Lan Yung-Chi, 2026/01/06

1 Definition

A *field* $\mathbf{F}$ is a set containing at least two distinct elements called 0 and 1, along with operations of addition and multiplication satifying all the properties listed below.

1. **Commutativity**

   $\alpha + \beta = \beta + \alpha$ and $\alpha\beta = \beta\alpha$, for all $\alpha, \beta \in \mathbf{F}$.

2. **Associativity**

   $(\alpha + \beta) + \lambda = \alpha + (\beta + \lambda)$ and $(\alpha\beta)\lambda = \alpha(\beta\lambda)$, for all $\alpha, \beta, \lambda \in \mathbf{F}$.

3. **Identities**

   $\lambda + 0 = \lambda$ and $1\lambda = \lambda$, for all $\lambda \in \mathbf{F}$.

4. **Additive Inverse**

   For every $\alpha \in \mathbf{F}$, there exists a unique $\beta \in \mathbf{F}$ such that $\alpha + \beta = 0$.

5. **Multiplicative Inverse**

   For every $\alpha \in \mathbf{F}$ with $\alpha \neq 0$, there exists a unique $\beta \in \mathbf{F}$ such that $\alpha\beta = 1$.

6. **Distributive Property**

   $\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta$, for all $\lambda, \alpha, \beta \in \mathbf{F}$.

Note

In linear algebra we rarely deal with fields other than $\mathbf{R}$ and $\mathbf{C}$, but other fields do exist such as the set of rational numbers along with the usual operations of addition and multiplication, and the set $\{0, 1\}$ with the usual operations of addition and multiplication except that $1 + 1$ is defined to equal 0.

2 Exercise

Prove that the set of *complex numbers* with the following operations of addition and multiplication is a field. For the sake of simplicity, we can trivially say that $\mathbf{R}$ is a field, and safely use all calculation techniques from $\mathbf{R}$.

2.1 Definition

- A complex number is an ordered pair (a, b), where $a, b \in \mathbf{R}$, written as $a + b\,i$.
- The set of all complex numbers is denoted by $\mathbf{C}$:

$$\mathbf{C} = \{a + b\,i \mid a, b \in \mathbf{R}\}.$$

- Addition and multiplication on $\mathbf{C}$ are defined by

$$(a + b\,i) + (c + d\,i) = (a + c) + (b + d)\,i, \tag{1}$$

$$(a + b\,i)(c + d\,i) = (ac - bd) + (ad + bc)\,i; \tag{2}$$

  with $a, b, c, d \in \mathbf{R}$.

2.2 Proof

1. **Commutativity**

   For all $\alpha, \beta \in \mathbf{C}$, we can write $\alpha = a + b\,i$ and $\beta = c + d\,i$ with some $a, b, c, d \in \mathbf{R}$, then

$$\begin{aligned}
\alpha + \beta &= (a + b\,i) + (c + d\,i) \\
&= (a + c) + (b + d)\,i && \text{by (1)} \\
\beta + \alpha &= (c + d\,i) + (a + b\,i) \\
&= (c + a) + (d + b)\,i && \text{by (1)} \\
&= \alpha + \beta && \text{by comm. of } \mathbf{R}
\end{aligned}$$

$$\begin{aligned}
\alpha\beta &= (a + b\,i)(c + d\,i) \\
&= (ac - bd) + (ad + bc)\,i && \text{by (2)} \\
\beta\alpha &= (c + d\,i)(a + b\,i) \\
&= (ca - db) + (da + cb)\,i && \text{by (2)} \\
&= \alpha\beta && \text{by comm. of } \mathbf{R}
\end{aligned}$$

2. **Associativity**

For all $\alpha, \beta, \lambda \in \mathbf{C}$, write $\alpha = a + b\,i$, $\beta = c + d\,i$, $\lambda = e + f\,i$ with some $a, b, c, d, e, f \in \mathbf{R}$, then

$$
\begin{aligned}
(\alpha + \beta) + \lambda &= [(a + b\,i) + (c + d\,i)] + (e + f\,i) && \\
&= [(a + c) + (b + d)\,i] + (e + f\,i) && \text{by (1)} \\
&= [(a + c) + e] + [(b + d) + f]\,i && \text{by (1)} \\
\alpha + (\beta + \lambda) &= (a + b\,i) + [(c + d\,i) + (e + f\,i)] && \\
&= (a + b\,i) + [(c + e) + (d + f)\,i] && \text{by (1)} \\
&= [a + (c + e)] + [b + (d + f)]\,i && \text{by (1)} \\
&= (\alpha + \beta) + \lambda && \text{by asso. of } \mathbf{R}
\end{aligned}
$$

