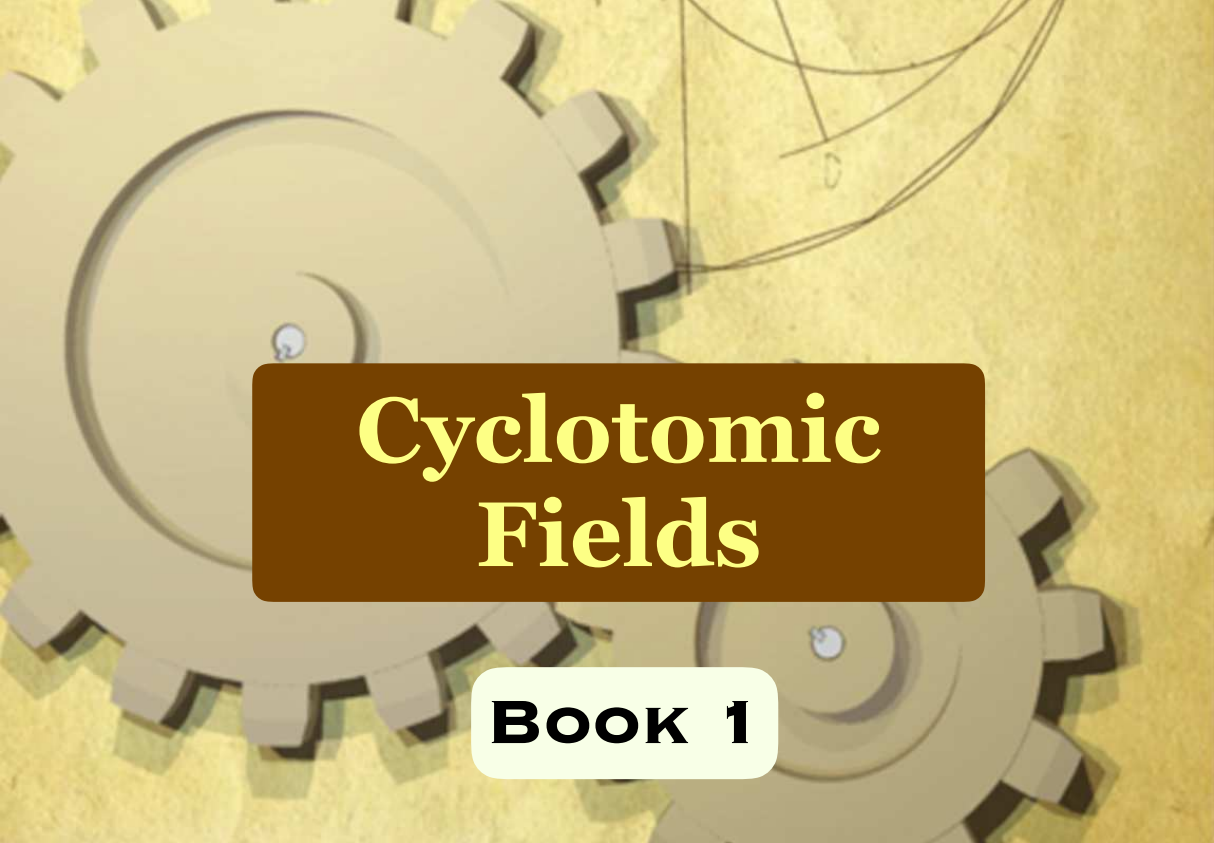


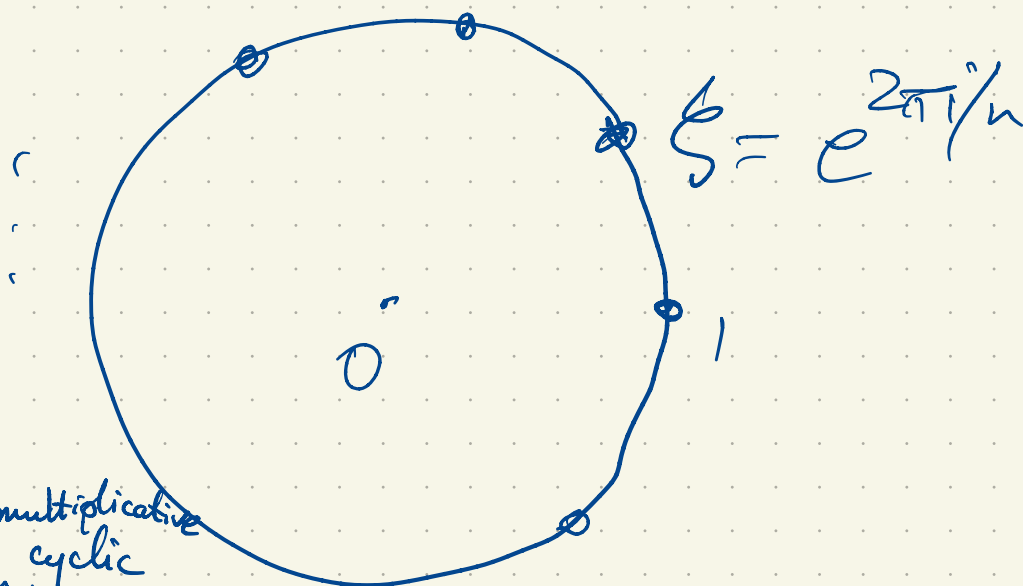


Cyclotomic Fields

Book 1

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

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



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

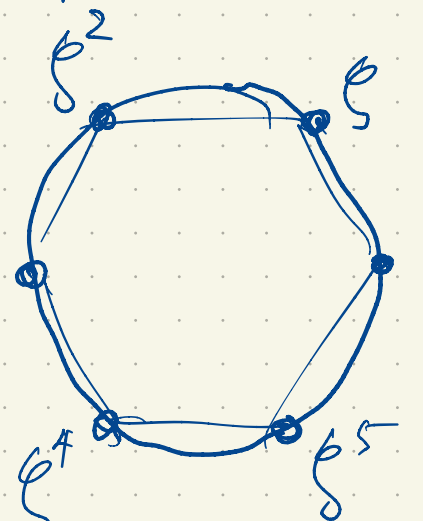
$$\phi(n) = |\{k \in \{1, 2, \dots, n\} : \gcd(k, n) = 1\}|$$

