Lecture 30
March 25th, 2015

$\alpha = a+bi$, $a, b \in \mathbb{R}$

$N(\alpha) = a^2+b^2$, norm

Norm multiplication property: $N(\alpha\beta) = N(\alpha)N(\beta)$

$\alpha = a+bi$, $\beta = c+di$

$\alpha\beta = ac-bd + (ad+bc)i$

$N(\alpha\beta) = (ac-bd)^2+(ad+bc)^2 = a^2c^2+b^2d^2+a^2d^2+b^2c^2 = (a^2+b^2)(c^2+d^2) = N(\alpha)N(\beta)$

Complex numbers form a field

$\alpha = a+bi \neq 0 \neq 0 \iff a \neq 0$ or $b \neq 0$

$\iff a^2+b^2 \neq 0$

$\alpha^{-1} = \frac{1}{\alpha} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$

"vector sector"

$\alpha = x+yi+zj+wk$

Hamiltonians (4-D skew-field)

$x, y, z, w \in \mathbb{R}$, $i^2=j^2=k^2=-1$, $ij=k=-ji$

$N(\alpha) = x^2+y^2+z^2+w^2$

Fundamental Theorem of Algebra: $a_0x^d + a_1x^{d-1} + \cdots + a_dx^0 = 0$, $a_0 \neq 0$, $a_i \in \mathbb{C}$, always has a sol. in complex #.

[Complex numbers are algebraically closed).

In number theory, we are interested in $\mathbb{Z}[i] = \{a+bi, a, b \in \mathbb{Z}\}$ Gaussian Integers

$\mathbb{Z} \leftrightarrow \mathbb{Z}[i]$

ring

(1). ring sum, multiplication

(2). divisibility, $a|b$ if $b=ac$, $c \in \mathbb{Z}$, $a+bi \mid c+di$ if $c+di = (a+bi)(e+fi)$, $e+fi \in \mathbb{Z}[i]$

(3) units $ab=1$, $a, b \in \mathbb{Z}$, $a = \pm 1$, units in $\mathbb{Z}[i]$ $(a+bi)(c+di)=1$

(4). prime numbers: p is a prime in $\mathbb{Z}$

if $p=ab$ implies a or b a unit $a = \pm 1$

Gaussian Units Thm. Units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$

Proof: use the norm

($\Rightarrow$) α is a unit in $\mathbb{Z}[i] \iff N(\alpha)=1 \iff \alpha$ is a unit $\Rightarrow \alpha\beta = 1$ for some $\beta \iff N(\alpha\beta)=1$

$\| N(\alpha)N(\beta) \Rightarrow N(\alpha)=1$

($\Leftarrow$) $N(\alpha)=1 \Rightarrow \alpha \cdot \bar{\alpha} = 1$, where $\bar{\alpha} = a-bi$

$N(\alpha) = a^2+b^2=1$. $a^2=1$, $b^2=0 \rightarrow \alpha = \pm 1$

or $a^2=0$, $b^2=1 \rightarrow \alpha = \pm i$

Gaussian Primes: α is a prime in $\mathbb{Z}[i]$

if $\alpha = \beta \cdot \gamma$ implies β or γ is a unit

Gaussian Prime THM: Gaussian prime:

(1). $1+i \leftarrow$ Norm 2

(2) $p \equiv 1 \bmod 4$ $p=a^2+b^2$, $a+bi$ is a Gaussian prime $\leftarrow$ Norm p

(3) $p \equiv 3 \mod 4$. p is a Gaussian prime $\leftarrow$ Norm p^2

$p = (a+bi)(c+di)$ $\qquad$ $\underline{a+bi,\ c+di \text{ not units}}$

$\alpha = \beta\gamma$ $\qquad$ $p^2 = (a^2+b^2)(c^2+d^2)$ $\qquad$ $\downarrow a^2+b^2 \neq 1,\ c^2+d^2 \neq 1$

$N(\alpha) = N(\beta)N(\gamma)$ $\qquad$ $a^2+b^2 = p$ contradiction

If $N(\alpha)$ is a prime #. $N(\beta)=1$ or $N(\alpha)=1$, i.e. β or γ is a unit

so α is a Gaussian prime.

$N(\alpha) = 2$: $\alpha = 1+i$

$N(\alpha) = p \equiv 1 \mod 4$

$p = a^2+b^2$ Then $\alpha = a+bi$, is a G.P. $\quad a-bi$ is also a G.P.

$b+ai = i(a-bi)$

Conversely, we show that there are no primes

Sps α is a G.P.

$N(\alpha) \neq 1$

So there exists a prime p s.t. $p \mid N(\alpha)$

If $p=2$, $\quad 1+i \mid \alpha$

[$\alpha = a+bi$, $N(\alpha) = a^2+b^2$, $\alpha \mid a^2+b^2$, a, b both even or both odd]

$\underset{\text{unit}}{\alpha = (1+i)\ (*)}$ $\qquad \dfrac{a+bi}{1+i} = \dfrac{(a+bi)(1-i)}{(1+i)(1-i)} = \dfrac{(a+b)+(a+b)i}{2} \in \mathbb{Z}[i]$