Field Theory

Book 1

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

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

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

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

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

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

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

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

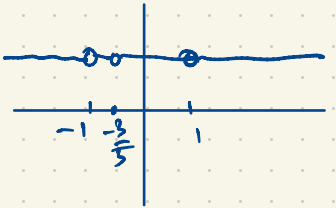
eg. $5x^2 + \pi x + \sqrt{2} \in \mathbb{R}[x]$.

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

The unique solution to this division problem is $\frac{6x+8}{x^2-1} \in \mathbb{R}(x)$ = {rational functions in x 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.

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

$\frac{a}{d} = ad^{-1}$ or $d^{-1}a$

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

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

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

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

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

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

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

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

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

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 $f(x) = a(x - r_1)(x - r_2)\cdots(x - r_n)$ 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. $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_i \in \mathbb{R}$)

$x^2+2 \in \mathbb{R}[x]$ 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. $x^4+1 = (x^2+1)(x^2+1)$

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

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 $\mathbb{C}$

$0.999999\ldots = 1.000000\ldots$

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

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

The subset $\mathbb{Q} \subset \mathbb{R}$ can be characterised 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

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

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

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

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

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

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

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

$$2\overline{)1.99999\dots}\quad 0.99999\dots$$

The hyperreal number system ${}^*\mathbb{R}$ (or $\mathbb{R}^*$ or $\tilde{\mathbb{R}}$ 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	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 $\frac{1}{2} \times 2 \times 1 = 2 \times \frac{1}{2} = 1$
$\frac{1}{2} \times 2 \times 2 = 2 \times \frac{1}{2} = 1$

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

+	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.

+	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, $1+1=0$.

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

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

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

+	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 $e = d^{-1}de = d^{-1}0 = 0$, 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 $\mathbb{F}_2$, $\mathbb{F}_4$, ..., $-1 = 1$ so $x^2 - 1 = (x-1)^2$ has only one distinct root.)

If F is any field and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in F[x] = \{$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 $F = \mathbb{F}_5$.

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

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

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

Check: $2 \cdot 0 + 3 \cdot 2 = 1$ ✓
$3 \cdot 0 + 4 \cdot 2 = 3$

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

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

$8 - 9 = -1 = 4$

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

$\alpha + \beta = 36$
$\alpha - \beta = 83$
$\alpha\beta = 41$
$\alpha/\beta = \frac{9}{27} = 9 \times 15 = 135 = 34$
$\frac{\alpha}{\beta} = \frac{9}{27} = \frac{1}{3} = 34$

101	27	
1	0	101
0	1	27
1	−3	20
−1	4	7
3	−11	6
−4	15	(1)

In $\mathbb{F}_{101}$, $101 = 0$,
$5 \times 27 = 1$.

$\gcd(101, 3) = 1$ $\quad -1 \times 101 + 34 \times 3 = 1$

101	3	
1	0	101
0	1	3
1	−33	2
−1	34	(1)

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

83
27
110 = 9

$83 + 27 = 9$
$9 - 27 = 83$

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

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 $\mathbb{Z}$)

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

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

$\theta^4 = 2\theta^2 + 3\theta$

$\alpha + \beta = (\theta^2 - 3) + (\theta^2 + \theta + 1) = 2\theta^2 + \theta - 2$

$\alpha - \beta = (\theta^2 - 3) - (\theta^2 + \theta + 1) = -\theta - 4$

$\alpha\beta = (\theta^2 - 3)(\theta^2 + \theta + 1) = \theta^4 + \theta^3 - 2\theta^2 - 3\theta - 3 = (2\theta^2 + 3\theta) + (2\theta + 3) - 2\theta^2 - 3\theta - 3 = 2\theta$

$\alpha/\beta = a + b\theta + c\theta^2$

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

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

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

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

$a + b + 3c = 1$
$a + 3b + 3c = 0$
$a + 3b + 3c = -3$

$$\left[\begin{array}{ccc|c} 1 & 1 & 3 & 1 \\ 1 & 3 & 3 & 0 \\ 1 & 3 & 3 & -3 \end{array}\right] \sim \cdots \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & -3/2 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 3/2 \end{array}\right]$$

i.e. $\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} -3/2 \\ -2 \\ 3/2 \end{bmatrix}$

To check, verify that these values of a, b, c satisfy our three linear equations.

