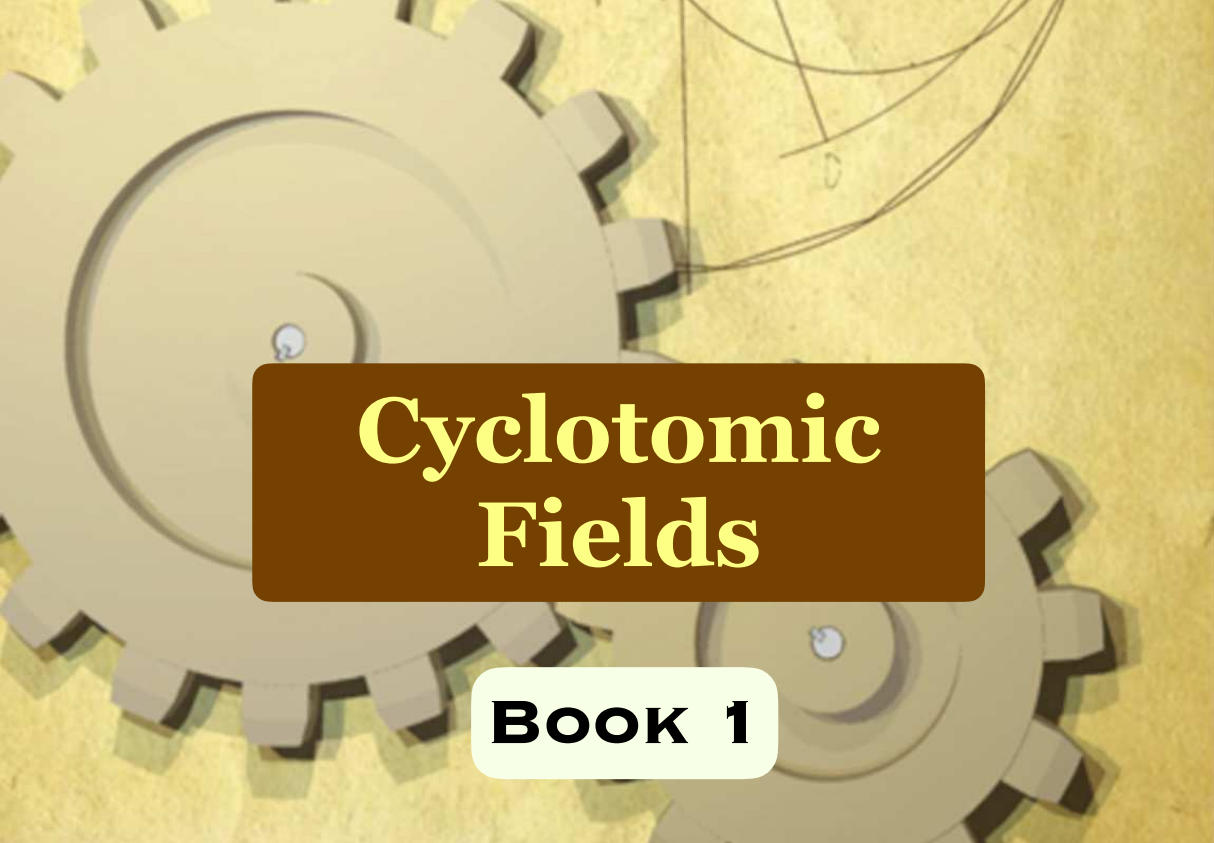


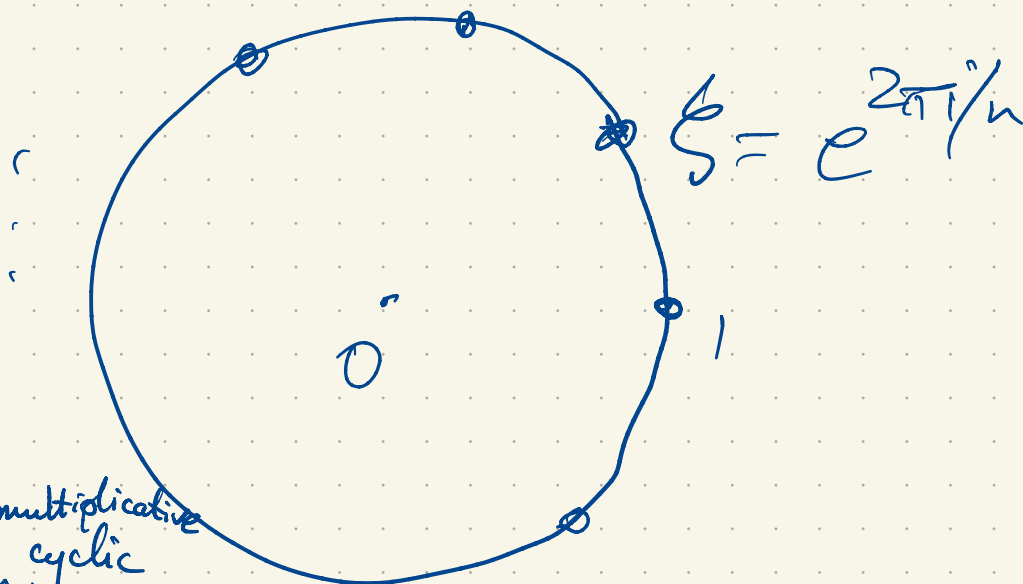


Cyclotomic Fields

Book 1

A (complex) n^{th} root of unity is a value $\xi \in \mathbb{C}$ satisfying $\xi^n = 1$.

$$\xi = e^{2\pi i \frac{k}{n}} = e^{2\pi i \frac{\phi}{\chi}}$$



Solutions of $z^n = 1$ form a ^{multiplicative} cyclic group of order n .

There are $\phi(n)$ primitive n^{th} roots of unity.

Euler's totient function

$\phi(n)$ = number of generators in any cyclic group of order n .

eg. $n=6$ $\phi(6) = 2$.

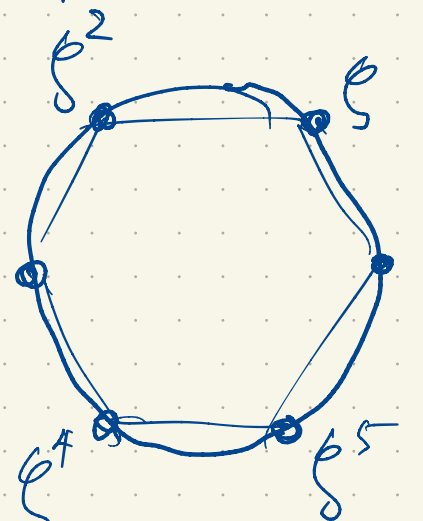
$$\phi(n) = |\{k \in \{1, 2, \dots, n\} : \gcd(k, n) = 1\}|$$

1, 5 relatively prime to 6.

All sixth roots of unity are ξ^k , $1 \leq k \leq n$. $-1 = \xi^3$

If $z^n = 1$ and $w^m = 1$ then $(zw)^{mn} = 1$

The product of an m^{th} root of unity with an n^{th} root of unity is an $(mn)^{\text{th}}$ root of unity (in fact an $\text{lcm}(m, n)^{\text{th}}$ root of unity).



A cyclotomic field is a field $\mathbb{Q}[\xi]$ where $\xi \in \mathbb{C}$ is a root of unity.

$$\xi^n = 1 \Rightarrow 1 + \xi + \xi^2 + \dots + \xi^{n-1} = 0$$

$$z^n - 1 = (z-1)(1 + z + z^2 + \dots + z^{n-1})$$

$$n=6: z^6 - 1 = \Phi_1(z) \Phi_2(z) \Phi_3(z) \Phi_6(z) \quad (\text{factorization into irreducible factors in } \mathbb{Q}[x] \text{ or } \mathbb{Z}[x])$$

Roots: $1, -1, \xi^2, \xi^4, \xi, \xi^5$
 primitive sixth roots of 1.

