Units in quadratic number fields

$K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ square-free

$$\mathcal{O}_K = \mathbb{Z}[\alpha], \quad \alpha = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4 \end{cases}$$

Imaginary quadratic field: $d<0$

$r_1 = 0$, $r_2 = 1 \Rightarrow \mathcal{O}_K^\times =$ roots of unity in K

$a, b \in \mathbb{Z}$ $\quad a + b\alpha \in \mathcal{O}_K^\times$

$$\Updownarrow$$

$$|N(a+b\alpha)| = 1$$

$d \equiv 2, 3 \pmod 4$

$$N(a+b\alpha) = (a+b\sqrt{d})(a-b\sqrt{d}) =$$

$$= a^2 - db^2 \geq 0 \quad (\text{since } d<0)$$

$$a^2 - db^2 = 1 \Leftrightarrow \begin{cases} \text{if } |d| > 1, \text{ then } b=0, a = \pm 1 \\ \text{if } d = -1 \text{ then } a = \pm 1, b = 0 \\ \qquad\qquad \text{or } a = 0, b = \pm 1 \end{cases}$$

$d \equiv 1 \pmod 4$

$$N(a+b\alpha) = \left(a + \frac{b}{2} + \frac{b}{2}\sqrt{d}\right)\left(a + \frac{b}{2} - \frac{b}{2}\sqrt{d}\right)$$

$$= \left(a + \frac{b}{2}\right)^2 - \frac{b^2}{4}d = 1$$

$$\Updownarrow$$

$$(2a+b)^2 - b^2 d = 4$$

if $d \le -7 \Rightarrow b = 0,\ a = \pm 1$

if $d = -3$ $\quad (2a+b)^2 + 3b^2 = 4$

$b = 0 \Rightarrow a = \pm 1$

$b = 1 \Rightarrow (2a+1)^2 = 1 \Rightarrow a = 0$ or $a = -1$

$b = -1 \Rightarrow (2a-1)^2 = 1 \Rightarrow a = 0$ or $a = 1$

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{-3})} = \left\{ \pm 1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2} \right\}$$

<u>Real quadratic fields</u> $\quad d > 0$

$$r_1 = 2,\ r_2 = 0 \xRightarrow{\text{Thm } 12.4} \mathcal{O}_K^\times = \mu_K \times \mathbb{Z}$$

$\mu_K = \{\pm 1\}$

$$\mathcal{O}_K^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

We can fix an embedding $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$

s.t. $\sqrt{d} > 0$

$$s : \mathcal{O}_K^\times \to \mathbb{Z}/2\mathbb{Z} \quad \text{sign}$$

$$x \longmapsto \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \end{cases} \quad \text{in this fixed embedding into } \mathbb{R}$$

$\operatorname{Ker}(s) \simeq \mathbb{Z}$ — the group of positive units in $K \subset \mathbb{R}$

<u>Def</u> The fundamental unit of K is the generator u of $\operatorname{Ker}(s)$, s.t. $u > 1$

$\mathcal{O}_K^\times = \{\pm u^n,\ n \in \mathbb{Z}\} \subset \mathbb{R}^\times$

If $x = a + b\sqrt{d}$ is a unit, $N(x) = \pm 1$

$N(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1$

$x,\ x^{-1},\ -x,\ -x^{-1}$ are of the form

$$\pm a \pm b\sqrt{d}$$

Only one of these 4 numbers is > 1

if x is a unit and $x > 1$, then

$$a,\ b > 0$$

$\Rightarrow$ if $u = a_1 + b_1\sqrt{d}$ is the fund. unit,

then $a_1, b_1 > 0$

<u>Case $d \equiv 2, 3 \pmod 4$</u> $\quad \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$

$x = a + b\sqrt{d} \in \mathcal{O}_K^\times \overset{12.1}{\Longleftrightarrow} N(x) = \pm 1$

$\Longleftrightarrow \quad a^2 - d b^2 = \pm 1, \quad a, b \in \mathbb{Z} \quad (*)$

$(*)$ is called Pell's equation

Dirichlet's unit thm $\Rightarrow$ all solutions of Pell's equation are of the form

$(\pm a_n, \pm b_n)$, where

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n \qquad n \geq 1$$

$u = a_1 + b_1\sqrt{d}$ is the fundam. unit.

