

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

December 4, 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.

Contents

1	Toga (2022/09/19)	2
1.1	Exercise 1.1	2
2	Mohehe (2022/09/27)	2
2.1	Exercise 1.1	2
3	Mohehe (2022/09/19)	2
3.1	Exercise 1.2	2
4	Mohehe (2022/10/8)	4
4.1	Exercise 1.3	4
4.2	Exercise 1.4	5
4.3	Exercise 1.5	7
4.4	Exercise 1.6	8
4.5	Exercise 1.7	8
5	Johno (2022/11/27)	9
5.1	Exercise 2.1	9
6	Mohehe (2022/11/31)	10
6.1	Exercise 2.2	10
6.2	Exercise 2.3	10
6.3	Exercise 2.4	10

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 (2022/09/27)

2.1 Exercise 1.1

- (b) 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. Therefore, $\beta = \gamma$ holds.
- (c) We have $\alpha + (\beta - \alpha) = \alpha + (\beta + (-\alpha)) = \alpha + ((-\alpha) + \beta) = (\alpha + (-\alpha)) + \beta = 0 + \beta = \beta + 0 = \beta$ by definition. Therefore, $\alpha + (\beta - \alpha) = \beta$ holds.
- (d) We have $\alpha 0 + \alpha 0 = \alpha(0 + 0) = \alpha 0 = \alpha 0 + 0$ by definition, hence $\alpha 0 = 0$ by Exercise 1(b). We also have $\alpha \cdot 0 = 0 \cdot \alpha$ by definition. Therefore, $\alpha \cdot 0 = 0 \cdot \alpha = 0$.
- (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 Mohehe (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 \mathcal{N} (or \mathcal{Z}) to \mathcal{Q} [1], where \mathcal{Q} is a field [2]. We can make \mathcal{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 $a, b \in \mathcal{N}$. Note that the additive and multiplicative identities become $\varphi^{-1}(0)$ and $\varphi^{-1}(1)$, respectively. For each $\alpha \in \mathcal{N}$, 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 $\alpha, \beta, \gamma, \alpha', \beta' \in \mathcal{N}$. 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)
- 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) $-\varphi(\alpha) \in \mathcal{Q}$ holds by definition, so $\varphi^{-1}(-\varphi(\alpha)) \in \mathcal{N}$ 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 ($\alpha \in \mathcal{N}$), 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 ($\alpha \neq \varphi^{-1}(0)$), $(1/\varphi(\alpha)) \in \mathcal{Q}$ holds by definition, so $\varphi^{-1}(1/\varphi(\alpha)) \in \mathcal{N}$ 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 ($\alpha \in \mathcal{N}$), 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)

$$\begin{aligned}
9) \quad \alpha \otimes (\beta \oplus \gamma) &= \alpha \otimes (\varphi^{-1}(\varphi(\beta) + \varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(\varphi(\beta) + \\
&\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha)(\varphi(\beta) + \varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta) + \varphi(\alpha)\varphi(\gamma)) = \\
&\varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\beta))) + \varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha \otimes \beta) + \varphi(\alpha \otimes \\
&\gamma)) = \alpha \otimes \beta \oplus \alpha \otimes \gamma \text{ holds. (distributive law stands)}
\end{aligned}$$

4 Mohehe (2022/10/8)

4.1 Exercise 1.3

For two integers a and b , we denote by $a \% b$ the remainder after dividing a by b , and write $b \mid a$ if and only if $a \% b = 0$. For clarity, we denote the ordinary sum and product of two integers a and b by $a +_{\mathbb{Z}} b$ and $a \cdot_{\mathbb{Z}} b$, respectively. Note that $\alpha + \beta = (\alpha +_{\mathbb{Z}} \beta) \% m$ and $\alpha\beta = (\alpha \cdot_{\mathbb{Z}} \beta) \% m$ for $\alpha, \beta \in \mathbb{Z}_m$.

(a) Let $\alpha, \beta, \gamma \in \mathbb{Z}_m, k \in \mathbb{Z}$

1' Proof : if m is a prime, \mathbb{Z}_m is a field.

