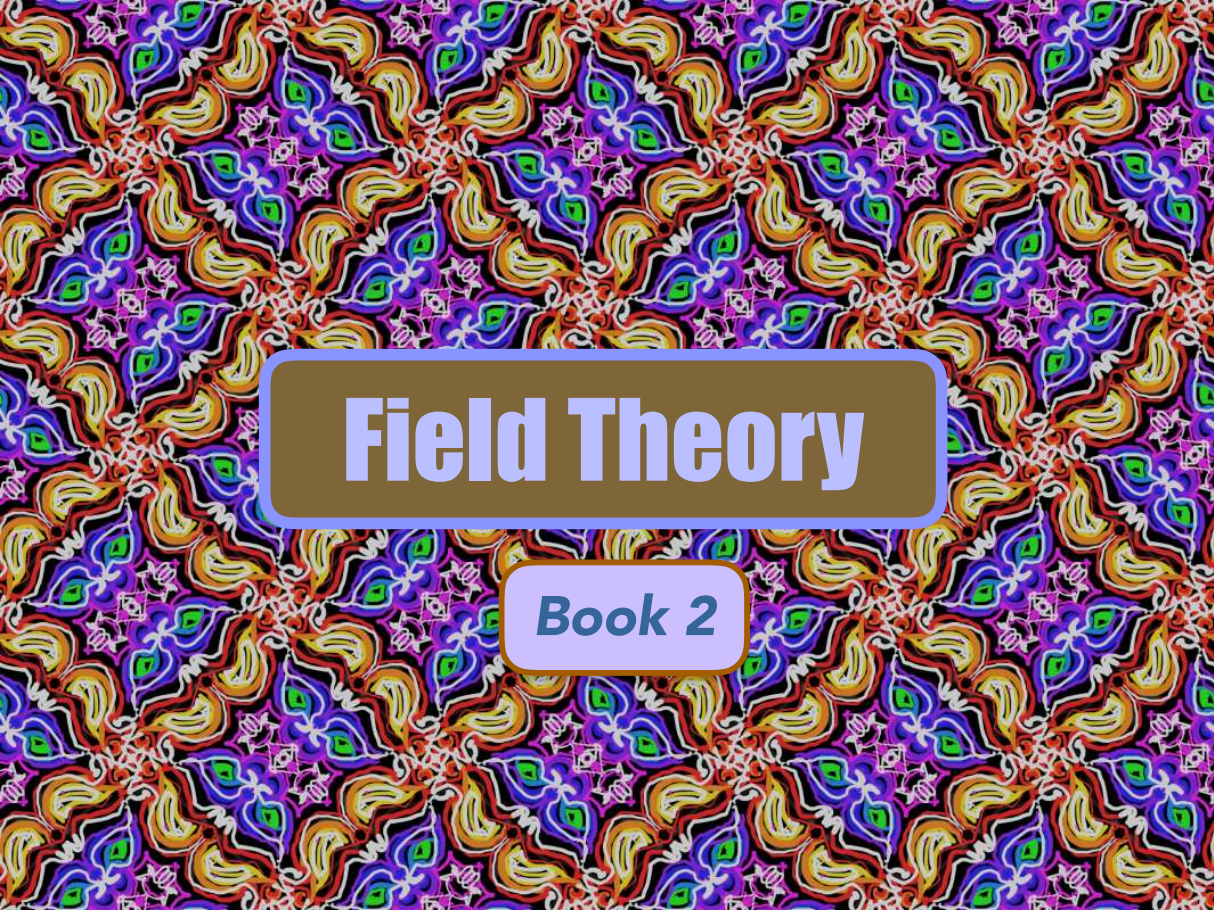




Field Theory

Book 2

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. $\square$

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

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

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

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

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

Also $1, \pi, \pi^2, \pi^3, \dots$ are linearly independent over $\mathbb{Q}$. (since π is transcendental).

An extension $E \supseteq F$ is finite if $[E : F] < \infty$, i.e. $[E : F] = n$ is a positive integer.

eg. $\mathbb{C} \supseteq \mathbb{R}$ is a quadratic extension, hence finite, $[\mathbb{C} : \mathbb{R}] = 2$.

A finite extension of $\mathbb{Q}$ i.e. $E \supseteq \mathbb{Q}$ with $[E : \mathbb{Q}] = n$, a positive integer, is called a number field (or algebraic number field). Here every element $\alpha \in E$ is algebraic over $\mathbb{Q}$. Why?

$1, \alpha, \alpha^2, \dots, \alpha^n$ are $n+1$ vectors in an n -dimensional vector space $E \supseteq \mathbb{Q}$ so this list is linearly dependent i.e. $q_1 + q_2\alpha + q_3\alpha^2 + \dots + q_{n+1}\alpha^n = 0$ for some $q_1, \dots, q_{n+1} \in \mathbb{Q}$, not all zero, i.e. α is a root of some nonzero polynomial $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Q}[x]$.

