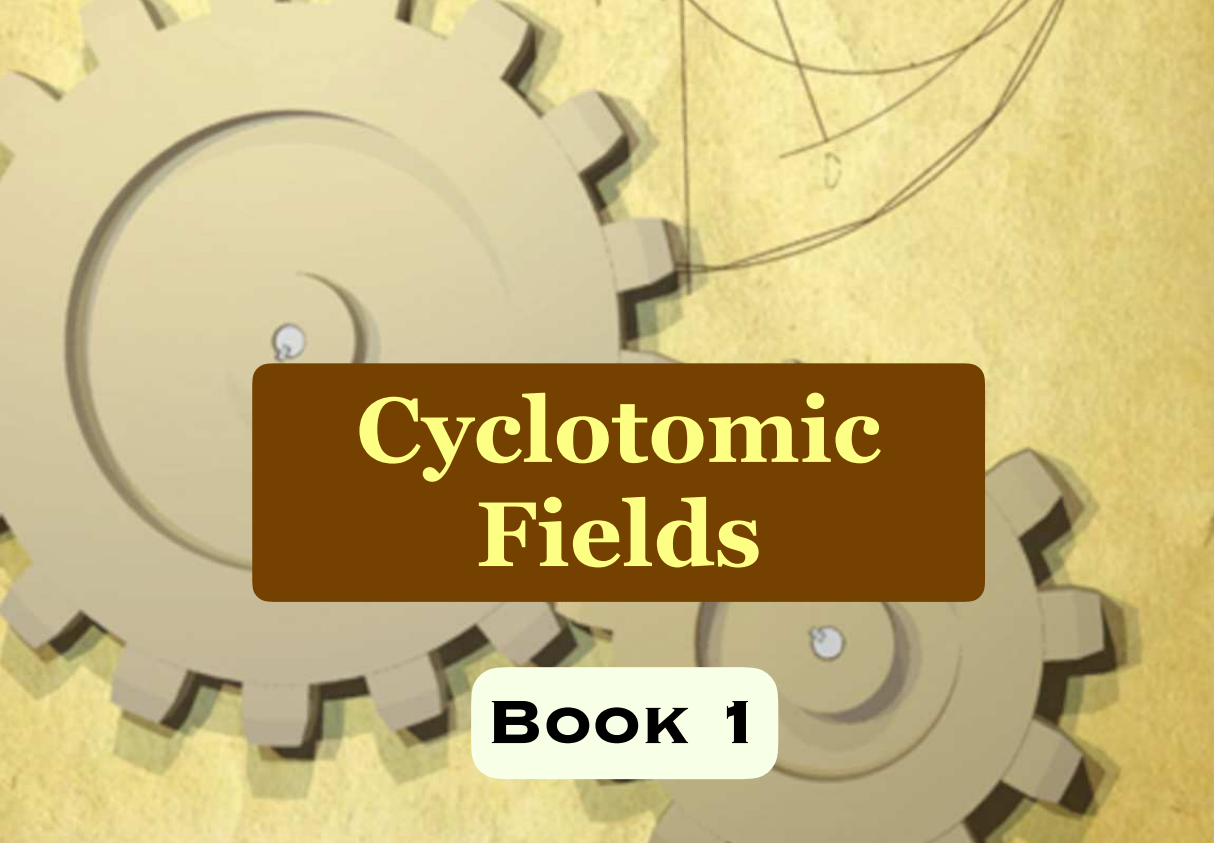
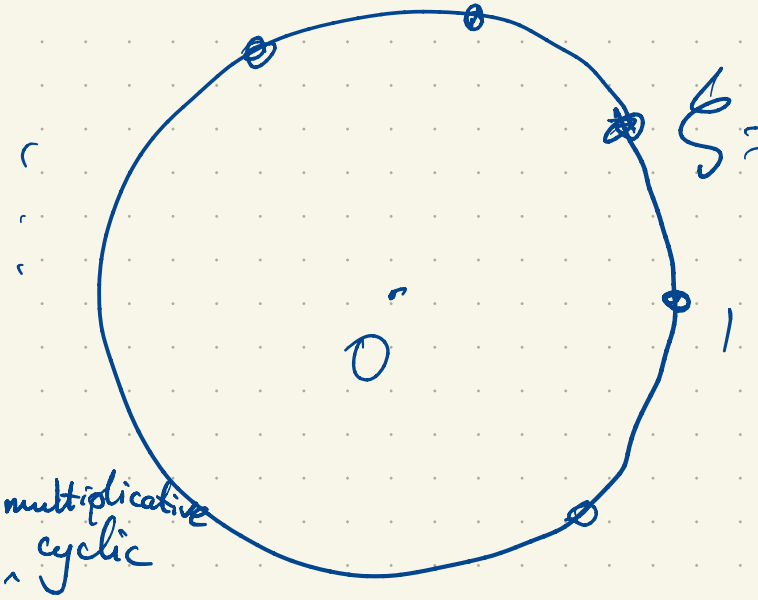

