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

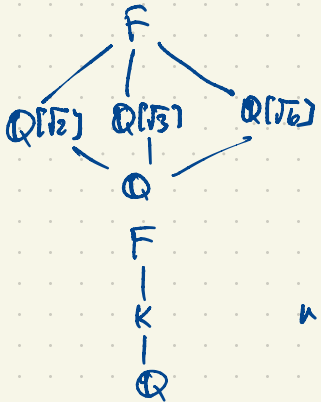
so $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for F over $\mathbb{Q}$ and $[F:\mathbb{Q}] = 4$ (a quartic extension of $\mathbb{Q}$)

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.

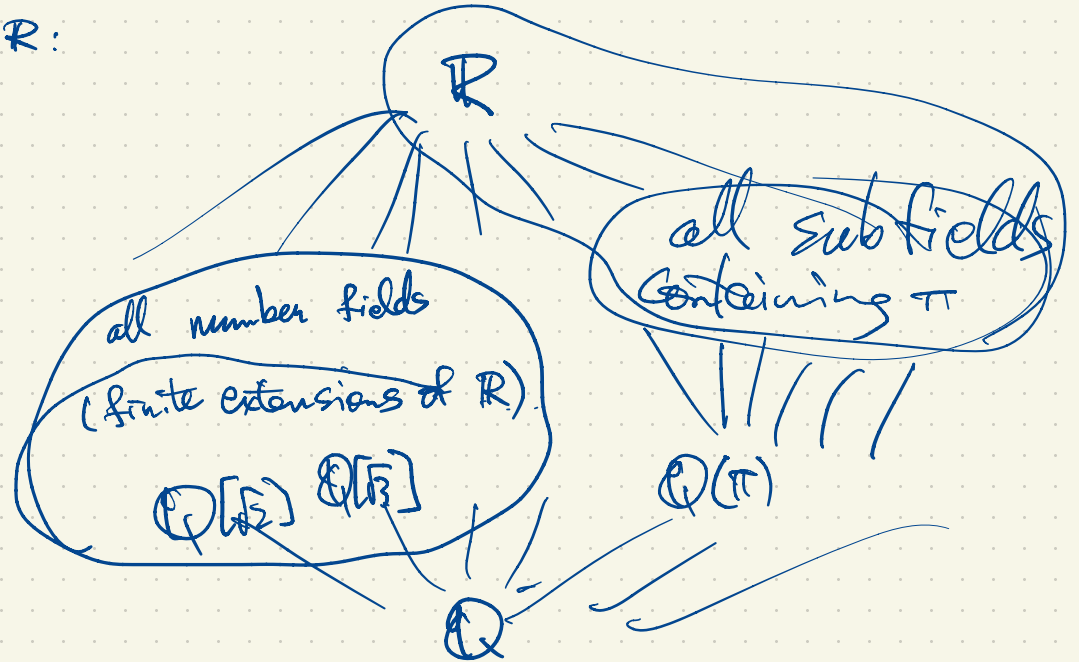
To extend the ring $\mathbb{Q}[\pi]$ to a field, we divide elements of $\mathbb{Q}[\pi]$ inside $\mathbb{R}$:

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

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 $\mathbb{Q}[\alpha] = E$.

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

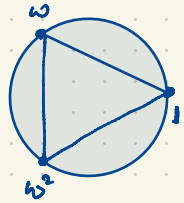
$\mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{73}]$ where θ is any root of $x^2 - \frac{5}{2}x - 3$.

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

$\phi(a) = a$ for all $a \in \mathbb{Q}$.

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

If $\operatorname{char} K = 0$ 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 $\phi(\sqrt{2})^2 = (a+b\sqrt{3})^2$ $\quad (a+b\sqrt{3})^2 = 2$

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

$\phi(\sqrt{2}\sqrt{2})$ $\quad 2ab\sqrt{3} = 2 - a^2 - 3b^2$

$\phi(2) = 2$

If $ab \neq 0$ then

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

contradicting Euclid's proof.

