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.

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

$\mathbb{Q}^{2\times 2} = \{2\times 2 \text{ matrices over } \mathbb{Q}\} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Q} \right\}$ 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)

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

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).

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

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

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 $\left\{\begin{bmatrix}a&b\\-b&a\end{bmatrix} : a,b\in\mathbb{R}\right\} \subset \mathbb{R}^{2\times2}$ 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 $a+bi \longmapsto \begin{bmatrix}a&b\\-b&a\end{bmatrix}$ $(a,b\in\mathbb{R})$.

$\mathbb{Q}[\sqrt{2}] = \{ a+b\sqrt{2} : a,b \in \mathbb{Q} \}$

$\alpha = 5+3\sqrt{2}$, $\beta = 7-\sqrt{2}$

$\alpha+\beta = 12+2\sqrt{2}$

$\alpha-\beta = -2+4\sqrt{2}$

$\alpha\beta = (5+3\sqrt{2})(7-\sqrt{2}) = 35 - 5\sqrt{2} + 21\sqrt{2} - 6 = 29 + 16\sqrt{2}$

$\frac{\alpha}{\beta} = \frac{5+3\sqrt{2}}{7-\sqrt{2}} = \frac{5+3\sqrt{2}}{7-\sqrt{2}} \cdot \frac{7+\sqrt{2}}{7+\sqrt{2}} = \frac{35+5\sqrt{2}+21\sqrt{2}+6}{47} = \frac{41+26\sqrt{2}}{47} = \frac{41}{47} + \frac{26}{47}\sqrt{2}$

Alternatively, $\frac{\alpha}{\beta} = \alpha\beta^{-1}$

in matrix representation: $\underbrace{\begin{bmatrix} 5 & 3 \\ 6 & 5 \end{bmatrix}}_{\alpha} \cdot \frac{1}{47}\begin{bmatrix} 7 & 1 \\ 2 & 7 \end{bmatrix} = \frac{1}{47}\begin{bmatrix} 41 & 26 \\ 52 & 41 \end{bmatrix}$

$\beta \longmapsto \begin{bmatrix} 7 & -1 \\ -2 & 7 \end{bmatrix}$

$\beta^{-1} \longmapsto \frac{1}{47}\begin{bmatrix} 7 & 1 \\ 2 & 7 \end{bmatrix}$

Similar: $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\theta]$, $\theta = \sqrt[3]{2}$.

$\{ a+b\theta : a,b \in \mathbb{Q} \}$ is not a field, not even a ring since it's not closed under multiplication.

$\mathbb{Q}[\theta] = \{ a+b\theta+c\theta^2 : a,b,c \in \mathbb{Q} \}$. <u>is</u> a field.

$\theta^3 = 2$

$\theta^4 = 2\theta$

$\theta^5 = 2\theta^2$

$\theta^6 = 4$

$\alpha = 5+3\theta$

$\beta = 7-\theta$

$\alpha+\beta = 12+2\theta$

$\alpha-\beta = -2+4\theta$

$\alpha\beta = (5+3\theta)(7-\theta) = 35 - 5\theta + 21\theta - 3\theta^2$

$= 35 + 16\theta - 3\theta^2$

$$\frac{\alpha}{\beta} = \frac{5+3\theta}{7-\theta} = \boxed{a} + \boxed{b}\,\theta + \boxed{c}\,\theta^2 = \frac{251}{341} + \frac{182}{341}\theta + \frac{26}{341}\theta^2 = \frac{1}{341}\left(251 + 182\theta + 26\theta^2\right)$$

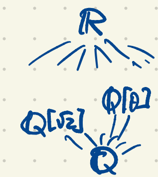
$\theta^3 = 2$

$\theta^3 - 2 =$

rational coefficients $a, b, c \in \mathbb{Q}$

$\theta = \sqrt[3]{2}$

θ is a root of $x^3 - 2 = (x-\theta)(x^2 + \theta x + \theta^2)$



$$5 + 3\theta = (a + b\theta + c\theta^2)(7-\theta)$$
$$= 7a + (7b-a)\theta + (7c-b)\theta^2 - 2c$$
$$= (7a - 2c) + (7b-a)\theta + (7c-b)\theta^2$$

