Keith Conrad day 3

K = quadratic field = $\mathbb{Q}[\sqrt{d}]$ $d \in \mathbb{Z}$ squarefree

Not that $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ so for m and n in $\mathbb{Z}$
if $m|n$ in $\mathcal{O}_K$ then $\frac{n}{m} \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ so $m|n$ in $\mathbb{Z}$

Def: In any commutative ring A an ideal is an additive subgroup $I \subset A$ that 'swallows' up multiplication
~~$\forall A$~~: $\alpha \in A, x \in I \Rightarrow \alpha x \in I$

Ex. $2\mathbb{Z}$ is an ideal in $\mathbb{Z}$, $2\mathbb{Z}+2$ is not.

· given $\alpha_1, \alpha_2, \dots \alpha_n \in A$ then
$$(\alpha_1, \alpha_2, \dots \alpha_n) := A\alpha_1 + A\alpha_2 + \dots A\alpha_2$$
$$= \{a_1\alpha_1 + \dots a_n\alpha_n \mid a_i \in A\}$$

If such an ideal has $n=1$ (i.e. $(a) = Aa$) then the ideal is called principal.

Ex in $\mathbb{Z}[10]$, $(3, 1+\sqrt{10}) = \mathbb{Z}[\sqrt{10}]\cdot 3 + \mathbb{Z}[\sqrt{10}](1+\sqrt{10})$
is not principal (pf later)

! $(6,15) = \mathbb{Z}\cdot 6 + \mathbb{Z}\cdot 15 = \mathbb{Z}\cdot 3 = (3)$ is principal

Ex $\{0\} = (0)$ zero ideal $A = (1)$ unit ideal if $1 \in I \Rightarrow I = A$

Check that in $\mathbb{Z}[\sqrt{-5}]$ · $(7, 2+\sqrt{-5}) = (1)$ $1\in$

$N(2+\sqrt{-5}) = 9 \in (7, 2+\sqrt{-5})$
$\Rightarrow 27, 28 \Rightarrow 1 \in$

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

$2, 1+\sqrt{-5} \in RHS$ ($= 2-(1-\sqrt{-5})$)
$2, 1-\sqrt{-5} \in LHS$ ($= 2-(1+\sqrt{-5})$)

! $(3, 1+\sqrt{10}) \neq (3, 1-\sqrt{10})$
how to proof ?

Def The product of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A is
$$\mathfrak{a}\mathfrak{b} = \{a_1b_1 + a_2b_2 + \dots a_nb_n \mid n \geq 1, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Properties: 1, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$
, 2, $(\alpha)\mathfrak{b} = \alpha\mathfrak{b}$

LHS every element

Pf (2): on LHS any element is

$(\alpha x_1) b_1 + \dots + (\alpha x_n) b_n$
$= \alpha(x_1 b_1 + \dots x_n b_n) \in \alpha b$

so $(1) b = b$ Not $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$ $\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$

3) $(\alpha)(\beta) = (\alpha\beta)$

Pf Any element on LHS $= \alpha x_1 \beta y_1 + \dots \alpha x_n \beta y_n$
$= \alpha\beta(x_1 y_1 + \dots x_n y_n)$

Any element on RHS is $\alpha\beta x = \alpha \cdot \beta x) \in (\alpha)(\beta)$.

Thus if $\gamma = \alpha\beta \Rightarrow (\gamma) = (\alpha\beta) = (\alpha)(\beta)$

Is converse true?

