Fields

Book II

Eg. $\alpha = \sqrt{2+\sqrt{2}}$

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

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

$\alpha^4 - 4\alpha^2 + 4 = 2$

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

The minimal poly. of α over $\mathbb{Q}$ is $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

(Exercise: $f(x)$ is irreducible in $\mathbb{Q}[x]$ so it really is the min. poly. of α over $\mathbb{Q}$.)

The roots of $f(x)$ are

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

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

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

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

$$f(x) = x^4 - 4x^2 + 2 = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$$

In this case $E = \mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3 : a,b,c,d \in \mathbb{Q}\}$ contains all the roots of $f(x)$ so it is a normal extension of $\mathbb{Q}$. $\beta = (*) + (*)\alpha + (*)\alpha^2 + (*)\alpha^3 = \alpha^3 - 3\alpha$

$\alpha\beta = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{4-2} = \sqrt{2} = \alpha^2 - 2$

$\Rightarrow \beta = \dfrac{\alpha^2-2}{\alpha} \in \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$

$\beta = \alpha - \frac{2}{\alpha} = \alpha - (4\alpha - \alpha^3) = \alpha^3 - 3\alpha$

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

$\alpha^3 - 4\alpha + \frac{2}{\alpha} = 0 \Rightarrow \frac{2}{\alpha} = 4\alpha - \alpha^3$

$\alpha^4 = 4\alpha^2 - 2$

$\alpha^6 = 4\alpha^4 - 2\alpha^2$

$= 4(4\alpha^2 - 2) - 2\alpha^2$

$= 14\alpha^2 - 8$

Look for an automorphism $\sigma : E \to E$ $(E = \mathbb{Q}[\alpha])$ satisfying $\sigma(\alpha) = \beta$.

$\sigma(\beta) = \sigma(\alpha^3 - 3\alpha) = \sigma(\alpha)^3 - 3\sigma(\alpha) = \beta^3 - 3\beta = (\alpha^3-3\alpha)^3 - 3(\alpha^3 - 3\alpha) = (\alpha^3-3\alpha)((\alpha^3-3\alpha)^2 - 3)$

$= (\alpha^3-3\alpha)(\alpha^6 - 6\alpha^4 + 9\alpha^2 - 3) = (\alpha^3-3\alpha)(14\alpha^2 - 8 - 6(4\alpha^2-2) + 9\alpha^2 - 3) = (\alpha^3-3\alpha)(-\alpha^2+1) = \alpha(\alpha^2-3)(-\alpha^2+1)$

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

$\sigma(\sqrt{2}) = ?$

$\sqrt{2} = \alpha\beta$

$\sigma(\sqrt{2}) = \sigma(\alpha)\sigma(\beta)$

$= \beta\cdot(-\alpha)$

$= -\alpha\beta$

$= -\sqrt{2}$

$\sigma(\alpha) = \beta$

$\sigma(-\alpha) = -\sigma(\alpha) = -\beta$

$\sigma(\beta) = -\alpha$

$\sigma(-\beta) = -\sigma(\beta) = -(-\alpha)$

$= \alpha$

$\sigma : \alpha \longmapsto \beta = \alpha^3 - 3\alpha \longmapsto -\alpha \longmapsto -\beta \longmapsto \alpha$

Aut $E = \langle\sigma\rangle$ of order 4; cyclic.

$G = \text{Aut}\,E = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \sigma^3\}$

Galois correspondence

$$\begin{array}{ccc}
\mathbb{Q}[\alpha] & & G \\
2\,| & & 2\,| \\
\mathbb{Q}[\sqrt{2}] & & \langle\sigma^2\rangle = \{1, \sigma^2\} \\
2\,| & & 2\,| \\
\mathbb{Q} & & \langle 1\rangle
\end{array}$$

$\sigma^2(\sqrt{2}) = \sigma(\sigma(\sqrt{2}))$

$= \sigma(-\sqrt{2}) = \sqrt{2}$.

