Primes in $\mathbb{Z}[i]/\mathbb{Z}[w]$

Goal: To try to understand how primes in $\mathbb{Z}$ behave in $\mathbb{Z}[i]/\mathbb{Z}[w]$

Suppose $p \in \mathbb{Z}$ is a prime in $\mathbb{Z}$.

Consider $p \in \mathbb{Z}[i]/\mathbb{Z}[w]$

Case I: p stays prime in $\mathbb{Z}[i]/\mathbb{Z}[w]$

Example: (1) 3 is prime in $\mathbb{Z}[i]$

Pf: Suppose not, then $3 = (a+bi)(c+di)$

$$N(3) = N(a+bi)\,N(c+di)$$
$$9 = N(a+bi)\,N(c+di)$$
$$\Rightarrow N(a+bi) = N(c+di) = 3$$

Let's analyze possibilities for $a+bi$

If $N(a+bi) = 3$

$\Rightarrow a^2+b^2 = 3$ No solutions

$\rightarrow\leftarrow$

(We will see later that any prime of the form $4k+3$ stays prime in $\mathbb{Z}[i]$.)

(2) 5 stays prime in $\mathbb{Z}[w]$

Suppose not $5 = (a+bw)(c+dw)$

$25 = N(a+bw)\ N(c+dw)$

$\Rightarrow N(a+bw) = 5 = N(c+dw)$

what are norm 5 elements in $\mathbb{Z}[w]$?

$a^2+b^2-ab = 5$

Suppose $ab \leq 0$

then $0 \leq a^2 + b^2 + (-ab) = 5$

$5 = 5 \quad \rightarrow\leftarrow$

$= 4+1 \quad \rightarrow\leftarrow$

$= 2+3 \quad \rightarrow\leftarrow$

$= 3+1+1 \quad \rightarrow\leftarrow$

$= 2+2+1 \quad \rightarrow\leftarrow$

Suppose $ab > 0$

$$a^2+b^2-ab = a^2+b^2-ab-ab+ab$$
$$= (a-b)^2+ab \geq 0$$
$$\| $$
$$5$$
$$\rightarrow \leftarrow$$

When an integer prime p stays prime in $\mathbb{Z}[i]/\mathbb{Z}[\omega]$ we say p is inert. (Type I)

When $p \in \mathbb{Z}$ is not inert

$$p = \alpha\beta$$

α is not a unit
β is not a unit

$$p = \bar{p} = \bar{\alpha}\bar{\beta}$$

$$p^2 = \underbrace{\alpha\bar{\alpha}}_{\uparrow}\ \underbrace{\beta\bar{\beta}}_{\uparrow}$$
$$\mathbb{Z} \quad \mathbb{Z}$$

$\alpha\bar{\alpha} = p \Rightarrow \alpha, \bar{\alpha}$ is already a prime
$\beta\bar{\beta} = p$

$p = \alpha\bar{\alpha}$

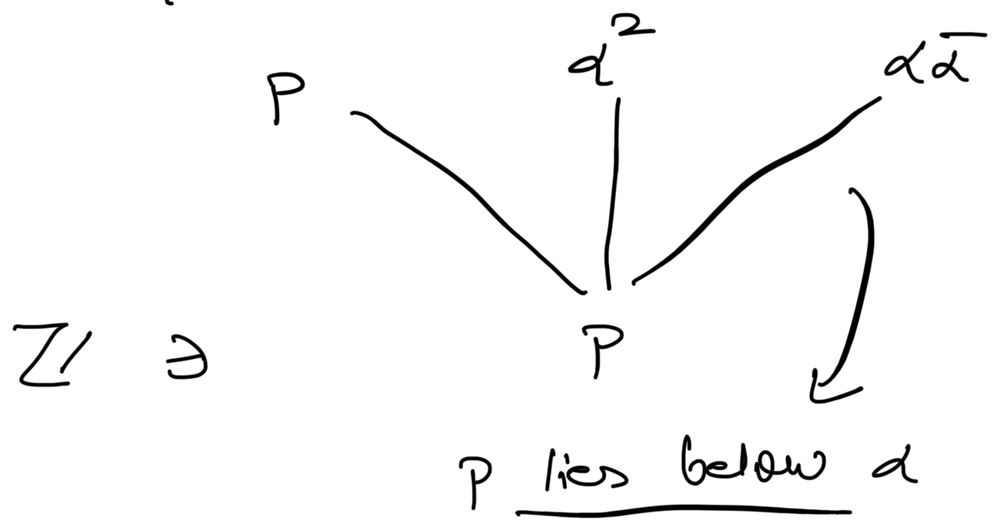
$\bar{\alpha}$ is α times a unit

p ramifies in $\mathbb{Z}[i]/\mathbb{Z}[w]$ (Type R)

$\bar{\alpha}$ is not α times a unit

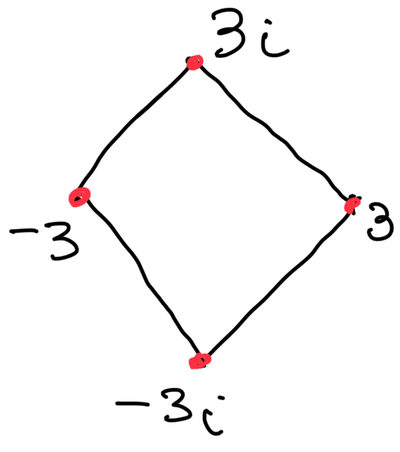
p splits in $\mathbb{Z}[i]/\mathbb{Z}[w]$ (Type S)

