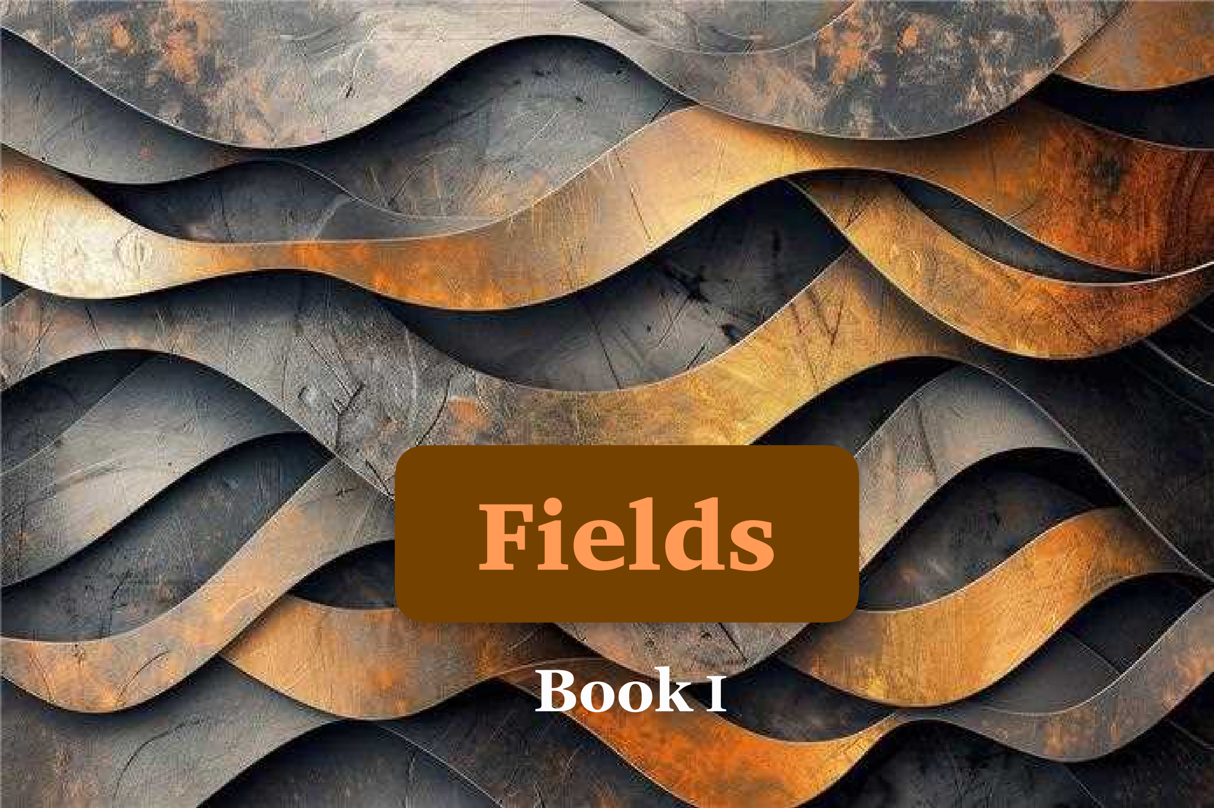

Fields

Book I

Fields

Let F be a set containing distinct elements called 0 and 1 (thus $0 \neq 1$). Suppose addition, subtraction, multiplication and division are defined for all elements of F (except division by 0 is not defined).
Thus $a+b,\ a-b,\ ab,\ \frac{a}{d} \in F$ whenever $a, b, d \in F$ and $d \neq 0$.
Define $-a = 0 - a$.

If the following properties are satisfied by *all* elements $a, b, c, d \in F$ with $d \neq 0$, then F is a field.

$$a + b = b + a \qquad a + (b + c) = (a + b) + c \qquad ab = ba$$
$$a + 0 = a \qquad a(bc) = (ab)c \qquad 1a = a$$
$$a + (-a) = 0 \qquad a(b + c) = ab + ac \qquad \frac{a}{d} d = a$$
$$a + (-b) = a - b$$

$\mathbb{Q}^{2\times 2} = \{2\times 2 \text{ matrices over } \mathbb{Q}\} = \left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix} : a,b,c,d \in \mathbb{Q}\right\}$ is not a field.