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

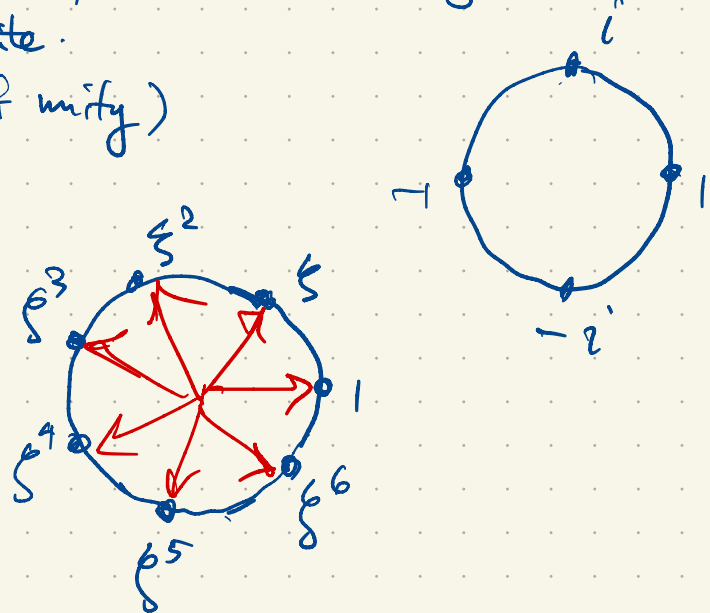
$$\alpha^2 = \xi^2 + \xi^4 + \xi + 2\xi^3 + 2\xi^5 + 2\xi^6$$

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

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

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

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



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

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

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

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

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

$$2.645751311\dots$$

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

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

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

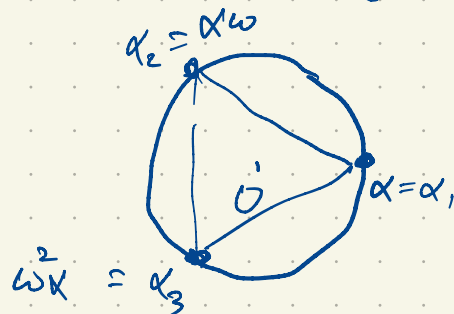
$\mathbb{Q}[\alpha]$ is a field with basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ over $\mathbb{Q}$

$\mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ 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.



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

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

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

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.

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

This field has exactly 6 automorphisms.

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

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

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

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

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

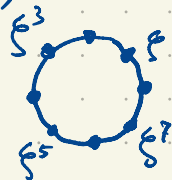
Whenever R is a ring with identity, $R^\times = \{\text{units in } R\}$ is a multiplicative group.

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

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

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

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



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

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

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

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

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

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

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 $E = \mathbb{Q}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Q}\}$.

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

$$\sigma^2 = 1$$

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

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

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

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

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

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

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

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

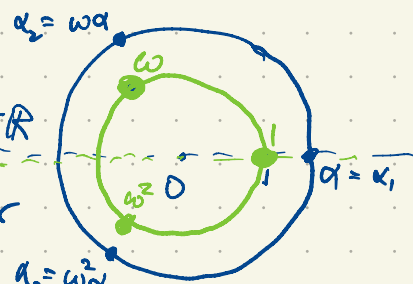
$\mathbb{Q}[\sqrt{7}] \supset \mathbb{Q}$ is a Galois extension of degree 2 with automorphism group of order 2 (abelian) so by the Kronecker-Weber Theorem, $\sqrt{7} \in \mathbb{Q}[\xi_n]$ for some n . (Actually in $\mathbb{Q}[\xi_{28}]$.)

$\alpha = \sqrt[3]{7} = 7^{1/3}$ 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 $F = \mathbb{Q}[\alpha, \omega\alpha, \omega^2\alpha]$
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

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

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

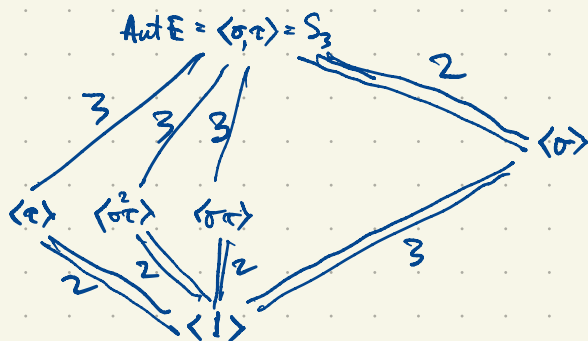
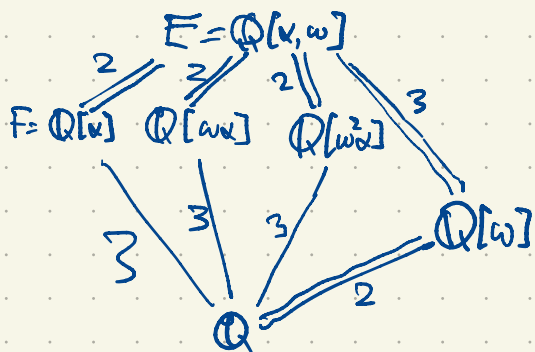
$$\sigma(\omega) = \sigma\left(\frac{\omega\alpha}{\alpha}\right) = \frac{\sigma(\omega\alpha)}{\sigma(\alpha)} = \frac{\omega^2\alpha}{\omega\alpha} = \omega$$

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

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

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

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



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

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

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 $\mathbb{Q}$?

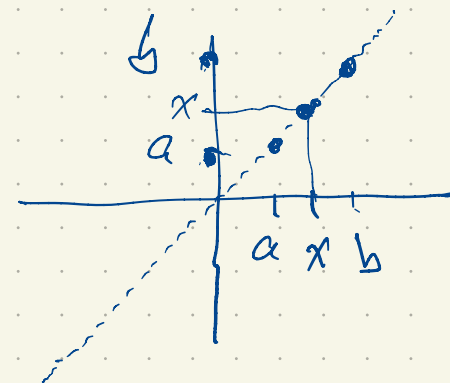
Aut $F = \{\text{bijections } f: F \rightarrow F \text{ such that } f(a)+f(b)=f(a+b), f(a)f(b)=f(ab) \text{ for all } a,b \in F\}$.

$\mathbb{Q}$ 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 $F = \mathbb{Q}[\alpha]$ $\xrightarrow{F = \text{splitting field of } m(x)}$ where α 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 $\alpha \mapsto \alpha'$.

