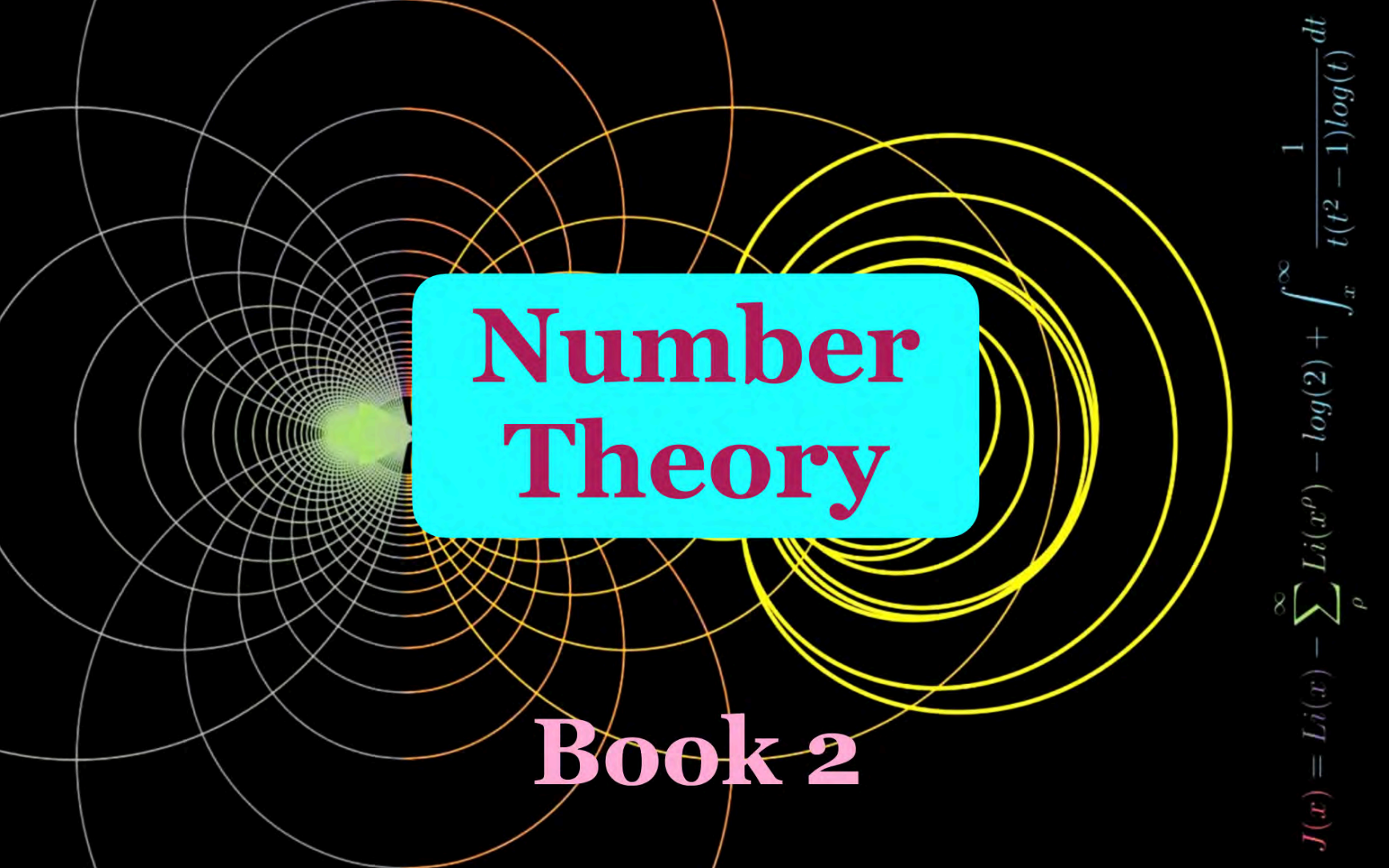

Number
Theory
Book 2
$J(x) = Li(x) - \sum_{\rho}^{\infty} Li(x^{\rho}) - \log(2) + \int_{x}^{\infty} \frac{1}{t(t^2-1)\log(t)} dt$

If R is any ring with identity then $R^\times = \{\text{units in } R\} = \{\text{invertible elements in } R\} = \{u \in R : uv = vu = 1 \text{ for some } v \in R\}$.
The units in the ring of $n \times n$ matrices over R form a mult. gp. $GL_n(R)$.
The units $R^\times$ the unit group of R.

If R is a commutative ring with identity then $R^\times$ is abelian.

Take $\mathcal{O} = \{\text{alg. integers in } K\}$ $K \supseteq \mathbb{Q}$ finite extension. We want to describe $\mathcal{O}^\times$ = unit group of the extension, an abelian multiplicative group.

eg. $\mathbb{Z}^\times = \{\pm 1\}$. $|\mathcal{O}^\times| \geq 2$ since $\pm 1 \in \mathcal{O}^\times$.