$\frac{\alpha}{\beta} = -\frac{3}{2} - 2\theta + \frac{3}{2}\theta^2$

Note: These computations are exact and don't rely on any decimal approximations.

(But decimal approximations are sometimes helpful for checking your work.)

Similar to HW1 #3: Find a polynomial $m(x) \in \mathbb{Q}[x]$ having α as a root.

Why must α be a root of some polynomial $m(x) \in \mathbb{Q}[x]$ of degree 3?

We are in a 3-dimensional vector space E over $\mathbb{Q}$ with basis $1, \theta, \theta^2$.

So any set of four vectors in E is linearly dependent: $1, \alpha, \alpha^2, \alpha^3 \in E$

So α^3 = linear combination of $1, \alpha, \alpha^2$.

$\alpha = \theta^2 - 3$

$\theta^3 = 2\theta + 3$

$\theta^4 = 2\theta^2 + 3\theta$

$\theta^5 = 2\theta^3 + 3\theta^2 = 2(2\theta+3) + 3\theta^2$

$= 3\theta^2 + 4\theta + 6$

$\theta^6 = 3\theta^3 + 4\theta^2 + 6\theta = 3(2\theta+3) + 4\theta^2 + 6\theta$

$= 4\theta^2 + 12\theta + 9$

$\alpha^3 = a + b\alpha + c\alpha^2$

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

$\theta^6 - 9\theta^4 + 27\theta^2 - 27 = a + b(\theta^2-3) + c(\theta^4 - 6\theta^2 + 9)$

$4\theta^2 + 12\theta + 9 - 9(2\theta^2+3\theta) + 27\theta^2 - 27 = a + b(\theta^2-3) + c(2\theta^2 + 3\theta - 6\theta^2 + 9)$

$$\begin{aligned} -18 &= a - 3b + 9c \\ -15 &= \quad\quad 3c \\ 13 &= \quad b - 4c \end{aligned} \quad \Rightarrow \begin{cases} c = -5 \\ b = -7 \\ a = 6 \end{cases}$$

$\Rightarrow \alpha^3 = 6 - 7\alpha - 5\alpha^2$

$\Rightarrow \alpha^3 + 5\alpha^2 + 7\alpha - 6 = 0$

A polynomial is monic if its highest degree term has coefficient 1 i.e. the leading coefficient is 1.

$m(x) = x^3 + 5x^2 + 7x - 6$ is a polynomial of degree 3 with rational coefficients having α as a root.

$2m(x) = 2x^3 + 10x^2 + 14x - 12 \in \mathbb{Q}[x]$ also has α as a root.

$2m(x)$ has leading term $2x^3$; its leading coefficient is 2.

Any poly of the form $h(x)m(x) \in \mathbb{Q}[x]$ has α as a root. $(h(x) \in \mathbb{Q}[x])$

These are the only polynomials having α as a root.

$m(x)$ is the unique monic polynomial in $\mathbb{Q}[x]$ of degree 3 having α as a root.

Eg. $\sqrt{2}$ has minimal polynomial $m(x) = x^2 - 2$ (the simplest poly. with rational coefficients having $\sqrt{2}$ as a root),
$\sqrt{3}$ has minimal poly. $x^2 - 3$.

$m(x)$ has $\sqrt{2}$ as a root $\Rightarrow$ $m(x)$ has $-\sqrt{2}$ as a root since $\sqrt{2}$ and $-\sqrt{2}$ are conjugates
So $m(x)$ has factors $(x-\sqrt{2})$, $(x+\sqrt{2})$
so $(x-\sqrt{2})(x+\sqrt{2}) = x^2 - 2$ as a factor.

What is the minimal poly. of $\alpha = \sqrt{2} + \sqrt{3}$? (i.e. the simplest poly. with rational coefficients having α as a root) (monic of smallest possible degree)

If $m(x) = ax^2 + bx + c$ $(a, b, c \in \mathbb{Q})$ has $\alpha = \sqrt{2} + \sqrt{3}$ as a root then $\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ and this cannot happen as we will see later in the course.