Suppose m is a prime,

- 1) $\alpha + \beta = (\alpha +_{\mathbb{Z}} \beta) \% m = (\beta +_{\mathbb{Z}} \alpha) \% m = \beta + \alpha$ (addition is commutative)
- 2) Since $\alpha +_{\mathbb{Z}} (\beta + \gamma) = \alpha +_{\mathbb{Z}} (\beta +_{\mathbb{Z}} \gamma) \% m \equiv \alpha +_{\mathbb{Z}} (\beta +_{\mathbb{Z}} \gamma) = (\alpha +_{\mathbb{Z}} \beta) +_{\mathbb{Z}} \gamma \equiv (\alpha +_{\mathbb{Z}} \beta) \% m +_{\mathbb{Z}} \gamma = (\alpha + \beta) +_{\mathbb{Z}} \gamma \pmod{m}$ holds, $\alpha + (\beta + \gamma) = (\alpha +_{\mathbb{Z}} (\beta + \gamma)) \% m = ((\alpha + \beta) +_{\mathbb{Z}} \gamma) \% m = (\alpha + \beta) + \gamma$ holds. (addition is associative)
- 3) $\alpha + 0 = (\alpha +_{\mathbb{Z}} 0) \% m = \alpha \% m = \alpha$ (there exists additive identity)
By it and 1), if β and γ are additive identity, $\beta = \beta + \gamma = \gamma + \beta = \gamma$ (additive identity is unique)
- 4) If $\alpha +_{\mathbb{Z}} \beta = m$, $\alpha + \beta = (\alpha +_{\mathbb{Z}} \beta) \% m = m \% m = 0$ (there exists additive inverse)
- 5) $\alpha\beta = (\alpha \cdot_{\mathbb{Z}} \beta) \% m = (\beta \cdot_{\mathbb{Z}} \alpha) \% m = \beta\alpha$ (multiplication is commutative)
- 6) Since $\alpha \cdot_{\mathbb{Z}} (\beta\gamma) = \alpha \cdot_{\mathbb{Z}} ((\beta \cdot_{\mathbb{Z}} \gamma) \% m) \equiv \alpha \cdot_{\mathbb{Z}} (\beta \cdot_{\mathbb{Z}} \gamma) = (\alpha \cdot_{\mathbb{Z}} \beta) \cdot_{\mathbb{Z}} \gamma \equiv ((\alpha \cdot_{\mathbb{Z}} \beta) \% m) \cdot_{\mathbb{Z}} \gamma = (\alpha\beta) \cdot_{\mathbb{Z}} \gamma \pmod{m}$ holds, $\alpha(\beta\gamma) = (\alpha \cdot_{\mathbb{Z}} (\beta\gamma)) \% m = ((\alpha\beta) \cdot_{\mathbb{Z}} \gamma) \% m = (\alpha\beta)\gamma$ holds. (multiplication is associative)
- 7) $\alpha 1 = (\alpha \cdot_{\mathbb{Z}} 1) \% m = \alpha \% m = \alpha$ (there exists multiplicative identity)
By it and 5), if β and γ are multiplicative identity, $\beta = \beta\gamma = \gamma\beta = \gamma$ (multiplicative identity is unique)
- 8) For all $\alpha (\alpha \neq 0)$, suppose there doesn't exist β that makes $\alpha\beta = 1$. There exist $\beta, \gamma \in \mathbb{Z}_m$ with $\beta \neq \gamma$ and $\alpha\beta = \alpha\gamma$, because β is any one from 0 to $m-1$ and $\alpha\beta$ is any one from 0 to $m-1$ except 1. Therefore, $(\alpha \cdot_{\mathbb{Z}} \beta +_{\mathbb{Z}} (-\alpha \cdot_{\mathbb{Z}} \gamma)) = \alpha \cdot_{\mathbb{Z}} (\beta +_{\mathbb{Z}} (-\gamma)) = km$ holds. The right side has divisor m , but it contradicts that the left side doesn't have divisor of m except 1, because $0 < \alpha < (m-1)$ and $((-m) < (\beta +_{\mathbb{Z}} (-\gamma)) < 0$ or $0 < (\beta +_{\mathbb{Z}} (-\gamma)) < m$) holds. Thus,

there exists β that makes $\alpha\beta = 1$. (there exists multiplicative inverse)

A brief proof: Since each $\alpha \in \mathcal{Z}_m \setminus \{0\}$ is coprime to m , there exist integers x and y such that $\alpha \cdot_{\mathcal{Z}} x +_{\mathcal{Z}} m \cdot_{\mathcal{Z}} y = 1$ by [3]. Putting $x' = x \% m \in \mathcal{Z}_m$, we obtain $\alpha x' = (\alpha \cdot_{\mathcal{Z}} x) \% m = (\alpha \cdot_{\mathcal{Z}} x +_{\mathcal{Z}} m \cdot_{\mathcal{Z}} y) \% m = 1 \% m = 1$. Hence $x' = \alpha^{-1}$.

$$\begin{aligned} 9) \quad \alpha(\beta + \gamma) &= (\alpha \cdot_{\mathcal{Z}} (\beta + \gamma)) \% m = (\alpha \cdot_{\mathcal{Z}} ((\beta +_{\mathcal{Z}} \gamma) \% m)) \% m \equiv \\ &(\alpha \cdot_{\mathcal{Z}} (\beta +_{\mathcal{Z}} \gamma)) \% m = (\alpha \cdot_{\mathcal{Z}} \beta + \alpha \cdot_{\mathcal{Z}} \gamma) \% m \equiv ((\alpha \cdot_{\mathcal{Z}} \beta) \% m +_{\mathcal{Z}} \\ &(\alpha \cdot_{\mathcal{Z}} \gamma) \% m) \% m \equiv (\alpha \cdot_{\mathcal{Z}} \beta) \% m + (\alpha \cdot_{\mathcal{Z}} \gamma) \% m \equiv \alpha\beta + \alpha\gamma \\ &\text{holds. (distributive law stands)} \end{aligned}$$

In conclusion, if m is a prime, \mathcal{Z}_m is a field.

