

Field Theory

Book 3

Eg. $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

x	x^0	x^1	x^2	x^3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

\mathbb{F}_8

x	1	θ	θ^2	θ^3	θ^4	θ^5	θ^6
1	1	θ	θ^2	θ^3	θ^4	θ^5	θ^6
θ	θ	θ^2	θ^3	θ^4	θ^5	θ^6	1
θ^2							
θ^3							
\vdots							

etc.

x	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

mult. table for a Klein 4-group
(noncyclic group of order 4)

This cannot be a subgroup in the multiplicative group of any field F for the following reason:

It has four solutions of $x^2=1$ (roots of x^2-1)

Wedderburn's Theorem: If F is any field (finite or infinite), then any subgroup of F^* (the multiplicative group of nonzero elements) is cyclic.

[If $F = \mathbb{F}_q$, then F^* is cyclic of order $q-1$.

[The n^{th} roots of unity in \mathbb{C} form a cyclic group of order n .

An extension $F \supseteq \mathbb{Q}$ (i.e. a field of characteristic zero) can be a finite extension or an infinite extension i.e.

- $n = [F:\mathbb{Q}] < \infty$: F is a finite extension of \mathbb{Q} (i.e. an extension of finite degree n). These are number fields, also called algebraic number fields.

In this case F is a "simple" extension $F = \mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}$.

eg. $F = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

so $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for F over \mathbb{Q} and $[F:\mathbb{Q}] = 4$
 (a quartic extension of \mathbb{Q})

quadratic: degree 2
 cubic: " 3
 quartic: " 4
 quintic: " 5

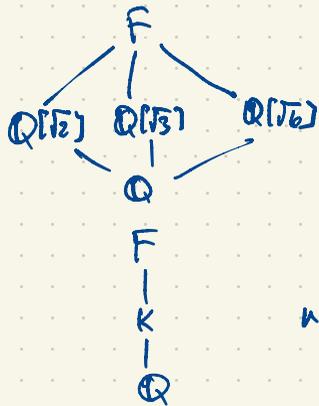
"Almost" any element $\alpha \in F$ generates F as a field: $F = \mathbb{Q}[\alpha]$.

If $\alpha = \sqrt{2} + \sqrt{3}$ then α has min. poly. $x^4 - 10x^2 + 1$

$$\begin{aligned} \alpha &= \sqrt{2} + \sqrt{3} \\ \alpha^2 &= 2 + 3 + 2\sqrt{6} \\ &= 5 + 2\sqrt{6} \end{aligned}$$

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

All five subfields of F .



If $n = [F:\mathbb{Q}] < \infty$ then F has only finitely many subfields and all have degree dividing n

$$n = [F:\mathbb{Q}] = [F:K][K:\mathbb{Q}] \Rightarrow [K:\mathbb{Q}] \text{ divides } n.$$

Every element $\alpha \in F$ (if $n = [F:\mathbb{Q}] < \infty$)
is algebraic over \mathbb{Q} .

Why? If $\alpha \in F$, $[F:\mathbb{Q}] = n$, then $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent over \mathbb{Q} .

$\Rightarrow a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0$ for some $a_0, a_1, \dots, a_n \in \mathbb{Q}$ not all zero.

$\Rightarrow \alpha$ is algebraic.

More than this, α is algebraic of degree dividing n .

$$F \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q} \quad \Rightarrow \quad n = [F:\mathbb{Q}] = [F:\mathbb{Q}[\alpha]] [\mathbb{Q}[\alpha]:\mathbb{Q}]$$

= degree of α over \mathbb{Q}

= degree of the min. poly.
of α over \mathbb{Q} .

• $[F:\mathbb{Q}] = \infty$ eg. $\mathbb{R}, \mathbb{C}, \dots$

Let $\alpha \in \mathbb{R}$ or \mathbb{C} and consider the field $\mathbb{Q}(\alpha)$ generated by α . This is the smallest extension of \mathbb{Q} containing α . If α is algebraic, this gives a finite extension $\mathbb{Q}[\alpha]$, $n = [\mathbb{Q}(\alpha):\mathbb{Q}] < \infty$.

Let's take π which is known to be transcendental. $\mathbb{Q}(\pi)$ is the subfield of \mathbb{R} containing π . $\mathbb{Q} \subset \mathbb{Q}(\pi) \subset \mathbb{R}$.