If $b = 0$ then

$a^2 = 2$

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

contradiction

If $a = 0$ 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

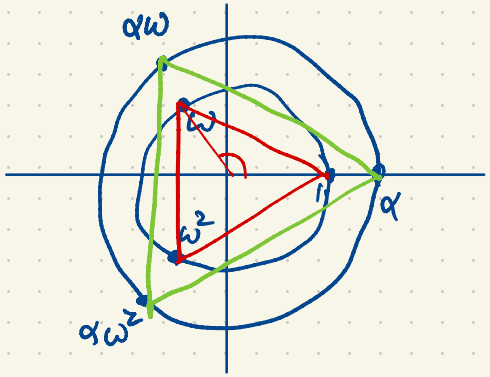
$K \neq K'$ but $K \cong K'$.

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

$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ $\quad \omega = e^{2\pi i/3}$

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.

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

$\mathbb{Q}[\alpha_2] \not\subseteq \mathbb{R}$.

$[\mathbb{Q}[\alpha_2] : \mathbb{Q}] = 3$. 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 $\mathbb{Q}[\alpha] \subseteq \mathbb{R}$ but $\mathbb{Q}[\alpha_2] \not\subseteq \mathbb{R}$.

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

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

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

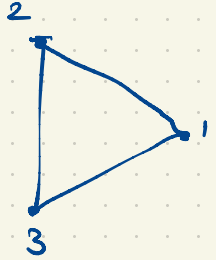
eg. in $\mathbb{Q}[\alpha]$, $(1+\alpha+2\alpha^2)(3-\alpha) = 3+2\alpha+5\alpha^2-2\alpha^3 = -1+2\alpha+5\alpha^2$
(since $\alpha^3 = 2$)

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.

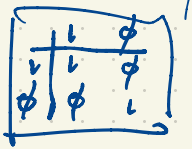
S_3 = {all permutations of 1, 2, 3}, $|S_3| = 3! = 6$.

$S_3 \cong$ symmetry group of an equilateral triangle



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

$\phi(a+b\sqrt{2}) = a-b\sqrt{2}$ is an isomorphism.



i.e. ϕ is bijective

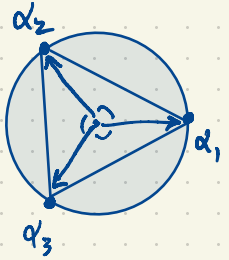
$\phi(uv) = \phi(u)\phi(v)$

$\phi(u+v) = \phi(u)+\phi(v)$ for all u, v.

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

The automorphisms of $\mathbb{Q}[\sqrt{2}]$ form a (cyclic) group $\{1, \phi\}$ of order 2

x^3-2 has three complex roots $\alpha_1, \alpha_2, \alpha_3$. Are $\alpha_1, \alpha_2, \alpha_3$ linearly dependent or not over $\mathbb{Q}$?



$\alpha_1+\alpha_2+\alpha_3 = 0 \Rightarrow \alpha_1, \alpha_2, \alpha_3$ are linearly dependent over $\mathbb{Q}$.

You can't have three lin. indep. vectors in $\mathbb{C}$ over $\mathbb{R}$ because $[\mathbb{C}:\mathbb{R}] = 2$.

$\alpha_1, \alpha_2, \alpha_3$ lie in an extension $E = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$

If $m(x) = x^3+bx+c$, $b,c \in \mathbb{Q}$ then the roots of $m(x)$ in $\mathbb{C}$ are linearly dependent over $\mathbb{Q}$

$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, some $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ not necessarily distinct.

$= x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3$

$\Leftrightarrow$ $\begin{cases} \alpha_1+\alpha_2+\alpha_3 = 0 \\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 = b \\ \alpha_1\alpha_2\alpha_3 = -c \end{cases}$

Eg. $E = \mathbb{Q}[\sqrt{2},\sqrt{3}]$ has four automorphisms $\iota, \sigma, \tau, \sigma\tau$

$= \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$

$[E:\mathbb{Q}] = 4$ since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis

$\iota(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

$\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$

$\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$

$\sigma\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$

These are the only automorphisms of E

θ	$\iota(\theta)$	$\sigma(\theta)$	$\tau(\theta)$	$\sigma\tau(\theta)$
1	1	1	1	1
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\sqrt{6}$	$\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$	$\sqrt{6}$

$\iota: \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$ $\sigma: \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}$ $\tau: \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}$ $\sigma\tau: \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}$