Cyclotomic
Fields
Book 1

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

$\zeta\ \xi \qquad \phi\ \xi\ \pi\ \chi$

$\xi\ \beta\ \theta$



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

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

Euler's totient function

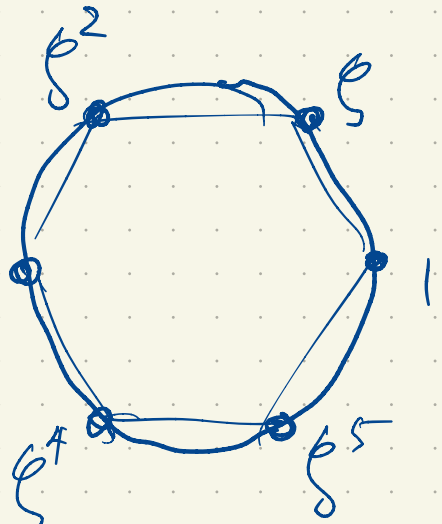
$\phi(n)$ = number of generators in any cyclic group of order n.

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

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

1, 5 relatively prime to 6.

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



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

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

$\zeta^n = 1 \Rightarrow \boxed{1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0}$

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

$$\Phi_1(z)\ \Phi_2(z)\ \Phi_3(z)\ \Phi_6(z)$$

$n=6$: $z^6 - 1 = (z-1)(z+1)(z^2+z+1)(z^2-z+1)$ (factorization into irreducible factors in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$)

Roots: 1, -1, ζ^3, ζ^2, ζ^4, ζ, ζ^5

primitive sixth roots of 1.

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

$$z^n - 1 = \prod_{\substack{d \mid n \\ d \geq 1}} \Phi_d(z)$$ 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 $1, 2, 3, 6$.

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

$\mathbb{Q}[\zeta_n] = \{$polynomials in ζ with coefficients in $\mathbb{Q}\}$
$= \{$linear combinations of $1, \zeta, \zeta^2, \ldots$ with rational coefficients$\}$
$= \{$linear combinations of $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ with coefficients in $\mathbb{Q}\}$

$\zeta = \zeta_n = e^{2\pi i/n}$

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

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

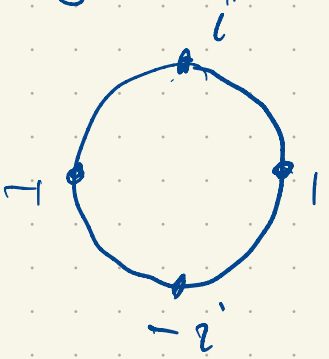
The homomorphism $\mathbb{Q} \xrightarrow{f} \{\text{roots of unity}\}$ is onto but not one-to-one.

$\alpha \mapsto e^{\alpha 2\pi i}$

$$f(\alpha+\alpha') = f(\alpha) f(\alpha')$$

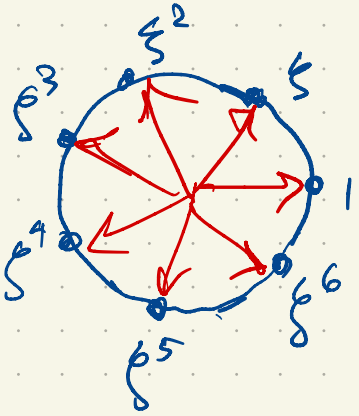
By the first isomorphism theorem for groups, $\{\text{roots of unity}\} \cong \mathbb{Q}/\mathbb{Z}$ (by $\ker f$).

Integer linear combinations of roots of unity are cyclotomic integers.
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

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

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

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

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

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

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

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

Multiply both sides by $\mp i$

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

$\xi = e^{2\pi i/7} = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$

$\mp i(2\alpha+1) = \mp i\left(1 + 2e^{2\pi i/7} + 2e^{4\pi i/7} + 2e^{8\pi i/7}\right) = \sqrt{7}$ ← 2.64575131...

$= \pm\left(2\sin\frac{2\pi}{7} + 2\sin\frac{4\pi}{7} + \sin\frac{8\pi}{7}\right) + i(\cdots)$ ← cosine terms

2.64575131...

$\sqrt{7} = 2\sin\frac{2\pi}{7} + 2\sin\frac{4\pi}{7} + 2\sin\frac{8\pi}{7}$ 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 $1, \xi, \xi^2, \cdots, \xi^{n-1}$

e.g. $\xi = e^{2\pi i/n}$. The primitive n^{th} roots of unity are ξ^k, $1 \le k \le n$, $\gcd(k,n) = 1$.

