The background features a complex pattern of overlapping circles in various colors (white, orange, yellow) that create a sense of depth and movement. A bright, glowing green and yellow point is located at the center of the pattern, from which the circles appear to radiate.

Number Theory

Book 2

$$J(x) = Li(x) - \sum_p^\infty Li(x^p) - \log(2) + \int_x^\infty \frac{1}{t(t^2 - 1)\log(t)} dt$$

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

$uv = vu = 1$ for some $v \in R$

If R is a commutative ring with identity then R^* is abelian.

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

eg. $\mathbb{Z}^* = \{\pm 1\}$. $|\mathcal{O}^*| \geq 2$ since $\pm 1 \in \mathcal{O}^*$.
 In a real quadratic field, $\mathcal{O}^* = \underbrace{\{\pm 1\}}_{\text{torsion part: the elements of finite order in } \mathcal{O} \text{ (roots of unity in } \mathcal{O})} \times \underbrace{\langle \alpha \rangle}_{\text{infinite cyclic group with generator } \alpha}$

eg. $K = \mathbb{Q}[\sqrt{2}]$, $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$,
 $\mathcal{O}^* = \{\pm (1+\sqrt{2})^k : k \in \mathbb{Z}\}$

$\alpha = 1+\sqrt{2}$ is a generator of the "infinite" part of \mathcal{O}^* \uparrow fundamental unit.

Note: $\alpha^{-1} = -1+\sqrt{2}$

$\mathcal{O}^* = \{\pm 1, \pm 1 \pm \sqrt{2}, \pm 3 \pm 2\sqrt{2}, \dots\}$ Solutions of $x^2 - 2y^2 = \pm 1$, are $\{(\pm 1, 0), (\pm 1, \pm 1), (\pm 3, \pm 2), \dots\}$
 $\langle \alpha \rangle = \langle 1+\sqrt{2} \rangle = \text{positive elements in } \mathcal{O}^*$

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

$\{\pm 1\} \times \langle -1-\sqrt{2} \rangle = \{\pm 1\} \times \langle 1+\sqrt{2} \rangle = \mathcal{O}^*$
 (Note: $\langle -1-\sqrt{2} \rangle$ is not canonical)

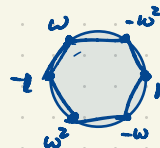
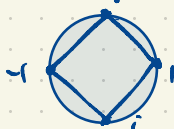
Imaginary quadratic fields $K = \mathbb{Q}[\sqrt{d}]$, $d < 0$

\mathcal{O}^* is finite since the equation $x^2 - dy^2 = \pm 1$ has only finitely many solutions

If $K = \mathbb{Q}[\sqrt{5}]$ then $\mathcal{O} = \mathbb{Z}[\sqrt{5}]$, $\mathcal{O}^* = \{\pm 1\}$.

\dots $\mathbb{Q}[\sqrt{3}]$ $\mathcal{O} = \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{3}}{2}$ $\mathcal{O}^* = \{\pm 1, \pm \omega, \pm \omega^2\}$
 $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$ $\mathcal{O} = \mathbb{Z}[i]$ $\mathcal{O}^* = \{\pm 1, \pm i\}$
 (Note: \mathcal{O}^* are sixth roots of unity)

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



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 $\mathcal{O}^\times = \{\text{roots of unity in } \mathcal{O}\} \times \text{free abelian group of rank } r_1 + r_2 - 1$

(torsion part of \mathcal{O}^\times)
finite cyclic group of even order

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

written additively,
 $r_1 + r_2 - 1 = \text{number of generators.}$

Every number field K can be embedded $K \hookrightarrow \mathbb{C}$ (one-to-one homomorphism of rings)
in $n = [K:\mathbb{Q}]$ distinct ways.
 r_1 of these embeddings have their image $\subset \mathbb{R}$; the other $2r_2$ such embeddings non-real.
 K has r_1 real and $2r_2$ non-real embeddings.

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 roots)

eg. $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$
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.

$|Aut K| \leq n$.
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 $r_1 = 2, r_2 = 0, n = r_1 + 2r_2 = 2, \text{rank } r_1 + r_2 - 1 = 2 + 0 - 1 = 1$.

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

Another example with Dirichlet's Unit Theorem

$$K = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\} \supset \mathbb{Q} \quad \text{degree } [K:\mathbb{Q}] = 4$$

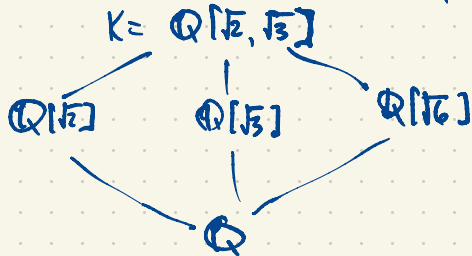
Every embedding $K \hookrightarrow \mathbb{C}$ is real ($K \hookrightarrow \mathbb{R}$) i.e. $r_1 = 4, r_2 = 0, n = r_1 + 2r_2 = 4 + 0 = 4$.