$\Phi_n(z)$ = minimal poly. of $\xi = e^{2\pi i/n}$ over $\mathbb{Q}$ (or over $\mathbb{Z}$)
 (simplest monic poly. with rational coefficients having ξ as a root)

$$z^n - 1 = \prod_{\substack{d|n \\ d \geq 1}} \Phi_d(z) \quad \text{product over all positive integer divisors of } n.$$

Divisors of 6 are $\pm 1, \pm 2, \pm 3, \pm 6$

Positive divisors of 6 are 1, 2, 3, 6.

$$\Phi_n(z) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (z - \xi^k) \quad \text{has as its roots the primitive } n^{\text{th}} \text{ roots of } 1.$$

$$\mathbb{Q}[\xi_n] = \{ \text{polynomials in } \xi \text{ with coefficients in } \mathbb{Q} \}$$

$$= \{ \text{linear combinations of } 1, \xi, \xi^2, \dots \text{ with rational coefficients} \}$$

$$= \{ \text{linear combinations of } 1, \xi, \xi^2, \dots, \xi^{n-1} \text{ with coefficients in } \mathbb{Q} \}$$

$$\xi = \xi_n = e^{2\pi i/n}$$

The roots of unity in $\mathbb{C}$ form a multiplicative group which is abelian but not cyclic.
 This multiplicative group is isomorphic to the additive group $\mathbb{Q}/\mathbb{Z}$.

$$\{\text{roots of unity in } \mathbb{C}\} = \{e^{i\alpha \cdot 2\pi} : \alpha \in \mathbb{Q}\} \quad \alpha \mapsto \alpha+1 \text{ doesn't change the value of } e^{i\alpha \cdot 2\pi}$$

The homomorphism $\mathbb{Q} \xrightarrow{f} \{\text{roots of unity}\}$ is onto but not one-to-one.
 $\alpha \mapsto e^{i\alpha \cdot 2\pi}$

By the first isomorphism theorem for groups, $\{\text{roots of unity}\} \cong \mathbb{Q}/\mathbb{Z}$.
 Integer linear combinations of roots of unity are cyclotomic integers. $\leftarrow \ker f$.
 This is a ring.

$\mathbb{Q}$ -linear combinations of roots of unity form a field, the field of cyclotomic numbers.
 Both these (ring and field) are countably infinite.

$i = \sqrt{-1}$ is a cyclotomic integer (a 4th root of unity)

$\sqrt{7}$ is a cyclotomic integer. (not really obvious)

$\sqrt[3]{7} = 7^{1/3}$ is not

$\xi = \xi_7 = e^{2\pi i/7}$ is a primitive 7th root of unity

$\alpha = \xi + \xi^2 + \xi^4$ is a cyclotomic integer

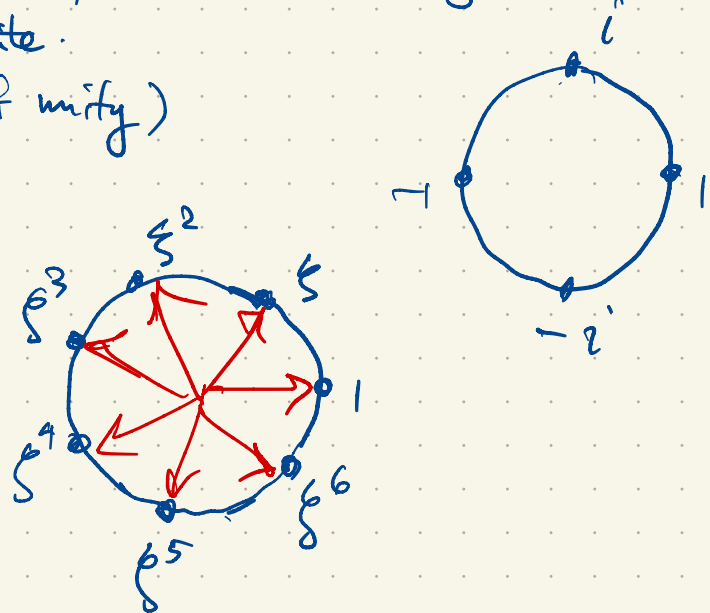
$$\alpha^2 = \xi^2 + \xi^4 + \xi + 2\xi^3 + 2\xi^5 + 2\xi^6$$

