain  $(-\alpha)(\alpha^{-1}\alpha) = (-\alpha)1$  by the definition of multiplication. We also have  $(-\alpha)1 = -\alpha$  by the definition of multiplication, thus  $(-1)\alpha = -\alpha$  holds.

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

- (f) We have  $(-\alpha)(-\beta) = ((-1)(\alpha))(-1)(\beta)$  by exercise 1.(e) We obtain  $((-1)(\alpha))(-1)(\beta) = ((\alpha)(-1))(-1)(\beta)$  because multiplication is commutative. We have  $((\alpha)(-1))(-1)(\beta) = (\alpha)((-1)(-1))(\beta)$  because multiplication is associative. We obtain  $(\alpha)((-1)(-1))(\beta) = (\alpha)((-1)(-1)^{-1})(\beta)$  because  $-1 = (-1)^{-1}$  We have  $(\alpha)((-1)(-1)^{-1})(\beta) = (\alpha 1)(\beta)$  by the definition of multiplication. We obtain  $(\alpha 1)(\beta) = \alpha\beta$  by the definition of multiplication, thus,  $(-\alpha)(-\beta) = \alpha\beta$ .

- (g) If  $\beta \neq 0$ , we have  $(\alpha\beta)\beta^{-1} = \alpha(\beta\beta^{-1})$  because multiplication is associative. We obtain  $\alpha(\beta\beta^{-1}) = \alpha 1$  by the definition of multiplication. We have  $\alpha 1 = \alpha$  by the definition of multiplication. We obtain  $0 \cdot \beta^{-1} = 0$  by exercise 1(d). thus if  $\beta \neq 0$ ,  $\alpha = 0$ . If  $\alpha \neq 0$ , we have  $(\alpha\beta)\alpha^{-1} = (\beta\alpha)\alpha^{-1}$  because multiplication is commutative. We obtain  $(\beta\alpha)\alpha^{-1} = \beta(\alpha\alpha^{-1})$  because multiplication is associative. We have  $\beta(\alpha\alpha^{-1}) = \beta 1$  by the definition of multiplication. We have  $\beta 1 = \beta$  by the definition of multiplication. We obtain  $0 \cdot \beta^{-1} = 0$  by exercise 1(d). thus if  $\alpha \neq 0$ ,  $\beta = 0$ . If  $\alpha = 0$  and  $\beta = 0$ ,  $\alpha\beta = 0$  by exercise 1.(d) 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  $\varphi$  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  $\alpha \neq \varphi^{-1}(0)$ .

## References

- [1] [https://proofwiki.org/wiki/Rational\\_Numbers\\_are\\_Countably\\_Infinite](https://proofwiki.org/wiki/Rational_Numbers_are_Countably_Infinite)
- [2] [https://proofwiki.org/wiki/Rational\\_Numbers\\_form\\_Field](https://proofwiki.org/wiki/Rational_Numbers_form_Field)