The subring $\mathbb{Q}[\pi] \subset \mathbb{R}$ generated by π using addition, subtraction, and multiplication only, is the subring

$$\mathbb{Q}[\pi] = \{ a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n : a_0, a_1, \dots, a_n \in \mathbb{Q}, n \geq 0 \}$$

eg. $\frac{27}{5}\pi^4 - \frac{19}{11}\pi^3 + 13\pi^2 + 105\pi - \frac{13}{11} \in \mathbb{Q}[\pi]$. It's not a field: $\pi \in \mathbb{Q}[\pi]$, $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$.

If $\frac{1}{\pi} = a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n$ for some n , and $a_0, a_1, \dots, a_n \in \mathbb{Q}$ then

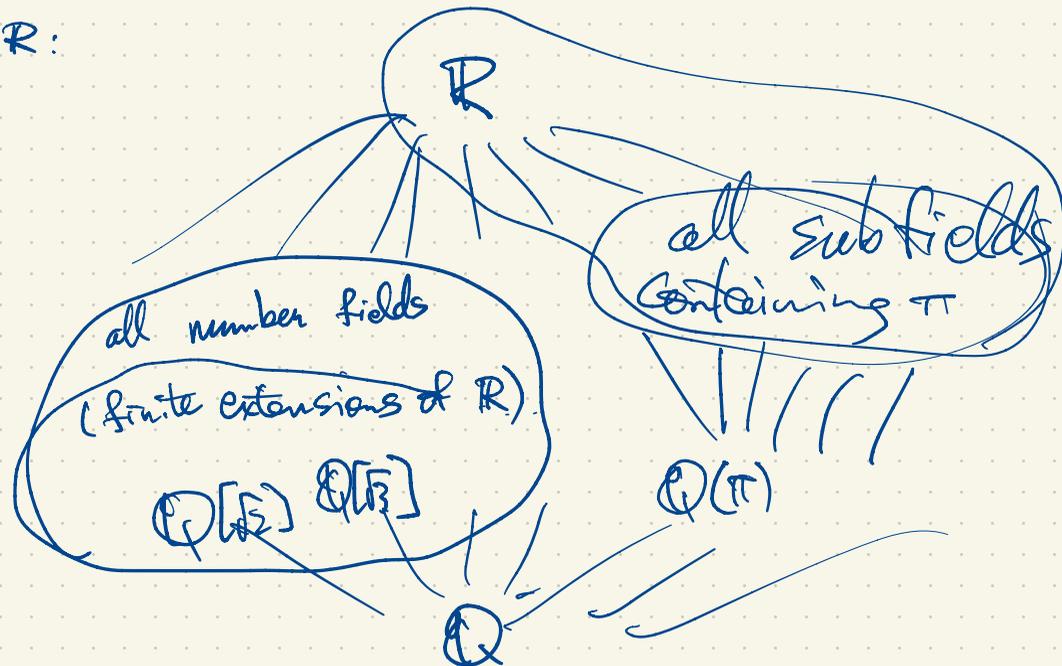
$$a_n\pi^{n+1} + a_{n-1}\pi^n + \dots + a_2\pi^3 + a_1\pi^2 + a_0\pi - 1 = 0. \quad \text{Contradiction.}$$

To extend the ring $\mathbb{Q}[\pi]$ to a field, we divide elements of $\mathbb{Q}[\pi]$ inside \mathbb{R} :

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

This is a field. It's a subfield. It's generated by π under $+$, $-$, \times , \div
So it is the smallest subfield containing π .

Subfields of \mathbb{R} :



About notation: $F[x]$ = the ring of all polynomials in x with coefficients in F .
(symbol/indeterminate)

$F(x)$ = the field of all rational functions in x with coefficients in F .
 $= \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x], g(x) \neq 0 \right\}$.

$F(x)$ is the field of quotients of $F[x]$.

