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

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

$5 \times \boxed{} = 3$

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 $\mathbb{R}$

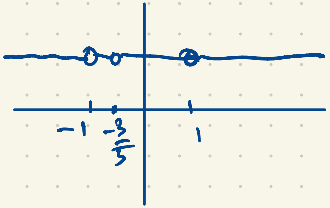
eg. $5x^2+\pi x+\sqrt{2} \in \mathbb{R}[x]$.

This is not a field; we can't 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.

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

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

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

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

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

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

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

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

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

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

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

$\mathbb{Q}[\sqrt{d}]$, $\mathbb{Q}[2^{1/3}]$, ... 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 $\mathbb{Q}[\sqrt{2}]$: $(5+\sqrt{2})(7-3\sqrt{2}) = 35 - 15\sqrt{2} + 7\sqrt{2} - 6 = 29 - 8\sqrt{2}$

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

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 $f(x) = a(x-r_1)(x-r_2)\cdots(x-r_n)$ where $a \in \mathbb{C}$ $(a \neq 0)$; $r_1, r_2, \ldots, r_n \in \mathbb{C}$.

(Fundamental Theorem of Algebra)

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

$x^2+2 \in \mathbb{R}[x]$ 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 $\frac{-b \pm \sqrt{b^2+4}}{2}$

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

$0.999999\ldots = 1.00000\ldots$

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

$$\frac{1}{3} = 0.33333\ldots$$
$$\frac{1}{3} = 0.33333\ldots$$
$$\frac{1}{3} = 0.3333\ldots$$
$$1 = 0.99999\ldots$$

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

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

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

$$\begin{array}{llllllllllll} \mathbb{Z} = \{ & \ldots, & -3, & -2, & -1, & 0, & 1, & 2, & 3, & \ldots \} & = \{\text{all integers}\} \\ & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \\ 2\mathbb{Z} = \{ & \ldots, & -6, & -4, & -2, & 0, & 2, & 4, & 6, & \ldots \} & \subset \mathbb{Z} \end{array}$$

proper subset

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

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

$$\begin{array}{lllllllll} \mathbb{N} = \{ & 1, & 2, & 3, & 4, & \ldots & & \ldots & \} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots & \\ \mathbb{Z} = \{ & 0, & 1, & -1, & 2, & -2, & 3, & -3, \ldots & \} \end{array}$$

natural numbers (some authors include 0)

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

($\mathbb{R}$ is uncountable)

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)

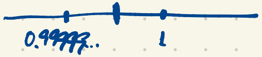
$\pi + e$, πe ?

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

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

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

If $0.99999\ldots < 1 = 1.00000\ldots$ then



the midpoint of this interval is the average value

$$\frac{0.9999\ldots + 1}{2} = \frac{1.99999\ldots}{2} = 0.99999\ldots$$

$$\begin{array}{r} 0.99999\ldots \\ 2\overline{)1.99999\ldots} \end{array}$$

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

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

(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

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	$\boxed{1}$

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. ~~If $\cancel{\tfrac{1}{2}}\times\cancel{2}\times 1 = 2\times\tfrac{1}{2} = 1$~~
~~$\cancel{\tfrac{1}{2}}\times\cancel{2}\times 2 = 2\times\tfrac{1}{2} = 1$~~

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

~~+~~	~~0~~	~~1~~	~~α~~	~~β~~
~~0~~	~~0~~	~~1~~	~~α~~	~~β~~
~~1~~	~~1~~	~~α~~	~~β~~	~~0~~
~~α~~	~~α~~	~~β~~	~~0~~	~~1~~
~~β~~	~~β~~	~~0~~	~~1~~	~~α~~

integers mod 4 is not a field
$2\cdot 2 = 0$ in integers mod 4

×	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$1+1$ cannot equal α.
Similarly " " " β
Of course $1+1 \neq 1$.
So by elimination, $1+1=0$.

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

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

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

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

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

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

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

+	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 F with five elements in which the multiplicative group $F^\times$ is Klein?

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

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

In the case $|F|=5$, 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 $d^{-1}d=1$ $(\frac{1}{d}d=1)$.

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

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

If $x^2-1=0$ then $(x+1)(x-1)=0$, so $x-1=0$ or $x+1=0$. So x^2-1 has at most two roots $x=1,-1$.

(If $-1\neq 1$ then x^2-1 has two distinct roots. But in $\mathbb{F}_2$, $\mathbb{F}_4$, $\ldots$, $-1=1$ so $x^2-1=(x-1)^2$ has only one distinct root.)

If F is any field and $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0 \in F[x]=\{$all polynomials in x with coefficients $a_0,a_1,\ldots,a_n\in F\}$ of degree n (i.e. $a_n\neq 0$) then f has at most n roots in F. (i.e. at most n distinct roots).