$$0 = 2 + 2\xi + 2\xi^2 + 2\xi^3 + 2\xi^4 + 2\xi^5 + 2\xi^6$$

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

$$\alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha = \frac{-1 \pm \sqrt{1-8}}{2} = \frac{-1 \pm \sqrt{-7}}{2} = \frac{-1 \pm i\sqrt{7}}{2}$$

$$2\alpha + 1 = \pm i\sqrt{7}$$



$$2\alpha + 1 = \pm i\sqrt{7}$$

$$\mp i(2\alpha + 1) = \sqrt{7}$$

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

$$\mp i(2\alpha + 1) = \mp i(1 + 2e^{2\pi i/7} + 2e^{4\pi i/7} + 2e^{8\pi i/7}) = \sqrt{7}$$

$$= \pm \left(2\sin\frac{2\pi}{7} + 2\sin\frac{4\pi}{7} + \sin\frac{8\pi}{7} \right) + i(\dots)$$

$$2.645751311\dots$$

$$\sqrt{7} = 2\sin\frac{2\pi}{7} + 2\sin\frac{4\pi}{7} + 2\sin\frac{8\pi}{7} \text{ is a cyclotomic integer.}$$

$$2\sin\frac{2\pi}{7} = -i(\xi - \xi^6) = -i\left[\left(\cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}\right) - \left(\cos\frac{2\pi}{7} - i\sin\frac{2\pi}{7}\right)\right]$$

Let $\xi = \xi_n$ primitive n^{th} root of unity, so the roots of $z^n = 1$ are $1, \xi, \xi^2, \dots, \xi^{n-1}$
 e.g. $\xi = e^{2\pi i/n}$. The primitive n^{th} roots of unity are ξ^k , $1 \leq k \leq n$, $\gcd(k, n) = 1$.
 The number of primitive n^{th} roots of unity is $\phi(n)$ Euler's totient function.

They are the roots of the n^{th} cyclotomic polynomial $\Phi_n(z) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (z - \xi^k) \in \mathbb{Z}[x]$

n	$\Phi_n(z)$
1	$z - 1$
2	$z + 1$
3	$z^2 + z + 1$
4	$z^2 + 1$
5	$z^4 + z^3 + z^2 + z + 1$
6	$z^2 - z + 1$
7	$z^6 + z^5 + \dots + z + 1$
8	$z^4 + 1$
9	$z^6 + z^3 + 1$
10	$z^4 - z^3 + z^2 - z + 1$
11	$z^{10} + z^9 + z^8 + \dots + z + 1$

If p is prime, $\Phi_p(z) = z^{p-1} + z^{p-2} + \dots + z + 1$

$\Phi_n(z)$ is irreducible in $\mathbb{Z}[z]$ and in $\mathbb{Q}[z]$ for all n .
 (If $n = p$ is prime, this uses Eisenstein)

If $m(x) \in \mathbb{Q}[x]$ is irreducible of degree n then $m(x) = (x-\alpha_1) \cdots (x-\alpha_n)$, and $\alpha = \alpha_1$ say, (α algebraic)

$\mathbb{Q} \subset \mathbb{Q}[\alpha] = \{ \text{polynomials in } \alpha \text{ with rational coefficients} \}$

Since $\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ ($a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$), $\mathbb{Q}[\alpha] = \{ c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_0, \dots, c_{n-1} \in \mathbb{Q} \}$