	ι	σ	τ	$\sigma\tau$
ι	ι	σ	τ	$\sigma\tau$
σ	σ	ι	$\sigma\tau$	τ
τ	τ	$\sigma\tau$	ι	σ
$\sigma\tau$	$\sigma\tau$	τ	σ	ι

Klein four-group

$\sigma\tau = \tau\sigma$
$\sigma^2 = \iota$
$\tau^2 = \iota$

Every field has at least one automorphism $\iota(\alpha) = \alpha$ for all α

$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3})$
$= (-\sqrt{2})(\sqrt{3}) = -\sqrt{6}$

$\tau(\sqrt{6}) = \tau(\sqrt{2})\tau(\sqrt{3})$
$= \sqrt{2}\cdot(-\sqrt{3}) = -\sqrt{6}$

$\sigma\tau(\sqrt{6}) = \sigma\tau(\sqrt{2})\,\sigma\tau(\sqrt{3})$
$= (-\sqrt{2})(-\sqrt{3})$
$= \sqrt{6}$

If $E \supseteq \mathbb{Q}$ is an extension of degree $n = [E:\mathbb{Q}] < \infty$ (number field)
then E has at most n automorphisms.

When $n = 2$, then E has exactly 2 automorphisms.

Consider $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\alpha]$ where $\alpha = \sqrt{2} + \sqrt{3}$.

α has min. poly. $m(x) = x^4 - 10x^2 + 1$ over $\mathbb{Q}$.

$= (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$ $\qquad \beta = \sqrt{2} - \sqrt{3}$

Roots of $m(x)$: $\alpha = \sqrt{2}+\sqrt{3}$

$\beta = \sqrt{2}-\sqrt{3}$

$-\beta = -\sqrt{2}+\sqrt{3}$

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

Suppose ϕ is any automorphism of E. Then $\phi(a) = a$ for all $a \in \mathbb{Q}$.

$$m(\phi(\alpha)) = \phi(\alpha)^4 - 10\phi(\alpha)^2 + 1 = \phi(\alpha^4 - 10\alpha^2 + 1) = \phi(0) = 0$$

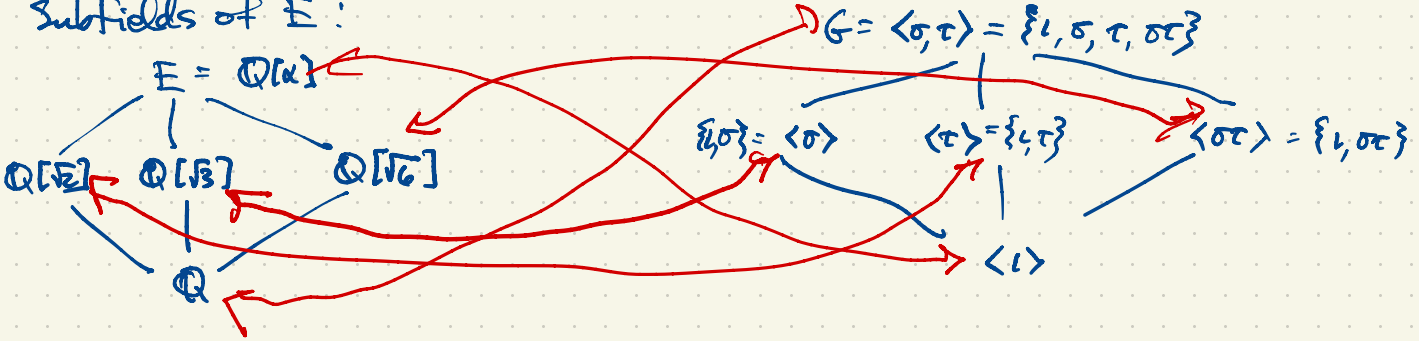
$\Rightarrow \phi(\alpha) \in \{\alpha, -\alpha, \beta, -\beta\}$. $\Rightarrow \phi = 1, \sigma\tau, \tau, \sigma$ respectively

since ϕ is determined by its action on a basis

As above $E = \mathbb{Q}[\alpha, \beta]$, $\alpha = \sqrt{2} + \sqrt{3}$, $\beta = \sqrt{2} - \sqrt{3}$ containing $\frac{1}{2}(\alpha+\beta) = \sqrt{2}$ and $\frac{1}{2}(\alpha-\beta) = \sqrt{3}$

$= \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Subfields of E:



$G = \mathrm{Aut}\, E = \{$ automorphisms of the field $E\}$ is a group.