$\sigma(\sqrt{2}) = \sigma(\alpha^2 - 2)$

$= \sigma(\alpha)^2 - 2 = \beta^2 - 2 = -\sqrt{2}$.

Compare:

$$\begin{array}{ccc} E = \mathbb{Q}[\sqrt{2}] & & G = \langle \tau \rangle \\ 2 \big| & & \big| 2 \\ \mathbb{Q} & & \langle \iota \rangle \end{array}$$

$G = \mathrm{Aut}\, E = \{\iota, \tau\}$, $\tau(a+b\sqrt{2}) = a-b\sqrt{2}$

Degree 2 extension : quadratic extension
" 3 " : cubic "
" 4 " : quartic "
" 5 " : quintic "

$\alpha = \sqrt[3]{2} = 2^{1/3}$

$E = \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ is an extension of degree $[E:\mathbb{Q}] = 3$
with basis $1, \underset{\sqrt[3]{2}}{\underset{\parallel}{\alpha}}, \alpha^2 = \sqrt[3]{4}$ $\quad (\alpha^3 = 2)$

α has min. poly. $x^3 - 2 \in \mathbb{Q}[x]$ which is irreducible

In $\mathbb{R}[x]$, $f(x) = x^3 - 2 = (x-\alpha)(x^2 + \alpha x + \alpha^2)$

Subfields

$$\begin{array}{c} E = \mathbb{Q}[\alpha] \\ \big| 3 \\ \mathbb{Q} \end{array}$$

If $E \supseteq F \supseteq \mathbb{Q}$ (i.e. F is an intermediate field) then the transitivity of degrees tells us $\underbrace{[E:\mathbb{Q}]}_{3} = [E:F][F:\mathbb{Q}]$

$$3 \times 1 \quad \text{or} \quad 1 \times 3$$

If $[F:\mathbb{Q}] = 1$ then $\{1\}$ is a basis for F over $\mathbb{Q}$ so $F = \{a1 : a \in \mathbb{Q}\} = \mathbb{Q}$

If $[E:F] = 1$ then (similarly) $E = F$.

More generally if $E \supseteq F$ is an extension of prime degree $p = [E:F]$ then the only intermediate extensions are E and F.

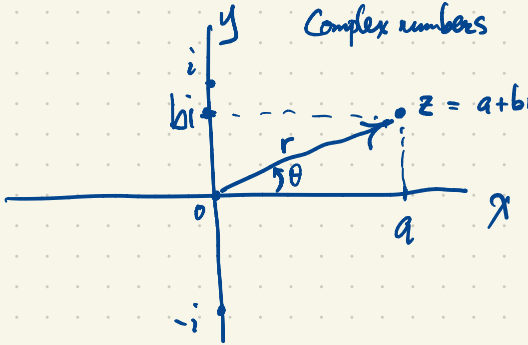
What are the automorphisms of $E = \mathbb{Q}[\alpha]$, $\alpha = \sqrt[3]{2}$? If $\phi \in \mathrm{Aut}\, E$ then $\phi(\alpha)^3 = \phi(\alpha^3) = \phi(2) = 2$

In $\mathbb{C}$, every poly. $f(x) \in \mathbb{C}[x]$ of degree n factors as $f(x) = a(x-r_1)(x-r_2)\cdots(x-r_n)$ $(a, r_1, r_2, \dots, r_n \in \mathbb{C})$.

eg. $x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)\cdots(x-\zeta^{n-1})$ where $\zeta = e^{2\pi i/n}$.

de Moivre's formula: $e^{i\theta} = \cos\theta + i\sin\theta$

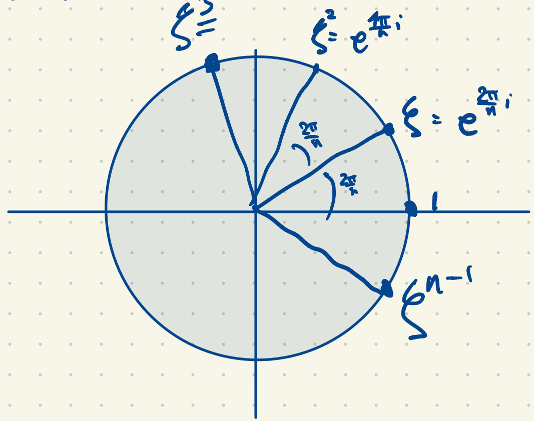
Complex numbers $\mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}$, $i = \sqrt{-1}$