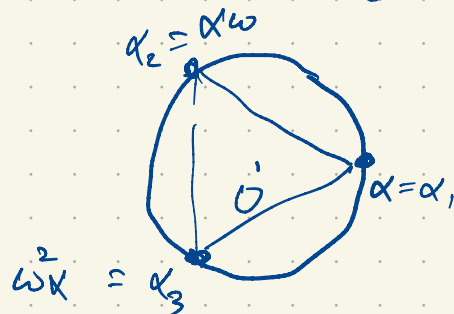
$\mathbb{Q}[\alpha]$ is a field with basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ over $\mathbb{Q}$

$\mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ is an extension field of degree n , i.e. dimension n .

All the fields $\mathbb{Q}[\alpha_i]$ ($i=1, 2, \dots, n$) are isomorphic but not necessarily equal.

eg. $m(x) = x^3 - 7 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
 $\uparrow$
 $\alpha_1 = \alpha = 7^{1/3}$

There are three complex cube roots of 7 but only one of them is real.



$$\omega = \zeta_3 = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}$$

$$\alpha_2^3 = (\alpha\omega)^3 = \alpha^3\omega^3 = 7$$

$$\mathbb{Q}[\alpha] \cong \mathbb{Q}[x] / (m(x)) = \{ c_0 + c_1x + c_2x^2 \bmod m(x) = x^3 - 7 : c_0, c_1, c_2 \in \mathbb{Q} \}$$

For $\xi = \zeta_7$, $m(x) = \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x-\xi)(x-\xi^2) \cdots (x-\xi^6)$

$$\mathbb{Q}[\xi] = \mathbb{Q}[\xi^2] = \mathbb{Q}[\xi^3] = \mathbb{Q}[\xi^4] = \mathbb{Q}[\xi^5] = \mathbb{Q}[\xi^6]$$

If $\xi = \zeta_n$ then $\mathbb{Q}[\xi]$ has $\phi(n)$ automorphisms $f_k(\xi) = \xi^k$ $1 \leq k \leq n$, $\phi(k) = n$.

An automorphism of a field F is a bijection $f: F \rightarrow F$ such that

$$\begin{aligned} f(\alpha + \beta) &= f(\alpha) + f(\beta) \\ f(\alpha\beta) &= f(\alpha)f(\beta) \end{aligned} \quad \text{for all } \alpha, \beta \in F.$$

If $F \supseteq \mathbb{Q}$ is an extension of degree n then F has at most n automorphisms.

$\mathbb{Q}[\xi_7] \supset \mathbb{Q}$ is an extension of degree 6 basis $1, \xi, \xi^2, \dots, \xi^5$ $\xi^6 = -1 - \xi - \xi^2 - \xi^3 - \xi^4 - \xi^5$

This field has exactly 6 automorphisms.

If $f \in \text{Aut } \mathbb{Q}[\xi]$, $\xi \mapsto \xi_j$ i.e. f any automorphism then $f(\xi) \in \{\xi, \xi^2, \dots, \xi^6\}$

$$\begin{aligned} \xi^7 &= 1 \Rightarrow f(\xi^7) = f(1) = 1 \\ f(\xi)^7 &= f(\xi)f(\xi)\dots f(\xi) = f(\xi^7) = 1 \end{aligned}$$

$$\begin{aligned} f(0) &= f(0+0) = f(0) + f(0) \Rightarrow f(0) = 0 \\ f(1) &= f(1^2) = f(1 \cdot 1) = f(1)f(1) \Rightarrow f(1) = 1 \end{aligned}$$

Minimal polynomial of $\xi = \xi_7$ over $\mathbb{Q}$ is $m(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = \Phi_7(x) = (x - \xi)(x - \xi^2) \dots (x - \xi^6)$

$$\text{Aut } \mathbb{Q}[\xi] = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

$$f_j(\xi) = \xi^j$$

$$f_3 f_2 = f_2 f_3 = f_2 \circ f_3 = f_6$$

$$f_2 f_3(\xi) = f_2(\xi^3) = f_2(\xi^3) = f_2(\xi^3) = (\xi^2)^3 = \xi^6$$

$$\begin{aligned} f_2^2 &= f_2 \circ f_2 = f_4 \\ f_2^3 &= f_2 \circ f_2 \circ f_2 = f_6 = f_1 \end{aligned}$$