$\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x] / (x^2-2) \cong \mathbb{Q}[\sqrt{2}]$ 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.
How do we "obtain" ("construct") automorphisms of $\mathbb{C}$?

If $f \in \text{Aut } \mathbb{C}$ i.e. $f: \mathbb{C} \rightarrow \mathbb{C}$ is bijective, $f(z+w) = f(z) + f(w)$, $f(zw) = f(z)f(w)$

then $f(\sqrt{2}) = \pm\sqrt{2}$
 $f(\sqrt{3}) = \pm\sqrt{3}$
 $f(\sqrt{5}) = \pm\sqrt{5}$
 $f(\sqrt{7}) = \pm\sqrt{7}$
 etc.

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

$$f(\sqrt{6}) = f(\sqrt{2}\sqrt{3}) = f(\sqrt{2})f(\sqrt{3})$$

Let E be the field of cyclotomic numbers, i.e. expressions of the form

$$a_1 z_1 + a_2 z_2 + \dots + a_n z_n, \quad a_i \in \mathbb{Q}, \quad z_i \text{ complex roots of unity i.e. } z_i^{n_i} = 1$$

E is countably infinite.

$\text{Aut } E$ is abelian. Suppose $f, g \in \text{Aut } E$ such that $f \circ g \neq g \circ f$
 then there exist $\alpha \in E$ such that $f(g(\alpha)) \neq g(f(\alpha))$.

We have $\alpha = a_1 z_1 + a_2 z_2 + \dots + a_n z_n$ for some $a_1, \dots, a_n \in \mathbb{Q}$
 $z_1, \dots, z_n$ roots of unity, $z_i^{n_i} = 1, n_i \geq 1$.

Let $m = \text{lcm}(n_1, \dots, n_n)$ so $z_1, \dots, z_n$ are m^{th} roots of unity, $z_i = \zeta^{k_i}, \zeta = \zeta_m, (\zeta^m = 1)$.

All terms are in $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta_m]$ of degree $\phi(m)$.

f, g act on $\mathbb{Q}[\zeta] \subset E$.
 $f(\zeta) = \zeta^r \quad (\gcd(r, m) = 1)$
 $g(\zeta) = \zeta^s \quad (\gcd(s, m) = 1)$

$$\left. \begin{aligned} f(g(\zeta)) &= (\zeta^s)^r \\ g(f(\zeta)) &= (\zeta^r)^s \end{aligned} \right\} = \zeta^{rs}$$

$$f(g(\alpha)) = \sum_i a_i \zeta^{k_i rs} = g(f(\alpha))$$

Although $E \supset \mathbb{Q}$ is not a finite extension,
 every finite subset of E is contained in a finite
 extension $\mathbb{Q}[\zeta_m]$ of degree $\phi(m) < \infty$.

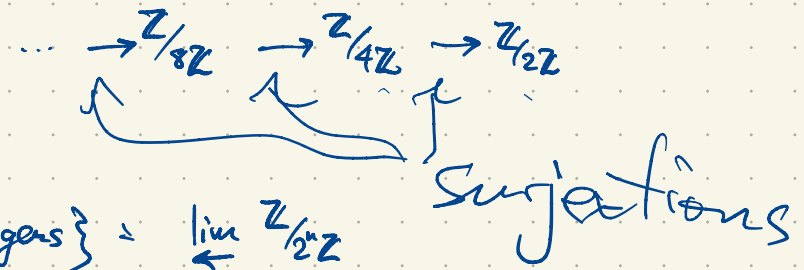
"local finiteness"

$E \subset A = \{\text{algebraic numbers}\}$ A is countable.

$\text{Aut } A$ is nonabelian
 $\text{Aut } E$ is abelian

E and A are countable
 Both $\text{Aut } E$ and $\text{Aut } A$ are uncountable.

Inverse Limits



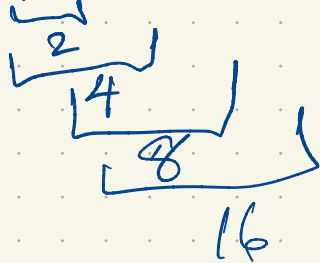
$$1 \cdot 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + \dots \in \mathbb{Z}_2 = \{2\text{-adic integers}\} = \varprojlim \mathbb{Z}/2^n\mathbb{Z}$$

eg. $11 = 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + \dots$

$$-1 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + \dots$$

$$1 + 2 + 4 + 8 + 16 + 32 + \dots = -1$$

$$1 + 1 + 2 + 4 + 8 + 16 + 32 + \dots$$



Direct Limits

$$S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_5 \rightarrow \dots$$



Inclusions

(injective)

$$S_\infty = \bigcup_{n=1}^{\infty} S_n$$

Historical interest in Cyclotomic Fields arises from the study of FLT (Fermat's Last Theorem)

The equation $x^n + y^n = z^n$ has no solution in positive integers for $n > 2$.

Fermat proved this for $n=4$.

Assume x, y, z, n are positive integers with $n > 2$ satisfying $x^n + y^n = z^n$.

WLOG n is an odd prime, $n=p$.

$$x^p + y^p = z^p = (x+y)(x+\xi y) \cdots (x+\xi^{p-1}y) \quad , \quad \xi = \xi_p \quad \text{in } \mathbb{Z}[\xi].$$

WLOG x, y, z are ^(pairwise) relatively prime. If a prime q divides the left side then $q|z$ and $q|(x+\xi^j y)$ for some j .

$$x+y \text{ and } x+\xi y \text{ divisible by } q \Rightarrow q | \xi(x+y) - (x+\xi y) = (\xi-1)x \Rightarrow q|x.$$

Euclid's Lemma: In $\mathbb{Z}$, if $q|uv$ then $q|u$ or $q|v$.

This relies on special facts about $\mathbb{Z}$.

This "fact" fails in $\mathbb{Z}[\xi]$ for most p . (Eg. in $\mathbb{Z}[\xi_{23}]$).

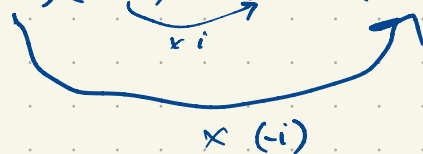
In $\mathbb{Z}$, primes and irreducibles are pretty much the same thing.