Note: $$a_n + b_n\sqrt{d} = (a_{n-1} + b_{n-1}\sqrt{d})(a_1 + b_1\sqrt{d})$$
$$= a_1 a_{n-1} + d\, b_1 b_{n-1} + (b_1 a_{n-1} + a_1 b_{n-1})\sqrt{d}$$

We know $a_1, b_1 \geq 1$ by the discussion above

By induction: $a_n > a_{n-1}$, $b_n > b_{n-1}$

To find $u = a_1 + b_1\sqrt{d}$ we can consider the sequence

$$d,\ 2^2 d,\ 3^2 d,\ \dots,\ k^2 d,\ \dots$$

and take smallest k, s.t.

$$k^2 d \pm 1 \text{ is a square}$$

then let $b_1 = k$ and $a_1 = \sqrt{k^2 d \pm 1}$

Example: take $d = 7$

$k=1$	$k=2$	$k=3$
7	$4 \cdot 7 = 28$	$9 \cdot 7 = 63$
$\cancel{6}$ $\cancel{8}$	$\cancel{27}$ $\cancel{29}$	$\cancel{62}$ $64 = 8^2$

$$\Downarrow$$

$$b_1 = 8, \quad a_1 = 3$$

fund. unit is $3 + 8\sqrt{7}$

<u>Case $d \equiv 1 \pmod 4$</u> $\quad \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Write $x \in \mathcal{O}_K$ as

$$x = \frac{1}{2}(a + b\sqrt{d}), \qquad a, b \in \mathbb{Z} \text{ of the same parity}$$

Then $N(x) = \frac{1}{4}(a^2 - b^2 d) = \pm 1$

$$\Updownarrow$$

$$a^2 - b^2 d = \pm 4 \qquad (**)$$

Write $u = \frac{1}{2}(a_1 + b_1\sqrt{d})$ for the fund. unit.; all solutions of $(**)$ are of the form (a_n, b_n) where

$$\frac{1}{2}(a_n + b_n\sqrt{d}) = \left(\frac{a_1 + b_1\sqrt{d}}{2}\right)^n$$

13. Ramification of primes in number fields

$\mathbb{Q} \subset K$, $\quad p \in \mathbb{Z}$ a prime

In $\mathcal{O}_K$: $\quad (p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \qquad (\star)$

for some distinct non-zero prime ideals $\mathfrak{p}_i \subset \mathcal{O}_K$ and some $e_i \geq 1$

Recall: the prime ideals appearing in (*) are exactly those prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ for which $\mathfrak{p} \cap \mathbb{Z} = (p)$ (see exercise sheet 7)

One says that the prime ideals $\mathfrak{p}_i$ from (*) lie over (p)

We have

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathcal{O}_K \\ \cup & & \cup \\ (p) = \mathfrak{p}_i \cap \mathbb{Z} & \hookrightarrow & \mathfrak{p}_i \end{array}$$

$$\Downarrow$$

$$\mathbb{F}_p = \mathbb{Z}/(p) \hookrightarrow \mathcal{O}_K/\mathfrak{p}_i$$

$\Rightarrow \mathrm{Char}\left(\mathcal{O}_K/\mathfrak{p}_i\right) = p$

$\Rightarrow \mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$ for some $f_i \geq 1$

<u>Prop 13.1</u> Let $n = [K:\mathbb{Q}]$. Then

$$n = \sum_{i=1}^{k} e_i f_i$$

<u>Proof</u> Take the norms of both sides in (*):

$$\mathrm{Norm}((p)) = |N_{K/\mathbb{Q}}(p)| = p^n$$

$$\mathrm{Norm}((p)) \overset{(*)}{=} \prod_{i=1}^{k} \mathrm{Norm}(\mathfrak{p}_i)^{e_i}$$

$$= \prod_{i=1}^{k} (p^{f_i})^{e_i} = p^{\sum_{i=1}^{k} e_i f_i}$$

use that $\mathrm{Norm}(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| = p^{f_i}$ $\square$