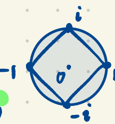
Every $z \in \mathbb{C}$ has unique representation as $z = a+bi$ $(a,b \in \mathbb{R})$ in rectangular coordinates

$a = \operatorname{Re} z$ = real part of z
$b = \operatorname{Im} z$ = imaginary part of z.
$r = |z| = \sqrt{a^2+b^2}$

The roots of $x^n - 1$ are the n^{th} roots of unity: $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ forming the vertices of a regular n-gon inscribed in the unit circle $|z| = 1$.



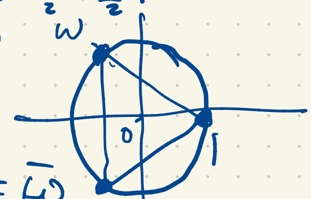
Eg. $n=4$
The fourth roots of unity are $\pm 1, \pm i$
$1, e^{\frac{i\pi}{2}} = i, e^{\frac{2i\pi}{2}} = e^{i\pi} = -1, e^{\frac{3i\pi}{2}} = -i$



Euler's Formula $e^{i\pi} = -1$

$e^{i\pi} + 1 = 0$

Eg. $n=3$: The three cube roots of unity in $\mathbb{C}$ are $1, \omega, \omega^2$ where
$\omega = e^{\frac{2\pi i}{3}} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$
$x^3 - 1 = (x-1)(x^2+x+1) = (x-1)(x-\omega)(x-\omega^2)$
$\omega = \frac{-1 \pm \sqrt{-3}}{2}$

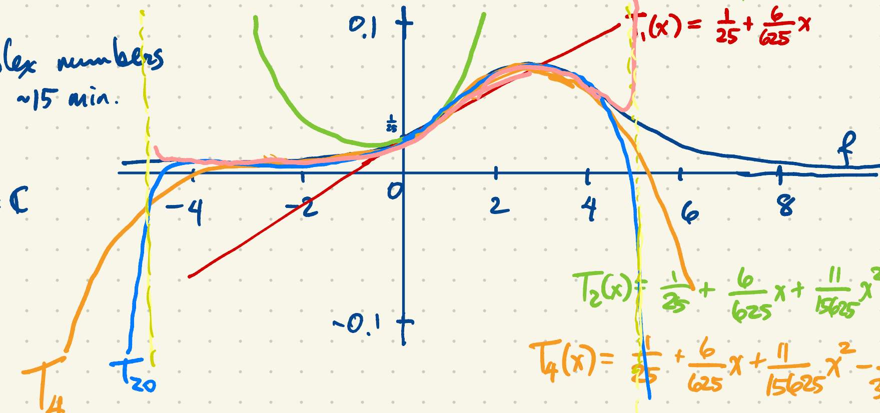


$\omega^2 = \overline{\omega}$

Follow links on course website
instructional videos $\longrightarrow$ complex numbers
~15 min.