$\mathbb{Z}[i]$, $i = \xi_4$ has unique factorization (Gaussian integers)

$\mathbb{Z}[\omega]$, $\omega = \xi_3$ " " (Eisenstein ")

Units (invertible elements) in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$
 $\mathbb{Z}[i]^\times =$

$$5 = (2+i)(2-i) = (1+2i)(1-2i) \quad \text{in } \mathbb{Z}[i]$$



$$5 = (-1-2i)(-1+2i)$$

$$\begin{aligned} 5 &= 5 \cdot 1 \\ &= 1 \cdot 5 \\ &= (-5) \cdot (-1) \\ &= (-1) \cdot (-5) \end{aligned}$$

In $\mathbb{Z}[\sqrt{-10}]$ we do not have unique factorization.

$N: \mathbb{Z}[\sqrt{-10}] \rightarrow \mathbb{Z}$ algebraic norm

$$N(a+b\sqrt{-10}) = (a+b\sqrt{-10})(a-b\sqrt{-10}) = a^2+10b^2.$$

$$N(x) = x\bar{x}$$

$$\overline{a+b\sqrt{-10}} = a-b\sqrt{-10} \text{ for } a, b \in \mathbb{Z}.$$

$$N(xy) = N(x)N(y)$$

Units in $\mathbb{Z}[\sqrt{-10}]$? If $uv=1$ then $N(u)N(v) = N(uv) = N(1) = 1.$
 $\Rightarrow N(u) = N(v) = 1$

If $N(a+b\sqrt{-10}) = 1$ then $a^2+10b^2 = 1 \Rightarrow a = \pm 1, b = 0$

$$\mathbb{Z}[\sqrt{-10}]^* = \{\pm 1\}$$

10 is reducible: We can factor $10 = uv$ where u, v are ^{not} units

$10 = 2 \cdot 5$. We'll check 2, 5 are irreducible.

$$10 = (\sqrt{-10})(-\sqrt{-10}) \quad \sim \quad \pm \sqrt{-10}$$

But $\pm\sqrt{-10}$ are not associates of 2, 5.

If $2 = uv$ $u, v \in \mathbb{Z}[\sqrt{-10}]$ then $N(2) = N(u)N(v)$
 $4 = (a^2+10b^2)(c^2+10d^2)$

$$\begin{array}{ccc} 1 & \times & 4 \\ \hline 2 & \times & 2 \\ \hline 4 & \times & 1 \end{array}$$

Similarly all of 2, 5, $\sqrt{-10}$, $-\sqrt{-10}$ are irreducible.

$\Rightarrow$ one of $u, v \in \{\pm 1\}$

Consider the field $E = \mathbb{Q}[\xi]$, $\xi = \xi_n$ eg. $\xi = e^{2\pi i/n}$ but any primitive n^{th} root of unity will do.
 $[E : \mathbb{Q}] = \phi(n)$ Euler's totient function. $\Phi_n(x) =$ cyclotomic polynomial, $\deg \Phi_n(x) = \phi(n)$.
 (minimal polynomial in $\mathbb{Q}[x]$ having ξ as a root)

$E \supseteq \mathbb{Q}$ is Galois: $G = \text{Aut } E$, $|G| = \phi(n)$, G abelian.

For $1 \leq k \leq n$, $\gcd(k, n) = 1$, $\sigma_k(\xi) = \xi^k$, $\sigma_k \sigma_l = \sigma_{kl}$

The ring of (algebraic) integers in $E = \mathbb{Q}[\xi]$ is the subset consisting of all $\alpha \in E$ which are roots of monic polynomials in $\mathbb{Z}[x]$.

$$G \cong (\mathbb{Z}/n\mathbb{Z})^\times = \text{units of the ring } \mathbb{Z}/n\mathbb{Z}$$

The algebraic integers in $\mathbb{Q}$ are just $\mathbb{Z}$, (ordinary integers).

$\Leftrightarrow$ the minimal poly. of α (monic poly. in $\mathbb{Q}[x]$ having α as a root, of minimal degree) is in $\mathbb{Z}[x]$.

eg. what are the (algebraic) integers in $E = \mathbb{Q}[\sqrt{5}]$?

$$= \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$$

Every ordinary integer $m \in \mathbb{Z}$ is an alg. int. because it is a root of $x - m \in \mathbb{Z}[x]$ monic.

$\sqrt{5}$ is a root of $x^2 - 5 \in \mathbb{Z}[x]$ monic so $\sqrt{5}$ is an alg. int.

Every element of the form $a + b\sqrt{5}$, $a, b \in \mathbb{Z}$ is an alg. int.

$\frac{1}{2}$ is not an alg. int. $x - \frac{1}{2} \in \mathbb{Q}[x]$ is its min. poly.

$2x - 1 \in \mathbb{Z}[x]$ is not monic.

But there are more alg. integers in E other than $\mathbb{Z}[\sqrt{5}]$.

$\alpha = \frac{1+\sqrt{5}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{5} \in E$ is a root of

$$x^2 - \frac{1+5+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \alpha; \quad \alpha \text{ is a root of } x^2 - x - 1 \in \mathbb{Z}[x].$$

Claim: The alg. integers in $\mathbb{Z}[\sqrt{5}]$ are just elements in $\mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{5}}{2}$

Clearly $\{\text{alg. integers in } E\} \supseteq \mathbb{Z}[\alpha]$. Conversely:

$\tau \in \text{Aut } E$, $\tau(a + b\sqrt{5}) = a - b\sqrt{5}$.

If $\beta \in E$ is an alg. integer then so is $\tau(\beta)$.

If $m(x)$ is the min. poly of β then $m(\beta) = 0$

$$m(x) = x^2 + ax + b \quad (a, b \in \mathbb{Z})$$

$$\beta^2 + a\beta + b = 0 \quad \tau(\beta)^2 + a\tau(\beta) + b = 0$$

$\beta + \pi(\beta) \Big\{ \beta \pi(\beta) \Big\}$ are alg. int.

Say $\beta = c + d\sqrt{5}$, $c, d \in \mathbb{Q}$.

$\beta + \pi(\beta) = 2c$ is an alg. int.

Case (i) $c \in \mathbb{Z} \Rightarrow$

Case (ii) $c = c' + \frac{1}{2}$, $c' \in \mathbb{Z}$

Details in Appendices (or P. Samuel)

Alg. int. in $E = \mathbb{Q}[\sqrt{5}]$ are $\mathbb{Z}[\sqrt{5}] \cup (\mathbb{Z}[\sqrt{5}] + \alpha) = \left\{ \frac{a+b\sqrt{5}}{2} : a, b \in \mathbb{Z}; a \equiv b \pmod{2} \right\} = \mathbb{Z}[\alpha]$

The alg. integers in $\mathbb{Q}(\sqrt{5})$ are just $\mathbb{Z}[\sqrt{5}]$ (This however is not obvious).