<u>Cor.</u> $k \leq n$, i.e. there are at most n prime ideals in the decomp. $(*)$

<u>Def</u> The prime number p <u>ramifies</u> in $\mathcal{O}_K$, if $e_i > 1$ for at least one i in $(*)$. The prime ideal $\mathfrak{p}_i$ is <u>ramified over $\mathbb{Q}$</u> if $e_i > 1$, otherwise $\mathfrak{p}_i$ is <u>unramified/$\mathbb{Q}$</u>. If $\mathfrak{p}_i$ is ramified/$\mathbb{Q}$ and $f_i = 1$, then $\mathfrak{p}_i$ is <u>totally ramified/$\mathbb{Q}$</u>.

<u>Geometric intuition</u> Recall that for a ring R, $\mathrm{Spec}(R) = \{\text{prime ideals in } R\}$

$\mathrm{Spec}(R)$ is a topological space with Zariski topology (see lecture 6)

If $f: R_1 \to R_2$ a morphism of rings, $\mathfrak{p} \in \operatorname{Spec}(R_2)$ then $f^{-1}(\mathfrak{p}) \in \operatorname{Spec}(R_1)$

$\Rightarrow$ get a map

$$\operatorname{Spec} R_2 \longrightarrow \operatorname{Spec} R_1$$

One can check that this map is continuous (exercise)

In our case: $f: \mathbb{Z} \hookrightarrow \mathcal{O}_K$

$$\Rightarrow \varphi: \operatorname{Spec} \mathcal{O}_K \longrightarrow \operatorname{Spec} \mathbb{Z}$$
$$\mathfrak{p} \longmapsto \mathfrak{p} \cap \mathbb{Z}$$

for a prime $p \in \mathbb{Z}$

$$\varphi^{-1}((p)) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$$

where $\mathfrak{p}_i$ are primes from (*)

Geometric example: $R_1 = \mathbb{C}[y]$, $R_2 = \mathbb{C}[x]$

$$f: \mathbb{C}[y] \hookrightarrow \mathbb{C}[x]$$
$$y \longmapsto x^2$$

$$\operatorname{Spec} \mathbb{C}[x] = \{(0), (x-a) \text{ for } a \in \mathbb{C}\}$$
$$= \mathbb{C} \amalg \{(0)\}$$

$$f^{-1}((0)) = (0)$$

$$f^{-1}(\overbrace{(x-a)}^{p}) = (y-a^2)$$

because $f(y-a^2) = x^2-a^2 \in p$

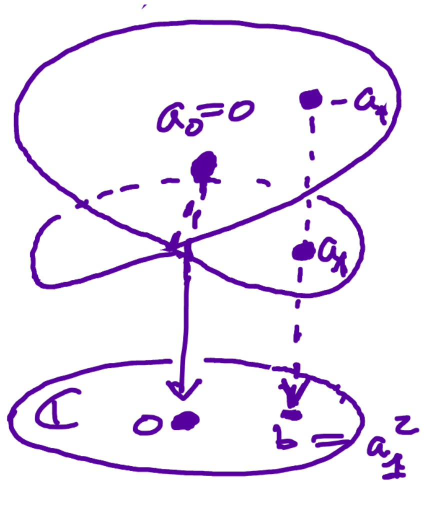
$\Rightarrow$ since $f^{-1}((x-a))$ is a prime ideal, and the ideal $(y-a^2)$ is maximal, we have

$$f^{-1}((x-a)) = (y-a^2)$$

$$\varphi: \operatorname{Spec}\mathbb{C}[x] \longrightarrow \operatorname{Spec}\mathbb{C}[y]$$
$$a\in\mathbb{C} \longmapsto a^2 \in \mathbb{C}$$
$$(0) \longmapsto (0)$$

Let $p = (y-b) \in \operatorname{Spec}\mathbb{C}[y]$

Then



$$f(y-b)\cdot\mathbb{C}[x] =$$
$$= (x^2-b)\cdot\mathbb{C}[x]$$

if $b\neq 0$ then $(x^2-b) = (x-\sqrt{b})\cdot(x+\sqrt{b})$

$$= q_1\cdot q_2$$

$f(p)\cdot\mathbb{C}[x] = q_1\cdot q_2$ unramified if $b=0$ then $f(p)\cdot\mathbb{C}[x]$