In a real quadratic field, $\mathcal{O}^\times = \{\pm 1\} \times \langle \alpha \rangle$ (torsion part: the elements of finite order in $\mathcal{O}$ (roots of unity in $\mathcal{O}$); $\langle \alpha \rangle = \{\alpha^k : k \in \mathbb{Z}\}$ infinite cyclic group with generator α)

eg. $K = \mathbb{Q}[\sqrt{2}]$, $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$,
$\mathcal{O}^\times = \{\pm (1+\sqrt{2})^k : k \in \mathbb{Z}\}$
$\alpha = 1+\sqrt{2}$ is a generator of the "infinite" part of $\mathcal{O}^\times$.
Note: $\alpha^{-1} = -1+\sqrt{2}$
$\mathcal{O}^\times = \{\pm 1, \pm 1 \pm \sqrt{2}, \pm 3 \pm 2\sqrt{2}, \cdots\}$
$\langle \alpha \rangle = \langle 1+\sqrt{2} \rangle$ = positive elements in $\mathcal{O}^\times$.
$\{\pm 1\} \times \langle 1-\sqrt{2} \rangle = \{\pm 1\} \times \langle 1+\sqrt{2} \rangle = \mathcal{O}^\times$
($\{\pm 1\} \times \langle 1+\sqrt{2} \rangle$: canonical; $\langle 1-\sqrt{2} \rangle$: not canonical)

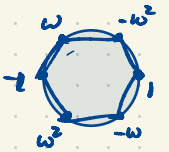
Solutions of $x^2 - 2y^2 = \pm 1$ are $\{(\pm 1, 0), (\pm 1, \pm 1), (\pm 3, \pm 2), \cdots\}$.

$\mathcal{O}^\times = \{\text{units}\} = \{\text{solutions of Pell's equation } x^2 - dy^2 = \pm 1\}$

Imaginary quadratic fields $K = \mathbb{Q}[\sqrt{d}]$, $d < 0$
$\mathcal{O}^\times$ is finite since the equation $x^2 - dy^2 = \pm 1$ has only finitely many solutions

If $K = \mathbb{Q}[\sqrt{-5}]$ then $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, $\mathcal{O}^\times = \{\pm 1\}$.
$\cdots$ $\mathbb{Q}[\sqrt{-3}]$ $\mathcal{O} = \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$ $\mathcal{O}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ sixth roots of unity
$\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$ $\mathcal{O} = \mathbb{Z}[i]$ $\mathcal{O}^\times = \{\pm 1, \pm i\}$

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



Dirichlet's Unit Theorem If $\mathcal{O}$ is the ring of integers in a number field $K \supseteq \mathbb{Q}$ ($[K:\mathbb{Q}] < \infty$),

then $\mathcal{O}^\times$ = {roots of unity in $\mathcal{O}$} (torsion part of $\mathcal{O}^\times$; finite cyclic group of even order) $\times$ free abelian group of rank r_1+r_2-1

$$\cong \mathbb{Z}^{r_1+r_2-1} = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r_1+r_2-1}$$

written additively.

r_1+r_2-1 = number of generators.

What are r_1, r_2?

$K \supseteq \mathbb{Q}$ is a number field. $K = \mathbb{Q}[\alpha]$ for some $\alpha \in K$. (Not canonical.)

$$\cong \mathbb{Q}[x]/(m(x))$$

$m(x) \in \mathbb{Q}[x]$ irreducible

has r_1 real roots, $2r_2$ non-real roots (r_2 complex conjugate pairs)

e.g. $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$ degree 4 over $\mathbb{Q}$

$= \mathbb{Q}[\sqrt{2}+\sqrt{3}]$

K can be embedded in $\mathbb{C}$ in $n = [K:\mathbb{Q}]$ ways (not canonically), $n = r_1 + 2r_2$.

by mapping $x \mapsto$ any of the roots of $m(x)$.

Dirichlet's Unit Theorem applies to all number fields, Galois or not. $|\mathrm{Aut}\, K| \le n$.

Equality iff K is a Galois extension

Eg. $K = \mathbb{Q}[\sqrt{d}]$, d squarefree, $d \neq 0,1$. $K \cong \mathbb{Q}[x]/(x^2-d)$

If $d>0$ then $r_1=2$, $r_2=0$, $n = r_1+2r_2 = 2$, rank $r_1+r_2-1 = 2+0-1 = 1$.

If $d<0$ then $r_1=0$, $r_2=1$, $n = r_1+2r_2 = 2$, rank $r_1+r_2-1 = 0+1-1 = 0$.

The class number h_K of a number field can be computed analytically by