Field Theory

Book 1

Informally, a field is a "number system" in which we can add, subtract, multiply, and divide.

Eg. $\mathbb{R} = \{\text{real numbers}\}$ eg. $\pi \in \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, $i \notin \mathbb{R}$, $7 \in \mathbb{R}$

$\mathbb{Q} = \{\text{rational numbers}\}$ $\frac{3}{5} \in \mathbb{Q}$, $7 \in \mathbb{Q}$

$\mathbb{C} = \{\text{complex numbers}\} = \{a+bi : a,b \in \mathbb{R}\}$, $i = \sqrt{-1}$

$\mathbb{Z} = \{\text{integers}\} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is not a field. It is a ring.

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

$\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are fields

$5 \times \square = 3$
solution is $\frac{3}{5} \in \mathbb{Q}$.

eg. $\alpha = 3+\sqrt{2}$, $\beta = 7 - 3\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$

$\alpha + \beta = 10 - 2\sqrt{2}$

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

$\alpha\beta = (3+\sqrt{2})(7-3\sqrt{2}) = 21 - 9\sqrt{2} + 7\sqrt{2} - 6 = 15 - 2\sqrt{2}$

$$\frac{\alpha}{\beta} = \frac{3+\sqrt{2}}{7-3\sqrt{2}} \cdot \frac{7+3\sqrt{2}}{7+3\sqrt{2}} = \frac{21 + 9\sqrt{2} + 7\sqrt{2} + 6}{49 - 18} = \frac{27 + 16\sqrt{2}}{31} = \frac{27}{31} + \frac{16}{31}\sqrt{2}$$

Similar: $\mathbb{R}[x]$ is the ring of all polynomials in x with coefficients in $\mathbb{R}$

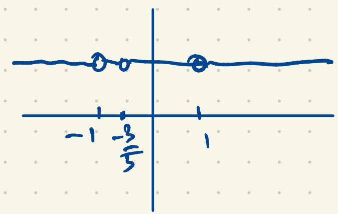
eg. $5x^2 + \pi x + \sqrt{2} \in \mathbb{R}[x]$.

This is not a field; we cannot divide $5x+3$ by x^2-1 in $\mathbb{R}[x]$ i.e. $(x^2-1) \times \boxed{?} = 5x+3$

The unique solution to this division problem is $\frac{5x+3}{x^2-1} \in \mathbb{R}(x) = \{\text{rational functions in } x \text{ with coefficients in } \mathbb{R}\}$

$= \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x],\ g(x) \neq 0 \right\}$.

In $\mathbb{R}(x)$, $\frac{5x+3}{x^2-1} \cdot \frac{x^2-1}{5x+3} = 1$



$\mathbb{Q}[\sqrt{4}] = \mathbb{Q}[2] = \mathbb{Q}$

Like $\mathbb{Q}[\sqrt{2}]$: $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{-7}]$, ...

$\mathbb{Q}[i] = \{a+bi : a,b \in \mathbb{Q}\}$

If $\alpha = \sqrt[3]{2} = 2^{1/3}$

$\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a,b,c \in \mathbb{Q}\}$

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.

$$a + b = b + a \qquad a + (b + c) = (a + b) + c \qquad ab = ba$$

$$a + 0 = a \qquad a(bc) = (ab)c \qquad 1a = a$$

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

$$a + (-b) = a - b$$

In $\mathbb{Q}[\alpha]$, $\alpha = 2^{1/3}$:

$$= \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$$

$\alpha^3 = 2$
$\alpha^4 = 2\alpha$

$$\frac{1+\alpha+\alpha^2}{2+\alpha-\alpha^2} = a + b\alpha + c\alpha^2 \qquad \text{Find } a, b, c \in \mathbb{Q}$$

$$1+\alpha+\alpha^2 = (a+b\alpha+c\alpha^2)(2+\alpha-\alpha^2) = 2a + (a+2b)\alpha + (-a+b+2c)\alpha^2 + (-b+c)\overset{2}{\alpha^3} - c\overset{2\alpha}{\alpha^4}$$

$$= (2a-2b+2c) + (a+2b-2c)\alpha + (-a+b+2c)\alpha^2 \qquad a, b, c \in \mathbb{Q}$$

$$\begin{cases} 2a - 2b + 2c = 1 \\ a + 2b - 2c = 1 \\ -a + b + 2c = 1 \end{cases}$$

(There are other ways to solve this...)

