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 $\mathbb{Q}$.

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

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

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

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

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

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

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

$\alpha^6 = 4\alpha^4 - 2\alpha^2$
$= 4(4\alpha^2 - 2) - 2\alpha^2$
$= 14\alpha^2 - 8$

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

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

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

$\mathrm{Aut}\, E = \langle\sigma\rangle$ of order 4; cyclic.

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

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

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

$\sigma(\alpha) = \beta$

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

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

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

Galois correspondence

$$\begin{array}{ccc}
\mathbb{Q}[\alpha] & & G = \mathrm{Aut}\,E = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \sigma^3\} \\
2| & & 2| \\
\mathbb{Q}[\sqrt{2}] & & \langle\sigma^2\rangle = \{1, \sigma^2\} \\
2| & & 2| \\
\mathbb{Q} & & \langle 1 \rangle
\end{array}$$

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

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

Compare:

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

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

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 $1, \underset{\sqrt[3]{2}}{\overset{\shortparallel}{\alpha}}, \alpha^2 = \sqrt[3]{4}$ $(\alpha^3 = 2)$

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

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

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

3×1 or 1×3

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.

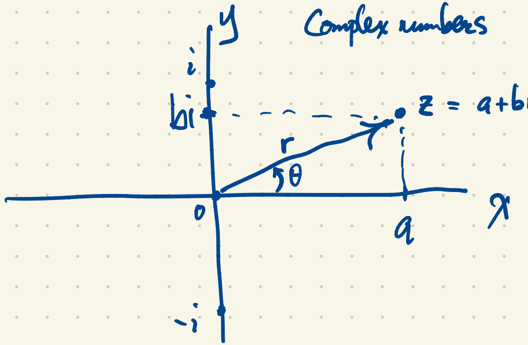
What are the automorphisms of $E = \mathbb{Q}[\alpha]$, $\alpha = \sqrt[3]{2}$? If $\phi \in \mathrm{Aut}\, E$ then $\phi(\alpha)^3 = \phi(\alpha^3) = \phi(2) = 2$

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

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

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

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



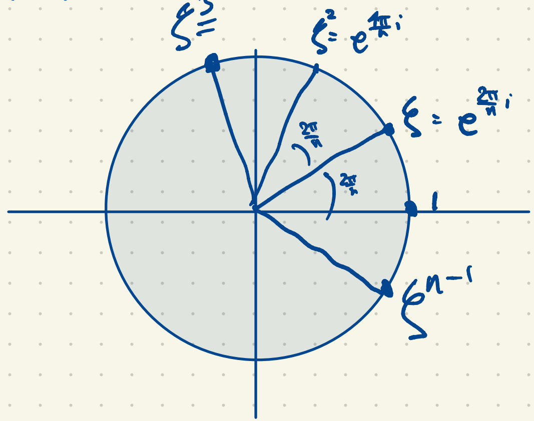
Every $z \in \mathbb{C}$ has unique representation as $z = a+bi$ $(a,b \in \mathbb{R})$ in rectangular coordinates

$a = \operatorname{Re} z$ = real part of z

$b = \operatorname{Im} z$ = imaginary part of z.

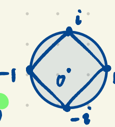
$r = |z| = \sqrt{a^2+b^2}$

The roots of x^n-1 are the n^{th} roots of unity: $1, \xi, \xi^2, \ldots, \xi^{n-1}$ 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 $e^{i\pi} = -1$

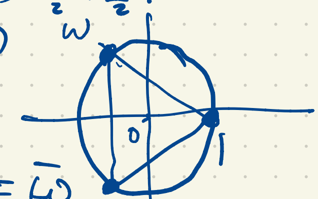
$e^{i\pi} + 1 = 0$

Eg. n=3: The three cube roots of unity in $\mathbb{C}$ are $1, \omega, \omega^2$ where

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

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

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

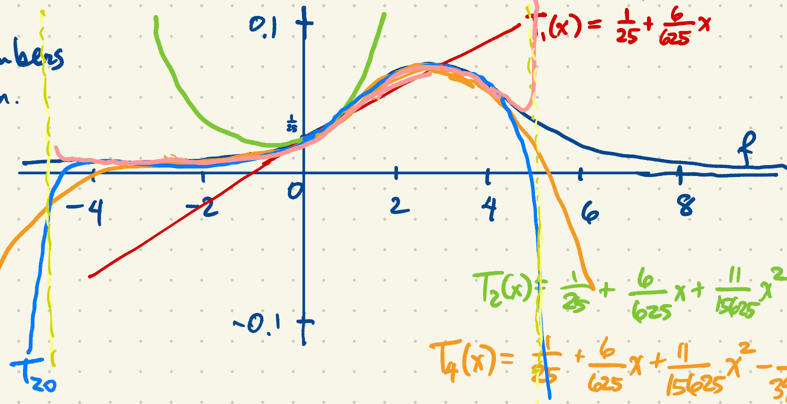


$\omega^2 = \overline{\omega}$

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 $|3 \pm 4i| = 5$



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

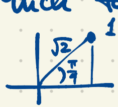
$T_2(x) = \frac{1}{25} + \frac{6}{625}x + \frac{11}{15625}x^2$

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

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)



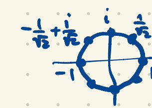
$1+i = \sqrt{2}e^{\frac{i\pi}{4}}$

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

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

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

$= -32 + 32i$



$= e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}$ 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. $r^{\frac{1}{n}}e^{i\frac{\theta+2k\pi}{n}}$, $k = 0, 1, 2, \ldots, n-1$