2' Proof : If \mathcal{Z}_m is a field, m is a prime.

By contraposition, it is equivalent to prove "If m is not a prime, \mathcal{Z}_m is not a field." We can show 1) to 7) and 9) in the same way as 1'. For each m , suppose there exist α and β that make $\alpha\beta = 1$. m is not a prime, so let p be one of prime factors of m and then we have $m = p \cdot_{\mathcal{Z}} p' \cdot (p' \in \mathcal{Z} \text{ and } 1 < p' < m)$. If $\alpha = p$, by $\alpha\beta = 1$ and $m = p \cdot_{\mathcal{Z}} p'$, we have $\alpha \cdot_{\mathcal{Z}} \beta = k \cdot_{\mathcal{Z}} m + 1 (k \in \mathcal{Z}) \Leftrightarrow p \cdot_{\mathcal{Z}} \beta = k \cdot_{\mathcal{Z}} p \cdot_{\mathcal{Z}} p' +_{\mathcal{Z}} 1 \Leftrightarrow (\beta +_{\mathcal{Z}} (-k \cdot_{\mathcal{Z}} p')) \cdot_{\mathcal{Z}} p = 1$. The right side is 1 but the left one is not 1 because of $1 < p$ and $\beta +_{\mathcal{Z}} (-k \cdot_{\mathcal{Z}} p') \in \mathcal{Z}$. Therefore It is contradicted. For each m , there doesn't exist α and β that make $\alpha\beta = 1$. In conclusion, "If m is not a prime, \mathcal{Z}_m is not a field." and "If \mathcal{Z}_m is a field, m is a prime."

Because of 1' and 2', \mathcal{Z}_m is a field if and only if m is a prime.

(b) 4

(c) 5

4.2 Exercise 1.4

Define $\alpha_n = \overbrace{1 + \dots + 1}^{n \text{ terms}}$ for $n \in \{1, 2, \dots\}$. Then,

$$\begin{aligned} \alpha_m \alpha_n &= \alpha_m (\overbrace{1 + \dots + 1}^{n \text{ terms}}) \\ &= \alpha_m ((\overbrace{1 + \dots + 1}^{(n-1) \text{ terms}}) + 1) \\ &= \alpha_m (\overbrace{1 + \dots + 1}^{(n-1) \text{ terms}}) + \alpha_m \cdot 1 && \text{(by distributive law)} \\ &= \alpha_m (\overbrace{1 + \dots + 1}^{(n-1) \text{ terms}}) + \alpha_m && \text{(by definition of multiplicative identity)} \\ &= \dots \end{aligned}$$

$$\begin{aligned}
&= \alpha_m(1+1) + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} \\
&= \alpha_m \cdot 1 + \alpha_m \cdot 1 + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} && \text{(by distributive law)} \\
&= \overbrace{\alpha_m + \cdots + \alpha_m}^{n \text{ terms}} && \text{(by definition of multiplicative identity)} \\
&= \overbrace{1 + \cdots + 1}^{m \text{ terms}} + \overbrace{(1 + \cdots + 1)}^{m \text{ terms}} + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} \\
&= \overbrace{1 + \cdots + 1}^{m \text{ terms}} + \overbrace{((1 + \cdots + 1) + 1)}^{(m-1) \text{ terms}} + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} \\
&= \overbrace{1 + \cdots + 1}^{m \text{ terms}} + \overbrace{(1 + (1 + \cdots + 1))}^{(m-1) \text{ terms}} + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} && \text{(by commutative property)} \\
&= \overbrace{1 + \cdots + 1}^{(m+1) \text{ terms}} + \overbrace{(1 + \cdots + 1)}^{(m-1) \text{ terms}} + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} && \text{(by associative property)} \\
&= \cdots \\
&= \overbrace{1 + \cdots + 1}^{(2m-2) \text{ terms}} + \overbrace{(1+1)}^{(n-2) \text{ terms}} + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} \\
&= \overbrace{1 + \cdots + 1}^{2m \text{ terms}} + \overbrace{\alpha_m + \cdots + \alpha_m}^{(n-2) \text{ terms}} && \text{(by associative property)} \\
&= \cdots \\
&= \overbrace{1 + \cdots + 1}^{m(n-1) \text{ terms}} + \alpha_m \\
&= \cdots \\
&= \overbrace{1 + \cdots + 1}^{(mn-2) \text{ terms}} + (1+1) \\
&= \overbrace{1 + \cdots + 1}^{mn \text{ terms}} && \text{(by associative property)} \\
&= \alpha_{mn}
\end{aligned}$$

for all m, n .