$\mathbb{Q} \dots \dots \dots \mathbb{Z}$.

$$\mathbb{Q}[\sqrt{2}] = \{ f(\sqrt{2}) : f(x) \in \mathbb{Q}[x] \}$$
$$= \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}.$$

If $f(x) = \frac{5}{3}x^3 + x^2 - 4x + \frac{11}{2} \in \mathbb{Q}[x]$
then $f(\sqrt{2}) = \frac{5}{3}\sqrt{2}^3 + \sqrt{2}^2 - 4\sqrt{2} + \frac{11}{2}$
 $= \frac{10}{3}\sqrt{2} + 2 - 4\sqrt{2} + \frac{11}{2}$
 $= \frac{15}{2} - \frac{2}{3}\sqrt{2}$

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{u}{v} : u, v \in \mathbb{Q}[\sqrt{2}], v \neq 0 \right\} = \mathbb{Q}[\sqrt{2}]$$

(This ring $\mathbb{Q}[\sqrt{2}]$ is already a field)

$$\mathbb{Q}(\pi) \supset \mathbb{Q}[\pi].$$

ring which
is not a field

Let $\alpha \in \mathbb{C}$. Then $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ iff α is algebraic.

there are infinitely many quadratic extensions of \mathbb{Q} . Suppose $E \supset \mathbb{Q}$ with $[E:\mathbb{Q}] = 2$.
Then E has a basis $\{1, \theta\}$ i.e. every element of E is uniquely expressible as
 $a + b\theta$ $a, b \in \mathbb{Q}$. Since $\theta^2 \in E$, $\theta^2 = a + b\theta$ for some $a, b \in \mathbb{Q}$, i.e. $\theta^2 - b\theta - a = 0$.
 $\Rightarrow \theta = \frac{b \pm \sqrt{b^2 + 4a}}{2} = \frac{b \pm \sqrt{\delta}}{2}$ where $\delta = b^2 + 4a \in \mathbb{Q}$. Now $E = \mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{\delta}]$

Clarify what we mean by: the same field.

If $K, K' \subseteq \mathbb{C}$ are two subfields then one of three things can happen:

- $K = K'$
- or • $K \neq K'$ but $K \cong K'$ (isomorphic)
- or • $K \not\cong K'$ (not isomorphic).

Eg. $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{3}]$ (two subfields of \mathbb{C} that are actually equal)

$\mathbb{Q}[\sqrt{2}] \neq \mathbb{Q}[\sqrt{3}]$. The field $\mathbb{Q}[\sqrt{2}]$ has roots of $x^2 - 2$ but $\mathbb{Q}[\sqrt{3}]$ has no roots of $x^2 - 2$ ($x^2 - 2$ is reducible in one field but irreducible in the other.)

An isomorphism between two fields $\phi: K \rightarrow K'$ is a bijection such that $\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$ and $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ for all $\alpha, \beta \in K$.

For any isomorphism $\phi: K \rightarrow K'$, we must have $\phi(0) = 0$.

Proof: $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$. Subtract $\phi(0)$ from both sides to get $\phi(0) = 0$.

Next: show $\phi(1) = 1$. Proof: $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$ where $\phi(1) \neq 0$. Since ϕ is bijective.

Multiply both sides by $\phi(1)^{-1}$ so $\phi(1)^{-1}\phi(1) = \phi(1)^{-1}\phi(1)\phi(1) = \phi(1)$.

$$2 = 1 + 1$$

$$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2$$

... $\phi(n) = n$ for every positive integer

$$3 = 1 + 1 + 1 = 2 + 1$$

$$\phi(3) = \phi(2+1) = \phi(2) + \phi(1) = 2 + 1 = 3$$

$$n = \underbrace{1 + 1 + \dots + 1}_{n \text{ terms}}$$

$$\text{char } K = \text{char } K'$$

If $\text{char } K = 0$ then the prime subfield of K is \mathbb{Q} . Same for K' .

In this case $K \supseteq \mathbb{Q}$ and $K' \supseteq \mathbb{Q}$ and $\phi(a) = a$ for all $a \in \mathbb{Q}$.

Suppose $\phi: \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}]$ is an isomorphism. Then $\phi(\sqrt{2}) = a + b\sqrt{3}$,
 $a, b \in \mathbb{Q}$.

$$\text{Then } \phi(\sqrt{2})^2 = (a + b\sqrt{3})^2 \quad (a + b\sqrt{3})^2 = 2$$

$$\phi(\sqrt{2})\phi(\sqrt{2})$$

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2$$

$$2ab\sqrt{3} = 2 - a^2 - 3b^2$$

$$\phi(2) = 2$$

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

contradicting Euclid's proof.