If $[E:\mathbb{Q}] = n$ then $|G| \leq n$.

What is $\mathrm{Aut}\,\mathbb{Q}$? $\mathrm{Aut}\,\mathbb{R}$? $\mathrm{Aut}\,\mathbb{C}$?

If $\phi: \mathbb{Q} \to \mathbb{Q}$ is an isomorphism (i.e. an automorphism of $\mathbb{Q}$) then $\phi(a) = a$ for all $a \in \mathbb{Q}$ as explained before, i.e. $\phi = \iota$ = identity function. $\mathrm{Aut}\,\mathbb{Q} = \{\iota\}$.

If $\phi: \mathbb{C} \to \mathbb{C}$ is an automorphism then $\phi = \iota$ or τ or $\cdots$

$\iota(z) = z$

$\tau(z) = \bar{z}$ where $\tau(a+bi) = a-bi$ for all $a, b \in \mathbb{R}$

τ is bijective since $\tau^{-1} = \tau$ i.e. $\tau^2 = \iota$ $\quad \tau(\tau(z)) = \bar{\bar{z}} = z$

$\tau(z+z') = \overline{z+z'} = \bar{z} + \bar{z}' = \tau(z) + \tau(z')$

$z, z' \in \mathbb{C}$

$\tau(zz') = \tau(z)\tau(z')$

$\overline{zz'} = \bar{z}\,\bar{z}'$

$\iota, \tau \in \mathrm{Aut}\,\mathbb{C}$ Are there other automorphisms?

Galois correspondence

Fact: If $E \supseteq \mathbb{Q}$ is a number field i.e. $n = [E:\mathbb{Q}] < \infty$ then E has at most n automorphisms.

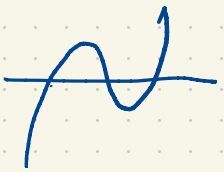
Why? later...

If $E \supseteq \mathbb{Q}$, $[E:\mathbb{Q}] = n$ with exactly n automorphisms (the maximum number) then the extension $E \supseteq \mathbb{Q}$ is called Galois. In this case there is a one-to-one correspondence between subgroups of $G = \mathrm{Aut}\, E$ and subfields of E.

Eg. $E = \mathbb{Q}[\alpha]$ where α is a root of $f(x) = x^3 - 3x + 1$.
$f(x)$ is irreducible in $\mathbb{Q}[x]$. $= (x-\alpha)(x-\beta)(x-\gamma)$
$[E:\mathbb{Q}] = 3$.

$E = \{a + b\alpha + c\alpha^2 : a,b,c \in \mathbb{Q}\}$
$1, \alpha, \alpha^2$ is a basis for E over $\mathbb{Q}$

We will show that E has 3 automorphisms.



$\alpha^3 - 3\alpha + 1 = 0 \Rightarrow \alpha^3 = 3\alpha - 1$
$\alpha^4 = 3\alpha^2 - \alpha$
$\alpha^5 = 3\alpha^3 - \alpha^2 = 3(3\alpha-1) - \alpha^2$
$= -\alpha^2 + 9\alpha - 3$
$\alpha^6 = -\alpha^3 + 9\alpha^2 - 3\alpha$
$= -(3\alpha - 1) + 9\alpha^2 - 3\alpha$
$= 9\alpha^2 - 6\alpha + 1$

Alternatively
$\alpha^6 = (\alpha^3)^2 = (3\alpha-1)^2$
$= 9\alpha^2 - 6\alpha + 1$

$G = \mathrm{Aut}\, E = \{1, \sigma, \sigma^2\}$, $\sigma^3 = 1$
G is cyclic of order 3.