We can do linear algebra over any field F.

Eg. Solve the linear system over $F = \mathbb{F}_5$.

$$\begin{cases} 2x + 3y = 1 \\ 3x + 4y = 3 \end{cases}$$

$$\left[\begin{array}{cc|c} 2 & 3 & 1 \\ 3 & 4 & 3 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 4 & 3 \\ 3 & 4 & 3 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 4 & 3 \\ 0 & 2 & 4 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 4 & 3 \\ 0 & 1 & 2 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 2 \end{array}\right]$$ which has unique solution $(x,y) = (0,2)$.

$\frac{1}{2} = 3$

$2 \times 3 = 1$

Check: $2 \cdot 0 + 3 \cdot 2 = 1$ ✓

$3 \cdot 0 + 4 \cdot 2 = 3$

Alternatively: $\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, $\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}^{-1} = \frac{1}{-1} \begin{bmatrix} 4 & -3 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} -4 & 3 \\ 3 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 3 & 3 \end{bmatrix}$

$8 - 9 = -1 = 4$

Multiply on the left by $\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 3 \\ 3 & 3 \end{bmatrix}$:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}}_{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$$ (same answer as before).

Eg. $\mathbb{F}_{101} = \{0, 1, 2, \cdots, 100\}$, $\alpha = 9$, $\beta = 27$

$\alpha + \beta = 36$

$\alpha - \beta = 83$

$\alpha\beta = 41$

$\alpha / \beta = \frac{9}{27} = 9 \times 15 = 135 = 34$

$\frac{\alpha}{\beta} = \frac{9}{27} = \frac{1}{3} = 34$

In $\mathbb{F}_{101}$, $101 = 0$,

$15 \times 27 = 1$.

101	27	
1	0	101
0	1	27
1	-3	20
-1	4	7
3	-11	6
-4	15	①

$\begin{array}{r} 83 \\ \underline{27} \\ 110 = 9 \end{array}$

$83 + 27 = 9$

$9 - 27 = 83$

$\alpha\beta = 9 \cdot 27 = 243 - 202 = 41$

Inverse of $\beta = 27$ mod 101

$\gcd(27, 101) = 1 = 27r + 101s$, $r, s \in \mathbb{Z}$

(extended Euclidean algorithm)

$-4 \times 101 + 15 \times 27 = 1$

$15 \times 27 \equiv 1 \mod 101$ (in $\mathbb{Z}$)

$\gcd(101, 3) = 1$

101	3	
1	0	101
0	1	3
1	-33	2
-1	34	①

$-1 \times 101 + 34 \times 3 = 1$

$101 - 3 \times 27$
$= 101 - 81 = 20$

Field computations in number fields

Similar to HW1 #2,3: Let $f(x) = x^3-2x-3 \in \mathbb{Q}[x]$. Let $\theta \in \mathbb{C}$ be any root of $f(x)$.

Consider $E = \{a + b\theta + c\theta^2 : a,b,c \in \mathbb{Q}\}$.

Facts (assume this!) E is a field. Every element $\alpha \in E$ is uniquely expressible as $\alpha = a+b\theta+c\theta^2$
$= a\cdot 1 + b\cdot\theta + c\cdot\theta^2$

i.e. E is a 3-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \theta, \theta^2\}$.

Choose $\alpha = \theta^2-3$, $\beta = \theta^2+\theta+1$. Compute

$$0 = f(\theta) = \theta^3 - 2\theta - 3 \Rightarrow \theta^3 = 2\theta+3$$
$$\theta^4 = 2\theta^2+3\theta$$

$$\alpha+\beta = (\theta^2-3)+(\theta^2+\theta+1) = 2\theta^2+\theta-2$$
$$\alpha-\beta = (\theta^2-3)-(\theta^2+\theta+1) = -\theta-4$$
$$\alpha\beta = (\theta^2-3)(\theta^2+\theta+1) = \theta^4+\theta^3-2\theta^2-3\theta-3 = (\cancel{2\theta^2}+\cancel{3\theta})+(2\theta+\cancel{3})\cancel{-2\theta^2}\cancel{-3\theta}\cancel{-3} = 2\theta$$
$$\alpha/\beta = a+b\theta+c\theta^2$$
$$\alpha = (a+b\theta+c\theta^2)\beta$$
$$\theta^2-3 = (a+b\theta+c\theta^2)(\theta^2+\theta+1) = c\theta^4+(b+c)\theta^3+(a+b+c)\theta^2+(a+b)\theta+a$$
$$= c(2\theta^2+3\theta)+(b+c)(2\theta+3)+(a+b+c)\theta^2+(a+b)\theta+a$$
$$= (a+b+3c)\theta^2+(a+3b+5c)\theta+(a+3b+3c)$$