$\text{Aut } \mathbb{Q}[\xi_n]$ is abelian

$$\begin{aligned} \text{Aut } \mathbb{Q}[\xi_n] &\cong \underbrace{(\mathbb{Z}/n\mathbb{Z})^\times}_{0, 1, \dots, n \text{ under addition mod } n \text{ (a ring)}} = \{k \in \mathbb{Z} : 1 \leq k \leq n, \gcd(k, n) = 1\} \text{ abelian group of order } \phi(n) \\ &= [\mathbb{Q}[\xi_n] : \mathbb{Q}] \end{aligned}$$

Whenever R is a ring with identity, $R^\times = \{\text{units in } R\}$ is a multiplicative group.

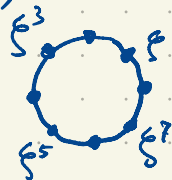
$$\mathbb{Z}^\times = \{\pm 1\}$$

$$\{n \times n \text{ real matrices}\}^\times = GL_n(\mathbb{R}) = \{\text{invertible } n \times n \text{ real matrices}\}$$

$$\text{Aut } \mathbb{Q}[\xi_8] = \{f_1, f_3, f_5, f_7\}$$

$$f_j(\xi) = \xi^j$$

$$\xi = \xi_8 = e^{2\pi i/8} = \frac{1+i}{\sqrt{2}}$$



$$\xi^2 = i \text{ has min. poly. } x^2 + 1$$

$$(x-\xi)(x-\xi^3)(x-\xi^5)(x-\xi^7) = x^4 + 1 \text{ is the min. poly. of } \xi$$

$$f_7(\xi) = \xi^7 = \bar{\xi}$$

$$f_7(z) = \bar{z}$$

$$| \text{Aut } E | = [E : \mathbb{Q}]$$

Kronecker-Weber Theorem Every Galois extension $E \supset \mathbb{Q}$ having an abelian group $\text{Aut } E$ is a subfield of a cyclotomic extension: $E \subseteq \mathbb{Q}[\xi_n]$ for some n .

Converse is easy: $\text{Aut } \mathbb{Q}[\xi_n]$ is abelian and if $E \subseteq \mathbb{Q}[\xi_n]$ then $\text{Aut } E$ is abelian.

Eg: $\sqrt{7} \notin \mathbb{Q}$; $\sqrt{7}$ generates the extension $E = \mathbb{Q}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Q}\}$.

$$\text{Aut } E = \{1, \sigma\}$$

$$\sigma^2 = 1$$

$$\sigma(a + b\sqrt{7}) = a - b\sqrt{7} \text{ where } a, b \in \mathbb{Q}$$

$$1(a + b\sqrt{7}) = a + b\sqrt{7}$$

$$= (x - \sqrt{7})(x + \sqrt{7})$$

$$\sqrt{7} \text{ has min. poly. } m(x) = x^2 - 7 \in \mathbb{Q}[x].$$

$$m(\sqrt{7}) = 0$$

$$\text{If } f \in \text{Aut } E \text{ then } m(f(\sqrt{7})) = f(\sqrt{7})^2 - 7 = f(\sqrt{7}^2) - 7 = f(7) - 7 = 7 - 7 = 0$$

