(Palestra 9)

K = quadratic field

How do we find prime ideals in $\mathcal{O}_K$?

Thm: Any prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is a factor of $(p) = p\mathcal{O}_K$ for some prime number p. Moreover, if $\mathfrak{p} \mid (p)$, $N(\mathfrak{p}) = p$ or p^2.

Ex: $\mathbb{Z}[i]$

$(5) = (1+2i)(1-2i)$

$(3) =$ prime

Pf: As ideals in $\mathcal{O}_K$,

$\mathfrak{p}\bar{\mathfrak{p}} = (N\mathfrak{p})$ and $N\mathfrak{p} \geq 1$.

$\downarrow$

$= (p_1)(p_2)\cdots(p_r)$

$N\mathfrak{p} = p_1 p_2 \cdots p_r$, p_i prime numbers

$N((p_i)) = p_i^2$

By unique prime ideal factorization in $\mathcal{O}_K$, $\mathfrak{p} \mid (p_i)$ for some prime number p_i

If $\mathfrak{p} \mid (p)$ where p is a prime number, then $(p) = \mathfrak{p}\mathfrak{b}$ for some ideal $\mathfrak{b}$

$\Rightarrow N((p)) = N(\mathfrak{p}\mathfrak{b})$

$|N(p)| = N\mathfrak{p} \, N\mathfrak{b}$ in $\mathbb{Z}^+$

$p^2 = N\mathfrak{p} \, N\mathfrak{b}$

$\Rightarrow N\mathfrak{p} = p$ or p^2

Rule for factoring (p) in $\mathcal{O}_K$:

$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

root of $x^2 - d = f(x)$, $\alpha = \sqrt{d}$

root of $f(x) = x^2 - x + \frac{1-d}{4}$, $\alpha = \frac{1+\sqrt{d}}{2}$

Given prime number p:

① If $f(x) \bmod p$ is irreducible, then $(p) = p\mathcal{O}_K$ is prime of norm p^2.

② If $f(x) \equiv (x-c)(x-c') \bmod p$ then $(p) = (p, \alpha - c)(p, \alpha - c')$ where factors have norm p.

Ex: $\mathbb{Z}[\sqrt{10}]$ $\alpha=\sqrt{10}$ $f(x)=x^2-10$

p	$x^2-10 \bmod p$	(p)	
2	$x\cdot x=x^2 \bmod 2$	$(2,\sqrt{10})^2$	$\longrightarrow N=2$
3	$(x+1)(x-1) \bmod 3$	$(3,\sqrt{10}+1)(3,\sqrt{10}-1)$	$\longrightarrow N=3$
5	$x^2 \bmod 5$	$(5,\sqrt{10})^2$	$\longrightarrow N=5$
7	irreducible	(7)	$\longrightarrow N=49$

No ideal of norm 7.

What ideals in $\mathbb{Z}[\sqrt{10}]$ have norm 10?

$N(\mathfrak{a})=10 \Rightarrow \mathfrak{a}=\mathfrak{p}\mathfrak{q}$, $N(\mathfrak{p})=2$, $N(\mathfrak{q})=5 \Rightarrow \mathfrak{q}=(2,\sqrt{10})$ or $(5,\sqrt{10})$ $(\sqrt{10})$

The ideals $\mathfrak{p}_2=(2,\sqrt{10})$

$\mathfrak{p}_3=(3,\sqrt{10}+1)$, $\overline{\mathfrak{p}_3}=(3,\sqrt{10}-1)$

$\mathfrak{p}_5=(5,\sqrt{10})$

are all nonprincipal: Try to solve $|N(\alpha)|=2,3,5$ in $\mathbb{Z}[\sqrt{10}]$

Yesterday we saw $x^2-10y^2=\pm 2,\pm 3,\pm 5$

$(4+\sqrt{10})=\mathfrak{p}_2\mathfrak{p}_3 \longrightarrow (4+\sqrt{10})\mathfrak{p}_2=(2)\mathfrak{p}_3=2\mathfrak{p}_3$