Eg. consider $f(x) = \dfrac{1}{x^2-6x+25}$

This function has poles at $x = 3 \pm 4i \in \mathbb{C}$
with $|3 \pm 4i| = 5$



$T_1(x) = \frac{1}{25} + \frac{6}{625}x$

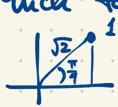
$T_2(x) = \frac{1}{25} + \frac{6}{625}x + \frac{11}{15625}x^2$

$T_4(x) = \frac{1}{25} + \frac{6}{625}x + \frac{11}{15625}x^2 - \frac{84}{390625}x^3 - \frac{779}{9765625}x^4$

By the Binomial Theorem

$(1+i)^{11} = 1 + 11i - 55 - 165i + 330 + 462i - 462 - 330i + 165 + 55i - 11 - i = -32 + 32i$

Much ~~faster~~ way to evaluate powers $z^n = (x+iy)^n = x^n + nx^{n-1}yi + \cdots + i^n y^n$ (Binomial Theorem)



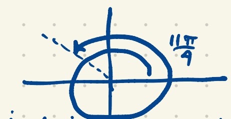
$1+i = \sqrt{2}e^{i\frac{\pi}{4}}$

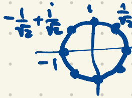
$|1+i| = \sqrt{1^2+1^2} = \sqrt{2}$

$(1+i)^{11} = \left(\sqrt{2}e^{\frac{i\pi}{4}}\right)^{11} = 32\sqrt{2}\, e^{\frac{i11\pi}{4}}$

$= 32\sqrt{2} \cdot \left(\frac{-1+i}{\sqrt{2}}\right)$

$= -32 + 32i$





$\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}} = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}$ eighth root of unity

$\zeta = \frac{1+i}{\sqrt{2}}$

$\zeta^{11} = \zeta^3 = \frac{-1+i}{\sqrt{2}}$

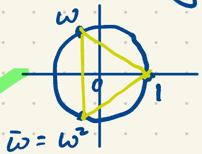
n^{th} roots of $z = re^{i\theta}$, $r = |z|$

all complex numbers whose n^{th} power is z

$z^{\frac{1}{n}} = r^{\frac{1}{n}}e^{\frac{i\theta}{n}},\ r^{\frac{1}{n}}e^{\frac{i\theta}{n}+\frac{2\pi i}{n}},\ r^{\frac{1}{n}}e^{\frac{i(\theta+4\pi)}{n}},\ \ldots,\ r^{\frac{1}{n}}e^{i\frac{\theta+2(n-1)\pi}{n}}$

i.e. $r^{\frac{1}{n}}e^{i\frac{\theta+2k\pi}{n}}$, $k = 0, 1, 2, \ldots, n-1$

Cube roots of unity in $\mathbb{C}$: $1, \omega, \omega^2 = \bar{\omega}$



$$\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2} = \frac{-1}{2} + \frac{\sqrt{3}}{2} i$$

$$\omega^2 + \omega + 1 = 0$$

ω is a root of $x^3 - 1 = (x-1)(x^2+x+1) = (x-1)(x-\omega)(x-\omega^2)$

$\tau(\omega) = \omega^2$

$\mathbb{Q}[\omega] \quad G = \langle \tau \rangle$

$2 \mid \qquad 2 \mid$

$\mathbb{Q} \quad \langle \iota \rangle$

Galois correspondence

$G = \operatorname{Aut} \mathbb{Q}[\omega] = \langle \tau \rangle = \{\iota, \tau\}$

where $\tau(z) = \bar{z}$

Now let $\alpha = \sqrt[3]{2}$, $\quad F = \mathbb{Q}[\alpha]$.

The min. poly. of α over $\mathbb{Q}$ is $x^3 - 2 \in \mathbb{Q}[x]$.

$F = \mathbb{Q}[\alpha] = \{ a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q} \}$, $\quad \operatorname{Aut} F = \{\iota\}$

$3 \mid$

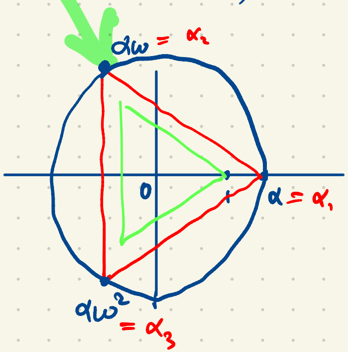
$\mathbb{Q}$

$$x^3 - 2 = (x-\alpha)(x^2 + \alpha x + \alpha^2)$$

The other roots of x^3-2 are not in $F = \mathbb{Q}[\alpha]$ i.e. the extension $F \supset \mathbb{Q}$ is not normal.