$= (x^2) = q^2$, where

$q = (x)$

$\Rightarrow$ the map φ is ramified over $b=0$

$\varphi(a) = a^2$

$\varphi' = 2a$ the derivative

φ ramifies at points where $\varphi' = 0$

$\Leftrightarrow a = 0$

More generally: $K_1 \subset K_2$ number fields

$\mathcal{O}_{K_1} \subset \mathcal{O}_{K_2}$

$\cup$

p prime

$$p\cdot\mathcal{O}_{K_2} = \prod_{i=1}^{k} p_i^{e_i}$$

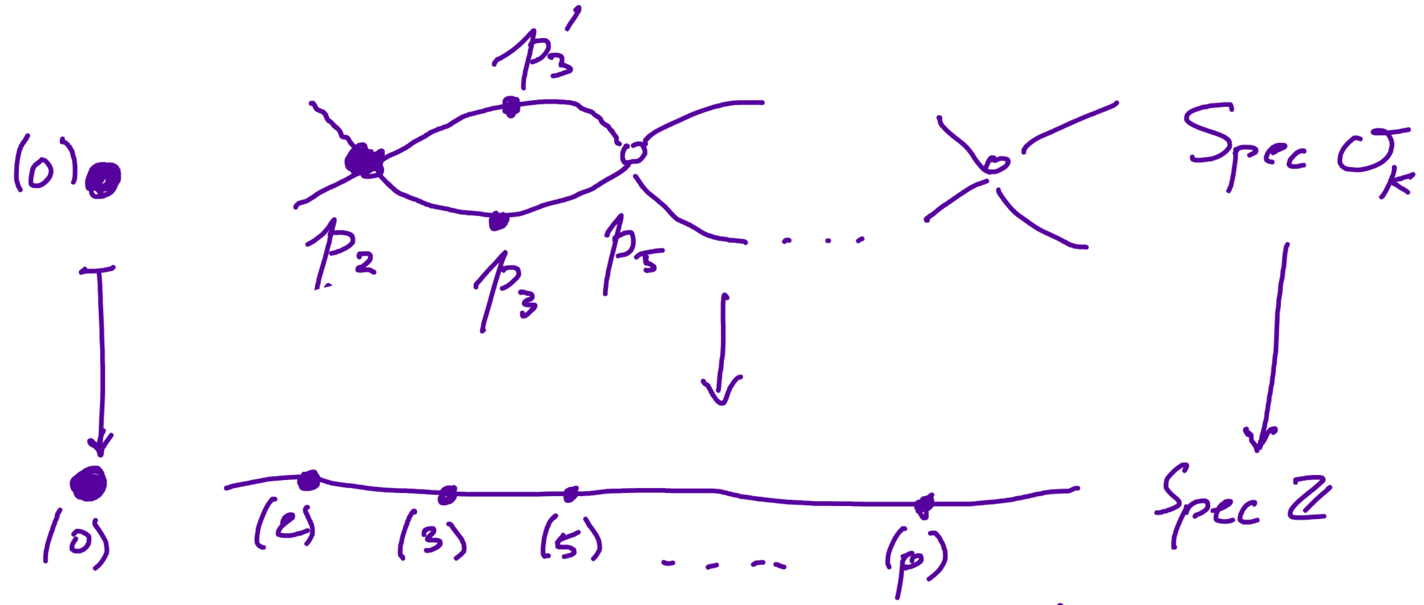
p ramifies if one of $e_i > 1$, and we again have the formula

$$[K_2 : K_1] = \sum_{i=1}^{k} e_i f_i$$

(proof later)

Which primes ramify under field extensions? Are there only fin. many ramified primes? If K is a number field, is there at least one $p \in \mathbb{Z}$ ramified in K?

To answer these questions we will introduce some "local" objects (discrete valuation rings) <u>Next week</u>



$\mathfrak{p}_2$ is ramified $(e_2 = 2)$

$\mathfrak{p}_5$ has bigger residue field $(f_5 = 2)$