$\mathbb{Q}[\alpha]$ is an n-dimensional vector space over $\mathbb{Q}$ ← the scalars
with basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

$\mathbb{Q}[\sqrt{d}]$, $\mathbb{Q}[2^{1/3}]$, ... are examples of (algebraic) number fields

More generally, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, a_2, \ldots, a_{n-1} \in \mathbb{Q}\}$

(α is a root of a polynomial of degree n with rational coefficients

$x^2 - d$ has roots $\pm\sqrt{d}$

$x^3 - 2$ has roots $\alpha = 2^{1/3}$, $\omega\alpha$, $\omega^2\alpha$ where $\omega = \frac{-1+\sqrt{-3}}{2} = \frac{-1+i\sqrt{3}}{2}$

In $\mathbb{Q}[\sqrt{2}]$: $(5+\sqrt{2})(7-3\sqrt{2}) = 35 - 15\sqrt{2} + 7\sqrt{2} - 6 = 29 - 8\sqrt{2}$ $\qquad \overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$

Conjugates to $(5-\sqrt{2})(7+3\sqrt{2}) = 29 + 8\sqrt{2}$

If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree n, then $f(x) = a(x-r_1)(x-r_2)\cdots(x-r_n)$ (Fundamental Theorem of Algebra)
where $a \in \mathbb{C}$ $(a \neq 0)$; $r_1, r_2, \ldots, r_n \in \mathbb{C}$.

If $f(x) \in \mathbb{R}[x]$ ($f(x)$ is a poly. in x with real coefficients i.e. $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_i \in \mathbb{R}$)

$x^2+2 \in \mathbb{R}[x]$ has two complex roots but no real roots.

Every $f(x) \in \mathbb{R}[x]$ of degree 3 has at least one real root.

If $f(x) \in \mathbb{R}[x]$ has degree 4 then $f(x)$ factors into quadratic × quadratic
or quadratic × linear × linear
or linear × linear × linear × linear

eg. $x^4+1 = (x^2 \quad +1)(x^2 \quad +1)$

$x^4+x^2+1 = (x^2+x+1)(x^2-x+1) = ((x^2+1)+x)((x^2+1)-x) = (x^2+1)^2 - x^2 = x^4+2x+1-x^2 = x^4+x^2+1$

x^2+bx-1 has two real roots $\dfrac{-b \pm \sqrt{b^2+4}}{2}$

$x^4+1 = (x^2+bx+1)(x^2-bx+1) = x^4+(2-b^2)x^2+1$, so $b=\sqrt{2}$

$x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$

$x^4+1 = (x^4+2x^2+1) - 2x^2 = (x^2+1)^2 - 2x^2 = (x^2+1)^2 - (\sqrt{2}x)^2 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$

x^4+1 is reducible in $\mathbb{R}[x]$ but irreducible in $\mathbb{Q}[x]$.

there is a nontrivial factorization of x^4+1 over $\mathbb{R}$ but not over $\mathbb{Q}$.

In $\mathbb{R}[x]$, every irreducible poly. has degree 1 or 2. This can be proved using $\mathbb{C}$

$0.999999\ldots = 1.000000\ldots$

$10x = 9.999999\ldots$
$x = 0.999999\ldots$
$9x = 9 \Rightarrow x = \frac{9}{9} = 1$

$\frac{1}{3} = 0.33333\ldots$
$\frac{1}{3} = 0.33333\ldots$
$\frac{1}{3} = 0.33333\ldots$
$1 = 0.99999\ldots$

The subset $\mathbb{Q} \subset \mathbb{R}$ can be characterized by the decimal expansions:
$\alpha \in \mathbb{R}$ is rational iff it has a repeating decimal expansion

eg. $\alpha = 1.362626262\ldots = 1.3\overline{62}$ is rational

$1000\alpha = 1362.62626262\ldots$
$10\alpha = 13.62626262\ldots$
$990\alpha = 1349$
$\alpha = \dfrac{1349}{990} = \dfrac{19 \cdot 71}{2 \cdot 3^2 \cdot 5 \cdot 11}$

$\dfrac{42}{80} = \dfrac{21}{40} = \dfrac{3 \cdot 7}{2^3 \cdot 5} = 0.52500000$
$= 0.5249999\ldots$

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \{\text{all integers}\}$

$2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} \subset \mathbb{Z}$ proper subset

$2\mathbb{Z} = \{\text{even integers}\}$

$|2\mathbb{Z}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N}| < |\mathbb{R}|$

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$ natural numbers (some authors include 0)

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$

There is no one-to-one correspondence between $\mathbb{N}$ and $\mathbb{R}$ ($\mathbb{R}$ is uncountable)
(or any countable set i.e. any set whose elements can be listed in a sequence)

see links on website

Some real numbers that are irrational

$\sqrt{2} \notin \mathbb{Q}$ (elementary ; Euclid)

$\pi \notin \mathbb{Q}$ (harder ; maybe 25 minutes to prove in this class)

$e \notin \mathbb{Q}$ (maybe 12 minutes to prove)

$\pi + e$, πe ?

We think $\pi + e$ and πe are both irrational but all we know is: they can't both be rational.

$$\underbrace{\sqrt{2}}_{\text{irrational}} + \underbrace{(5-\sqrt{2})}_{\text{irrational}} = 5$$