What are the units?

First consider: Units in $\mathbb{Z}$ are $\mathbb{Z}^\times = \{\pm 1\}$.

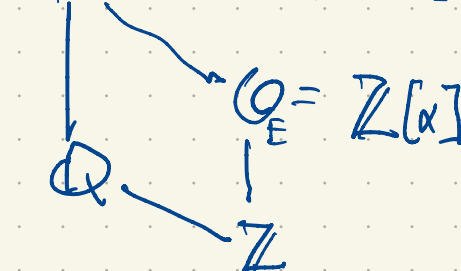
Units in $\mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{5}}{2}$:

$$\mathbb{Z}[\alpha]^\times = \left\{ \pm 1, \pm \alpha, \pm \alpha^{-1}, \pm \alpha^2, \pm \alpha^{-2}, \dots \right\} \quad \alpha = \frac{1+\sqrt{5}}{2}, \quad -\alpha^{-1} = \frac{-1+\sqrt{5}}{2}$$

$$\mathbb{Q}_{\mathbb{Q}[\alpha]}^\times = \mathbb{Z}[\alpha]^\times = \left\{ \pm \alpha^k : k \in \mathbb{Z} \right\} \cong \underbrace{\{\pm 1\}}_{\text{roots of unity}} \times \langle \alpha \rangle$$

$\alpha, \bar{\alpha}$ roots of $x^2 - x - 1$
 $x(x-1) = 1$
 $\alpha(\alpha-1) = 1$
 $\frac{1}{\alpha} = \alpha - 1$

$E = \mathbb{Q}[\sqrt{5}] = \mathbb{Q}[\alpha]$, $\alpha = \frac{1+\sqrt{5}}{2} = 1.618\dots$



A (algebraic) number field is a finite extension $E \supseteq \mathbb{Q}$. (Not necessarily Galois)

$\mathcal{O}_E = \{ \text{algebraic integers in } E \} = \{ \alpha \in E : f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbb{Z}[x] \}$

$\mathcal{O}_E^\times = \{ \text{units in } \mathcal{O}_E \}$ mult. (finitely generated) abelian group. Every (finitely generated) abelian group is a product of cyclic groups. (finitely)

"units in E"
abuse of terminology

$\mathcal{O}_E^\times = (\text{finite abelian group}) \times \mathbb{Z}^k$

"torsion subgroup of $\mathcal{O}_E^\times$ "
roots of unity in E.

torsion-free
(free abelian)
of rank k
rank = number of generators of the free part

Dirichlet's Theorem on Units in Number Fields gives the rank of the group of units.

$E = \mathbb{Q}[\alpha]$ for some $\alpha \in E$, $n = [E : \mathbb{Q}]$, $m(x)$ = irreducible in $\mathbb{Q}[x]$ minimal poly. of α over $\mathbb{Q}$, $\deg m(x) = n$.
 $m(x)$ has n roots in $\mathbb{C}$, distinct (some in E). If all roots are in E , then the extension is Galois with $|\text{Aut } E| = n$; otherwise $|\text{Aut } E| < n$.

$n = r + 2s$ where r is the number of real roots; s pairs of non-real roots in $\mathbb{C}$ (in complex conjugate pairs)

Dirichlet's Theorem The rank of $\mathcal{O}_E^\times$ is $r + s - 1$. There are $n = r + 2s$ embeddings $E \hookrightarrow \mathbb{C}$. (injective homomorphisms)

Eg. $\mathbb{Q}$, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
 $r = 1$ of these embeddings are real;
 $s = 0$ the other $2s$ embeddings are non-real.

Rank of $\mathcal{O}_{\mathbb{Q}}^\times$ is $r + s - 1 = 1 + 0 - 1 = 0$.

$$\mathcal{O}_{\mathbb{Q}}^\times = \{\pm 1\} = \mathbb{Z}^\times$$

$$\alpha = \frac{1+\sqrt{5}}{2} \quad m(x) = x^2 - x - 1 = (x - \alpha)(x - \bar{\alpha}), \quad \bar{\alpha} = \frac{1-\sqrt{5}}{2} = 1 - \alpha$$

$$r = 2 \quad \begin{array}{l} \alpha \mapsto \alpha \\ \alpha \mapsto \bar{\alpha} \end{array}$$

$$s = 0$$

$$\text{Rank} = r + s - 1 = 2 + 0 - 1 = 1$$

"Real quadratic field"

$$\omega = \zeta_3 = e^{2\pi i/3} \quad m(x) = x^2 + x + 1 = \Phi_3(x)$$

$$r = 0 \quad \begin{array}{l} \omega \mapsto \omega \\ \omega \mapsto \bar{\omega} \end{array}$$

$$s = 1$$

$$\text{Rank} = r + s - 1 = 0 + 1 - 1 = 0$$

$$\mathcal{O}_{\mathbb{Q}[\omega]}^\times = \mathbb{Z}[\omega]^\times = \{\pm 1, \pm \omega, \pm \bar{\omega}\}$$

Eisenstein integers

"Imaginary quadratic field"

Pell's Equation $x^2 - ny^2 = \pm 1$, $n \in \mathbb{Z} \iff x + y\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ is a unit.

If $n \neq \pm 1$ and n squarefree (not divisible by p^2 for any prime) then there are infinitely many solutions.

Eg. $x^2 - 5y^2 = 1$ has infinitely many integer solutions $(\pm 1, 0), (\pm 9, \pm 4), \dots$
 $x^2 - 5y^2 = -1$ $(\pm 2, \pm 1), \dots$

$$(x + y\sqrt{5})(x - y\sqrt{5}) = 1$$

$$(2 + \sqrt{5})(-2 - \sqrt{5}) = 1$$

$$(9 + 4\sqrt{5})(9 - 4\sqrt{5}) = 1$$

What are the units in $\mathbb{Q}[\xi]$ i.e. $\mathbb{Z}[\xi]$? $\xi = \xi_n$

$$\mathbb{Q}[\xi]$$

Let's consider $\xi = \xi_p$, p odd prime.

$E = \mathbb{Q}[\xi]$, $\xi = \xi_p$ has degree $[E:\mathbb{Q}] = \phi(p) = p-1$.