$\alpha = \sqrt{2} + \sqrt{3}$
$\alpha^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$
~~$\alpha^4 = 25 + 24 + 20\sqrt{6} = 49 + 20\sqrt{6}$~~
$\alpha^4 - 10\alpha^2 = (49 + 20\sqrt{6}) - 10(5 + 2\sqrt{6}) = -1$
$\alpha^4 - 10\alpha^2 + 1 = 0$

$\alpha^2 - 5 = 2\sqrt{6}$
$\alpha^4 - 10\alpha^2 + 25 = 24$
$\alpha^4 - 10\alpha^2 + 1 = 0$

Fact: $x^4 - 10x^2 + 1$ is the minimal polynomial of α.

Note: $\alpha^4 - 10\alpha^2 + 1 = 0$ is not the minimal polynomial; it is "merely" a number.

x is not a number. It is an indeterminate. (a symbolic)

$m(x) = x^4 - 10x^2 + 1$ is a symbolic expression.
$m(\alpha) = \alpha^4 - 10\alpha^2 + 1 = 0$ is an actual number.

Another way to find the minimal poly. of $\alpha = \sqrt{2}+\sqrt{3}$:

If $m(x) \in \mathbb{Q}[x]$ has $\sqrt{2}+\sqrt{3}$ a root, it must also have $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$ as roots.

Explanations later!

$$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$
$$= ((x-\sqrt{2})-\sqrt{3})((x-\sqrt{2})+\sqrt{3})((x+\sqrt{2})-\sqrt{3})((x+\sqrt{2})+\sqrt{3})$$
$$= ((x-\sqrt{2})^2-3)((x+\sqrt{2})^2-3)$$
$$= (x^2-2\sqrt{2}x-1)(x^2+2\sqrt{2}x-1)$$
$$= ((x^2-1)-2\sqrt{2}x)((x^2-1)+2\sqrt{2}x)$$
$$= (x^2-1)^2-(2\sqrt{2}x)^2$$
$$= x^4-2x^2+1-8x^2$$
$$= x^4-10x^2+1$$

$\pi = 3.1415926\cdots$
$= 3+\frac{1}{10}+\frac{4}{100}+\frac{1}{1000}+\cdots$

A number $\alpha \in \mathbb{C}$ is <u>algebraic</u> if $f(\alpha)=0$ for some nonzero polynomial $f(x) \in \mathbb{Q}[x]$.

eg. Every rational number is algebraic. If $\alpha \in \mathbb{Q}$ then α is a root of $x-\alpha \in \mathbb{Q}[x]$.

$\sqrt{2}$ is algebraic since it's a root of $x^2-2 \in \mathbb{Q}[x]$.

$\sqrt{3}$ . . . . . $x^2-3 \in \mathbb{Q}[x]$

$\sqrt{2}+\sqrt{3}$ . . . . . $x^4-10x^2+1 \in \mathbb{Q}[x]$

π is not algebraic. There is no nonzero poly. in $\mathbb{Q}[x]$ having π as a root.

i.e. π is transcendental (i.e. not algebraic)

e is transcendental (easier!)

If α and β are algebraic then so is $\alpha+\beta$; also $\alpha-\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ (assuming $\beta \neq 0$).

So the set of all algebraic numbers is a field $\mathbb{A}$ (blackboard bold A)

$i \in \mathbb{A}$ since it is a root of x^2+1.

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$\mathbb{Q} \subset \mathbb{A} \subset \mathbb{C}$

The set of all real algebraic numbers is $\mathbb{R} \cap \mathbb{A}$ is a field since the intersection of two subfields of $\mathbb{C}$ is always a field.

If $\alpha, \beta \in \mathbb{R} \cap \mathbb{A}$ then $\alpha+\beta,\ \alpha-\beta,\ \alpha\beta,\ \frac{\alpha}{\beta} \in \mathbb{R} \cap \mathbb{A}$. $(\beta \neq 0)$

$\underbrace{\mathbb{Z} \subset \mathbb{Q}}_{\text{countable}} \subset \underbrace{\mathbb{R}}_{\text{uncountable}}$ $\qquad$ $\underbrace{\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \cap \mathbb{A}}_{\text{countable}} \subset \mathbb{R}$ $\qquad$ $\underbrace{\mathbb{A}}_{\text{countable}} \subset \underbrace{\mathbb{C}}_{\text{uncountable}}$

There exist transcendental numbers

Theorem e is irrational.