Dirichlet's unit theorem: $\mathcal{O}^\times \cong \{\pm 1\} \times \mathbb{Z}^3$ i.e. $\mathcal{O}^\times = \{\pm \alpha^i \beta^j \gamma^k : i, j, k \in \mathbb{Z}\}$

the only roots of \mathbb{R} are ± 1

$$r_1 + r_2 - 1 = 4 + 0 - 1 = 3 \text{ gives the rank}$$

What are the generators α, β, γ unity in this case? (fundamental units)



There are all the five subfields of K by Galois theory.

$$\pm (1 + \sqrt{2})^k \text{ units in } \mathbb{Q}[\sqrt{2}]$$

$$\pm (2 + \sqrt{3})^k \text{ --- } \mathbb{Q}[\sqrt{3}]$$

$$\pm (5 + 2\sqrt{6})^k \text{ --- } \mathbb{Q}[\sqrt{6}]$$

$$x^2 - 2y^2 = \pm 1 = (1 + \sqrt{2})(1 - \sqrt{2}) = -1$$

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

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 1$$

$$x^2 - 6y^2 = \pm 1 \quad (5, 2) \text{ fundamental solution}$$

$$(5 + 2\sqrt{6})(5 - 2\sqrt{6}) = 1$$

$$\mathcal{B} \mathcal{O}^\times = \pm (1 + \sqrt{2})^k (2 + \sqrt{3})^l (5 + 2\sqrt{6})^m, \quad k, l, m \in \mathbb{Z}?$$

No, these are only 25% of the units in K .

First of all, $\mathcal{O} = \{\text{alg. int. in } K\} \cong \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$.

Since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are alg. int.

If $x = \frac{\sqrt{2} + \sqrt{6}}{2}$ then $\alpha^2 = \frac{2 + 6 + 4\sqrt{3}}{4} = 2 + \sqrt{3}$, $\alpha^2 - 2 = \sqrt{3}$, $\alpha^4 - 4\alpha^2 + 1 = 0 \Rightarrow \alpha$ is an alg. int.

In fact $\alpha \in \mathcal{O}^\times$.

$\beta = \sqrt{2} + \sqrt{3}$ then $\beta^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$.

$\beta^2 - 5 = 2\sqrt{6} \Rightarrow \beta^4 - 10\beta^2 + 1 = 0$
 $1 = 10\beta^2 - \beta^4 = \beta \cdot (10\beta - \beta^3)$

Checked using PARI/GP.

$f: \mathbb{C} \rightarrow \mathbb{C}$ is analytic in a region $\Omega \subset \mathbb{C}$ (open set) if f' exists in Ω .
 In this case at every point $z_0 \in \Omega$ there is a series expansion $f(z) = \sum_{n=0}^{\infty} a_n (z-z_0)^n$
 in some disk $|z-z_0| < r$ in Ω .



A function f is meromorphic in Ω if at every point $z_0 \in \Omega$ it has a Laurent expansion $f(z) = \sum_{n=-k}^{\infty} a_n (z-z_0)^n$, $k \in \mathbb{Z}$
 When $a_{-k} \neq 0$ with $k < 0$, we have a pole of order k (assuming k is the largest such).

f has a simple pole at z_0 if $e^{\frac{1}{z}}$ has an essential singularity at 0 ("worse" than a pole)
 $f(z) = \frac{a_{-1}}{z-z_0} + a_0 + a_1(z-z_0) + a_2(z-z_0)^2 + \dots$ $0 < |z-z_0| < r$
 a_{-1} = Residue of f at z_0 . $in \Omega$



$$\frac{1}{2\pi i} \int_{\gamma} f(z) dz = a_{-1} = \lim_{z \rightarrow z_0} (z-z_0) f(z)$$

$\zeta(s), \zeta_K(s)$ is meromorphic in \mathbb{C} with a simple pole at $s=1$.

Class number formula

$$\lim_{s \rightarrow 1} (s-1) \zeta_K(s) = \frac{2^{r_1} (2\pi)^r \text{Reg}_K h_K}{w_K \sqrt{|\text{disc } K|}}$$

residue of $\zeta_K(s)$
 at its simple pole

Reg_K = regulator of K

h_K = class number

w_K = number of roots of unity in K .

r_1 = no. of real embeddings $K \hookrightarrow \mathbb{R}$

$2r_2$ = non-real embeddings $K \hookrightarrow \mathbb{C}$

$$n = [K:\mathbb{Q}] = r_1 + 2r_2$$

Every number field $K \supseteq \mathbb{Q}$ has the form $K = \mathbb{Q}[\alpha] \cong \mathbb{Q}[x] / (m(x))$ $m(x) = \text{min. poly. of } \alpha \text{ over } \mathbb{Q}$

eg. $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ has $r_1 = 4$ real embeddings $K \hookrightarrow \mathbb{R}$
 $r_2 = 0$ non-real \dots $K \hookrightarrow \mathbb{C}$

eg. $\alpha = \sqrt{2} + \sqrt{3}$ is a generator

$$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x] / (x^4 - 10x^2 + 1)$$

\uparrow
 $r_1 = 4$ real roots $\pm\sqrt{2} \pm \sqrt{3}$
 $r_2 = 0$ non-real roots.