If $(\alpha)(\beta) = (\gamma)$ does $\alpha\beta = \gamma$? Not quite

$(\alpha)(\beta) = (\gamma) \Rightarrow (\alpha\beta) = (\gamma)$ $\alpha\beta \in \alpha\beta A = \gamma A \ni \gamma$

$\Rightarrow \gamma | \alpha\beta$ and $\alpha\beta | \gamma$

In $\mathcal{O}_K$ or $\mathbb{Z}[\sqrt{d}]$ we get $\alpha\beta = \gamma u$ u = unit

Thm $(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta)$

Pf Any element on LHS is a finite sum of products

$(\alpha x_i + \beta y_i)(\gamma w_i + \delta z_i) = \underline{\alpha\gamma} x_i w_i + \underline{\alpha\delta} x_i z_i + \underline{\beta\gamma} y_i w_i + \underline{\beta\delta} y_i z_i$

LHS $\subset$ RHS

Conversely $\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta \in$ LHS. $\Rightarrow$ RHS $\subset$ LHS

Ex: In $\mathbb{Z}[\sqrt{10}]$ $(2, \sqrt{10})(3, 1+\sqrt{10}) = (4+\sqrt{10})$

LHS: $(6, 2+2\sqrt{10}, 3\sqrt{10}, 10+\sqrt{10})$

$= ((4+\sqrt{10})(4-\sqrt{10}), (4+\sqrt{10})(-2+\sqrt{10}), (4+\sqrt{10})(-5+2\sqrt{10}), (4+\sqrt{10})(5-\sqrt{10})$

$\frac{2+2\sqrt{10}}{4+\sqrt{10}} = -2+\sqrt{10}$

LHS $= (4+\sqrt{10}) \cdot (4-\sqrt{10}, -2+\sqrt{10}, -5+2\sqrt{10}, 5-\sqrt{10})$
$= (4+\sqrt{10}) \cdot (1)$
$= (4+\sqrt{10})$ $\quad \{5-\sqrt{10} + -4+\sqrt{10}\} = 1$

Def when $A = \mathbb{Z}[\sqrt{d}]$ or $\mathcal{O}_K$ K quadratic field

and $\mathfrak{a} \subset A$ is an ideal, we define its <u>conjugate</u> ideal to be

$\bar{\mathfrak{a}} = \{\bar{x} \mid x \in \mathfrak{a}\}$.

Ex
- $\overline{(\alpha)} = \{\overline{x \cdot y} \mid y \in A\} = \{\bar{\alpha}\bar{y} \mid y \in A\} = \{\bar{\alpha} z \mid z \in A\} = (\bar{\alpha})$

since $\overline{\frac{1+\sqrt{d}}{2}} = 1 - \left(\frac{1+\sqrt{d}}{2}\right)$

- $\overline{(\alpha_1, \dots \alpha_n)} = (\bar{\alpha}_1, \dots \bar{\alpha}_n)$ $\quad \bar{\bar{\mathfrak{a}}} = \mathfrak{a}$

Ex. In $\mathbb{Z}[\sqrt{10}]$

- $\overline{(2,\sqrt{10})} = (2,-\sqrt{10}) = (2,\sqrt{10})$
- $\overline{(3,1+\sqrt{10})} = (3,1-\sqrt{10}) \neq (3,1+\sqrt{10})$

Thm For any (nonzero) ideal in $\mathcal{O}_K$, say $\mathfrak{a}$, $\mathfrak{a}\bar{\mathfrak{a}}$ is a principal ideal with a generator in $\mathbb{Z}^+$

Ex: In $\mathbb{Z}[\sqrt{10}]$, let $\mathfrak{a} = (1+2\sqrt{10}, 1-\sqrt{10})$

$\mathfrak{a}\bar{\mathfrak{a}} = (1+2\sqrt{10})(1-\sqrt{10}) \cdot (1-2\sqrt{10}, 1+\sqrt{10})$

$= (-39, 21+3\sqrt{10}, 21-3\sqrt{10}, -9)$

$= 3(-13, 7+\sqrt{10}, 7-\sqrt{10}, -3)$

$= 3\cdot(1) = (3)$

! thm is false in $\mathbb{Z}[\sqrt{d}]$ for $d \equiv 1 \bmod 4$: $\mathfrak{a} = (2, 1+\sqrt{d})$

Note for $m,n \in \mathbb{Z}^+$ that $m\mathcal{O}_K = n\mathcal{O}_K \Rightarrow m|n$ and $n|m$ in $\mathcal{O}_K$
$\Rightarrow m|n$ and $n|m$ in $\mathbb{Z}$ $\Rightarrow m = n$

Thus the generator of $\mathfrak{a}\bar{\mathfrak{a}}$ is unique.

