Field Theory

Book 3

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

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

	2^0	2^1	2^2	2^3
$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$\mathbb{F}_8$

$\times$	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				etc.			
θ^3							
$\vdots$				$\vdots$			

$\times$	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 $F^\times$ (the multiplicative group of nonzero elements) is cyclic.

[If $F = \mathbb{F}_q$, then $F^\times$ 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 $F = \mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}$.

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

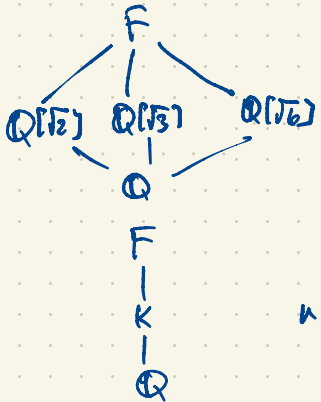
so $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for F over $\mathbb{Q}$ and $[F:\mathbb{Q}] = 4$ (a quartic extension of $\mathbb{Q}$)

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

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

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

$\Rightarrow$ α is algebraic.

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

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

$= $ 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

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

eg. $\frac{27}{5}\pi^4 - \frac{19}{11}\pi^3 + 13\pi^2 + 105\pi - \frac{13}{111} \in \mathbb{Q}[\pi]$. It's not a field: $\pi \in \mathbb{Q}[\pi]$, $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$.

If $\frac{1}{\pi} = q_0 + q_1\pi + q_2\pi^2 + \cdots + q_n\pi^n$ for some n and $q_0, q_1, \ldots, q_n \in \mathbb{Q}$ then

$q_n\pi^{n+1} + q_{n-1}\pi^n + \cdots + q_2\pi^3 + q_1\pi^2 + q_0\pi - 1 = 0$. Contradiction.

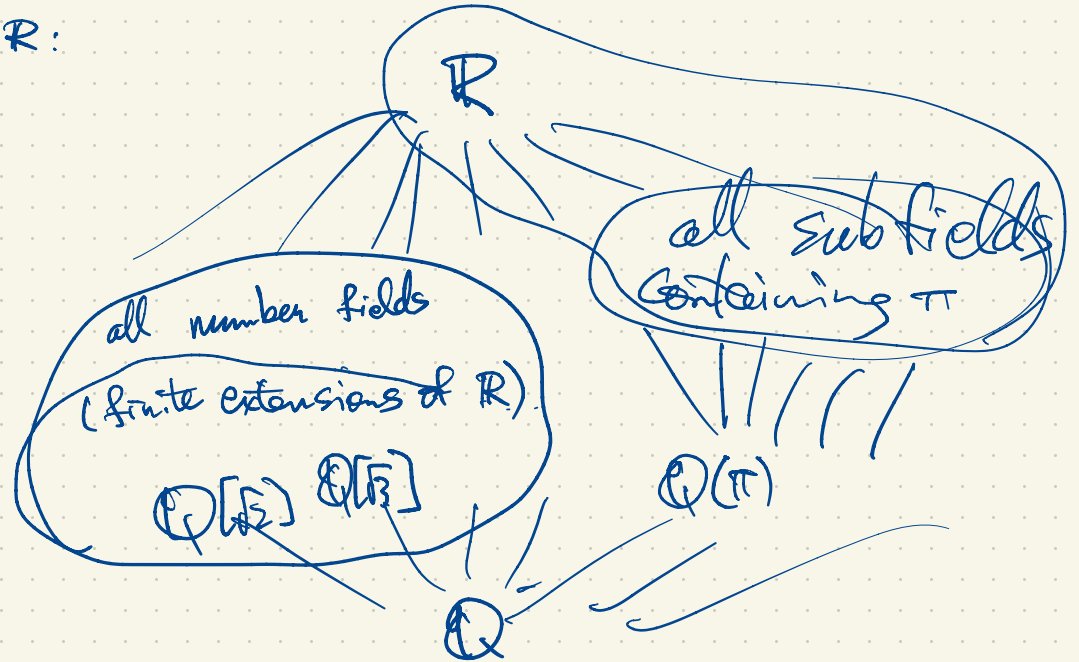
To extend the ring $\mathbb{Q}[\pi]$ to a field, we divide elements of $\mathbb{Q}[\pi]$ inside $\mathbb{R}$:

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

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 (symbol/indeterminate) with coefficients in F.