Scale by factor of α

$x^3 - 2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ where $\alpha_1 = \alpha$, $\quad \alpha_2 = \alpha\omega$, $\quad \alpha_3 = \alpha\omega^2$



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

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

basis $\{1, \omega\}$ so $[E:F] = 2$

basis $1, \alpha, \alpha^2$ so $[F:\mathbb{Q}] = 3$

$$E \supset F \supset \mathbb{Q}$$

$E = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha, \omega]$, $\quad F = \mathbb{Q}[\alpha]$

$[E : \mathbb{Q}] = 2 \cdot 3 = 6$

$\omega = \frac{1}{2}\alpha_1^2\alpha_2$
$= \frac{1}{2} \cdot 2^{2/3} \cdot 2^{1/3}\omega$
$= \omega$

There are $3! = 6$ permutations of $\alpha_1, \alpha_2, \alpha_3$.

x	$\sigma(x)$	$\tau(x)$
α_1	α_2	α_1
α_2	α_3	α_3
α_3	α_1	α_2
α	$\alpha\omega$	α
ω	ω	ω^2

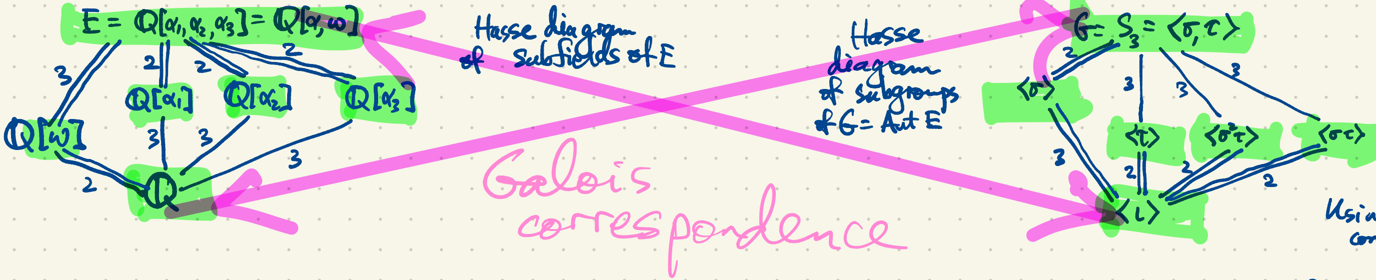
$\tau(x)$ ← complex conjugation

In $S_3 = \langle \sigma, \tau \rangle$, $\quad \sigma = (1\,2\,3)$, $\quad \tau = (2\,3)$.

$$\sigma(\omega) = \sigma\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\sigma(\alpha_2)}{\sigma(\alpha_1)} = \frac{\alpha_3}{\alpha_2} = \frac{\alpha\omega^2}{\alpha\omega} = \omega$$

$$\sigma\left(\frac{\alpha\omega}{\alpha}\right)$$

$$\tau(\omega) = \tau\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\alpha_3}{\alpha_1} = \frac{\alpha\omega^2}{\alpha} = \omega^2 = \bar{\omega}$$



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

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

Double lines indicate normality.

Using right-to-left composition

A subgroup $H \le G$ is <u>normal</u> if its left and right cosets agree i.e. $gH = Hg$ for all $g \in G$.

$\sigma^2\tau = (132)(23) = (13)$

$\sigma\tau = (123)(23) = (12)$

$\tau = (23)$

Eg. in $G = S_3$, $H = \langle\sigma\rangle = \langle(123)\rangle$ is normal.

eg. $(12)H = (12)\{\underset{id}{()},\ \underset{\sigma}{(123)},\ \underset{\sigma^2}{(132)}\} = \{(12), (23), (13)\}$

$(12)(123) = (1)(23) = (23)$

$H(12) = \{(), (123), (132)\}(12) = \{(12), (13), (23)\}$

E is the <u>splitting field</u> of

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

$E = \mathbb{Q}[\alpha, \alpha\omega, \alpha\omega^2] = \mathbb{Q}[\alpha, \omega]$

$\langle\tau\rangle$ is a subgroup of G which is <u>not</u> normal in G.