$(4-\sqrt{10})=\mathfrak{p}_2\overline{\mathfrak{p}_3} \longrightarrow (4-\sqrt{10})\mathfrak{p}_2=2\overline{\mathfrak{p}_3}$

$(2)=\mathfrak{p}_2^2$

$(\sqrt{10})=\mathfrak{p}_2\mathfrak{p}_5 \longrightarrow \sqrt{10}\,\mathfrak{p}_2=2\mathfrak{p}_5$

$(\alpha)=\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$ and $\mathfrak{b}$

$\alpha\in\mathfrak{a}$, $\alpha\in\mathfrak{b}$

Definition: For nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, we write $\mathfrak{a}\sim\mathfrak{b}$ if there are $x,y\in\mathcal{O}_K-\{0\}$ s.t. $x\mathfrak{a}=y\mathfrak{b}$.
This is an equivalence relation on ideals.

Thm: We have $\mathfrak{a}\sim(1)\Leftrightarrow\mathfrak{a}$ is principal.

Pf: If $\mathfrak{a}=(\alpha)=\alpha\cdot(1)$ so $\mathfrak{a}\sim(1)$ using $x=1,y=\alpha$.
Conversely, if $\mathfrak{a}\sim(1)$, then $x\mathfrak{a}=y(1)=(y)$
for some $x,y\in\mathcal{O}_K-\{0\}$.
$\Rightarrow \exists\alpha\in\mathfrak{a}$ s.t. $x\alpha=y$

So $x\mathfrak{a}=x\alpha\cdot(1)=x(x)\Rightarrow\mathfrak{a}=(\alpha)$.

The equivalence class of $\mathfrak{a}$ is denoted $[\mathfrak{a}]$ and is called an ideal class.

If $\mathfrak{a}\sim\mathfrak{a}'$ and $\mathfrak{b}\sim\mathfrak{b}'$, then $\mathfrak{a}\mathfrak{b}\sim\mathfrak{a}'\mathfrak{b}'$

$x\mathfrak{a}=x'\mathfrak{a}'$ and $y\mathfrak{b}=y\mathfrak{b}'$

$\Downarrow$

$xy\,\mathfrak{a}\mathfrak{b}=x'y'\mathfrak{a}'\mathfrak{b}'$

$[\mathfrak{a}][\mathfrak{b}]=[\mathfrak{a}\mathfrak{b}]$

Ex: $[\mathfrak{a}][(1)] = [\mathfrak{a}]$, $[\mathfrak{a}][\bar{\mathfrak{a}}] = [(N\mathfrak{a})] = [(1)]$

The ideal class group $Cl(K)$ of a quadratic field K is its ideal classes under this multiplication identity: $[(1)]$

inverse of $[\mathfrak{a}]$ is $[\bar{\mathfrak{a}}]$.

Ex $Cl(\mathbb{Z}[\sqrt{10}])$, $\overline{\mathfrak{p}_2} = \mathfrak{p}_2 \Rightarrow [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$

$\overline{\mathfrak{p}_3} \neq \mathfrak{p}_3 \not\Rightarrow [\mathfrak{p}_3]^{-1} \neq [\mathfrak{p}_3]$

Thm: $Cl(K)$ is trivial, i.e. all ideals in $\mathcal{O}_K$ are principal $\Leftrightarrow$ $\Leftrightarrow \mathcal{O}_K$ has unique factorization of elements.

Thm: For every quad. field K, $Cl(K)$ is finite. More precisely, there's a $C_K > 0$ s.t. every ideal class contains an ideal $\mathfrak{a}$ with $N(\mathfrak{a}) \leq C_K$.

$\forall_{n \geq 1} \{\mathfrak{a} : N(\mathfrak{a}) = n\}$ is finite

Ex: $N(\mathfrak{a}) = 36 = 2^2 3^2$

$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$

$\mathfrak{p} \mid (2) \to N(\mathfrak{p}) = 2$ or 4

$\mathfrak{p} \mid (3) \to N(\mathfrak{p}) = 3$ or 9

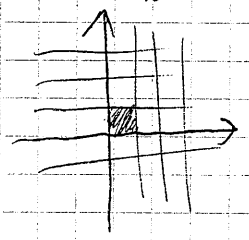
$\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

$\mathbb{Z}$

$\mathbb{C}[x]/\langle x^3 - x \rangle$

$\mathbb{C}[x]$

ideal class gp is $\cong \mathbb{C}/\mathbb{Z}[i]$



The size of $Cl(K)$ is called the class number of K and is denoted $h(K)$.