Proof Suppose e is rational, so $e = \frac{a}{b}$ in lowest terms (a, b positive integers, $\gcd(a,b) = 1$). Then

$$e = \frac{a}{b} = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + \frac{1}{720} + \cdots + \cdots \frac{1}{(b-1)!} + \frac{1}{b!} + \frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \cdots$$

$$b!e = b!\frac{a}{b} = \underbrace{(b-1)!a}_{\text{integer}} = \underbrace{b!\left(1 + 1 + \frac{1}{2} + \cdots + \frac{1}{b!}\right)}_{\text{integer}} + \underbrace{\frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \cdots}_{\text{fractions}}$$

We'll show this sum is between 0 and 1.

$$\frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \cdots < \frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \cdots = \frac{1/(b+1)}{1 - \frac{1}{b+1}} = \frac{1}{(b+1)-1} = \frac{1}{b} \leq 1$$

Contradiction! $\square$

Geometric series: $1 + r + r^2 + r^3 + \cdots = \frac{1}{1-r}$ if $|r| < 1$

$r + r^2 + r^3 + r^4 + \cdots = \frac{r}{1-r}$ $\cdots$ Use $r = \frac{1}{b+1} < 1$

Suppose $F \subseteq E$ where F and E are fields. Assuming we are consistent in our definitions of binary operations, we say F is a subfield of E, and E is an extension field of F.

Eg. $\mathbb{R} \subset \mathbb{C}$

$\mathbb{F}_3 = \{0,1,2\} \subset \mathbb{Q}$ but in $\mathbb{F}_3$, $2+2=1$ whereas in $\mathbb{Q}$, $2+2 \neq 1$.

NOT A SUBFIELD

$\mathbb{F}_2 \subset \mathbb{F}_4$ subfield.

$\mathbb{F}_2 \not\subset \mathbb{F}_3$

The set $\mathbb{Q}^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Q} \right\} = R$ is a ring. It's not commutative but it has identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

The subset $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b \in \mathbb{Q} \right\} \subset R$ is a subring.

If $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in S$ and $A \neq 0$ then A is invertible. $\det A = a^2+b^2 \neq 0$, $A^{-1} = \frac{1}{a^2+b^2}\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

Although R is noncommutative, S is commutative.

Elements of S have the form $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = aI + bW$, $W = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $W^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$

$$(aI+bW)(cI+dW) = acI + adW + bcW - bdI = (ac-bd)I + (ad+bc)W$$

$$(cI+dW)(aI+bW) = (ac-bd)I + (ad+bc)W$$

S is a field. (a subfield of R)

$\{aI : a \in \mathbb{Q}\} \subset S$ is a subfield

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

An isomorphism $\mathbb{Q}[i] \longrightarrow S$ is given by $a+bi \longmapsto aI+bW$

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

$R = \mathbb{R}^{2\times 2} = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R}\right\}$ is a noncommutative ring with identity; it has a subset

$S = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b \in \mathbb{R}\right\} \subset R$ which is a subring which is a field, hence a subfield.

Elements $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = aI + bW$ $\left(I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ W = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right)$ can be rewritten as $a+bi$ $(i = \sqrt{-1})$

using the isomorphism $S \to \mathbb{C}$, $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \overset{\phi}{\mapsto} a+bi$.

$\phi(xy) = \phi(x)\phi(y)$

$\phi(x+y) = \phi(x) + \phi(y)$

ϕ is bijection

$\mathbb{Q}[\sqrt{2}] \cong \left\{\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a,b \in \mathbb{Q}\right\}$

$a + b\sqrt{2} \longmapsto \begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$

In matrix form, $\begin{bmatrix} 5 & 7 \\ 14 & 5 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 6 & 1 \end{bmatrix} = \begin{bmatrix} 47 & 22 \\ 44 & 47 \end{bmatrix}$

In numerical form, $(5+7\sqrt{2})(1+3\sqrt{2}) = 47 + 22\sqrt{2}$ $\quad // \ I+W$

$// \ \{0, I, W, W^2\}$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\} \cong \left\{\begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a,b \in \mathbb{F}_2\right\} \subset \mathbb{F}_2^{2\times 2} = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{F}_2\right\}$