Assume there exists an n with $\alpha_n = 0$ but $\alpha_k \neq 0$ for any $k < n$. It suffices to prove that n is a prime.

Suppose n is not any prime. Let p be one of prime factors of n and then we have $n = pp'(p' \in \mathcal{N}$ and $p' > 1)$. By $\alpha_m \alpha_n = \alpha_{mn}$ for all m and n , $\alpha_n = \alpha_p \alpha_{p'}$ holds. We have either $\alpha_p = 0$ or $\alpha_{p'} = 0$ (or both) because of $\alpha_n = 0$ and Exercise 1.1 (g). However, it is contradictory to $\alpha_p = 0$ and $\alpha_{p'} = 0$. Therefore, n is a prime.

4.3 Exercise 1.5

- (a) For the followings, it is used that \mathcal{Q} and \mathcal{R} are fields. Note that $\sqrt{2} \in \mathcal{R}$ and $\sqrt{2} \notin \mathcal{Q}$

Let $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{Q}(\sqrt{2}) \subset \mathcal{R}$.

For all $\alpha_1, \alpha_2 \in \mathcal{Q}(\sqrt{2})$, $\alpha_1 + \alpha_2 \in \mathcal{Q}(\sqrt{2})$ and $\alpha_1\alpha_2 \in \mathcal{Q}(\sqrt{2})$ by the followings.

There exist $a, b, c, d \in \mathcal{Q}$, $\alpha_1 = a + b\sqrt{2}$ and $\alpha_2 = c + d\sqrt{2}$ hold.

We have $\alpha_1 + \alpha_2 = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ and $(a + c), (b + d) \in \mathcal{Q}$, so $\alpha_1 + \alpha_2 \in \mathcal{Q}(\sqrt{2})$.

In addition, we have $\alpha_1\alpha_2 = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ and $(ac + 2bd), (ad + bc) \in \mathcal{Q}$, so $\alpha_1\alpha_2 \in \mathcal{Q}(\sqrt{2})$

- 1) $\alpha_1 + \alpha_2 = \alpha_2 + \alpha_1$ (addition is commutative)
- 2) $\alpha_1 + (\alpha_2 + \alpha_3) = (\alpha_1 + \alpha_2) + \alpha_3$ (addition is associative)
- 3) We have $0 = 0 + 0\sqrt{2} \in \mathcal{Q}(\sqrt{2})$ and $\alpha_1 + 0 = \alpha_1$
($\mathcal{Q}(\sqrt{2})$ has additive identity)
- 4) For all $\alpha_1 \in \mathcal{Q}(\sqrt{2})$, put $\alpha_1 = a + b\sqrt{2}$ with $a, b \in \mathcal{Q}$. There exists $\alpha'_1 \in \mathcal{Q}(\sqrt{2})$ with $\alpha'_1 = (-a) + (-b)\sqrt{2}$. We have $\alpha_1 + \alpha'_1 = a + b\sqrt{2} + (-a) + (-b)\sqrt{2} = a - a + b\sqrt{2} - b\sqrt{2} = 0$. Therefore, to every $\alpha_1 \in \mathcal{Q}(\sqrt{2})$, there corresponds $\alpha'_1 \in \mathcal{Q}(\sqrt{2})$ with $\alpha_1 + (-\alpha_1) = 0$
- 5) $\alpha_1\alpha_2 = \alpha_2\alpha_1$ (multiplication is commutative)
- 6) $\alpha_1(\alpha_2\alpha_3) = (\alpha_1\alpha_2)\alpha_3$ (multiplication is associative)
- 7) We have $1 = 1 + 0\sqrt{2} \in \mathcal{Q}(\sqrt{2})$ and $\alpha_1 \cdot 1 = \alpha_1$
($\mathcal{Q}(\sqrt{2})$ has multiplicative identity)
- 8) For all $\alpha_1 \in \mathcal{Q}(\sqrt{2})$ with $\alpha_1 \neq 0$, put $\alpha_1 = a + b\sqrt{2}$ with $a, b \in \mathcal{Q}$. In this case, $a \neq 0$ or $b \neq 0$ holds by the followings.
"If $\alpha_1 = 0$, we have $\alpha_1 = a + b\sqrt{2} = 0 \Leftrightarrow a = -b\sqrt{2}$. Therefore, $a = b = 0$ by $a, b \in \mathcal{Q}$."
Let $\alpha''_1 = \frac{a}{a^2 - 2b^2} + \left(-\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in \mathcal{Q}(\sqrt{2})$. Note that we have $a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2})$ and $a, b \in \mathcal{Q}$ with $(a \neq 0 \text{ or } b \neq 0)$, so we have $a + b\sqrt{2} \neq 0$ and $a - b\sqrt{2} \neq 0$, and then $a^2 - 2b^2 \in \mathcal{Q}$ with $a^2 - 2b^2 \neq 0$. We have $\alpha_1\alpha''_1 = (a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} + \left(-\frac{b}{a^2 - 2b^2}\right)\sqrt{2}\right) = \frac{a^2 - ab\sqrt{2} + ab\sqrt{2} - 2b^2}{a^2 - 2b^2} = 1$. Therefore, to every $\alpha_1 \in \mathcal{Q}(\sqrt{2})$ with $\alpha_1 \neq 0$, there exists $\alpha''_1 \in \mathcal{Q}(\sqrt{2})$ with $\alpha_1\alpha''_1 = 1$
- 9) $\alpha_1(\alpha_2 + \alpha_3) = \alpha_1\alpha_2 + \alpha_1\alpha_3$ (distributive law stands)