$\mathbb{Z}[i]/\mathbb{Z}[w]$

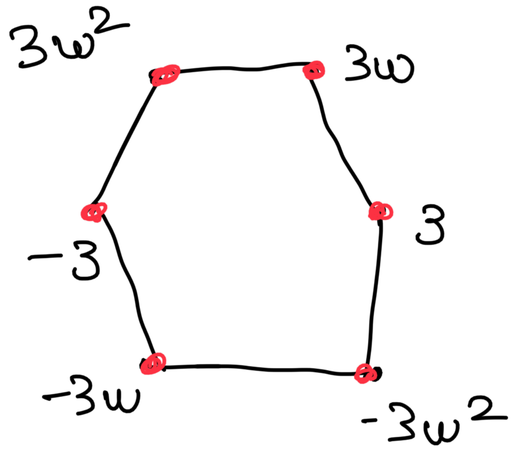


$\mathbb{Z} \ni$ p lies below α

Primagons



in $\mathbb{Z}[i]$



in $\mathbb{Z}[\omega]$

Lemma: The only prime that ramifies in $\mathbb{Z}[i]$ is 2.

Suppose: $p = \alpha\bar{\alpha}$ $\quad$ $\bar{\alpha}$ is unit times α

$\alpha = a+bi$

$\bar{\alpha} = a-bi$ $\longrightarrow$

1) $b=0$ or
2) $a=0$ or
3) $a=-b$ or
4) $a=b$

1) If $b=0$, $\Rightarrow$ $p=a^2$ $\rightarrow\leftarrow$
2) If $a=0$ $\Rightarrow$ $p=b^2$ $\rightarrow\leftarrow$
3) If $a=-b$ then $p=2a^2$ $\Rightarrow p=2$ $a=\pm 1$
4) If $a=b$ then $p=2a^2$ $\nearrow\!\!\nearrow$

Exc: The only prime that ramifies in $\mathbb{Z}[\omega]$ is 3.

$p = \alpha\bar{\alpha}$ where $\bar{\alpha} = \alpha$ times a unit

Say $\alpha = a+b\omega$ $\bar{\alpha} = a+b\omega^2 = a+b(-1-\omega)$

$= (a-b) - b\omega$

i) $\alpha = \bar{\alpha} \Rightarrow a = a-b \Rightarrow b = 0$ & $p = a^2$ $\rightarrow\leftarrow$

ii) $\alpha = -\bar{\alpha} \Rightarrow a = -a+b \Rightarrow 2a = b$ $\alpha = a+2a\omega$

$= a(1+2\omega)$ $(-a-2a\omega) = -a^2(1+2\omega)^2$

$= -a^2(1+4\omega^2+4\omega) = -a^2(1+4(-1)$

$p = 3a^2 \Rightarrow p = 3$

(iii) $\bar{\alpha} = \alpha w \Rightarrow a + bw^2 = aw + bw^2$

$$(a-b) - bw = aw + b(-1-w)$$

$$(a-b) - bw = -b + w(a-b)$$

$$a - b = -b \Rightarrow a = 0$$

$$P = \alpha^2 w = b^2 w^2 w = b^2 \quad \rightarrow\leftarrow$$

iv) $\bar{\alpha} = -\alpha w \Rightarrow a + bw^2 = -aw - bw^2$

$$(a-b) - bw = -aw + b(1+w)$$

$$a - b = b \Rightarrow a = 2b$$

$$P = -\alpha^2 w = -(2b + bw)^2 w = -b^2 (2+w)^2 w$$

$$P = -b^2(4+w^2+4w)w$$

$$= -b^2(4w+1+4w^2)$$

$$= -b^2(1-4) = 3b^2 \Rightarrow P = 3$$

v) $\bar{d} = \alpha w^2$

$$a+bw^2 = aw^2+b \Rightarrow a = b$$

$$P = \alpha^2 w^2 = (a+aw)^2 w^2 = a^2(1+w)^2 w^2$$

$$= a^2(1+w^2+2w)w^2$$

$$= a^2(w^2+w+2)$$

$$= a^2 \longrightarrow\!\!\leftarrow$$

vi) $\overline{\alpha} = -\alpha w^2$

$a+bw^2 = (-a-bw)w^2$

$= -aw^2 - b \Rightarrow a = -b$

$p = -\alpha^2 w^2 = -(a-aw)^2 w^2$

$= -a^2(1-w)^2 w^2$

$= -a^2(1+w^2-2w)w^2$

$= -a^2(w^2+w-2)$

$= 3a^2 \Rightarrow p = 3$

Thm: 1) p is inert in $\mathbb{Z}[i]$ $\iff$ $p = 4k+3$

2) p splits in $\mathbb{Z}[i]$ $\iff$ $p = 4k+1$

Thm: p is inert in $\mathbb{Z}[\omega]$ $\iff$ $p = 3k+2$

p splits in $\mathbb{Z}[\omega]$ $\iff$ $p = 3k+1$

We will see a proof later in this course!

→ Consider $\{1, 5, 9, 13, 17, 21, \ldots\}$.

Show that there are infinitely many primes in this set.

→ Same question as before but with set $\{1, 4, 7, 10, 13, 16, \ldots\}$.

↳ Discussed in Review Session of 2/15/2023