$= \{a+b\alpha : a,b \in \mathbb{F}_2\}$

$\beta = \alpha^2 = \alpha + 1$

commutative subring with 4 elements

$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = aI + bW$

noncommutative ring with identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$|\mathbb{F}_2^{2\times 2}| = 16$

$W = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

$W^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = I + W$

$W^3 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$(aI + bW)(cI + dW)$

$= acI + (ad+bc)W + bd\,W^2$

$= (ac+bd)I + (ad+bc+bd)W + I$

If $F \subseteq E$ is a subfield F and extension field E, then E is a vector space over F.
for $a_1, \dots, a_k \in E$ and $c_1, \dots, c_k \in F$, $\quad c_1a_1 + c_2a_2 + \dots + c_ka_k \in E$
"vectors" "scalars"
The degree of the extension is the dimension of this vector space, denoted $[E:F]$.
Eg. the extension $\mathbb{R} \subset \mathbb{C}$ has degree 2 since $\{1, i\}$ is a basis;
(every $z \in \mathbb{C}$ is uniquely expressible as a linear combination $z = a \cdot 1 + b \cdot i$, $a, b \in \mathbb{R}$.)
$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ is also an extension of degree 2 since every $u \in \mathbb{Q}[\sqrt{2}]$ is uniquely expressible as $u = a \cdot 1 + b\sqrt{2}$, $a, b \in \mathbb{Q}$. So $\{1, \sqrt{2}\}$ is a basis.

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
$[\mathbb{C}:\mathbb{R}] = 2$
$[\mathbb{R}:\mathbb{Q}] = \infty$
$[\mathbb{C}:\mathbb{Q}] = \infty$
$[\mathbb{C}:\mathbb{C}] = 1$ with basis $\{1\}$.
$[F:F] = 1$ with basis $\{1\}$: every element $u \in F$ is uniquely expressible as $u = u \cdot 1$, $u \in F$.
$\mathbb{R} \supset \mathbb{Q}$ has infinite degree (dimension) since there is no finite list of real numbers that spans the vector space.

$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \dots \subset \mathbb{R}$

Claim: $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.
$\sqrt{3} \notin \mathbb{Q}$ $\quad \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}, \sqrt{11}, \dots$ are irrational using Euclid's arguments
If $\sqrt{3} \in \mathbb{Q}$ then $\sqrt{3} = \frac{a}{b}$, a, b are positive integers in lowest terms i.e. $\gcd(a,b) = 1$. Then $3 = \frac{a^2}{b^2}$ so $a^2 = 3b^2$. So $a = 3r$ for some $r \in \mathbb{Z}$, so $9r^2 = 3b^2$, $3r^2 = b^2$, $b = 3s$ for some $s \in \mathbb{Z}$, $\gcd(a,b) \geq 3$, a contradiction.

Claim: $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ i.e. $\sqrt{3} = a + b\sqrt{2}$ has no solution with $a, b \in \mathbb{Q}$.

Suppose $\sqrt{3} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Then $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ so $2ab\sqrt{2} = 3 - a^2 - 2b^2$.

If $ab \neq 0$ then $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$, a contradiction.

If $b = 0$ then $0 = 3 - a^2$ so $a^2 = 3$, $a = \pm\sqrt{3} \notin \mathbb{Q}$, a contradiction.

If $a = 0$ then $0 = 3 - 2b^2$ so $2b^2 = 3$, $4b^2 = 6$, $2b = \pm\sqrt{6} \notin \mathbb{Q}$, a contradiction. □

So $1, \sqrt{2}, \sqrt{3} \in \mathbb{R}$ are linearly independent over $\mathbb{Q}$.

- $1 \neq 0$
- $\sqrt{2} \neq$ scalar multiple of 1. ($\sqrt{2} \notin \mathbb{Q}$ by Euclid)
- $\sqrt{3} \neq$ linear combination of $1, \sqrt{2}$. (proved above)

$\sqrt{8} = 2\sqrt{2}$

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19}, \sqrt{23}, \ldots$ are linearly independent.

$[\mathbb{R} : \mathbb{Q}] = \infty$ (in fact uncountable)