Def Set $N(\mathfrak{a})$ = generator in $\mathbb{Z}^+$ of $\mathfrak{a}\cdot\bar{\mathfrak{a}}$

Ex: In $\mathbb{Z}[\sqrt{10}]$, $N((1+2\sqrt{10}), (1-\sqrt{10})) = 3$

For $\mathfrak{a} = (\alpha)$ $\mathfrak{a}\cdot\bar{\mathfrak{a}} = (\alpha)\overline{(\alpha)} = (\alpha)(\bar{\alpha}) = (\alpha\bar{\alpha}) = (N(\alpha))$

then $N((\alpha)) = |N(\alpha)|$. The trivial factors of $\mathfrak{a}$ are (1) and $\mathfrak{a}$

If $\mathfrak{a}$ has no other ideal factors in $\mathcal{O}_K$ we call $\mathfrak{a}$ = prime ideal

Thm: If $N(\mathfrak{a}) = p$ = prime number then $\mathfrak{a}$ is prime ideal.

Suppose $N(\mathfrak{a}) = p$ and $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ then $N(\bar{\mathfrak{a}}) = N(\mathfrak{b}\mathfrak{c}) \overset{!}{=} N(\mathfrak{b})N(\mathfrak{c})$

$\Rightarrow p = N(\mathfrak{b})\cdot N(\mathfrak{c})$ in $\mathbb{Z}^+ \Rightarrow N(\mathfrak{b}) = 1$ or $N(\mathfrak{c}) = 1$

$N((1)) = (N(1)) = 1$ Notice $(N(\mathfrak{a})) = \mathfrak{a}\bar{\mathfrak{a}} \subset \mathfrak{a} \Rightarrow N(\mathfrak{a}) \in \mathfrak{a}$

So if $N(\mathfrak{b}) = 1$ then $1 \in \mathfrak{b} \Rightarrow \mathfrak{b} \in \mathcal{O}_K = (1)$

Thm. In $\mathcal{O}_K$, every ideal $\neq (0)$ or (1) is a product of prime ideals

- In $\mathcal{O}_K$, if we have $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$

Then $r = s$ and after relabeling $\mathfrak{p}_i = \mathfrak{q}_i$ for all i

$x^2 - 10y^2 = 6$

$(x + y\sqrt{10})(x - y\sqrt{10}) = (4+\sqrt{10})(4-\sqrt{10})$ as equation of principal ideals

$\mathfrak{p} = (2, \sqrt{10}) = \bar{\mathfrak{p}}$ $\qquad \mathfrak{p}\mathfrak{q} = (4+\sqrt{10})$

$\mathfrak{q} = (3, 1+\sqrt{10})$ $\qquad \mathfrak{p}\bar{\mathfrak{q}} = (4-\sqrt{10})$

$\bar{\mathfrak{q}} = (3, 1-\sqrt{10})$

check

$\mathfrak{p}\bar{\mathfrak{p}} = (2), \mathfrak{q}\bar{\mathfrak{q}} = (3)$ $\qquad N((x+y\sqrt{10})) = |N(x+y\sqrt{10})| = |x^2 - 10y^2|$
$= 6$

$(x+y\sqrt{10})(x-y\sqrt{10}) = \mathfrak{p}\mathfrak{q}\mathfrak{p}\bar{\mathfrak{q}}$ By unique fact. $\Rightarrow$

N: 2 3 2 3

$(x+y\sqrt{10}) = \mathfrak{p}\mathfrak{q}$ or $\mathfrak{p}\bar{\mathfrak{q}}$
$= (4+\sqrt{10})$ or $(4-\sqrt{10})$

$\Rightarrow x + y\sqrt{10} = (4 \pm \sqrt{10}) \cdot u \quad u \in \mathbb{Z}[\sqrt{10}]^\times$

Correct derivation of yesterday's bogus method.