$(13)\langle\tau\rangle = (13)\{(), (23)\} = \{(13), (132)\}$

$\langle\tau\rangle(13) = \{(), (23)\}(13) = \{(13), (123)\}$

The extension $\underset{\mathbb{Q}[\alpha_1]}{\mathbb{Q}[\alpha]} \supset \mathbb{Q}$ of degree $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ is <u>not</u> normal

since the min. poly. of α over $\mathbb{Q}$ is $x^3 - 2$

with $\mathbb{Q}[\alpha]$ containing only one of the three roots of $x^3 - 2$.

In $E = \mathbb{Q}[\alpha, \omega]$ the splitting field of $x^3-2 = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2)$, can we find a single element $\beta \in E$ generating E i.e. $E = \mathbb{Q}[\beta] = \{a_0 + a_1\beta + a_2\beta^2 + \cdots + a_5\beta^5 : a_0, a_1, \dots, a_5 \in \mathbb{Q}\}$?

Such an element β must be in E but not in $\mathbb{Q}[\omega] \cup \mathbb{Q}[\alpha] \cup \mathbb{Q}[\alpha\omega] \cup \mathbb{Q}[\alpha\omega^2]$.

In a 6-dimensional vector space, we must find a vector not contained in this union of four proper subspaces of dimension 2, 3, 3, 3 respectively.

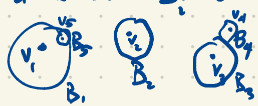
In $\mathbb{R}^3$, can $\mathbb{R}^3$ be a union of finitely many proper subspaces? No because each proper subspace of $\mathbb{R}^3$ has only dimension ≤ 2 so it covers a slice of the unit ball of volume 0. A finite union of proper subspaces covers zero volume of the unit ball; it can never cover the total volume $\frac{4}{3}\pi$ of the unit ball.

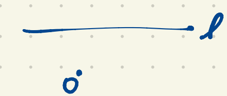
In $\mathbb{Q}^3$, i.e. points of $\mathbb{R}^3$ with rational coordinates, can $\mathbb{Q}^3 = U_1 \cup U_2 \cup U_3 \cup \cdots \cup U_k$ with $U_i \le \mathbb{Q}^3$ proper subspaces? The volume of $\mathbb{Q}^3$ (as a subset of $\mathbb{R}^3$) is zero.

$\mathbb{Q}^3 = \{v_1, v_2, v_3, v_4, \dots\}$ is countably infinite.

Let $\varepsilon > 0$. We will show that the volume of $\mathbb{Q}^3$ is at most ε.

Take a ball B_i of radius small enough centered at v_i such that its volume is less than $\frac{\varepsilon}{2^i}$. $(i = 1,2,3,4,\dots)$





$\bigcup_{i=1}^{\infty} B_i$ has volume $< \frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \frac{\varepsilon}{8} + \frac{\varepsilon}{16} + \cdots = \varepsilon$. Now $\mathbb{Q}^3 \subset \bigcup_{i=1}^{\infty} B_i$, so $\mathrm{Vol}(\mathbb{Q}^3) < \varepsilon$.

Try another approach. Suppose $\mathbb{Q}^3 = U_1 \cup U_2 \cup \cdots \cup U_k$, $U_i \le \mathbb{Q}^3$ proper distinct subspaces, so $\dim U_i \in \{0,1,2\}$.

Take a line $\ell \subset \mathbb{Q}^3$ not through the origin. Then ℓ is contained in at most one of the subspaces U_i. With careful choice we may assume ℓ is not contained in any U_i. (Not hard.) Each U_i intersects ℓ in at most one point. This is a contradiction.