$F(x)$ = the field of all rational functions in x with coefficients in F.

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

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

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

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

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

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

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

then $f(\sqrt{2}) = \frac{5}{3}\sqrt{2}^3 + \sqrt{2}^2 - 4\sqrt{2} + \frac{11}{2}$

$$= \frac{10}{3}\sqrt{2} + 2 - 4\sqrt{2} + \frac{11}{2}$$
$$= \frac{15}{2} - \frac{2}{3}\sqrt{2}$$

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

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

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

$\mathbb{Q}\left[\frac{5+\sqrt{73}}{4}\right] = \mathbb{Q}\left[\frac{5-\sqrt{73}}{4}\right] = \mathbb{Q}[\sqrt{73}]$ $\qquad$ $\mathbb{Q}[\sqrt{72}] = \mathbb{Q}[6\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$

Above: a quadratic extension $E \supset \mathbb{Q}$, $[E:\mathbb{Q}]$. If $\alpha \in E - \mathbb{Q}$ then $\mathbb{Q}[\alpha] = E$.

$E \supseteq \mathbb{Q}[\alpha] \supset \mathbb{Q} \Rightarrow 2 = [E:\mathbb{Q}] = \underbrace{[E:\mathbb{Q}[\alpha]]}_{=1}\underbrace{[\mathbb{Q}[\alpha]:\mathbb{Q}]}_{2 \neq 1} \Rightarrow$

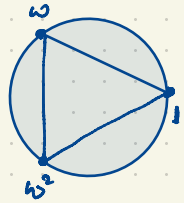
$\mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{73}]$ where θ is any root of $x^2 - \frac{5}{2}x - 3$.

All the quadratic extensions of $\mathbb{Q}$ are $\qquad \sqrt{8} = 2\sqrt{2} \Rightarrow \mathbb{Q}[\sqrt{8}] = \mathbb{Q}[\sqrt{2}]$

$\ldots, \mathbb{Q}[\sqrt{-5}], \mathbb{Q}[\sqrt{-3}], \mathbb{Q}[\sqrt{-2}], \mathbb{Q}[\sqrt{-1}], \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{6}], \mathbb{Q}[\sqrt{7}], \mathbb{Q}[\sqrt{10}], \mathbb{Q}[\sqrt{11}], \ldots$

No two fields in this list are the same. In fact, no two of them are isomorphic.

If ω is a root of $x^2 + x + 1$ then $\omega^3 = 1$ and so ω is a cube root of unity.



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

roots: $1, \omega, \omega^2$ $\qquad$ root: 1 $\qquad$ roots: ω, ω^2 (primitive cube roots of 1)

$[\mathbb{Q}[\omega]:\mathbb{Q}] = 2$

So it's in our list above... which one is it?

$\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{-3}]$ Same field!

$x^2 + x + 1$ has roots $\frac{-1 \pm \sqrt{-3}}{2} = \omega, \omega^2$.

$\omega = \frac{-1+\sqrt{-3}}{2} \Rightarrow \sqrt{-3} = 2\omega + 1$

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 • $K \ncong K'$ (not isomorphic).

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

$\mathbb{Q}[\sqrt{2}] \ncong \mathbb{Q}[\sqrt{3}]$. 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 $\phi : K \to K'$ 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 $\phi : K \to K'$, 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 $\phi(1) = 1$ (the 1 in K maps to the 1 in K').

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 $\phi(1)^{-1}\phi(1) = \phi(1)^{-1}\phi(1)\phi(1) = \phi(1)$.

$2 = 1+1$

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

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

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

... $\phi(n) = n$ for every positive integer $n = \underbrace{1+1+\cdots+1}_{n \text{ terms}}$

$\mathrm{char}\, K = \mathrm{char}\, K'$

If $\mathrm{char}\, K = 0$ 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 $\phi : \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{3}]$ is an isomorphism. Then $\phi(\sqrt{2}) = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$.

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

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

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

$\phi(2) = 2$

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

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

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

If $ab \neq 0$ then

$\sqrt{3} = \dfrac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q}$

contradicting Euclid's proof.