$r = 0$ no real embeddings

$$n = r + 2s = p-1$$

$$s = \frac{p-1}{2}$$

Rank of $\mathcal{O}_E^\times$ is $n + s - 1 = 0 + \frac{p-1}{2} - 1 = \frac{p-3}{2}$.

$$\mathcal{O}_E^\times = \langle -\xi \rangle \times \{\text{free abelian of rank } \frac{p-3}{2}\}$$

We have $2p$ roots of unity in E i.e. $\pm 1, \pm \xi, \dots, \pm \xi^{p-1}$ (cyclic).

Extension $E \supseteq \mathbb{Q}$ is Galois if $G = \text{Aut } E$ has order $|G| = n = [E:\mathbb{Q}]$. There are two very special maps $E \rightarrow \mathbb{Q}$ called the trace and the norm,

$$T(\alpha) = \sum_{\sigma \in G} \sigma(\alpha), \quad N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha). \quad \text{If } \tau \in G \text{ then } \tau(T(\alpha)) = \sum_{\sigma \in G} \tau(\sigma(\alpha)) = \sum_{\rho \in G} \rho(\alpha) = T(\alpha) \quad \rho = \tau\sigma$$

$$\Rightarrow T(\alpha) \in \mathbb{Q}. \quad \text{Similarly, } N(\alpha) \in \mathbb{Q}.$$

If $\alpha \in \mathcal{O} = \mathcal{O}_E = \{\text{algebraic integers in } E\} \hat{=} \{\alpha \in E : f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbb{Z}[x]\}$.

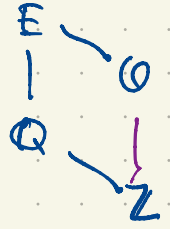
E is the field of quotients of $\mathcal{O} = \mathcal{O}_E$.

If $\alpha, \beta \in E$ then

$$\frac{\alpha}{\beta} = \frac{\alpha \prod_{\sigma \in G, \sigma \neq \text{id}} \sigma(\beta)}{\prod_{\sigma \in G, \sigma \neq \text{id}} \sigma(\beta)} = \frac{\alpha \prod_{\sigma \in G, \sigma \neq \text{id}} \sigma(\beta)}{N(\beta)} \in E.$$

algebraic conjugates of β

If $\alpha \in \mathcal{O}$ then $N(\alpha) \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$



$\mathbb{Q}[\sqrt{2}]$ is a field; it is the field of quotients (fractions) of $\mathbb{Z}[\sqrt{2}]$.

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{\boxed{a} + \boxed{b}\sqrt{2}}{\boxed{c} + \boxed{d}\sqrt{2}} \quad \text{in } \mathbb{Q}$$

$a, b, c, d \in \mathbb{Q}$

For $\xi = \xi_p$, p prime, $E = \mathbb{Q}[\xi]$, we show $\mathcal{O}_E = \mathbb{Z}[\xi]$. (This extends to any $\xi = \xi_n$.)

Of course $\mathcal{O} \supseteq \mathbb{Z}[\xi]$; we must prove the reverse inclusion.

Claim: $\varepsilon = 1 - \xi \in \mathcal{O}$ is irreducible.

$$G = \text{Aut } E = \{\sigma_1, \sigma_2, \dots, \sigma_{p-1}\} \quad p-1 = |G| = \phi(p)$$

$$N(\varepsilon) = \prod_{k=1}^{p-1} \sigma_k(\varepsilon) = \prod_{k=1}^{p-1} (1 - \xi^k) = p.$$

ε is irreducible.

If $\varepsilon = uv$, $u, v \in \mathcal{O}$ then $p = N(\varepsilon) = \underbrace{N(u)}_{\in \mathbb{Z}} \underbrace{N(v)}_{\in \mathbb{Z}} \Rightarrow N(u) = \pm 1$ and $N(v) = \pm p$ or the other way around.

p has $p-1$ irreducible factors in $p = \sum_{k=1}^{p-1} \sigma_k(\varepsilon)$, $\varepsilon = 1 - \xi$.

All the factors $\sigma_k(\varepsilon) = 1 - \xi^k$, $1 \leq k \leq p-1$ are associates:

$$1 - \xi^k = (1 - \xi)(1 + \xi + \xi^2 + \dots + \xi^{k-1})$$

$$\underbrace{\hspace{10em}}_{\in \mathcal{O}}$$

↓
Apply $\sigma_r \in G$

$$1 - \xi^r = 1 - \xi^{kr} = (1 - \xi^r) \underbrace{(1 + \xi^r + \xi^{2r} + \dots + \xi^{(k-1)r})}_{\in \mathcal{O}}$$

For $r, s \in \{1, 2, \dots, p-1\}$, there exists $k \in \{1, 2, \dots, p-1\}$ such that $kr \equiv s \pmod{p}$.

$$1 - \xi^r \mid 1 - \xi^s$$

$$\text{Similarly } 1 - \xi^s \mid 1 - \xi^r$$

$$\text{So } 1 - \xi^r = u(1 - \xi^s), \quad u \in \mathcal{O}^*$$

$$1 - \xi^r = (\quad)(1 - \xi^s) = (\quad)(\quad)(1 - \xi^r)$$

$$p = \underbrace{(1 - \xi)(1 - \xi^2) \dots (1 - \xi^{p-1})}_{\varepsilon} = u \varepsilon^{p-1}, \quad u \in \mathcal{O}^*$$

p ramifies in the extension $\mathbb{Q}[\xi] \supset \mathbb{Q}$ i.e. p has an irreducible factor with exponent > 1 .

Let $\alpha \in \mathbb{Q}[\xi]$, $\xi = \xi_p$, p prime; so $\alpha = a_0 + a_1\xi + a_2\xi^2 + \dots + a_{p-2}\xi^{p-2}$, $a_i \in \mathbb{Q}$
 $(\xi^{p-1} = -1 - \xi - \dots - \xi^{p-2})$

Suppose $\alpha \in \mathcal{O}$ i.e. α is an algebraic integer.