$$\Rightarrow f(\sqrt{7}) \in \{\sqrt{7}, -\sqrt{7}\}$$

$$f(a + b\sqrt{7}) = f(a) + f(b)f(\sqrt{7}) = a \pm b\sqrt{7}$$

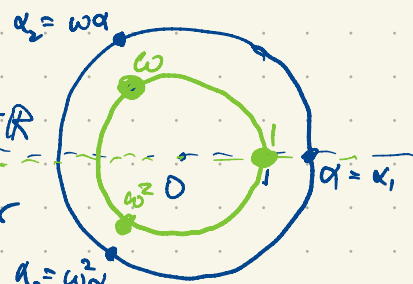
$\mathbb{Q}[\sqrt{7}] \supset \mathbb{Q}$ is a Galois extension of degree 2 with automorphism group of order 2 (abelian) so by the Kronecker-Weber Theorem, $\sqrt{7} \in \mathbb{Q}[\xi_n]$ for some n . (Actually in $\mathbb{Q}[\xi_{28}]$.)

$\alpha = \sqrt[3]{7} = 7^{1/3}$ has min. poly. $x^3 - 7 = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$ where $\omega = e^{2\pi i/3}$ primitive cube root of 1.

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

The splitting field of $x^3 - 7$ is $E = \mathbb{Q}[\alpha, \omega\alpha, \omega^2\alpha]$
all the roots

irreducible in $F = \mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$
 $1, \alpha, \alpha^2$ is a basis for the extension $\mathbb{Q}[\alpha] \supset \mathbb{Q}$
of degree 3 $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$



$1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2$ is a basis for E over F

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

$$\omega^2 = -1 - \omega$$

$\text{Aut } E \cong S_3$ $\text{Aut } E = \langle \sigma, \tau \rangle$ where τ is complex conjugation

and $\sigma : \alpha \mapsto \omega\alpha \mapsto \omega^2\alpha \mapsto \alpha$, $\sigma : \omega \mapsto \omega$

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

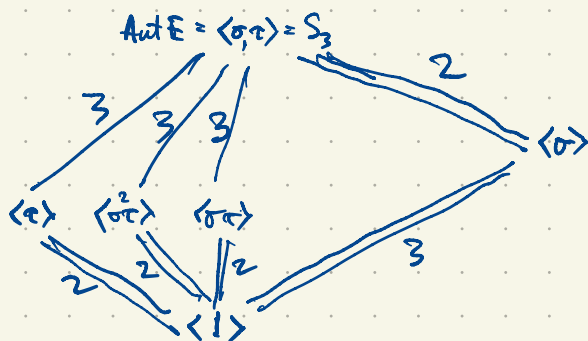
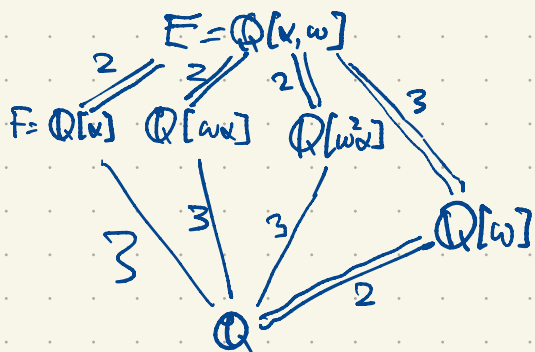
$$\sigma(\omega) = \sigma\left(\frac{\omega\alpha}{\alpha}\right) = \frac{\sigma(\omega\alpha)}{\sigma(\alpha)} = \frac{\omega^2\alpha}{\omega\alpha} = \omega$$

$$\tau(\alpha) = \alpha, \quad \tau(\omega) = \bar{\omega} = \omega^2 = -1 - \omega$$

$$\sigma = (1\ 2\ 3) \in S_3$$

$$\tau = (2\ 3)$$

$$[E : \mathbb{Q}] = 6 = |\text{Aut } E|$$



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

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

All subfields of E

$\alpha = 7^{1/3}$ is not a cyclotomic integer. If α is a cyclotomic integer then so are $\omega\alpha, \omega^2\alpha$ (conjugates of α).

But then $E = \mathbb{Q}[\alpha, \omega\alpha, \omega^2\alpha] \subset \{\text{cyclotomic numbers}\}$ and then $\text{Aut } E$ would be abelian. Contradiction!