If $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ then the degree of $f(x)$, denoted $\deg f(x)$, is the largest d such that $a_d \neq 0$.

$$\deg(3x^2 + 5x + 7) = 2$$

$$\deg(0x^2 + 5x + 7) = \deg(5x + 7) = 1$$

$$\deg(7) = \deg(7x^0) = 0$$

$\deg 0$ is sometimes left undefined (not 0) or $\deg 0 = -\infty$.

$$\deg[(3x^2 + 5x + 7)(x^3 - 4x - 11)] = \deg(3x^5 + \dots - 77) = 5$$

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$$

If $g(x) = x^3 - 4x - 11$ then $\deg g(x) = 3$

$$\deg(0g(x)) = \deg 0$$

$$\deg 0 + \deg g(x) = \deg 0 + 3$$

$$\deg 0 = (\deg 0) + 3$$

There is no integer value for $\deg 0$ that satisfies this.
(We don't choose $+\infty$; we choose $-\infty$.)

Let $\alpha \in \mathbb{C}$. If α is the root of some nonzero poly. $f(x) \in \mathbb{Q}[x]$ (i.e. $f(\alpha) = 0$) then α is algebraic of degree n where n is the smallest degree of any such polynomial $f(x)$. In this case, the smallest degree monic polynomial having α as a root is the minimal polynomial of α (over $\mathbb{Q}$).

eg. $\sqrt{14}$ is algebraic of degree 2 with min. poly. $x^2 - 14 \in \mathbb{Q}[x]$.

Look at powers $1, \alpha, \alpha^2, \alpha^3, \dots$

$$\alpha = \sqrt{14} \Rightarrow 1, \alpha \text{ lin. indep.}$$

$$1, \alpha, \alpha^2 \text{ lin. dep.}$$

$$\alpha^2 = 0 \cdot \alpha + 14 \cdot 1$$

$\alpha = \sqrt{2} + \sqrt{3}$ is algebraic of degree 4 with min. poly. $x^4 - 10x^2 + 1$. Why is $\alpha = \sqrt{2} + \sqrt{3}$ not a root of any smaller degree poly. with rational coefficients?

If $x^4 - 10x^2 + 1 = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Q}[x]$ then one of $f(x), g(x)$ is a ^(non-zero) constant polynomial. Assuming we start with a monic poly. with integer coefficients, it suffices to check that there is no nontrivial factorization over $\mathbb{Z}[x]$.

If $x^4 - 10x^2 + 1 = f(x)g(x)$, $f(x), g(x) \in \mathbb{Z}[x]$, neither $f(x)$ nor $g(x)$ is constant then either

(i) $\deg f(x) = 1$, $\deg g(x) = 3$; or

(ii) $\deg f(x) = \deg g(x) = 2$. (The case $\deg f(x) = 3$, $\deg g(x) = 1$ is essentially case (i)).

In both cases we obtain a contradiction.

In case (i), $x^4 - 10x^2 + 1 = (x+a)(x^3+bx^2+cx+d)$, $ad=1$, $a=d=\pm 1$.

In this case $m(x)$ has ± 1 as a root but $m(1) = -8 = m(-1)$, a contradiction.

In case (ii), $m(x) = x^4 - 10x^2 + 1 = (x^2+ax+b)(x^2-ax+c)$, $a, b, c \in \mathbb{Z}$ (since there is no x^3 term on the left).

Once again, $bc=1$ so $b=c=\pm 1$. Now

$$m(x) = x^4 - 10x^2 + 1 = (x^2 + ax \pm 1)(x^2 - ax \pm 1). \text{ Comparing } x^2 \text{ terms on both sides,}$$

$$-10 = \pm 2 - a^2 \text{ i.e. } a^2 = 10 \pm 2 = 8 \text{ or } 12.$$

This is a final contradiction so $m(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Note: $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}[x]$ as well as in $\mathbb{Q}[x]$: it factors nontrivially as

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

This polynomial has no roots in $\mathbb{Z}$ or in $\mathbb{Q}$ or in $\mathbb{R}$.

$x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}[x]$. Every polynomial of degree ≥ 3 in $\mathbb{R}[x]$ is reducible.

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

The polynomial $x - \sqrt{2}$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$. It has a root $\sqrt{2} \in \mathbb{R}$.

Theorem: If $f(x) \in \mathbb{Z}[x]$ is monic, then $f(x)$ is reducible in $\mathbb{Q}[x]$ iff $f(x)$ is reducible in $\mathbb{Z}[x]$. Assume this, and use it!