from 1) to)9, $\mathcal{Q}(\sqrt{2})$ is a field.

- (b) Let $\mathcal{Z}(\sqrt{2})$ be the set of all numbers of the form $\alpha + \beta\sqrt{2}$, where α and β are integers. If $\mathcal{Z}(\sqrt{2})$ is a field, $2 = 2 + 0\sqrt{2} (\in \mathcal{Z}(\sqrt{2}))$ has multiplicative inverse. There exists $\exists\beta_1 = \{\alpha + \beta\sqrt{2} | \beta_1 \in \mathcal{Z}(\sqrt{2})\}$ with $2\beta_1 = 1 \iff$

$\beta_1 = \frac{1}{2}$. However, $\frac{1}{2} \notin \mathcal{Z}(\sqrt{2})$ holds, so $\mathcal{Z}(\sqrt{2})$ is not a field.

Another way : Let $\mathcal{Z}(\sqrt{2})$ be the set of all numbers of the form $\alpha + \beta\sqrt{2}$, where α and β are integers. $\mathcal{Z}(\sqrt{2})$ is not a field since there is no multiplicative inverse for $2 + \sqrt{2} \in \mathcal{Z}(\sqrt{2})$ by the followings.

Suppose there exists multiplicative inverse for $2 + \sqrt{2}$. There exists $\exists \beta_1 \in \mathcal{Z}(\sqrt{2})$ with $\beta_1 = \alpha + \beta\sqrt{2}$ and $(2 + \sqrt{2})\beta_1 = 1$ by supposition. Therefore, we have $(2 + \sqrt{2})\beta_1 = (2 + \sqrt{2})(\alpha + \beta\sqrt{2}) = 2(\alpha + \beta) + (\alpha + 2\beta)\sqrt{2} = 1 \iff 2(\alpha + \beta) - 1 = -(\alpha + 2\beta)\sqrt{2} \implies 2(2(\alpha + \beta)^2 - 2(\alpha + \beta)) - 1 = 2(\alpha + 2\beta)^2$. It is contradicted because the left is odd number and the right is even number. Therefore, $(2 + \sqrt{2})\beta_1 = 1$ is contradicted and then there is no multiplicative inverse for $2 + \sqrt{2}$.

4.4 Exercise 1.6

- (a) Let P be such set of all polynomials with integer coefficients, $\text{id} \in P$ be $\text{id}(x) = x$ ($x \in \mathcal{R}$), and $I \in P$ be $I(x) = 1$ ($x \in \mathcal{R}$).

Suppose there exists $q \in P$ with $\text{id} \cdot q = I$. Then, we have $\text{id}(0) \cdot q(0) = 0$, and it is contradicted to supposition. Therefore, there does not exist $q \in P$ with $\text{id} \cdot q = I$. In other words, id does not have the multiplicative inverse. In conclusion, the set of all polynomials with integer coefficients does not form a field.

- (b) the set of all polynomials with real number coefficients does not form a field for the same reason.

4.5 Exercise 1.7

- (a) Suppose \mathfrak{F} is a field. Let $(\alpha, \beta) \in \mathfrak{F}$ with $\alpha, \beta \in \mathcal{R}$. Then, additive identity would be $(0, 0)$, because for all α, β , we have $\alpha + 0 = \alpha, \beta + 0 = \beta$. In addition, multiplicative identity would be $(1, 1)$, because for all α, β , we have $\alpha 1 = \alpha, \beta 1 = \beta$.

Here, think about $(0, 1) (\neq (0, 0))$. For all (α, β) , we have $(0, 1)(\alpha, \beta) = (0, \beta) (\neq (1, 1))$. Therefore, $(0, 1)$ does not have multiplicative inverse. In conclusion, \mathfrak{F} is not a field.

