$K/\mathbb{Q}$ is galois with group $\{1, \sigma\}$
for $\sigma(\sqrt{d}) = -\sqrt{d}$.

Reminder:

The quadratic number fields are precisely the fields $K = \mathbb{Q}(\sqrt{d}\,)$ for all squarefree integers $d \in \mathbb{Z} \smallsetminus \{0, 1\}$, and

$$\boxed{\mathcal{O}_K \;=\; \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod (4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod (4) \end{cases}}$$

Definition 3.5.6: We have the following cases:

(a) If $d > 0$, there exist precisely two distinct embeddings $\sigma_1, \sigma_2 \colon K \hookrightarrow \mathbb{R}$ and we call K *real quadratic.* In this case we obtain a natural embedding

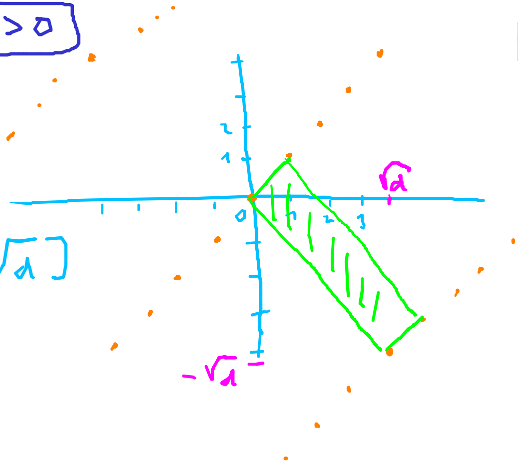
$$(\sigma_1, \sigma_2) \colon K \longhookrightarrow \mathbb{R}^2.$$

(b) If $d < 0$, there exist precisely two distinct embeddings $\sigma, \bar{\sigma} \colon K \hookrightarrow \mathbb{C}$ that are conjugate under complex conjugation, and we call K *imaginary quadratic.* In this case we obtain a natural embedding

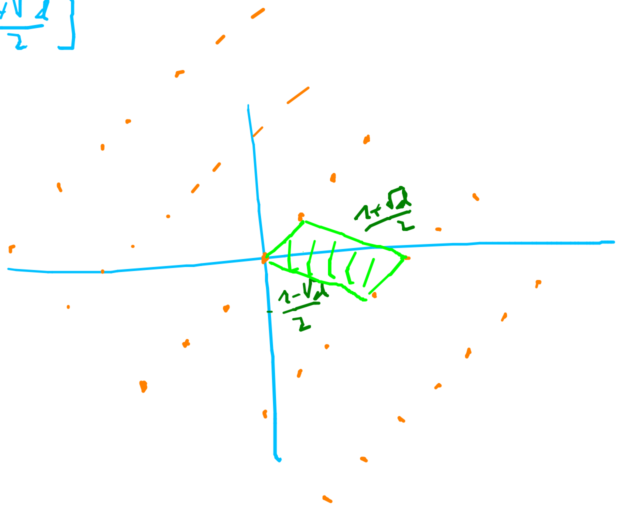
$$\sigma \colon K \longhookrightarrow \mathbb{C}.$$

$\boxed{d>0}$ $\mathbb{R}^2$

$\mathbb{Z}[\sqrt{d}]$

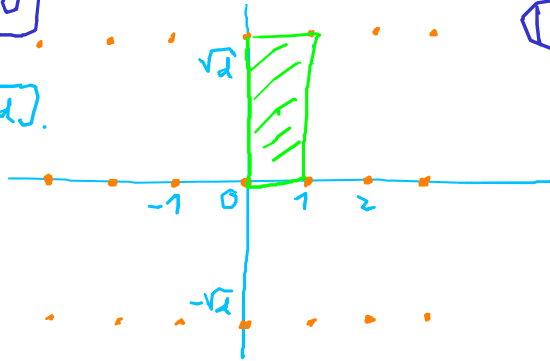


$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

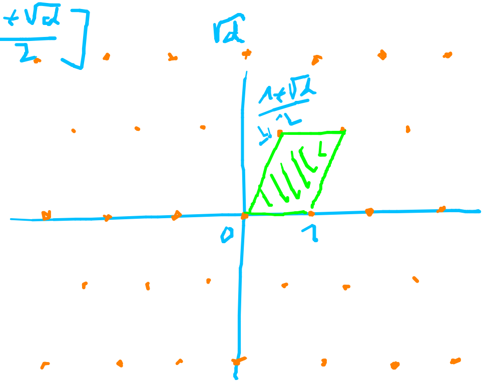


$\boxed{d<0}$ $\mathbb{C}$

$\mathbb{Z}[\sqrt{d}]$.



$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$



3.6 Cyclotomic fields

Fix an integer $n \geqslant \cancel{1}\ 2$

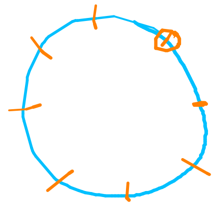
$\Uparrow$ ζ is integral over $\mathbb{Z}$.

Definition 3.6.1: (a) An element $\zeta \in \mathbb{C}$ with $\boxed{\zeta^n = 1}$ is called an *n-th root of unity.*

(b) An element $\zeta \in \mathbb{C}^\times$ of precise order n is called a *primitive n-th root of unity.*

Proposition 3.6.2: The n-th roots of unity form a cyclic subgroup $\mu_n \subset \mathbb{C}^\times$, which is generated by any primitive n-th root of unity, for instance by $e^{\frac{2\pi i}{n}}$.