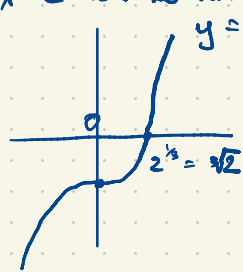
For $f(x) \in \mathbb{Q}[x]$ of degree ≥ 3 , $f(x)$ is reducible in $\mathbb{Q}[x]$ iff it has a root in $\mathbb{Q}$.

This is not true for $\deg f(x) \geq 4$.

Eg. $f(x) = x^4 + x^2 + 1$ has no roots in $\mathbb{Q}$ but it is reducible in $\mathbb{Q}[x]$

eg. $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ since it has no roots in $\mathbb{Q}$. You need to master this point!

$x^3 - 2$ has no rational roots: it has one real root $2^{1/3} \notin \mathbb{Q}$ essentially by Euclid's argument.



$y = x^3 - 2$ If $x = 2^{1/3} \in \mathbb{Q}$, $x^3 = 2$, write $x = \frac{a}{b}$ with a, b positive integers in lowest terms ($\gcd(a, b) = 1$) then $\frac{a^3}{b^3} = 2$ so $a^3 = 2b^3$ is even so a is even.

ie. $a = 2r$ for some positive integer r , so $8r^3 = 2b^3$ and $b^3 = 4r^3$ is even so b is even ie. $b = 2s$ for some $s \in \mathbb{Z}$. This contradicts $\gcd(a, b) = 1$.

Now if $x^3 - 2$ is reducible in $\mathbb{Q}[x]$ then $x^3 - 2 = (x+a)(x^2+bx+c)$, $a, b, c \in \mathbb{Q}$ but then $-a \in \mathbb{Q}$ is a root, contradiction.

For $f(x) \in F[x]$ where F is a field ($f(x)$ is a polynomial in x with coefficients in the field F) and $r \in F$, we have:

r is a root of $f(x)$

ie. $f(r) = 0$

ie. r is a "zero" of $f(x)$

iff

$x-r$ is a $\begin{cases} \text{linear factor} \\ \text{divisor} \end{cases}$ of $f(x)$ ie. factor of degree 1.

ie. $f(x) = (x-r)q(x)$, $q(x) \in F[x]$

In one direction this "iff" statement is obvious: if $f(x) = (x-r)q(x)$ then $f(r) = (r-r)q(r) = 0$.

What about the converse? By the Division Algorithm, $f(x) = q(x)(x-r) + a(x)$, $\deg a(x) < \deg(x-r)$

If r is a root of $f(x)$ then $f(r) = 0 = \underbrace{q(r)}_0 \underbrace{(r-r)}_0 + a \Rightarrow a = 0$
 $\Rightarrow f(x) = q(x)(x-r)$

$\deg a(x) < \deg(x-r)$
 $0 \text{ or } -\infty$
 $a(x) = a = \text{constant}$

We require the Division Algorithm for this.

Review the Division Algorithm for integers $\mathbb{Z}$:

Let $n, d \in \mathbb{Z}$ with $d \geq 1$. (OK for d negative but we cannot use $d=0$.) In general d won't divide n evenly; there is a remainder.

Theorem There exist unique $q, r \in \mathbb{Z}$ such that $n = qd + r$, $0 \leq r < d$.

Eg. $n=65$, $d=7$, $65 = \underline{9} \cdot 7 + \underline{2}$ $7 \nmid 65$ $\neq$

$$65 = \underline{8} \cdot 7 + \underline{9}$$

$$91 = \underline{13} \cdot 7 + \underline{0}$$

$\begin{matrix} \text{quotient} & \text{remainder} \end{matrix}$ $7 \mid 91$

d divides n ($d \mid n$) $\iff n$ is a multiple of d , $n = qd$ (i.e. $r=0$).

Similarly in $F[x]$, F any field. eg. $\mathbb{Q}[x]$, $\mathbb{R}[x]$, ... not $\mathbb{Z}[x]$.

Theorem (Division Algorithm for polynomials) Let F be any field and let $f(x), d(x) \in F[x]$ where $\deg d(x) \geq 1$. Then there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)d(x) + r(x), \quad \deg r(x) < \deg d(x).$$

Eg. $F = \mathbb{Q}$, $f(x) = x^3 - 2x - 3$, $d(x) = x^2 + x + 1$.