$$
\begin{aligned}
(\alpha\beta)\lambda &= [(a + b\,i)(c + d\,i)](e + f\,i) && \\
&= [(ac - bd) + (ad + bc)\,i](e + f\,i) && \text{by (2)} \\
&= [(ac - bd)e - (ad + bc)f] + [(ac - bd)f + (ad + bc)e]\,i && \text{by (2)} \\
&= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)\,i && \text{by dist. of } \mathbf{R} \\
\alpha(\beta\lambda) &= (a + b\,i)[(c + d\,i)(e + f\,i)] && \\
&= (a + b\,i)[(ce - df) + (cf + de)\,i] && \text{by (2)} \\
&= [a(ce - df) - b(cf + de)] + [a(cf + de) + b(ce - df)]\,i && \text{by (2)} \\
&= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)\,i && \text{by dist. of } \mathbf{R} \\
&= (\alpha\beta)\lambda && \text{by comm. of } \mathbf{R}
\end{aligned}
$$

3. **Identities**

For all $\lambda \in \mathbf{C}$, write $\lambda = a + b\,i$ for some $a, b \in \mathbf{R}$, then

$$
\begin{aligned}
\lambda + 0 &= (a + b\,i) + (0 + 0\,i) && \\
&= (a + 0) + (b + 0)\,i && \text{by (1)} \\
&= a + b\,i && \text{by iden. of } \mathbf{R} \\
&= \lambda
\end{aligned}
$$

$$
\begin{aligned}
1\lambda &= (1 + 0\,i)(a + b\,i) && \\
&= (1a + 0b) + (1b + 0a)\,i && \text{by (2)} \\
&= a + b\,i && \text{by iden. and mul. of } \mathbf{R} \\
&= \lambda
\end{aligned}
$$

4. **Additive Inverse**

   For every $\alpha \in \mathbf{C}$, write $\alpha = a + b\,i$ for some $a, b \in \mathbf{R}$, then we can find a unique $\beta = c + d\,i \in \mathbf{C}$ such that $\alpha + \beta = 0$ by the following manner:

$$\begin{aligned} \alpha + \beta &= (a + b\,i) + (c + d\,i) & \\ &= (a + c) + (b + d)\,i & \text{by (1)} \\ &= 0 + 0\,i & \text{by assumption} \\ \Rightarrow (c, d) &= (-a, -b) & \text{by add.inv. of } \mathbf{R} \end{aligned}$$

   Thus β is the unique additive inverse of α.

5. **Multiplicative Inverse**

   For every $\alpha \in \mathbf{C}$, write $\alpha = a + b\,i$ for some $a, b \in \mathbf{R}$ with $a \neq 0$ and $b \neq 0$, then we can find a unique $\beta = c + d\,i \in \mathbf{C}$ such that $\alpha\beta = 1$ by the following manner:

$$\begin{aligned} \alpha\beta &= (a + b\,i)(c + d\,i) & \\ &= (ac - bd) + (ad + bc)\,i & \text{by (2)} \\ &= 1 + 0\,i & \text{by assumption} \end{aligned}$$

   That is, $ac - bd = 1$ and $ad + bc = 0$. By solving these two equations for c and d, we have

$$(c, d) = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right),$$

   thus β is the unique multiplicative inverse of α.

6. **Distributive Property**

   For all $\alpha, \beta, \lambda \in \mathbf{C}$, write $\alpha = a + b\,i$, $\beta = c + d\,i$, $\lambda = e + f\,i$ with some $a, b, c, d, e, f \in \mathbf{R}$, then

$$\begin{aligned} \lambda(\alpha + \beta) &= (e + f\,i)[(a + b\,i) + (c + d\,i)] & \\ &= (e + f\,i)[(a + c) + (b + d)\,i] & \text{by (1)} \\ &= [e(a + c) - f(b + d)] + [e(b + d) + f(a + c)]\,i & \text{by (2)} \\ &= (ea + ec - fb - fd) + (eb + ed + fa + fc)\,i & \text{by dist. of } \mathbf{R} \end{aligned}$$

$$\begin{aligned} \lambda\alpha + \lambda\beta &= [(e + f\,i)(a + b\,i)] + [(e + f\,i)(c + d\,i)] & \\ &= [(ea - fb) + (eb + fa)\,i] + [(ec - fd) + (ed + fc)\,i] & \text{by (2)} \\ &= (ea - fb + ec - fd) + (eb + fa + ed + fc)\,i & \text{by (1)} \\ &= \lambda(\alpha + \beta) & \text{by comm. of } \mathbf{R} \end{aligned}$$