I worked this out with $K = \mathbb{Q}[\sqrt{5}]$ $\text{Reg}_K = 1$ in this case $h_K = 2$.

Remarks about computation:

$$\zeta_K(2) \approx 1.855557$$

$$1/\rho_K(2) \approx 0.53892$$

$\frac{\zeta_K(s)}{\zeta(s)}$ has no pole at 1. It's a Dirichlet L-function. $= (1 - \frac{1}{3^s})^{-1} (1 - \frac{1}{7^s})^{-1} (1 + \frac{1}{11^s})^{-1} (1 + \frac{1}{13^s})^{-1} (1 + \frac{1}{17^s})^{-1} (1 + \frac{1}{19^s})^{-1} (1 - \frac{1}{23^s})^{-1} \dots$

The Riemann zeta function $\zeta(s) = \frac{1}{s-1} + O(1)$ as $s \rightarrow 1$ i.e. Residue of $\zeta(s)$ at $s=1$ is 1.

$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$ converges by comparison with $\int_1^{\infty} \frac{1}{t^x} dt = \frac{1}{x-1}$ $\frac{1}{x-1} < \zeta(x) < \frac{1}{x-1} + 1$

($x > 1$)
real

Remarks about class number h_K of a quadratic number field $K = \mathbb{Q}[\sqrt{d}]$:

We know only finitely many imaginary quadratic fields have class number 1, for
 $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ eg. $h_{\mathbb{Q}[\sqrt{-5}]} = 2$

In fact $h_K \rightarrow \infty$ as $d \rightarrow -\infty$

We know much less about the real quadratic fields.

We think there are infinitely many real quadratic fields with class number 1.

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743.999\,999\,999\,999\,250\,725\,9\dots$$

$x^2 + x + 41$ has prime values for $x = 0, 1, 2, 3, \dots, 39$

There is no nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ having only prime values.

There is no known polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 which is prime infinitely often.

Is $x^2 + 1$ prime infinitely often? Open problem.

$$\text{disc}(x^2 + x + 41) = 1 - 4 \cdot 41 = -163.$$

$$640320^3 + 744 = 262\,537\,412\,640\,768\,744$$

The polynomial $x^2 + x + k$ has prime values for $x = 0, 1, 2, \dots, k-2$ ($k > 0$)

$$\iff k \in \{1, 2, 3, 5, 11, 17, 41\}$$

$$\iff h_{\mathbb{Q}[\sqrt{d}]} = 1, \quad d = 1 - 4k$$

$$\iff d \in \{-3, -7, -11, -19, -43, -67, -163\}$$

Where do Dirichlet L-functions come from?

Dirichlet characters are functions $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ satisfying $\chi(ab) = \chi(a)\chi(b)$ and some additional properties $\chi(1) = 1$, $\chi(0) = 0$ unless $\chi = 1$ identically (we usually ignore this case)

$\chi(n) = \chi(1)\chi(n) \Rightarrow \chi(1) = 0$ or 1 .

χ should be a function on $\mathbb{Z}/n\mathbb{Z}$ i.e. $\chi(a) = \chi(b)$ whenever $a \equiv b \pmod{n}$.

$$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{\chi} \mathbb{C}$$

(χ is a Dirichlet character mod n in this case)

The Dirichlet L-function corresponding to χ is

$$L_{\chi}(s) = L(\chi, s) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} = \prod_p \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right)$$

proof: use FTA (Fund. Thm. of Arithmetic: unique factorization in \mathbb{Z})

$$\frac{1}{1 - \frac{\chi(p)}{p^s}} = 1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \frac{\chi(p)^3}{p^{3s}} + \dots$$

Euler factorization

eg. There are $\phi(20) = 8$ Dirichlet characters mod 20 including

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	...
$\chi(k)$	0	1	0	1	0	0	0	1	0	1	0	-1	0	-1	0	0	0	-1	0	-1	0	1	0	1	0	0	

$$L(\chi, s) = 1 + \frac{1}{3^s} + \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} - \frac{1}{13^s} - \frac{1}{17^s} + \frac{1}{21^s} + \frac{1}{23^s} + \frac{1}{27^s} + \frac{1}{29^s} - \frac{1}{31^s} - \frac{1}{33^s} - \dots$$