Then $\sigma(\alpha) \in \mathcal{O}$ for every $\sigma \in \text{Aut } \mathbb{Q}$. Of course $\sigma = \sigma_k$, $\sigma_k(\xi) = \xi^k$, $1 \leq k \leq p-1$

$$\alpha_k = \sigma_k(\alpha) = a_0 + a_1\xi^k + a_2\xi^{2k} + \dots + a_{p-2}\xi^{(p-2)k}, \quad \alpha_1 = \alpha$$

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{p-1} \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{p-2} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(p-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{p-1} & \xi^{2(p-1)} & \dots & \xi^{(p-2)(p-1)} \end{bmatrix}}_M \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-2} \end{bmatrix}$$

Vandermonde matrix $\rightarrow M$

$$\det M = \prod_{1 \leq j < k \leq p-1} (\xi^k - \xi^j) = u\xi^{\binom{p-1}{2}}, \quad u \in \mathcal{O}^*$$

Pick $m \geq 1$ such that $p^m a_i \in \mathbb{Z}$. Such a positive integer exists; we can take the largest power of p dividing $\det M = u\xi^{\binom{p-1}{2}}$. Then $u\xi^{(p-1)m} \alpha = p^m \alpha = b_0 + b_1\xi + b_2\xi^2 + \dots + b_{p-2}\xi^{p-2}$, $b_i \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$

If $u \geq 1$ then the left side is divisible by $p = u\xi^{p-1}$, $(p) = (\xi)^{p-1} = (\xi^{p-1})$

If b_0 is not divisible by p then it's not divisible by ξ whereas $p^m \alpha$ and $b_1\xi + \dots + b_{p-2}\xi^{p-2}$ are divisible by ξ , contradiction.

We continue through $b_0, \dots, b_{p-2}$ cancelling p 's until $\alpha = b_0 + b_1\xi + b_2\xi^2 + \dots + b_{p-2}\xi^{p-2}$, $b_i \in \mathbb{Z}$.

So $\alpha \in \mathbb{Z}[\xi] = \mathbb{Z}[\xi]$. $\square$

If an ordinary integer $b \in \mathbb{Z}$ is divisible by ξ , then it must be divisible by $p = u\xi^{p-1}$.

We must prove $a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}$

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{p-2} \end{bmatrix} = M^{-1} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{p-1} \end{bmatrix}$$

$M^{-1} = \frac{1}{\det M}$ (classical adjoint of M)
 entries are algebraic integers

$$\xi = 1 - \xi$$

$$\mathbb{Z}[\xi] = \mathbb{Z}[\xi]$$

For $E = \mathbb{Q}[\xi]$, $\mathcal{O}_E = \mathbb{Z}[\xi] = \{b_0 + b_1\xi + b_2\xi^2 + \dots + b_{\phi(n)-1}\xi^{\phi(n)-1} : b_i \in \mathbb{Z}\}$, $\xi = \xi_n$.
 $\{1, \xi, \xi^2, \dots, \xi^{\phi(n)-1}\}$ is a base for the ring $\mathcal{O}$: every $\alpha \in \mathcal{O}$ is uniquely expressible as a $\mathbb{Z}$ -linear combination of $1, \xi, \xi^2, \dots, \xi^{\phi(n)-1}$. (analogue of basis for a vector space)
 Why do we care about a base for $\mathcal{O}$?

An (algebraic) number field is a finite extension $E \supseteq \mathbb{Q}$. So $\dim_{\mathbb{Q}} E = n < \infty$ and we call this the degree of the extension $n = [E : \mathbb{Q}]$. There is a basis $\alpha_1, \dots, \alpha_n$ for E over $\mathbb{Q}$.
 Without loss of generality, $\alpha_1, \dots, \alpha_n$ is also a base for the $\mathcal{O}_E = \{\text{algebraic integers in } E\}$.
 $= \{a_1\alpha_1 + \dots + a_n\alpha_n : a_1, \dots, a_n \in \mathbb{Z}\}$.
 (If $E = \mathbb{Q}[\xi]$, $\xi = \xi_n$, then we can take base $\{1, \xi, \xi^2, \dots, \xi^{\phi(n)-1}\}$.
 If $E = \mathbb{Q}[\sqrt{5}]$ then $\{1, \sqrt{5}\}$ is a basis. But $\mathbb{Z}[\sqrt{5}] \subset \mathcal{O}_E$ doesn't include $\frac{1+\sqrt{5}}{2}$. New basis
 $\{\underset{\alpha_1}{1}, \underset{\alpha_2}{\alpha}\}$ is a base for $\mathcal{O}_E = \mathbb{Z}[\alpha] = \{a+b\alpha : a, b \in \mathbb{Z}\}$.)

The following works in any number field, not necessarily Galois.
 Every element $\beta \in E$ determines a linear transformation $E \rightarrow E$, $x \mapsto \beta x$. With respect to our base $\alpha_1, \dots, \alpha_n$ for $\mathcal{O}_E$, β has an $n \times n$ matrix $[b_{ij}]_{1 \leq i, j \leq n}$ i.e. $\beta\alpha_i = \sum_{j=1}^n b_{ij}\alpha_j$ for all $i \in \{1, 2, \dots, n\}$.
 (see appendices on matrix representations of field extensions). $\uparrow$ $b_{ij} \in \mathbb{Q}$.

Every field element $\beta \in E$ has a trace and norm defined by
 $T(\beta) = \text{trace} \begin{bmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{bmatrix} = \sum_{i=1}^n b_{ii}$; $N(\beta) = \det \begin{bmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{bmatrix}$

$T: E \rightarrow \mathbb{Q}$ is $\mathbb{Q}$ -linear $T(\beta + \beta') = T(\beta) + T(\beta')$; $N(\beta\beta') = N(\beta)N(\beta')$.

If $\beta \in \mathcal{O}_E$ then $T(\beta), N(\beta) \in \mathbb{Z}$.

The discriminant of the extension is $\text{disc}_{\mathbb{Q}} E$ is the determinant of the $n \times n$ matrix whose ij -entry is $T(\alpha_i \alpha_j) \in \mathbb{Z}$.

In $E \supseteq \mathbb{Q}$ (finite extension) there are only finitely many primes that ramify and these are exactly the primes that divide the discriminant.