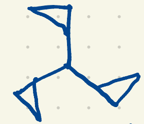
Galois theory handout: ignore "separable" for now.

Example of an extension $E \supset \mathbb{Q}$ of degree 3 with $G = \mathrm{Aut}\, E$ of order 3?

$f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ is irreducible

$f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ where $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$

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



has exactly 3 symmetries

Check that $\alpha^2 - 2$ is also a root of $f(x)$:

$f(\alpha^2-2) = (\alpha^2-2)^3 + (\alpha^2-2)^2 - 2(\alpha^2-2) - 1 = 0$ after collecting terms, so $\alpha^2 - 2 \in \{\alpha, \beta, \gamma\}$.

Can $\alpha^2 - 2 = \alpha$? No. If α is a root of $f(x) = x^3 + x^2 - 2x - 1$ and a root of $g(x) = x^2 - x - 2$ then α is a root of

$$\gcd(f(x), g(x)) = r(x) f(x) + s(x) g(x) \quad \text{by Euclid's Algorithm}$$

which is a factor of $f(x)$ of degree less than 3, a contradiction.

WLOG $\beta = \alpha^2 - 2$. Now $\beta^2 - 2$ is also a root of $f(x)$ by the same reasoning, so $\beta^2 - 2 \in \{\alpha, \beta, \gamma\}$.

As before, $\beta^2 - 2 \neq \beta$. If $\beta^2 - 2 = \alpha$ then $(\alpha^2-2)^2 - 2 = \alpha$: $\alpha^4 - 4\alpha^2 + 4 - 2 = \alpha$

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

but $\cancel{\gcd(x^3 + x^2 - 2x - 1,\ x^4 - 4x^2 - x + 2) = 1}$, contradiction. Better: $-1 - \alpha + 3\alpha^2 - 4\alpha^2 - \alpha + 2 = 0$

$$1 - 2\alpha - \alpha^2 = 0$$

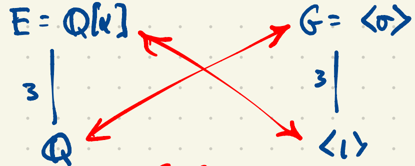
So $\beta^2 - 2 = \gamma$. Now $\gamma^2 - 2 = \alpha$. Indeed

$$\gamma^2 - 2 = (\beta^2-2)^2 - 2 = ((\alpha^2-2)^2-2)^2 - 2 = \alpha.$$

The map $x \mapsto x^2 - 2$ gives a cyclic permutation $\sigma: \alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$.

The field $E = \mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$ of degree $[E:\mathbb{Q}] = 3$ (a cyclic cubic extension)

has automorphism group $G = \mathrm{Aut}\, E = \langle \sigma \rangle = \{\iota, \sigma, \sigma^2\}$, cyclic of order 3.



Galois Correspondence

<u>Exercise</u>: Find three 3x3 matrices over $\mathbb{Q}$ A, B, C which are roots of $f(x)$ satisfying

$$B = A^2 - 2I \qquad A^3 + A^2 - 2A - I = 0$$
$$C = B^2 - 2I \qquad B^3 + B^2 - 2B - I = 0$$
$$A = C^2 - 2I \qquad C^3 + C^2 - 2C - I = 0.$$

(not HW)

In a finite (separable) extension $E \supseteq \mathbb{Q}$ of degree $[E : \mathbb{Q}] = n$, there exists $\beta \in E$ such that $E = \mathbb{Q}[\beta]$.

(don't worry about this technical condition for now)

degree $n < \infty$

(Theorem of the simple element or simple extension)

i.e. extension generated by a single element

Note: $\mathbb{C} \supset \mathbb{R}$ is a simple extension, $\mathbb{C} = \mathbb{R}[i]$.

$\mathbb{R} \supset \mathbb{Q}$ is not a simple extension. There is no $\beta \in \mathbb{R}$ satisfying $\mathbb{Q}[\beta] = \mathbb{R}$.

or $\mathbb{Q}(\beta) = \mathbb{R}$