$$f(x) = x^3 - 2x - 3 = (x-1)(x^2 + x + 1) + (-2x - 2)$$

$$\begin{array}{r} x-1 \\ x^2+x+1 \overline{) x^3-2x-3} \\ \underline{x^3+x^2+x} \\ -x^2-3x-3 \\ \underline{-x^2-x-1} \\ -2x-2 \end{array}$$

$$x^2 + x + 1 = \left(-\frac{1}{2}x\right)(-2x-2) + (1)$$

The Division Algorithm leads to Euclid's Algorithm (for $\mathbb{Z}$, $F[x]$, ...)
 not $\mathbb{Z}[x]$

$$\begin{array}{r} -\frac{1}{2}x \\ -2x-2 \overline{) x^2 + x + 1} \\ \underline{x^2 + x} \\ 1 \end{array}$$

$$\gcd(100, 27) = 1 = a \cdot 100 + b \cdot 27 \quad \text{for some } a, b \in \mathbb{Z}$$

$$100 = 3 \times 27 + 19$$

$$27 = 1 \times 19 + 8$$

$$19 = 2 \times 8 + 3$$

$$8 = 2 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

last nonzero remainder

$$\gcd(100, 27) = 1 = 3 - 2$$

$$= 3 - (8 - 2 \times 3)$$

$$= 3 \times 3 - 8$$

$$= 3 \times (19 - 2 \times 8) - 8$$

$$= 3 \times 19 - 7 \times 8$$

$$= 3 \times 19 - 7 \times (27 - 19)$$

$$= 10 \times 19 - 7 \times 27$$

$$= 10 \times (100 - 3 \times 27) - 37 \times 27$$

$$= 10 \times 100 - 37 \times 27$$

$$= 1$$

Continue
Monday

Euclid's Algorithm uses repeated application of the Division Algorithm.
 The last nonzero remainder is the gcd.

Shorthand

100	27	
1	0	100
0	1	27
1	-3	19
-1	4	8
3	-11	3
-7	26	2
10	-37	1
*	*	0

$$\gcd(100, 27) = 1 = 10 \times 100 - 37 \times 27$$

The gcd of two polynomials is the largest monic polynomial dividing both of them.
 Given $f(x), g(x) \in F[x]$ (F any field), $f(x), g(x)$ not both zero.

$d(x) = \gcd(f(x), g(x))$ is the largest monic polynomial such that $d(x) \mid f(x)$, $d(x) \mid g(x)$.
 We compute $d(x)$ using Euclid's Algorithm and it finds $a(x), b(x) \in F[x]$ such that
 $d(x) = a(x)f(x) + b(x)g(x)$.

Eg. $f(x) = x^3 - 2x - 3$
 $g(x) = x^2 + x + 1$

$$\gcd(f(x), g(x)) = 1 = \left(\frac{1}{2}x\right)f(x) + \left(-\frac{1}{2}x^2 + \frac{1}{2}x + 1\right)g(x) \quad (*)$$

$$f(x) = (x-1)g(x) + (-2x-2)$$

$$g(x) = \left(-\frac{1}{2}x\right)(-2x-2) + (1)$$

$$-2x-2 = (-2x-2)(1) + 0$$

$$1 = g(x) + \left(\frac{1}{2}x\right)(-2x-2)$$

$$= g(x) + \left(\frac{1}{2}x\right)(f(x) - (x-1)g(x))$$

$$= \left(\frac{1}{2}x\right)f(x) + \left(1 - \frac{1}{2}x^2 + \frac{1}{2}x\right)g(x)$$

Check: $\left(\frac{1}{2}x\right)(x^3 - 2x - 3) + \left(-\frac{1}{2}x^2 + \frac{1}{2}x + 1\right)(x^2 + x + 1) = 1$

x^2 terms: $-1 + 1 + \frac{1}{2} - \frac{1}{2} = 0$

x terms: $-\frac{3}{2} + \frac{1}{2} + 1 = 0$

constant: 1

Alternatively

	$f(x) = x^3 - 2x - 3$	$g(x) = x^2 + x + 1$	
①	1	0	$x^3 - 2x - 3$
②	0	1	$x^2 + x + 1$
③ = ① - (x)②	1	$-x + 1$	$-2x - 2$
④ = ② + $\frac{1}{2}$ ③	$\frac{1}{2}x$	$-\frac{1}{2}x^2 + \frac{1}{2}x + 1$	1
	*	*	0

Recall: we considered the field $\mathbb{Q}[\theta] = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Q}\}$, θ root of $f(x)$
 We computed $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ where $\alpha = \theta^2 - 3$, $\beta = \theta^2 + \theta + 1 = g(\theta)$
 To find $\frac{1}{\beta}$, use (*)
 $\frac{1}{\beta} = -\frac{1}{2}\theta^2 + \frac{1}{2}\theta + 1$
 $1 = \left(\frac{1}{2}x\right)f(x) + \left(-\frac{1}{2}x^2 + \frac{1}{2}x + 1\right)g(x)$
 $1 = \left(\frac{1}{2}\theta\right)f(\theta) + \left(-\frac{1}{2}\theta^2 + \frac{1}{2}\theta + 1\right)g(\theta)$