

# 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  $\mathbb{Q}[\sqrt{2}]$

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

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

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

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

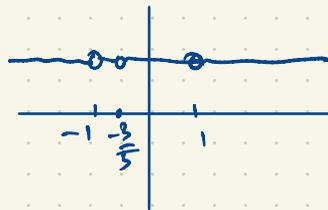
Similar:  $\mathbb{R}[x]$  is the ring of all polynomials in  $x$  with coefficients in  $\mathbb{R}$

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

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

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

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

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

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

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

$x^2 + 6x - 1$  has two real roots  $\frac{-6 \pm \sqrt{6^2 + 4}}{2}$

$$x^4 + 1 = (x^2 + 6x + 1)(x^2 - 6x + 1) = x^4 + (2 - 6^2)x^2 + 1, \text{ so } b = \sqrt{2}$$

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

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

$x^4 + 1$  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  $\mathbb{C}$

$$\begin{aligned} 0.999999\dots &= 1.000000\dots \\ 10x &= 9.999999\dots \\ x &= 0.999999\dots \\ \hline 9x &= 9 \Rightarrow x = \frac{9}{9} = 1 \end{aligned}$$

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

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

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

$$1 = 0.99999\dots$$

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.  $\alpha = 1.362626262\dots = 1.\overline{362}$  is rational

$$\begin{aligned} 1000\alpha &= 1362.62626262\dots \\ 10\alpha &= 13.62626262\dots \\ \hline 990\alpha &= 1349 \end{aligned}$$

$$\alpha = \frac{1349}{990} = \frac{17 \cdot 71}{2 \cdot 3^2 \cdot 5 \cdot 11}$$

$$\frac{12}{20} = \frac{21}{40} = \frac{3 \cdot 7}{2 \cdot 5} = 0.52500000\dots = 0.5249999\dots$$

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

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

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

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

natural numbers

(some authors include 0)

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

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

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

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

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

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

$\pi + e$  ?  $\pi e$  ?

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

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

Most real numbers are irrational in the sense that  $\mathbb{R}$  is uncountable and  $\mathbb{Q}$  is countable, so  
 $\{\text{irrationals}\} = \mathbb{R} - \mathbb{Q} = \{a \in \mathbb{R} : a \notin \mathbb{Q}\}$  is uncountable. We think of  $\mathbb{R}$  as a way of "filling in the gaps"  
between the rationals.

If  $0.99999\dots < 1 = 1.00000\dots$  then  the midpoint of this interval is the average value

$$\frac{0.99999\dots + 1}{2} = \frac{1.99999\dots}{2} = 0.99999\dots$$

$$2 \overline{) 1.99999\dots}$$

The hyperreal number system  ${}^*\mathbb{R}$  (or  $\mathbb{R}^*$  or  $\bar{\mathbb{R}}$  or ...)

The smallest field has two elements  $\mathbb{F}_2 = \{0, 1\}$  with

$$+ \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

$$\times \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

(integers mod 2)

We can't have  $1+1=1$  otherwise  $(1+1)-1 = 1-1=0$   
 $1=1+0=1+(1-1)$

This argument shows that for an addition table in any field, no entry can be repeated in any row or column.

The next smallest field has three elements

$$+ \begin{array}{c|ccc} & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$$

$$\times \begin{array}{c|ccc} & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$$

This is  $\mathbb{F}_3 =$  "integers mod 3"  
 $= \{0, 1, 2\}$ .

Rename  $\alpha = 1+1=2$

In the addition table for a field, every element appears exactly once in each row and column.  
 Similarly for the multiplication table, if we ignore the zero row and column.

eg.  $\cancel{\begin{array}{l} \frac{1}{2} \times 2 \times 1 = 2 \times \frac{1}{2} = 1 \\ \frac{1}{2} \times 2 \times 2 = 2 \times \frac{1}{2} = 1 \end{array}}$

$$\times \begin{array}{c|cccc} & 0 & 1 & \alpha & \beta \\ \hline 0 & 0 & 1 & \alpha & \beta \\ 1 & 1 & \alpha & \beta & 0 \\ \alpha & \alpha & \beta & 0 & 1 \\ \beta & \beta & 0 & 1 & \alpha \end{array}$$

$$+ \begin{array}{c|cccc} & 0 & 1 & \alpha & \beta \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & \alpha & \beta \\ \alpha & 0 & \alpha & \beta & 1 \\ \beta & 0 & \beta & 1 & \alpha \end{array}$$

$1+1$  cannot equal  $\alpha$ .  
 Similarly ...  $\beta$   
 Of course  $1+1 \neq 1$   
 So by elimination,  $1+1=0$ .

The field with four elements  $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$

$$+ \begin{array}{c|cccc} & 0 & 1 & \alpha & \beta \\ \hline 0 & 0 & 1 & \alpha & \beta \\ 1 & 1 & 0 & \beta & \alpha \\ \alpha & \alpha & \beta & 0 & 1 \\ \beta & \beta & \alpha & 1 & 0 \end{array}$$

The addition for any field  $F$  gives an abelian gp.  $(F, +)$   
 In the case of  $\mathbb{F}_4$ , this is the Klein 4-group.

integers mod 4 is not a field

$2 \cdot 2 = 0$  in integers mod 4

$$\begin{aligned} 1+1 &= \alpha \\ \alpha(1+1) &= \alpha \cdot \alpha \\ 0 &= \alpha + \alpha = \beta \end{aligned}$$

In any finite field  $F$ , the multiplicative group is cyclic.

The nonzero elements of any field  $F$  gives a multiplicative group  $F^* = \{a \in F : a \neq 0\}$  which is also abelian.

$$1+1=0 \\ \alpha + \alpha = \alpha(1+1) = \alpha \cdot 0 = 0$$

There is a unique field  $\mathbb{F}$  of order 5, the "integers mod 5",  $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ .  $\mathbb{F}_5^* = \{1, 2, 2^2, 2^3\}$ ,  $2^4 = 1$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Why can't we have a field  $\mathbb{F}$  with five elements in which the multiplicative group  $\mathbb{F}^*$  is Klein?

Why can't  $|\mathbb{F}| = 5$ ,  $\mathbb{F} = \{0, 1, \alpha, \beta, \gamma\}$ ,  $\alpha^2 = \beta^2 = \gamma^2 = 1$ ?

Wedderburn's Theorem says the multiplicative group must be cyclic.

In the case  $|\mathbb{F}| = 5$ , the polynomial  $x^2 - 1$  has at most two roots.

If  $\alpha^2 = \beta^2 = \gamma^2 = 1$  then  $x^2 - 1$  would have four roots  $1, \alpha, \beta, \gamma$ .

In the integers mod 8,  $x^2 - 1$  has four roots:  $1, 3, 5, 7$ .

But the integers mod 8  $(\mathbb{Z}/8\mathbb{Z})$  is not a field.

In a field, every nonzero element  $d \neq 0$  has an inverse  $d^{-1} = \frac{1}{d}$  such that  $d^{-1}d = 1$  ( $d \neq 1$ ).

We cannot multiply two nonzero elements and get 0 (in a field).

If  $de = 0$  ( $d, e \neq 0$ ) then  $\frac{1}{e}de = \frac{1}{e}0 = 0$ , a contradiction.

If  $x^2 - 1 = 0$  then  $\underbrace{(x+1)}_{\neq 0} \underbrace{(x-1)}_{\neq 0} = 0$