What are the automorphism groups of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$? And the field of cyclotomic numbers ($\mathbb{Q}$ linear combinations of roots of unity)? And the field $A = \{\text{complex algebraic numbers}\}$?

Aut $\mathbb{Q}$?

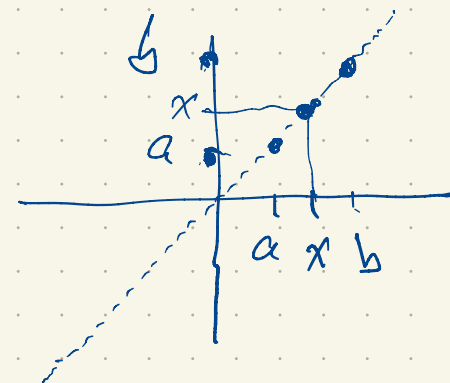
Aut $F = \{\text{bijections } f: F \rightarrow F \text{ such that } f(a)+f(b)=f(a+b), f(a)f(b)=f(ab) \text{ for all } a,b \in F\}$.

$\mathbb{Q}$ has trivial automorphism group: Aut $\mathbb{Q} = \{1\}$

$\mathbb{Q}[\sqrt{2}]$ has two automorphisms:
$$\begin{aligned} 1(a+b\sqrt{2}) &= a+b\sqrt{2} \\ \tau(a+b\sqrt{2}) &= a-b\sqrt{2} \end{aligned} \quad \text{for all } a,b \in \mathbb{Q}.$$

More generally if $F = \mathbb{Q}[\alpha]$ $\overset{F = \text{splitting field of } m(x)}{\text{where } \alpha \text{ has min. poly. } m(x) \in \mathbb{Q}[x]}$ (m irreducible, monic, $m(\alpha)=0$) then any $\alpha' \in F$ having $m(\alpha')=0$, then α and α' are conjugates and there is an automorphism of F mapping $\alpha \mapsto \alpha'$.

$\mathbb{Q}[\sqrt{2}] \cong \frac{\mathbb{Q}[x]}{(x^2-2)} \cong \mathbb{Q}[\sqrt{2}]$ An isomorphism:
$$\begin{aligned} x &\mapsto \sqrt{2} \\ a+b\sqrt{2} &\mapsto a+b\sqrt{2} \end{aligned}$$



$\mathbb{R}$ has trivial automorphism group.

If $f: \mathbb{R} \rightarrow \mathbb{R}$ is an automorphism then $f(a)=a$ for all $a \in \mathbb{Q}$.

$$f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = 2 \Rightarrow f(\sqrt{2}) = \pm\sqrt{2}.$$

Can $f(\sqrt{2}) = -\sqrt{2}$? If $f(\sqrt{2}) = -\sqrt{2}$ then

$$f(-\sqrt{2}) = \sqrt{2}$$

$$f(-\sqrt{2}) = f(-1)f(\sqrt{2}) = (-1)(-\sqrt{2})$$

There exists $\alpha \in \mathbb{R}$ such that $f(\alpha) = 2^{1/4}$, so $f(\alpha^2) = f(\alpha)^2 = \sqrt{2} = f(-\sqrt{2}) \Rightarrow -\sqrt{2} = \alpha^2$, Contradiction.

If f is any automorphism of $\mathbb{R}$, then f is order-preserving i.e. increasing (if $a < b$ then $f(a) < f(b)$).

If $a < b$ then $b-a > 0$ so $b-a = \alpha^2$ for some $\alpha > 0$ in $\mathbb{R}$ so

$$f(b)-f(a) = f(b-a) = f(\alpha^2) = f(\alpha)^2 > 0 \Rightarrow f(a) < f(b).$$

Since $\alpha \neq 0$

$\text{Aut } \mathbb{C}$ contains ι, τ where $\iota(z) = z$, $\tau(z) = \bar{z}$

If we restrict to "continuous" automorphisms, these are the only ones.