The background features a complex pattern of overlapping circles in various colors (white, orange, yellow) on a black field. A bright, multi-colored spot (green, yellow, orange) 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  $\pm 1 \in \mathcal{O}^*$ .

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

$\mathcal{O}^* = \underbrace{\{\pm 1\}}_{\text{torsion part: the elements of finite order in } \mathcal{O} \text{ (roots of unity in } \mathcal{O})} \times \underbrace{\langle \alpha \rangle}_{\text{infinite cyclic group with generator } \alpha}$

$\alpha = 1+\sqrt{2}$  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  $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ ,  $\mathcal{O}^* = \{\pm 1\}$ .

$\mathbb{Q}[\sqrt{-3}]$

$\mathcal{O} = \mathbb{Z}[\omega]$ ,  $\omega = \frac{-1+\sqrt{-3}}{2}$

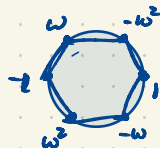
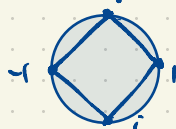
$\mathcal{O}^* = \{\pm 1, \pm \omega, \pm \omega^2\}$

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

$\mathbb{Q}[\sqrt{-4}] = \mathbb{Q}[i]$

$\mathcal{O} = \mathbb{Z}[i]$

$\mathcal{O}^* = \{\pm 1, \pm i\}$



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

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

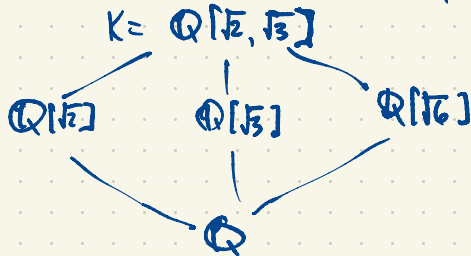
Every embedding  $K \hookrightarrow \mathbb{C}$  is real ( $K \hookrightarrow \mathbb{R}$ ) i.e.  $r_1 = 4, r_2 = 0, n = r_1 + 2r_2 = 4 + 0 = 4$ .

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  $\pm 1$

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

What are the generators  $\alpha, \beta, \gamma$  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  $x^2 = \frac{2 + 6 + 4\sqrt{3}}{4} = 2 + \sqrt{3}$ ,  $x^2 - 2 = \sqrt{3}$ ,  $x^4 - 4x^2 + 1 = 0 \Rightarrow x$  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.