LECTURE 33 Dec. 8/2003.

## Primes in $\mathbb{Z}[i]$:

$p \equiv 1 \pmod 4 \rightsquigarrow$ 2 primes $\begin{cases}\pi \\ \pi'\end{cases}$ in $\mathbb{Z}[i]$

$\pi \cdot \pi' = p$,
$\pi = a+bi$ & $a^2+b^2=p$.

$p \equiv 3 \pmod 4 \rightsquigarrow$ 1 prime $p$.
($p$ still prime in $\mathbb{Z}[i]$)

---

## Rings R analogous to $\mathbb{Z}[i]$

- $R = \mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2}\}$

  $\delta(a+b\sqrt{-2}) = a^2+2b^2$

  R is Euclidean wrt $\delta$.
- $R = \mathbb{Z}[\sqrt{-5}]$ ~~has~~ no unique factorization

  $2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

  ~~so~~ can't possibly be principal ideal domain or Euclidean domain

Consider in general, for $d$ not a square
$\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d}\} = \mathbb{Z}[X]/(X^2-d)$
→ Not quite the right analog.

Why is this not quite the right analog?

Consider $f(X) = X^2 + X + 1$

Roots $\alpha = -\frac{1 \pm \sqrt{-3}}{2}$ $\qquad 2\alpha + 1 = \pm\sqrt{-3}$

$$R = \mathbb{Z}[X]/(f(X)) = \mathbb{Z} + \mathbb{Z}\alpha$$
$$\underset{2}{\supset} \mathbb{Z} + \mathbb{Z}\sqrt{-3}$$

Two observations:

- there are <u>larger</u> "nice" rings than $\mathbb{Z}[\sqrt{-3}]$ with the same fraction field
- $\mathbb{Z}[\alpha]$ is a Euclidean domain, but $\mathbb{Z}[\sqrt{-3}]$ is not.

What is this notion of "nice" subring of a finite extension of $\mathbb{Q}$?

<u>Def</u> Algebraic integers $\alpha \in \mathbb{C}$ are the $\alpha$ which are roots of a monic poly. $f(X) \in \mathbb{Z}[X]$
$$\shortparallel$$
$$X^n + a_{n-1}X^{n-1} + \text{---} + a_0.$$

Suppose $\alpha$ satisfies $f(X)$ with $\mathbb{Q}$-coeffs where $f$ is monic and irreducible. Is $\alpha$ an algebraic integer?

Claim $\alpha$ is an algebraic integer $\Longleftrightarrow$ the monic irreducible polynomial $f(X) \in \mathbb{Q}[X]$ satisfied by $\alpha$ has integral coeffs.

Pf) See book $\boxtimes$

Application

Determine all algebraic integers in the field $\mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$

$$= \mathbb{Q}[X]/(X^2-d).$$

where $d \in \mathbb{Z}$ is squarefree.

(i.e. $d = \pm 1 \cdot p_1 \cdots p_k$ ($p_i \neq p_j$ for $i \neq j$))

Every element of $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ is an algebraic integer, since

$\alpha = a + b\sqrt{d}$ satisfies quadratic polynomial (monic):

$(X-\alpha)(X-\alpha') = X^2 - (2a)X + (a^2 - db^2)$

$(\alpha' = a - b\sqrt{d})$ with rational coeffs

& irred. if $b \neq 0$.

So assume $b \neq 0$. Then $\alpha = a + b\sqrt{d}$ is an algebraic integer $\Longleftrightarrow$

$$2a \in \mathbb{Z} \ \& \ a^2 - db^2 \in \mathbb{Z}$$

(Note: If $b = 0$, then $\alpha = a$ is an algebraic integer $\Leftrightarrow a \in \mathbb{Z}$.)

Case 1) $a$ is an integer

$\Rightarrow b^2 d$ is an integer (since $a^2 - db^2 \in \mathbb{Z}$)

$\Rightarrow b^2$ is an integer (as $d$ is square free)

$\Rightarrow b$ is an integer.

2) $a$ is in $\frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ (i.e. $2a = m$ is an odd integer)

$$a^2 = \frac{1}{4} m^2$$

$4a^2 = m^2$ is an integer so $4db^2$ is an integer. $db^2 = \frac{1}{4} n$ with $n$ odd

$\Rightarrow b = \frac{1}{2} n_0$ $\quad n_0$ odd integer.

So: $m^2 - d n_0^2 \equiv 0 \pmod 4$

But $m^2 \equiv n_0^2 \equiv 1 \pmod 4$

$\Rightarrow d \equiv 1 \pmod 4$

Then $a = \frac{1}{2} m$, $b = \frac{1}{2} n_0$ works.

<u>Therefore we have proved:</u>

<u>Prop</u> If $d$ is squarefree integer

1) If $d \equiv 2, 3 \pmod 4$ then the alg. integers in $\mathbb{Q}(\sqrt{d})$ form the ring $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$

2) If $d \equiv 1 \pmod 4$ then the alg. integers form the larger ring $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} + \mathbb{Z} \cdot \left(\frac{1+\sqrt{d}}{2}\right)$.

## Discriminants:

- The polynomial (monic irred.) satisfied by $\sqrt{d}$ is $X^2 - d$. Discrim. $= b^2 - 4ac = 4d$.
- The monic irred. polynomial satisfied by $\frac{1 \pm \sqrt{d}}{2}$ is
$$X^2 - X + \frac{(1-d)}{4}$$ has
$$\text{discriminant} = 1 - (1-d) = d.$$

We let $D$ denote this discriminant, i.e.

$$D := \begin{cases} 4d & \text{if } d \equiv 2,3 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

(where $d \in \mathbb{Z}$ is squarefree)

<u>Prop</u> $D$ has the following property:

(a) $D \equiv 0, 1 \pmod 4$

(b) $D$ is as squarefree as possible given condition (a).

---

$D < 0$ : then ring of integers $R$ is said to be imaginary quad'

$D > 0$ : then ring of integers $R$ is said to be real quadratic.

$D<0$: $-3, -4, -7, -8, -11, -15, \cdots$

$\uparrow$ $\mathbb{Z}\left[\frac{1\pm\sqrt{-3}}{2}\right]$, $\uparrow$ $\mathbb{Z}[i]$, ...

$D>0$: $5, 8, 12, 13, 17, \cdots$

---

The case $D<0$ is easier to study.

<u>Prop</u> If $D<0$ & $R$ is the associated ring of integers:

$R^\times$ is finite cyclic gp:

$D=-3 \Rightarrow$ order 6

$D=-4 \Rightarrow$ order 4

$D<-4 \Rightarrow$ order 2

$R^\times = \{\pm 1\}$.

<u>Prop</u> If $D>0$ then $R^\times$ is infinite.