Two values of C_K:

Kronecker (1850s): write $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha$

$C_K = (1 + |a|)(1 + |c|)$ $\hookrightarrow \sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$

Minkowski (1890s)

$$C_K = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4 \quad d > 0 \\ \frac{1}{2}\sqrt{d} & \text{if } d \equiv 1 \pmod 4 \quad d > 0 \\ \frac{4}{\pi}\sqrt{|d|} & \text{if } d \equiv 2,3 \pmod 4 \quad d < 0 \\ \frac{2}{\pi}\sqrt{|d|} & \text{if } d \equiv 1 \pmod 4 \quad d < 0 \end{cases}$$

	K	Kronecker	Minkowski	
	$\mathbb{Q}[i]$	4.0	1.2	$\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}], \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$
	$\mathbb{Q}[\sqrt{2}]$	5.8	1.4	
	$\mathbb{Q}[\sqrt{3}]$	7.4	1.7	have unique factorization!
	$\mathbb{Q}[\sqrt{-7}]$	5.8	1.6	
$h=2$	$\mathbb{Q}[\sqrt{10}]$	17.3	3.1	
$h=1$	$\mathbb{Q}[\sqrt{11}]$	18.6	3.3	
$h=2$	$\mathbb{Q}[\sqrt{-51}]$	22.2	4.5	

$\mathbb{Q}[\sqrt{10}]$ What are the ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq 3$?

(1)

$\mathfrak{p}_2 = (2, \sqrt{10})$

$\mathfrak{p}_3 = (3, \sqrt{10}+1)$, $\overline{\mathfrak{p}_3} = (3, \sqrt{10}-1)$ nonprime

So there are two ideal classes: $[1]$, $[\mathfrak{p}_2] = [\mathfrak{p}_3]$

$\mathbb{Z}[\sqrt{11}]$ $f(X) = X^2 - 11$ $\alpha = \sqrt{11}$

p	$x^2 - 11 \bmod p$	(p)
2	$(x-1)^2$	$(2, \sqrt{11}-1)^2 \to N=2$
3	irred	$(3) \longrightarrow N=9$

$Cl(\mathbb{Q}[\sqrt{11}])$ is rep^{d} by ideals (1) and $(2, \sqrt{11}-1) \overset{\checkmark}{=} (3+\sqrt{11})$

$h=1$ $\qquad x^2 - y^2 = \pm 2 \to (3,1)$

$\mathbb{Q}[\sqrt{-51}] \to \mathbb{Z}\left[\frac{1+\sqrt{-51}}{2}\right]$ $\alpha = \frac{1+\sqrt{-51}}{2}$ $f(X) = X^2 - X + 13$

p	$x^2 - x + 13 \bmod p$	(p)
2	irred	$(2) \to N=4$
3	$(x-2)^2$	$(3, \alpha-2)^2 \to N=3$

$N(\mathfrak{a}) \leq 4$

$Cl(\mathbb{Q}[\sqrt{-51}])$ is rep^{d} by (1) and $(3, \alpha-2) \overset{?}{=} (x + y\frac{1+\sqrt{-51}}{2})$

$N\left(x + y\frac{1+\sqrt{-51}}{2}\right) \overset{?}{=} 3 \to \left(x + \frac{y}{2}\right)^2 + \frac{51}{4}y^2 = 3$ ✗ impossible

$\therefore h=2$

To whet your appetite for next time:

Thm: The eq^{n} $y^2 = x^3 - 51$ has no $\mathbb{Z}$-solutions.

Rk: The congruence $y^2 \equiv x^3 - 51 \mod m$ has solutions for all m.
It does have $\mathbb{Q}$-solutions: $\left(\frac{1375}{9}, \frac{50986}{27}\right)$.