$K/\mathbb{Q}$ is galois finite.
$=$ splitting field of $X^n - 1$.



For the following we fix a primitive n-th root of unity ζ and set $K := \mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$.

Proposition 3.6.3: (a) An integral power ζ^a has order n if and only if $\gcd(a, n) = 1$.

(b) For any such a we have $\frac{1-\zeta^a}{1-\zeta} \in \mathcal{O}_K^\times$.

Proof: $\zeta \neq 1 \Rightarrow$ well defined.

$$\frac{1-\zeta^a}{1-\zeta} = 1 + \zeta + \ldots + \zeta^{a-1} \in \mathcal{O}_K$$

WLOG: $a > 0$

a coprime to $n \Rightarrow$ Pick $b > 0$ with $ab \equiv 1 \mod (n)$.

$$\Rightarrow \frac{1-\zeta}{1-\zeta^a} = \frac{1-\zeta^{ab}}{1-\zeta^a} = 1 + \zeta^a + \ldots + \zeta^{a(b-1)} \in \mathcal{O}_K.$$

qed.

Definition 3.6.4: The *n-th cyclotomic polynomial* Φ_n is the monic polynomial of degree $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ with the simple roots μ_n.

$$\Phi_n(X) = \prod_{\zeta\in\mu_n \text{ primitive}} (X-\zeta)$$

Theorem 3.6.5: The polynomial Φ_n is an irreducible element of $\mathbb{Z}[X]$.

Proof: Φ_n divides $X^n-1 \in \mathbb{Z}[X]$, monic. $\Rightarrow \Phi_n \in \mathbb{Z}[X]$.

$\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})$: $\forall \zeta \in \mu_n$ primitive: $\sigma(\zeta)$ primitive.

$\Rightarrow \sigma\Phi_n = \Phi_n \Rightarrow \Phi_n \in \mathbb{Q}[X]$.

Alternative: Use $X^n-1 = \prod_{m|n} \Phi_m(X)$.

Let $f \in \mathbb{Q}[X]$ be the minimal polynomial of ζ over $\mathbb{Q}$.

$\Rightarrow f \in \mathbb{Z}[X]$ and $f \mid X^n-1$.

Claim 1: For any prime $p \nmid n$: $f(\zeta^p) = 0$.

Proof: If not, let $g \in \mathbb{Z}[X]$ be the min. pol. of ζ^p over $\mathbb{Q}$. Then $f \cdot g \mid X^n-1$.

Write $X^n-1 = fgh$ with $h \in \mathbb{Z}[X]$.

$g(\zeta^p) = 0 \Rightarrow \zeta$ is a root of $g(X^p) \Rightarrow f \mid g(X^p)$. Write $g(X^p) = f\cdot k$ for $k \in \mathbb{Z}[X]$.

Reduce mod (p) ⇝ $\bar f, \bar g, \bar h, \bar k \in \mathbb{F}_p[X]$

$\Rightarrow \bar g^p(X) = \bar g(X^p) = \bar f \cdot \bar k \Rightarrow \bar f$ and $\bar g$ have a common zero in $\overline{\mathbb{F}_p}$.

$\Rightarrow X^n-1 \bmod (p) = \bar f \bar g \bar h$ has a multiple zero in $\overline{\mathbb{F}_p}$.

But $\frac{d}{dX}(X^n-1) = \underset{\neq 0 \text{ in } \mathbb{F}_p}{n} \cdot X^{n-1}$ is coprime to X^n-1 in $\mathbb{F}_p[X]$

$\Rightarrow$ Contradiction!

qed (Claim 1)

Claim 2: $\forall a \in \mathbb{Z}$ coprime to n: $f(\zeta^a) = 0$

Proof: WLOG: $a > 0$. Write $a = p_1 \cdots p_r$ with primes $p_i \nmid n$.

Apply Claim 1 to each p_i and $\zeta^{p_1 \cdots p_{i-1}}$ & do induction! $\square$

By Claim 2 we have $\Phi_n \mid f \mid \Phi_n \Rightarrow f = \Phi_n$ $\square$

Theorem 3.6.6: The extension $K/\mathbb{Q}$ is finite galois of degree $\varphi(n)$ and there is a natural isomorphism $e\colon \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ with the property

$$\forall \gamma \in \mathrm{Gal}(\overset{K/\mathbb{Q}}{\cancel{K(\zeta_n)/K}})\colon\ \gamma(\zeta) = \zeta^{e(\gamma)}.$$

Injektiv z: $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

and $[K/\mathbb{Q}] = \deg(\Phi_n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ $\Bigg\}$ $\Rightarrow$ ism.

Theorem 3.6.7: If $n = \ell^\nu$ for a prime ℓ and an integer $\nu \geqslant 1$, then:

(a) We have $\Phi_{\ell^\nu}(X) = \sum_{i=0}^{\ell-1} X^{i\ell^{\nu-1}}$.

(b) The ideal $(1-\zeta)$ of $\mathcal{O}_K$ satisfies $(1-\zeta)^{\ell^{\nu-1}(\ell-1)} = (\ell)$.

(c) The ideal $(1-\zeta)$ is the unique prime ideal of $\mathcal{O}_K$ above $(\ell) \subset \mathbb{Z}$ and has residue field $\mathcal{O}_K/(1-\zeta) \cong \mathbb{F}_\ell$.

(d) $\mathcal{O}_K = \mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(\Phi_{\ell^\nu})$.

(e) $\mathrm{disc}(\mathcal{O}_K) = \pm\ell^{\ell^{\nu-1}(\nu\ell-\nu-1)}$.