$$\text{If } b = 0 \text{ then } a^2 = 2$$

$$a = \pm\sqrt{2} \in \mathbb{Q} \\ \text{contradiction}$$

$$\text{If } a = 0 \text{ then } 3b^2 = 2$$

$$9b^2 = 6$$

$$(3b)^2 = 6$$

$$\sqrt{6} = \pm 3b \in \mathbb{Q}$$

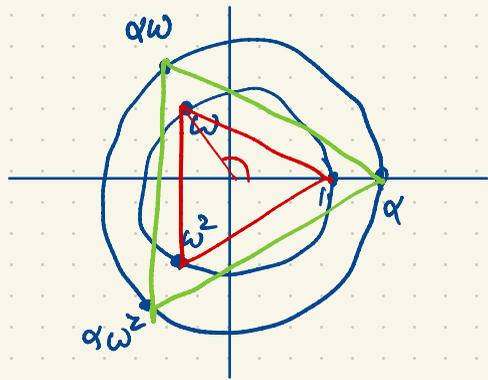
contradiction
by Euclid

Third possibility: $K, K' \subseteq \mathbb{C}$ subfields
 $K \neq K'$ but $K \cong K'$.

To give an example we need an extension of degree ≥ 3 .

$m(x) = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible.

n^{th} roots of any nonzero complex number form vertices of a regular n -gon in \mathbb{C}
 $m(x)$ has roots $\alpha = 2^{1/3}$ (the unique real root)



$1, \omega, \omega^2$ are the three cube roots of unity
 $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ $\omega = e^{2\pi i/3}$

ω, ω^2 are the two primitive cube roots of 1.

$$\alpha^3 = 2$$

$$(\alpha\omega)^3 = \alpha^3 \omega^3 = 2 \cdot 1 = 2$$

$$(\alpha\omega^2)^3 = \alpha^3 \omega^6 = 2 \cdot 1 = 2$$

$\left. \begin{array}{l} \alpha_1 = \alpha \\ \alpha_2 = \alpha\omega \\ \alpha_3 = \alpha\omega^2 \end{array} \right\}$ three roots of $m(x)$

$$m(x) = x^3 - 2 = (x - \alpha)(x - \alpha\omega)(x - \alpha\omega^2)$$

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

$[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$. with $1, \alpha, \alpha^2$ as basis.

$$\mathbb{Q}[\alpha_2] = \{a + b\alpha_2 + c\alpha_2^2 : a, b, c \in \mathbb{Q}\} \subset \mathbb{C}$$

$$\underline{\mathbb{Q}[\alpha_2] \not\subset \mathbb{R}}$$

$[\mathbb{Q}[\alpha_2] : \mathbb{Q}] = 3$. with basis $1, \alpha_2, \alpha_2^2$

$\mathbb{Q}[\alpha_1] = \mathbb{Q}[\alpha]$
 $\mathbb{Q}[\alpha_2] = \mathbb{Q}[\alpha\omega]$ } Not equal. because $\mathbb{Q}[\alpha] \subset \mathbb{R}$ but $\mathbb{Q}[\alpha_2] \not\subset \mathbb{R}$.

But $\mathbb{Q}[\alpha_1] \cong \mathbb{Q}[\alpha_2]$

The isomorphism $\phi: \mathbb{Q}[\alpha_1] \rightarrow \mathbb{Q}[\alpha_2]$ is

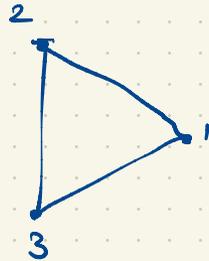
$$\phi(a + b\alpha_1 + c\alpha_1^2) = a + b\alpha_2 + c\alpha_2^2$$

eg. in $\mathbb{Q}[\alpha]$, $(1+\alpha+2\alpha^2)(3-\alpha) = 3+2\alpha+5\alpha^2-2\frac{\alpha^3}{2} = -1+2\alpha+5\alpha^2$
 in $\mathbb{Q}[\alpha_2]$, $(1+\alpha_2+2\alpha_2^2)(3-\alpha_2) = -1+2\alpha_2+5\alpha_2^2$

The three roots of $m(x) = x^3-2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2)$
 has three roots that are completely interchangeable.

$S_3 = \{\text{all permutations of } 1, 2, 3\}$, $|S_3| = 3! = 6$.

$S_3 \cong$ symmetry group of an equilateral triangle



In $\mathbb{Q}[\sqrt{2}]$, we have an isomorphism

An automorphism of a field is
 an isomorphism from the field
 to itself.

$\phi: \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{2}]$

$\phi(a+b\sqrt{2}) = a-b\sqrt{2}$

is an isomorphism.