Hopefully

$$\begin{aligned} 7a \quad\quad -2c &= 5 \\ -a + 7b \quad\quad &= 3 \\ -b + 7c &= 0 \end{aligned}$$

$$\left[\begin{array}{ccc|c} 7 & 0 & -2 & 5 \\ -1 & 7 & 0 & 3 \\ 0 & -1 & 7 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 0 & 49 & -2 & 26 \\ -1 & 7 & 0 & 3 \\ 0 & -1 & 7 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & -7 & 0 & -3 \\ 0 & 49 & -2 & 26 \\ 0 & 1 & -7 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & -7 & 0 & -3 \\ 0 & 1 & -7 & 0 \\ 0 & 49 & -2 & 26 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -49 & -3 \\ 0 & 1 & -7 & 0 \\ 0 & 0 & 341 & 26 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -49 & -3 \\ 0 & 1 & -7 & 0 \\ 0 & 0 & 1 & \frac{26}{341} \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & \frac{251}{341} \\ 0 & 1 & 0 & \frac{182}{341} \\ 0 & 0 & 1 & \frac{26}{341} \end{array}\right]$$

$$\begin{array}{r} 26 \\ \times\ 7 \\ \hline 182 \end{array} \qquad \begin{array}{r} 49 \\ \times\ 26 \\ \hline 294 \\ 98 \\ \hline 1274 \end{array} \qquad \begin{array}{r} 341 \\ \times\ 3 \\ \hline 1023 \end{array}$$

$$-3 + 49 \cdot \frac{26}{341}$$
$$= -3 + \frac{1274}{341}$$
$$= \frac{-1023 + 1274}{341} = \frac{251}{341}$$

Check: $\frac{1}{341}(251 + 182\theta + 26\theta^2)(7-\theta) = \frac{1}{341}\left(1757 + 1023\theta + 0\theta^2 - 52\right)$

$$= \frac{1}{341}(1705 + 1023\theta)$$
$$= 5 + 3\theta \quad ✓$$

$\mathbb{Q}[\theta]$ is a cubic field extension of $\mathbb{Q}$: it is a 3-dimensional vector space over $\mathbb{Q}$, with basis $1, \theta, \theta^2$.

Alternatively, use 3x3 matrices to represent elements of $\mathbb{Q}[\theta]$.

Take $T = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ to represent θ. $T^3 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = 2I$

$$E = \{ aI + bT + cT^2 : a,b,c \in \mathbb{Q} \} = \underbrace{\left\{ \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix} : a,b,c \in \mathbb{Q} \right\}}_{\text{This subring is a field.}} \subset \underbrace{\mathbb{Q}^{3\times 3}}_{\text{noncommutative ring with identity having zero divisors}}$$

$\mathbb{Q}[\theta] \cong E$ via the isomorphism

$$\begin{array}{ccc} \mathbb{Q}[\theta] & \cong & E \\ \Downarrow & & \Downarrow \\ a+b\theta+c\theta^2 & \longmapsto & aI+bT+cT^2 \end{array}$$

Are there any fields "between" $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}]$, or between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$?

Are there any fields "between" $\mathbb{R}$ and $\mathbb{C}$?

Suppose $\mathbb{R} \subset F \subset \mathbb{C}$ is a tower of fields (F is a subfield of $\mathbb{C}$ and $\mathbb{R}$ is a subfield of F).

$\subseteq$ vs $\subset$ '$\subset$' always means strict containment in this course.

$\leq$ vs $<$

Since $F \supset \mathbb{R}$, there exists $\alpha \in F$, $\alpha \notin \mathbb{R}$. Then $\alpha, 1$ are linearly independent over $\mathbb{R}$, i.e. $\alpha \neq a\cdot 1$ for any $a \in \mathbb{R}$. However $\mathbb{C}$ is 2-dimensional over $\mathbb{R}$ with basis $1, i$ (every complex number is uniquely expressible as $z = a\cdot 1 + b\cdot i$ with $a,b \in \mathbb{R}$). So $1, \alpha$ is a basis for F. So $F = \mathbb{C}$.