We'll see that $\beta = \alpha^2 - 2$ is also a root of $f(x)$. $\beta \in \mathbb{Q}[\alpha]$ since $\beta = \alpha^2 - 2$

$f(\beta) = \beta^3 - 3\beta + 1$
$= (\alpha^2-2)^3 - 3(\alpha^2-2) + 1$
$= (\alpha^6 - 6\alpha^4 + 12\alpha^2 - 8) + (-3\alpha^2 + 6) + 1$
$= \alpha^6 - 6\alpha^4 + 9\alpha^2 - 1$
$= (9\alpha^2 - 6\alpha + 1) - 6(3\alpha^2 - \alpha) + 9\alpha^2 - 1$
$= 0$

$\mathbb{Q} \subseteq \mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha]$
since $\gamma = \beta^2 - 2$
since $\alpha = \gamma^2 - 2$
$\Rightarrow \mathbb{Q}[\alpha] = \mathbb{Q}[\beta] = \mathbb{Q}[\gamma]$.

But can $\beta = \alpha$ (same root)? We must have $\beta \neq \alpha$ since $1, \alpha, \alpha^2$ are lin. indep.

(Or: if $\alpha = \beta = \alpha^2 - 2$ then $\alpha^2 - \alpha - 2 = 0$, a contradiction since the minimal poly. of α.)

Note that $\gamma = \beta^2 - 2$ must also be a root of $f(x)$.
Also $\delta = \gamma^2 - 2$ is also a root. Same argument as before.

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

$\delta = \gamma^2 - 2$
$= (-\alpha^2 - \alpha + 2)^2 - 2 = \alpha^4 + \alpha^2 + 4 + 2\alpha^3 - 4\alpha^2 - 4\alpha - 2$
$= \alpha^4 + 2\alpha^3 - 3\alpha^2 - 4\alpha + 2$
$= (3\alpha^2 - \alpha) + 2(3\alpha - 1) - 3\alpha^2 - 4\alpha + 2$
$= \alpha$

In the example above, $E = \mathbb{Q}[\alpha] = \mathbb{Q}[\beta] = \mathbb{Q}[\gamma]$ has exactly three automorphisms.

$G = \mathrm{Aut}\, E = \{1, \sigma, \sigma^2\}$, $\sigma : \alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$. (3-cycle) like $(1,2,3) \in S_3$.

Given $u = a + b\alpha + c\alpha^2 \in E$, $a, b, c \in \mathbb{Q}$, $\sigma(u) = \sigma(a + b\alpha + c\alpha^2) = \underbrace{\sigma(a)}_{a} + \underbrace{\sigma(b\alpha)}_{\sigma(b)\sigma(\alpha) = b\sigma(\alpha) = b\beta} + \underbrace{\sigma(c\alpha^2)}_{\sigma(c)\sigma(\alpha)^2 = c\beta^2}$

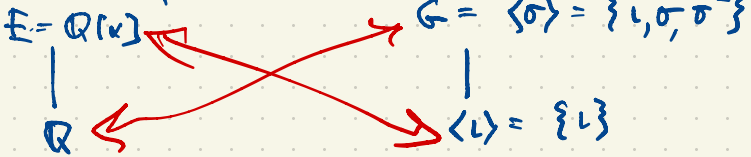
$= a + b\beta + c\beta^2$

$\sigma^2(u) = a + b\gamma + c\gamma^2$

$\sigma^3(u) = u$, $\sigma^3 = 1$

$E \supset \mathbb{Q}$ is a Galois extension with $|G| = 3 = [E : \mathbb{Q}]$.

Galois correspondence between subfields of E and subgroups of G:

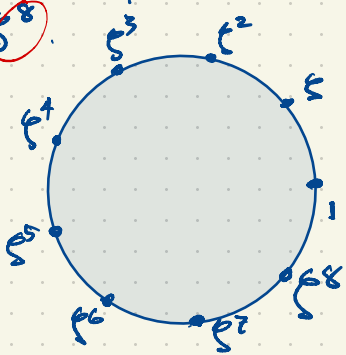


Where does the map $\alpha \mapsto \alpha^2 - 2$ come from? Look at $\mathbb{Q}[\zeta]$, ζ is a primitive 9th root of unity. In $\mathbb{C}$, the roots of $x^9 - 1$ are $1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8$.

$1, \zeta^3, \zeta^6$ imprimitive 9th roots of 1.

min. poly. $x - 1$; primitive cube roots, $x^2 + x + 1$

six primitive 9th roots of 1. roots of $x^6 + x^3 + 1$



$x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1)$

root 1; roots ζ^3, ζ^6; roots $\zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8$