Start with $E = \mathbb{Q}[\sqrt{5}]$ as an example using base $\{1, \alpha\}$, $\alpha = \frac{1+\sqrt{5}}{2}$.

$$\mathcal{O} = \mathcal{O}_E = \{a+b\alpha : a, b \in \mathbb{Z}\} = \mathbb{Z}[\alpha].$$

This extension has discriminant ----

$$T(a+b\alpha) = \begin{aligned} (a+b\alpha)1 &= a+b\alpha \\ (a+b\alpha)\alpha &= a\alpha + b\alpha^2 = a\alpha + b(\alpha+1) \\ &= b + (a+b)\alpha \end{aligned}$$

$$\alpha^2 = \alpha + 1$$

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

$$\alpha = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2} ; \quad \alpha = \frac{1+\sqrt{5}}{2}$$

The matrix representation of $\beta \in E$ is $\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$

$$\mathbb{Q}[\alpha] \cong \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{Q} \right\}.$$

$$\det \begin{bmatrix} T(1) & T(\alpha) \\ T(\alpha) & T(\alpha^2) \end{bmatrix} = \det \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} = 5$$

$$T(\beta) = 2a+b$$

$$N(\beta) = a^2 + ab - b^2$$

$$\det \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = a^2 + ab - b^2$$

$$\alpha^2 = \alpha + 1$$

$$T(\alpha^2) = T(\alpha)$$

The only ordinary (rational) prime $p \in \mathbb{Z}$ which ramifies is $p=5$.

5 is irreducible in $\mathbb{Z}$ but not in $\mathcal{O}$ where $5 = \sqrt{5}\sqrt{5}$.

Claim: $\sqrt{5}$ is irreducible in $\mathcal{O}$.

$$\text{If } \sqrt{5} = \beta\gamma, \quad \beta, \gamma \in \mathcal{O} \quad \text{then} \quad N(\sqrt{5}) = \underbrace{N(\beta)}_{\in \mathbb{Z}} \underbrace{N(\gamma)}_{\in \mathbb{Z}} = -5$$

$$\sqrt{5} = \underbrace{-1}_{a=-1} + \underbrace{2\alpha}_{b=2}$$

$$N(\sqrt{5}) = (-1)^2 + (-1)(2) - (2)^2 = -5.$$

$$\text{Or } \sqrt{5} \cdot (-\sqrt{5}) = -5.$$

One of $N(\beta)$ is ± 1 and the other is ∓ 5 .

$$N(\beta) = \pm 1 \Rightarrow \begin{aligned} \beta \cdot \beta' &= \pm 1 \\ \beta \cdot (\pm \beta') &= 1 \\ &\underbrace{\hspace{1cm}}_{\text{units in } \mathcal{O}} \end{aligned}$$

Actually $\mathcal{O}^\times$ is an infinite group.

$$\mathcal{O}^\times = \{ \pm \alpha^k : k \in \mathbb{Z} \}$$

$$E = \mathbb{Q}[\xi], \quad \xi = \xi_p, \quad p \text{ prime}; \quad \mathcal{O} = \mathbb{Z}[\xi] = \{a_0 + a_1 \xi + \dots + a_{p-2} \xi^{p-2} : a_i \in \mathbb{Z}\}$$

where $\underbrace{1 + \xi + \xi^2 + \dots + \xi^{p-2} + \xi^{p-1}}_{\Phi_p(\xi)} = 0$

Any $p-1$ of $1, \xi, \xi^2, \dots, \xi^{p-1}$ form a base for $\mathcal{O}$ over $\mathbb{Z}$. eg. $1, \xi, \dots, \xi^{p-2}$

or $\xi, \xi^2, \dots, \xi^{p-1}$ which we will use instead of $1, \xi, \dots, \xi^{p-2}$.

$$T(1) = p^{-1} \quad 1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{p-1 \times p-1}$$

$$T(\xi) = \xi + \xi^2 + \dots + \xi^{p-1} = -1$$

$$T(\xi^k) = -1 \quad \text{for } 1 \leq k \leq p-1$$

$$T(\xi^k \xi^l) = \begin{cases} -1 & \text{if } k+l \neq p \\ p^{-1} & \text{if } k+l = p \end{cases} \quad \text{"Gram" matrix}$$

$$\det [T(\xi^k \xi^l)]_{k,l} = (-1)^{\frac{p-1}{2}} p^{p-2}$$

$$\xi \mapsto \begin{bmatrix} 0 & 0 & \dots & 0 & -1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

$\xi \cdot \xi^{p-2} = \xi^{p-1} = -1 - \xi - \dots - \xi^{p-2}$

$$\begin{bmatrix} 1 & 2 & \dots & p \\ \vdots & \vdots & \ddots & \vdots \\ p-1 & p-1 & \dots & p-1 \end{bmatrix} \sim \begin{bmatrix} -1 & -1 & \dots & -1 \\ 0 & 0 & \dots & p \\ \vdots & \vdots & \ddots & \vdots \\ p & 0 & \dots & 0 \end{bmatrix}$$

The only prime that ramifies in E is p .

discriminant of $E = \mathbb{Q}[\xi] \supset \mathbb{Q}, \quad \xi = \xi_p, \quad p \text{ prime}$

E has unique factorization for primes $p < 23$; for $p = 23$, factorization is not unique.

Each extension $E \supset \mathbb{Q}$ has an ideal class group which measures the extent to which unique factorization fails. This group has order $h_E \geq 1$, and $h_E = 1$ iff E has unique factorization (i.e. $\mathcal{O}_E$ has unique factorization).

The naive approach to ^{trying to} prove FLT is not easy if $h_E > 1$ (unique factorization fails) but it can be salvaged to a large extent if h_p is not divisible by p .

Computing h_E is not truly elementary; use the analytic class number formula.

But there is an elementary way to check whether p divides $h_{\mathbb{Q}[\xi_p]}$ using Bernoulli numbers.

$$\frac{x}{e^x - 1} = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \frac{1}{30240}x^6 - \dots - \frac{691}{1307...0}x^{12} + \dots = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n, \quad B_n = n^{\text{th}} \text{ Bernoulli number}$$

$$g(x) = \frac{x}{e^x - 1} + \frac{1}{2}x \quad g(-x) = \frac{-x}{e^{-x} - 1} - \frac{1}{2}x = \frac{-xe^x}{1 - e^x} - \frac{1}{2}x = \frac{xe^x}{e^x - 1} - x = \frac{xe^x}{e^x - 1} - x \frac{e^x - 1}{e^x - 1} = \frac{x}{e^x - 1} = g(x)$$

even function

$$B_n: 1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, -\frac{1}{42}, \dots$$

We say a ^(odd) prime p is regular if $B_2, B_4, \dots, B_{p-3}$ have no numerators divisible by p .

Otherwise p is irregular. $\leftarrow e^{-x}$
 Heuristically, about 61% of the primes are regular
 37 is the smallest irregular prime