Is there any field extension $\mathbb{C} \subset F$ with F 2-dimensional over $\mathbb{C}$?
No, but there do exist fields $F \supset \mathbb{C}$ which are infinite-dimensional extensions.

Consider the ring $\mathbb{C}[x] = \{$polynomials in x with complex coefficients$\}$
$= \{ a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \; : \; a_i \in \mathbb{C}, \; n \geq 0 \}$

This is a ring but not quite a field e.g.

$$\frac{5 + 7x + ix^2}{3 - (4+i)x + 43x^2} \notin \mathbb{C}[x]$$

$\mathbb{C}(x) =$ field of fractions of $\mathbb{C}[x]$
$=$ field of rational functions in x with complex coefficients

Just like constructing $\mathbb{Q}$ from $\mathbb{Z}$.

Another example of this: We'll construct a countably infinite subfield of $\mathbb{R}$ containing π.
This contains the subring $\mathbb{Q}[\pi] = \{ a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n \; : \; n \geq 0, \; a_i \in \mathbb{Q} \}$

$\pi \in \mathbb{Q}[\pi]$ has no (multiplicative) inverse in $\mathbb{Q}[\pi]$ since if

$$1 = \pi(a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n) \qquad a_i \in \mathbb{Q}, \; n \geq 0,$$

a contradiction since π is transcendental. (π would be a root of a nonzero polynomial $a_n x^{n+1} + a_{n-1}x^n + \dots + a_2x^3 + a_1x^2 + a_0x - 1$)
(Lindemann 1800's)

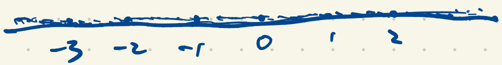
$\mathbb{Q}(\pi) = \{ \frac{a}{b} \; : \; a, b \in \mathbb{Q}[\pi], \; b \neq 0 \}$ is the field of quotients of the ring $\mathbb{Q}[\pi]$

$\mathbb{Q}(\sqrt{2}) = \{ \frac{a}{b} : a, b \in \mathbb{Q}[\sqrt{2}], \; b \neq 0 \} = \mathbb{Q}[\sqrt{2}]$ is already a field. $\sqrt{2}$ is algebraic: it is a root of a nonzero poly. $x^2 - 2 \in \mathbb{Q}[x]$

Every $\alpha \in \mathbb{C}$ is either algebraic or transcendental, never both.

$$\underbrace{\mathbb{Q}}_{\text{countable}} \subset \underbrace{\mathbb{R}}_{\text{uncountable}} \subset \underbrace{\mathbb{C}}_{\text{uncountable}}$$

$$\underbrace{\mathbb{Q} \subset \mathbb{A}}_{\text{countable}} \subset \underbrace{\mathbb{C}}_{\text{uncountable.}}$$



$\mathbb{A} = \{\text{algebraic numbers}\}.$

$$\begin{tikzcd}
 & & \mathbb{A} \arrow[dr, phantom, "\subset"] & \\
\mathbb{Q} \subset \mathbb{A} \cap \mathbb{R} \arrow[urr, phantom, "\subset"] \arrow[drr, phantom, "\subset"] & & & \mathbb{C} \\
 & & \mathbb{R} \arrow[ur, phantom, "\subset"] &
\end{tikzcd}$$

$\mathbb{Q} = \{a_1, a_2, a_3, a_4, \dots\}$

$$\begin{array}{cccc}
a_1 + a_1 x & a_1 + a_2 x & a_1 + a_3 x & \cdots \\
a_2 + a_1 x & a_2 + a_2 x & a_2 + a_3 x & \cdots \\
a_3 + a_1 x & a_3 + a_2 x & a_3 + a_3 x & \cdots \\
\vdots & \vdots & \vdots &
\end{array}$$

$\mathbb{Q}[\pi]$ is a countably infinite ring

so $\mathbb{Q}(\pi)$ is a countably infinite field.