- (b) Let $(\alpha_1, \beta_1), (\alpha_2, \beta_2), (\alpha_3, \beta_3) \in \mathfrak{F}$ with $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathcal{R}$.

- (A) (1) $(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2) = (\alpha_2, \beta_2) + (\alpha_1, \beta_1)$. (addition is commutative)
(2) $(\alpha_1, \alpha_1) + ((\alpha_2, \beta_2) + (\alpha_3, \beta_3)) = (\alpha_1 + \alpha_2 + \alpha_3, \beta_1 + \beta_2 + \beta_3) = ((\alpha_1, \beta_1) + (\alpha_2, \beta_2)) + (\alpha_3, \beta_3)$. (addition is associative)
(3) There exists $(0, 0) \in \mathfrak{F}$ such that $(\alpha_1, \beta_1) + (0, 0) = (\alpha_1, \beta_1)$ for every (α_1, β_1) . (\mathfrak{F} has additive identity)
(4) For every (α_1, β_1) , there exists $(-\alpha_1, -\beta_1) \in \mathfrak{F}$ such that $(\alpha_1, \beta_1) + (-\alpha_1, -\beta_1) = (0, 0)$.

- (B) (1) $(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2 - \beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1) = (\alpha_2, \beta_2)(\alpha_1, \beta_1)$.
(multiplication is commutative)
- (2) $((\alpha_1, \beta_1)(\alpha_2, \beta_2))(\alpha_3, \beta_3) = (\alpha_1\alpha_2\alpha_3 - \beta_1\beta_2\alpha_3 - \alpha_1\beta_2\beta_3 - \beta_1\alpha_2\beta_3, \alpha_1\beta_2\alpha_3 + \beta_1\alpha_2\alpha_3 + \alpha_1\alpha_2\beta_3 - \beta_1\beta_2\beta_3) = (\alpha_1, \beta_1)((\alpha_2, \beta_2)(\alpha_3, \beta_3))$. (multiplication is associative)
- (3) There exists $(1, 0) \in \mathfrak{F}$ such that $(\alpha_1, \beta_1)(1, 0) = (\alpha_1, \beta_1)$ for every (α_1, β_1) . (\mathfrak{F} has multiplicative identity)
- (4) For every $(\alpha_1, \beta_1) \neq (0, 0)$, there exists $\left(\frac{\alpha_1}{\alpha_1^2 + \beta_1^2}, -\frac{\beta_1}{\alpha_1^2 + \beta_1^2}\right) \in \mathfrak{F}$ such that $(\alpha_1, \beta_1)\left(\frac{\alpha_1}{\alpha_1^2 + \beta_1^2}, -\frac{\beta_1}{\alpha_1^2 + \beta_1^2}\right) = (1, 0)$.
- (C) $(\alpha_1, \beta_1)((\alpha_2, \beta_2) + (\alpha_3, \beta_3)) = (\alpha_1, \beta_1)(\alpha_2 + \alpha_3, \beta_2 + \beta_3) = (\alpha_1\alpha_2 + \alpha_1\alpha_3 - \beta_1\beta_2 - \beta_1\beta_3, \alpha_1\beta_2 + \alpha_1\beta_3 + \beta_1\alpha_2 + \beta_1\alpha_3) = (\alpha_1\alpha_2 - \beta_1\beta_2, \alpha_1\beta_2 + \beta_1\alpha_2) + (\alpha_1\alpha_3 - \beta_1\beta_3, \alpha_1\beta_3 + \beta_1\alpha_3) = (\alpha_1, \beta_1)(\alpha_2, \beta_2) + (\alpha_1, \beta_1)(\alpha_3, \beta_3)$. (distributive law stands)
- (c) Let \mathfrak{F}' be the set of all pairs of (α, β) of complex numbers.
- (a) Suppose \mathfrak{F}' is a field. Let $(\alpha, \beta) \in \mathfrak{F}'$ with $\alpha, \beta \in \mathcal{C}$. Then, additive identity would be $(0, 0)$, because for all α, β , we have $\alpha + 0 = \alpha, \beta + 0 = \beta$. In addition, multiplicative identity would be $(1, 1)$, because for all α, β , we have $\alpha 1 = \alpha, \beta 1 = \beta$.
Here, think about $(0, 1) \neq (0, 0)$. For all (α, β) , we have $(0, 1)(\alpha, \beta) = (0, \beta) \neq (1, 1)$. Therefore, $(0, 1)$ does not have multiplicative inverse. In conclusion, \mathfrak{F}' is not a field.
- (b) Suppose \mathfrak{F}' is a field. Let $(\alpha, \beta) \in \mathfrak{F}'$ with $\alpha, \beta \in \mathcal{C}$. Then, additive identity would be $(0, 0)$, because for all α, β , we have $\alpha + 0 = \alpha, \beta + 0 = \beta$. In addition, multiplicative identity would be $(1, 0)$, because for all α, β , we have $\alpha 1 - \beta 0 = \alpha, \alpha 0 + \beta 1 = \beta$.
Here, think about $(i, 1) \neq (0, 0)$. There exists (α, β) such that $(i, 1)(\alpha, \beta) = (\alpha i - \beta, \beta i + \alpha) = (1, 0)$. Then, we have $\alpha i - \beta = 1$, and $\beta i + \alpha = 0 \iff \alpha i - \beta = 0$. It is contradicted. Therefore, $(i, 1)$ does not have multiplicative inverse. In conclusion, \mathfrak{F}' is not a field.