$0 = \begin{bmatrix}0&0\\0&0\end{bmatrix}$, $I = \begin{bmatrix}1&0\\0&1\end{bmatrix}$ identity

$A+0=A$, $AI = A = IA$

$\begin{bmatrix}1&0\\0&0\end{bmatrix}$ has no inverse. $A\begin{bmatrix}1&0\\0&0\end{bmatrix} = I$ has no solution for A.

Moreover, $AB \neq BA$ in general.

$\mathbb{Q}^{2\times 2}$ is a (non-commutative) ring with identity.

It has a subring $D = \left\{\begin{bmatrix}a&0\\0&d\end{bmatrix} : a,d\in\mathbb{Q}\right\}$ is a commutative subring with identity.

But D is not a field since it has non-invertible elements.

D has zero divisors: $\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}0&0\\0&1\end{bmatrix} = \begin{bmatrix}0&0\\0&0\end{bmatrix}$. A field can never have zero divisors.

(If d is a zero divisor then $cd=0$ where $c,d\neq 0$ so $\left(\frac{c}{d}\right)d = c \neq 0$, contradiction)

$0\cdot\frac{1}{d} = \frac{0}{d} = \frac{cd}{d} =$

For a commutative ring R with identity, being able to divide is stronger than having no zero divisors.

An example of a commutative ring with identity having no zero divisors but not a field (division fails in general) is $\mathbb{Z}$

$\begin{bmatrix}a&b\\c&d\end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix}d&-b\\-c&a\end{bmatrix} = \begin{bmatrix}\frac{d}{ad-bc}&\frac{-b}{ad-bc}\\ \frac{-c}{ad-bc}&\frac{a}{ad-bc}\end{bmatrix}$

Eg. $F = \left\{\begin{bmatrix}a&b\\2b&a\end{bmatrix} : a,b\in\mathbb{Q}\right\} \subset \mathbb{Q}^{2\times 2}$ is a subring, containing $I = \begin{bmatrix}1&0\\0&1\end{bmatrix}$.

If $\begin{bmatrix}a&b\\2b&a\end{bmatrix} \neq \begin{bmatrix}0&0\\0&0\end{bmatrix}$ then $\begin{bmatrix}a&b\\2b&a\end{bmatrix}^{-1} = \frac{1}{a^2-2b^2}\begin{bmatrix}a&-b\\-2b&a\end{bmatrix}$ (Note: $a^2-2b^2\neq 0$ since $\sqrt{2}\notin\mathbb{Q}$)

Why is F a commutative subring? Elements of F have the form

$\begin{bmatrix}a&b\\2b&a\end{bmatrix} = aI + bS$ where $I = \begin{bmatrix}1&0\\0&1\end{bmatrix}$, $S = \begin{bmatrix}0&1\\2&0\end{bmatrix}$ so $F = \{aI+bS : a,b\in\mathbb{Q}\}$ is the span of $\{I,S\}$ in $\mathbb{Q}^{2\times 2}$ (F is a 2-dimensional subspace of $\mathbb{Q}^{2\times 2}$, a 4-dimensional vector space).

$$(aI+bS)(cI+dS) = acI + (ad+bc)S + bdS^2 = (cI+dS)(aI+bS) \quad , \quad S^2 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = 2I$$

$$= (ac+2bd)I + (ad+bc)S$$

Compare: $K = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$. is a field.

$$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = ac + (ad+bc)\sqrt{2} + 2bd = (ac+2bd) + (ad+bc)\sqrt{2}$$

Note: $F \cong K$ (they are isomorphic)

An explicit isomorphism $\phi : K \to F$ is given by $\phi(a+b\sqrt{2}) = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = aI + bS$.

ϕ is bijective

$$\phi(x+y) = \phi(x) + \phi(y)$$

$$\phi(xy) = \phi(x)\phi(y)$$

Similarly $\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b \in \mathbb{R} \right\} \subset \mathbb{R}^{2\times 2}$ is a subring isomorphic to $\mathbb{C}$.

An isomorphism $\mathbb{C} \to \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b \in \mathbb{R} \right\}$ is $a+bi \longmapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ $(a,b \in \mathbb{R})$.