

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. $x^4 - 10x^2 + 1$

$$\alpha = \sqrt{2} + \sqrt{3}$$

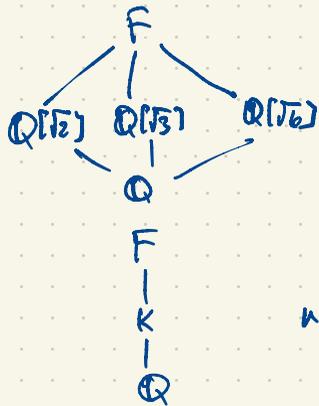
$$\alpha^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$$

$$\alpha^2 - 5 = 2\sqrt{6}$$

$$\alpha^4 - 10\alpha^2 + 25 = 24$$

$$\alpha^4 - 10\alpha^2 + 1 = 0$$

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

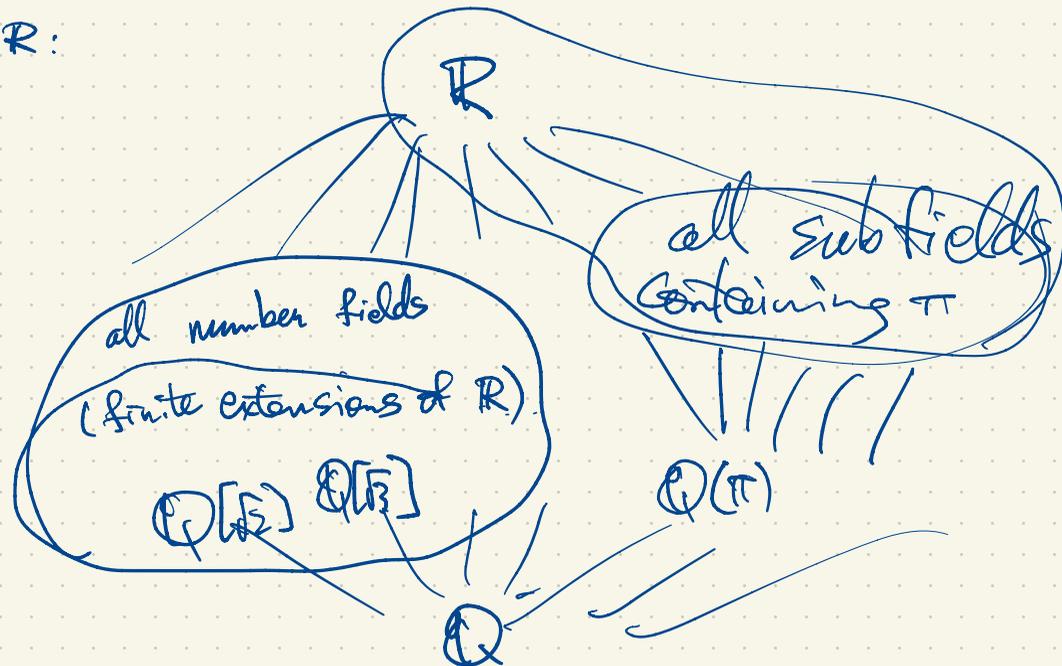
$$a_n\pi^{n+1} + a_{n-1}\pi^n + \dots + a_2\pi^3 + a_1\pi^2 + a_0\pi - 1 = 0. \quad \text{Contradiction.}$$

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 $E = \mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{\delta}]$

$$\text{eg. } \theta^2 = \frac{5}{2}\theta + 3 \Rightarrow \theta^2 - \frac{5}{2}\theta - 3 = 0 \Rightarrow \theta = \frac{\frac{5}{2} \pm \sqrt{\frac{25}{4} + 12}}{2} = \frac{\frac{5}{2} \pm \frac{1}{2}\sqrt{25+48}}{2} = \frac{5 \pm \sqrt{73}}{4}$$

$$\mathbb{Q}\left[\frac{5+\sqrt{73}}{4}\right] = \mathbb{Q}\left[\frac{5-\sqrt{73}}{4}\right] = \mathbb{Q}[\sqrt{73}]$$

$$\mathbb{Q}[\sqrt{12}] = \mathbb{Q}[6\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$$