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 $\Phi_n(z) = \prod_{\substack{1\le k\le n \\ \gcd(k,n)=1}} (z - \xi^k) \in \mathbb{Z}[x]$

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	$z^6+z^5+\cdots+z+1$
8	z^4+1
9	z^6+z^3+1
10	$z^5-z^4+z^3-z^2+1$
11	$z^{10}+z^9+z^8+\cdots+z+1$

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

$\Phi_n(z)$ 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)

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

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

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

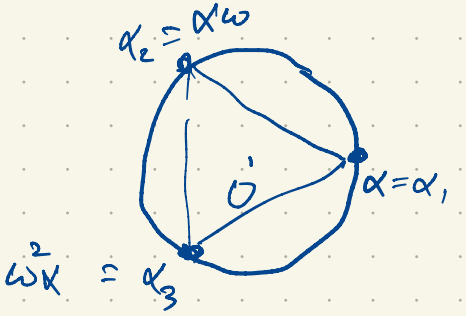
$\mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ is an extension field of degree n, i.e. dimension n.

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

eg. $m(x) = x^3 - 7 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$\alpha_1 = \alpha = 7^{1/3}$

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



$\omega = \zeta_3 = e^{2\pi i/3}$

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

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

$\mathbb{Q}[\alpha] \cong \mathbb{Q}[\alpha\omega] \cong \mathbb{Q}[\alpha\omega^2]$

but they are distinct because

$\mathbb{Q}[\alpha] \subset \mathbb{R}$ but $\mathbb{Q}[\alpha\omega] \not\subset \mathbb{R}$.

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

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

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

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

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

$$f(\alpha+\beta) = f(\alpha)+f(\beta)$$
$$f(\alpha\beta) = f(\alpha)f(\beta) \qquad \text{for all } \alpha,\beta \in F.$$

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

$\mathbb{Q}[\zeta_7] \supset \mathbb{Q}$ is an extension of degree 6 basis $1, \zeta, \zeta^2, \dots, \zeta^5$ $\quad \zeta^6 = -1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5$

This field has exactly 6 automorphisms.

If $f \in \mathrm{Aut}\,\mathbb{Q}[\zeta]$, $\zeta = \zeta_7$ i.e. f any automorphism then $f(\zeta) \in \{\zeta, \zeta^2, \dots, \zeta^6\}$

$\zeta^7 = 1 \Rightarrow f(\zeta^7) = f(1) = 1$ $\qquad f(0) = f(0+0) = f(0)+f(0) \Rightarrow f(0) = 0$

$f(\zeta)^7 = f(\zeta)f(\zeta)\cdots f(\zeta) = f(\zeta\zeta\cdots\zeta)$ $\qquad f(x) = f(1^2) = f(1\cdot 1) = f(x)f(1) \Rightarrow f(1) = 1$

Minimal polynomial of $\zeta = \zeta_7$ over $\mathbb{Q}$ is $m(x) = 1+x+x^2+x^3+x^4+x^5+x^6 = \Phi_7(x) = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^6)$

$\mathrm{Aut}\,\mathbb{Q}[\zeta] = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ $\qquad f_j(\zeta) = \zeta^j$

$f_3 f_2 = f_2 f_3 = f_2 \circ f_3 = f_6$ $\qquad f_2 f_3(\zeta) = f_2(\zeta^3) = f_2(\zeta)^3 = (\zeta^2)^3 = \zeta^6$

$f_2^2 = f_2 \circ f_2 = f_4$

$f_2^3 = f_2 \circ f_2 \circ f_2 = f_8 = f_1$

$\mathrm{Aut}\,\mathbb{Q}[\zeta_n]$ is abelian

$\mathrm{Aut}\,\mathbb{Q}[\zeta_n] \cong (\mathbb{Z}/n\mathbb{Z})^\times = \{k \in \mathbb{Z} : 1 \le k \le n,\ \gcd(k,n) = 1\}$ abelian group of order $\phi(n)$

$= [\mathbb{Q}[\zeta_n] : \mathbb{Q}]$

$0, 1, \dots, n$ under addition mod n (a ring)

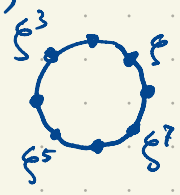
Whenever R is a ring with identity, $R^\times = \{\text{units in } R\}$ is a multiplicative group.

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

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

$\mathrm{Aut}\,\mathbb{Q}[\xi_8] = \{f_1, f_3, f_5, f_7\}$ $\qquad f_j(\xi) = \xi^j$

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



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

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

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

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

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

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

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

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

$\mathrm{Aut}\,E = \{\iota, \sigma\}$

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

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

$\sigma^2 = \iota$

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

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

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

If $f \in \mathrm{Aut}\,E$ 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.

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

irreducible in $\mathbb{Q}[\alpha]$