5 Johno (2022/11/27)

5.1 Exercise 2.1

- (a) We have $0 + x = x + 0 = x$ by definition.
- (b) It follows from definition that $0 + 0 = 0$, hence $0 = -0$ by the uniqueness of additive inverse.
- (c) We can prove this as in Exercise 1.1 (d).
- (d) The same as above.

- (e) Let $\alpha x = 0$ hold. If $\alpha \neq 0$, then $x = 1x = (\frac{1}{\alpha}\alpha)x = \frac{1}{\alpha}(\alpha x) = \frac{1}{\alpha}0 = 0$ by definition and Exercise 2.1 (c).
- (f) By definition and Exercise 2.1 (d), we have $1x + (-1)x = (1-1)x = 0x = 0$. Hence $-x = -(1x) = (-1)x$.
- (g) It follows from definition that $y + (x - y) = y + (-y + x) = (y - y) + x = 0 + x = x + 0 = x$.

6 Mohehe (2022/11/31)

6.1 Exercise 2.2

We have $Z_p^n = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in Z_p\}$. Moreover, Z_p has p members. Therefore, the number of the vectors in this vector space is p^n .

6.2 Exercise 2.3

Suppose \mathcal{V} is a vector space. If $x = (0, 1) \in \mathcal{V}$, we have $1(0, 1) = (0, 1)$ by definition of vector spaces, but we also have $1(0, 1) = (0, 0)$ by definition of \mathcal{V} . It is contradicted, so \mathcal{V} is not a vector space.

6.3 Exercise 2.4

- (a) For $(1, 0, 0) \in \mathcal{V}$ and $i \in \mathcal{C}$, we have $i(1, 0, 0) = (i, 0, 0) \notin \mathcal{V}$, because $i \notin \mathcal{R}$. Therefore \mathcal{V} is not a vector space.
- (b) Let $(0, a_2, a_3), (0, b_2, b_3), (0, c_2, c_3) \in \mathcal{V}$ and $\alpha, \beta \in \mathcal{C}$.
We have $(0, a_2, a_3) + (0, b_2, b_3) = (0, a_2 + b_2, a_3 + b_3) \in \mathcal{V}$ and $\alpha(0, a_2, a_3) = (0, \alpha a_2, \alpha a_3) \in \mathcal{V}$. Therefore \mathcal{V} is closed under addition and scalar multiplication.
 - (A) (1) $(0, a_2, a_3) + (0, b_2, b_3) = (0, a_2 + b_2, a_3 + b_3) = (0, b_2, b_3) + (0, a_2, a_3)$. (addition is commutative)
 - (2) $(0, a_2, a_3) + ((0, b_2, b_3) + (0, c_2, c_3)) = (0, a_2, a_3) + (0, b_2 + c_2, b_3 + c_3) = (0, a_2 + b_2 + c_2, a_3 + b_3 + c_3) = (0, a_2, a_3) + (0, b_2, b_3) + (0, c_2, c_3)$. (addition is associative)
 - (3) There exists $(0, 0, 0) \in \mathcal{V}$ such that $(0, a_2, a_3) + (0, 0, 0) = (0, a_2, a_3)$ for every $(0, a_2, a_3)$. (\mathcal{V} has additive identity)
 - (4) For every $(0, a_2, a_3)$, there exists $(0, -a_2, -a_3)$ such that $(0, a_2, a_3) + (0, -a_2, -a_3) = (0, 0, 0)$.
 - (B) (1) $\alpha(\beta(0, a_2, a_3)) = (0, \alpha\beta a_2, \alpha\beta a_3) = (\alpha\beta)(0, a_2, a_3)$. (multiplication by scalars is associative)
 - (2) We have $1(0, a_2, a_3) = (0, a_2, a_3)$ for $1 \in \mathcal{C}$ and for every $(0, a_2, a_3)$.

