Lec 9/29

Friday, September 29, 2017 10:21

$\mathbb{Z}_p$ = field of p elements

$\mathbb{R}[X]$: X^2+1 is prime

$\underbrace{\mathbb{R}[X]/(X^2+1)}$: remainder of p can be $\alpha + \beta\dot{X}$: $\alpha, \beta \in \mathbb{R}$

$(\dot{x^2+1}) = 0 \Rightarrow \dot{X}^2 = -1$ call $\dot{X} =: i$.

New ring $\mathbb{C} = \mathbb{R}[X]/(X^2+1) = \{\alpha + \beta\dot{X} : \alpha, \beta \in \mathbb{R}\}$

$$(\alpha_1 + \beta_1\dot{X}) + (\alpha_2 + \beta_2\dot{X}) = (\alpha_1+\alpha_2) + (\beta_1+\beta_2)\dot{X}$$

$$(\alpha_1 + \beta_1\dot{X})(\alpha_2 + \beta_2\dot{X}) = \alpha_1\alpha_2 + \alpha_1\beta_2\dot{X} + \alpha_2\beta_1\dot{X} + \beta_1\beta_2\dot{X}^2$$

$$= (\alpha_1\alpha_2 - \beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\dot{X}$$

assume $\alpha + \beta i \neq 0$ (α, β not both 0)

find $(x+iy)$ s.t. $(\alpha + i\beta)(x+iy) = 1$

$$\begin{array}{c} (\alpha+i\beta)(x+iy) \\ \shortparallel \\ (\alpha x - \beta y) + (\alpha y + \beta x)\, i \end{array}$$

$$(\alpha x - \beta y) = 1, \quad (\alpha y + \beta x) = 0$$

$$\alpha x - \beta y = 0$$
$$\beta x + \alpha y = 1$$

$$\begin{vmatrix} \alpha & -\beta \\ \beta & \alpha \end{vmatrix} = \alpha^2 + \beta^2 \neq 0.$$ so inverse exists.

Another way:

$$\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} = \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\left\{ \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

subring, field $\cong \mathbb{C}$.

$\mathbb{R}[X] \subset \mathbb{C}[X]$: X^2+1 is no longer prime:

$$X^2+1 = (X-i)(X+i)$$

Now all prime polynomials have deg 1.

Fundamental Theorem of Algebra:

Any $p \in \mathbb{C}[X]$ with $\deg p > 0$ has at least one root in $\mathbb{C}$.

so $p = (X - \xi_1) Q$ and $\deg Q = \deg p - 1$. but Q has a root too.

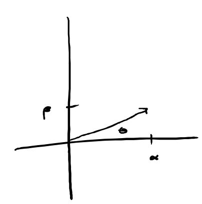
by induction, p has exactly $\deg p$ roots (accounting for multiplicity).

$p = (X-\xi_1)(X-\xi_2)\cdots(X-\xi_{\deg p})$ where $\xi_i \in \mathbb{C}$ $\forall i$.

$z = \alpha + \beta i$. $\quad \bar{z} = \alpha - \beta i$. $\quad z\bar{z} = \alpha^2 + \beta^2 > 0$ if $z \neq 0$.

So $z \dfrac{\bar{z}}{\alpha^2+\beta^2} = 1$.

$|z| = \sqrt{z\bar{z}}$ represents length of $\langle \alpha, \beta \rangle$ vector.



$$z^{-1} = \frac{\bar{z}}{|z|^2}$$

$z = \rho(\cos\theta + i \sin\theta)$ where $\rho = |z|$

$$\big(\rho_1(\cos\theta_1 + i\sin\theta_1)\big)\big(\rho_2(\cos\theta_2 + i\sin\theta_2)\big) = \rho_1\rho_2\big(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 + i(\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1)\big)$$

$= \rho_1 \rho_2 \left(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2) \right).$

$z^n = |z|^n (\cos n\theta + i \sin n\theta)$ De Moivre's formula.

solve $X^n = 1$: $\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$ for $0 \le k < n$

What about $X^n = -1$: take odd multiples of $\frac{2\pi}{n}$.

What about $X^n = \alpha + i\beta = \sqrt{\alpha^2+\beta^2} \, (\cos\varphi + i \sin\varphi)$

$|z|^n = \sqrt{\alpha^2+\beta^2} \Rightarrow |z| = \sqrt[2n]{\alpha^2+\beta^2}$, $\cos n\theta = \cos\varphi$, $\sin n\theta = \sin\varphi$

all such angles θ.