

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. $\pi \in \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, $i \notin \mathbb{R}$, $7 \in \mathbb{R}$

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

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

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

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

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

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

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

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

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

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

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

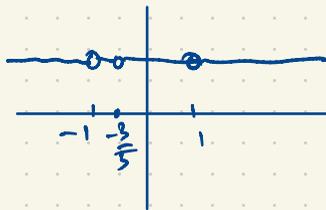
Similar: $\mathbb{R}[x]$ is the ring of all polynomials in x with coefficients in \mathbb{R}

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. $(x^2-1) \times \square = 5x+3$

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

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



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

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

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

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

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

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

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

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

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

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

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

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

More generally, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} : a_0, a_1, a_2, \dots, a_{n-1} \in \mathbb{Q}\}$
 (α is a root of a polynomial of degree n with rational coefficients)

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

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

In $\mathbb{Q}[\sqrt{2}]$: $(5 + \sqrt{2})(7 - 3\sqrt{2}) = 35 - 15\sqrt{2} + 7\sqrt{2} - 6 = 29 - 8\sqrt{2}$
 Conjugates to $(5 - \sqrt{2})(7 + 3\sqrt{2}) = 29 + 8\sqrt{2}$

$$\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$$

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

(Fundamental Theorem of Algebra)

If $f(x) \in \mathbb{R}[x]$ ($f(x)$ is a poly. in x with real coefficients i.e. $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $a_i \in \mathbb{R}$)
 $x^2 + 2 \in \mathbb{R}[x]$ 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 \times quadratic
 or quadratic \times linear \times linear
 or linear \times linear \times linear \times linear

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

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

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

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

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

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

$x^4 + 1$ 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}

$$0.999999\dots = 1.000000\dots$$

$$\frac{1}{3} = 0.33333\dots$$

$$\frac{1}{3} = 0.33333\dots$$

$$\frac{1}{3} = 0.33333\dots$$

$$1 = 0.99999\dots$$