- (C) (1) $\alpha((0, a_2, a_3) + (0, b_2, b_3)) = \alpha(0, a_2 + b_2, a_3 + b_3) = (0, \alpha a_2 + \alpha b_2, \alpha a_3 + \alpha b_3) = (0, \alpha a_2, \alpha a_3) + (0, \alpha b_2, \alpha b_3) = \alpha(0, a_2, a_3) + \alpha(0, b_2, b_3)$.
- (2) $(\alpha + \beta)(0, a_2, a_3) = (0, (\alpha + \beta)a_2, (\alpha + \beta)a_3) = (0, \alpha a_2 + \beta a_2, \alpha a_3 + \beta a_3) = (0, \alpha a_2, \alpha a_3) + (0, \beta a_2, \beta a_3) = \alpha(0, a_2, a_3) + \beta(0, a_2, a_3)$.

In conclusion, \mathcal{V} is a vector space.

- (c) For $(0, 1, 1), (1, 0, 1) \in \mathcal{V}$, we have $(0, 1, 1) + (1, 0, 1) = (1, 1, 2) \notin \mathcal{V}$, because $1 \neq 0$. Therefore \mathcal{V} is not a vector space.
- (d) Let $(a_1, a_2, a_3), (b_1, b_2, b_3), (c_1, c_2, c_3) \in \mathcal{V}$ with $a_1 + a_2 = b_1 + b_2 = c_1 + c_2 = 0$ and $\alpha, \beta \in \mathcal{C}$.

We have $(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3) \in \mathcal{V}$ because $a_1 + b_1 + a_2 + b_2 = 0$. Moreover, we have $\alpha(a_1, a_2, a_3) = (\alpha a_1, \alpha a_2, \alpha a_3) \in \mathcal{V}$ because $\alpha a_1 + \alpha a_2 = \alpha(a_1 + a_2) = 0$. Therefore \mathcal{V} is closed under addition and scalar multiplication.

- (A) (1) $(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3) = (b_1, b_2, b_3) + (a_1, a_2, a_3)$. (addition is commutative)
- (2) $(a_1, a_2, a_3) + ((b_1, b_2, b_3) + (c_1, c_2, c_3)) = (a_1, a_2, a_3) + (b_1 + b_1, b_2 + c_2, b_3 + c_3) = (a_1 + b_1 + c_1, a_2 + b_2 + c_2, a_3 + b_3 + c_3) = (a_1, a_2, a_3) + (b_1, b_2, b_3) + (c_1, c_2, c_3)$. (addition is associative)
- (3) There exists $(0, 0, 0) \in \mathcal{V}$ such that $(a_1, a_2, a_3) + (0, 0, 0) = (a_1, a_2, a_3)$ for every (a_1, a_2, a_3) . (\mathcal{V} has additive identity)
- (4) For every (a_1, a_2, a_3) , there exists $(-a_1, -a_2, -a_3)$ such that $(a_1, a_2, a_3) + (-a_1, -a_2, -a_3) = (0, 0, 0)$.
- (B) (1) $\alpha(\beta(a_1, a_2, a_3)) = (\alpha\beta a_1, \alpha\beta a_2, \alpha\beta a_3) = (\alpha\beta)(a_1, a_2, a_3)$. (multiplication by scalars is associative)
- (2) We have $1(a_1, a_2, a_3) = (a_1, a_2, a_3)$ for $1 \in \mathcal{C}$ and for every (a_1, a_2, a_3) .
- (C) (1) $\alpha((a_1, a_2, a_3) + (b_1, b_2, b_3)) = \alpha(a_1 + b_1, a_2 + b_2, a_3 + b_3) = (\alpha a_1 + \alpha b_1, \alpha a_2 + \alpha b_2, \alpha a_3 + \alpha b_3) = (\alpha a_1, \alpha a_2, \alpha a_3) + (\alpha b_1, \alpha b_2, \alpha b_3) = \alpha(a_1, a_2, a_3) + \alpha(b_1, b_2, b_3)$.
- (2) $(\alpha + \beta)(a_1, a_2, a_3) = ((\alpha + \beta)a_1, (\alpha + \beta)a_2, (\alpha + \beta)a_3) = (\alpha a_1 + \beta a_1, \alpha a_2 + \beta a_2, \alpha a_3 + \beta a_3) = (\alpha a_1, \alpha a_2, \alpha a_3) + (\beta a_1, \beta a_2, \beta a_3) = \alpha(a_1, a_2, a_3) + \beta(a_1, a_2, a_3)$.
- (e) For $(1, 0, 0), (0, 1, 0) \in \mathcal{V}$, we have $(1, 0, 0) + (0, 1, 0) = (1, 1, 0) \notin \mathcal{V}$, because $1 + 1 \neq 0$. Therefore \mathcal{V} is not a vector space.

References

- [1] https://proofwiki.org/wiki/Rational_Numbers_are_Countably_Infinite
- [2] https://proofwiki.org/wiki/Rational_Numbers_form_Field

[3] https://proofwiki.org/wiki/Bezout%27s_Identity