

מחלקת שורשים

הערה:  $\sqrt{d}$  אינו שייך ל- $R$  אם  $d$  אינו רבוע מושלם.  
 אם  $\sqrt{d} \in R$  אז  $R[\sqrt{d}] = R$ .

$(0,1) \cdot (1,0) = (0,0)$

$(x,y) = (0)$

המרחב  $R[x,y]$  הוא מרחב וקטורי על  $R$ .  
 המרחב  $R[x,y]$  הוא מרחב וקטורי על  $R$ .

המרחב  $R[x,y]$  הוא מרחב וקטורי על  $R$ .

$AB \subseteq A \cap B$  - זמין  $0 \neq A, B \subseteq R$   
 $A \cap B \neq \emptyset$  אם  $0 \neq ab \in AB \subseteq A \cap B$

קוץ

$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4} \end{cases}$

$\left\{ \begin{array}{l} a+b\sqrt{d} \\ \frac{a}{2} + \frac{b}{2}\sqrt{d} \end{array} \right\}$

$a+b\left(\frac{1+\sqrt{d}}{2}\right)$

$\frac{2a+b}{2} + \frac{b}{2}\sqrt{d}$

מחלקת שורשים

$N: R \rightarrow N \cup \{\infty\}$  (הפונקציה)  $N(a) = |R/\mathfrak{p}_a|$

$|R/\mathfrak{p}_{ab}| = |R/\mathfrak{p}_a| \cdot |R/\mathfrak{p}_b|$

$\mathfrak{p}_{ab} = \mathfrak{p}_a \mathfrak{p}_b \subseteq \mathfrak{p}_a \mathfrak{p}_b$



13-1)  $\mathbb{Z}/15\mathbb{Z}$  (mod 15)

$$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$|\mathbb{Z}/15\mathbb{Z}| = |\mathbb{Z}/3\mathbb{Z}| \cdot |\mathbb{Z}/5\mathbb{Z}|$$

$$|\mathbb{Z}/3\mathbb{Z}| = |\mathbb{Z}/3\mathbb{Z}|$$

(mod 15)  $\mathbb{Z} \rightarrow \mathbb{Z}/15\mathbb{Z}$

$$r \rightarrow ra + 15b$$

mod 15 ✓

x - mod 15

mod 15  $\mathbb{Z}/15\mathbb{Z}$  kernel

$$\ker = \{r \in \mathbb{Z} \mid ra = 0\}$$

$$\Downarrow$$

$$= \{r \in \mathbb{Z} \mid ra = r \cdot 15b = 0\} = 15\mathbb{Z}$$

$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  (mod 15)

mod 15

mod 15

mod 15  $\mathbb{Z}/15\mathbb{Z}$

$$N(x) = x \cdot \bar{x}$$

mod 15

$$\bar{x} = a - b\sqrt{15}$$

$$x = a + b\sqrt{15} \in \mathbb{Z}[\sqrt{15}]$$



$$\text{tr}(X) = X + \bar{X}$$

הערות  
-1777 0.11

הוכחה  
1) נניח  $(a, b) \in \mathbb{R}^2$

2)  $\text{tr}(X)$  חיובי

$$N(X) = \pm 1 \quad (\Leftrightarrow) \quad X \in \text{SU}(2) \quad (3)$$

הוכחה: נניח  $a, b \in \mathbb{R}$  ונניח  $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{נניח } \alpha = a + b \left( \frac{1 + \sqrt{3}}{2} \right)$$

$$\alpha = a + b \left( \frac{1 + \sqrt{3}}{2} \right) = \frac{2a + b}{2} + \frac{b}{2} \sqrt{3}$$

$$N(\alpha) = \left( \frac{2a+b}{2} + \frac{b}{2} \sqrt{3} \right) \left( \frac{2a+b}{2} - \frac{b}{2} \sqrt{3} \right) \quad \text{הוכחה}$$

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

$$N(\alpha) = 1 \quad \text{אם } a, b \in \mathbb{R} \quad \text{אז } a^2 + ab + b^2 = 1$$

$$\begin{aligned} b = \pm 1, a = 0 & \quad \text{הוכחה} \\ b = 0, a = \pm 1 & \\ a = \pm 1, b = \mp 1 & \end{aligned}$$

$$- \text{אם } a^2 + b^2 \geq 8 \quad |a|, |b| \geq 2 \quad \text{אז } a^2 + ab + b^2 \geq 1$$

$$a^2 + ab + b^2 \geq 1$$

$$(3 + 2\sqrt{2})^n - \sqrt{2}(\sqrt{2} + 1)^n + \sqrt{2} = 0 \quad \text{הוכחה}$$

הוכחה

הוכחה

$$\underbrace{(3 + 2\sqrt{2})^n}_a = \sqrt{2} \underbrace{(\sqrt{2} + 1)^n}_b - 1 \quad \text{הוכחה}$$

R/ Rab / R

(R, S, D, M, N, P)

Ra / Rab =

הוכחה

N(X)

R, X, S, D, M, N, P



$$\begin{cases} ax + by = 0 \\ ax + by = 9a \end{cases}$$

Q. 9: (a)  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$

$$\begin{cases} ax + by = 0 \\ ax + by = 9a \end{cases}$$

(b)  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$

$$N(a) = \begin{pmatrix} a \\ 0 \end{pmatrix}$$

$$\begin{cases} ax + by = 0 \\ ax + by = 9a \end{cases}$$

for  $\overline{ax + by} = 0$   
 $(a + bN)(x + yN) = 0$   
 $N = a^{-1} \cdot 0 = 0$

(2)  $\mathbb{Z} \cup \mathbb{Z} = \mathbb{Z} \cup \mathbb{Z}$

$N(a) \in \mathbb{Z}$  for  $a \in \mathbb{Z}$   
 $N(a) \in \mathbb{Z}$  for  $a \in \mathbb{Z}$

$$N(a) = 1 = N(a) \cdot N(a^{-1})$$

for  $\overline{ax + by} = 0$   
 $\overline{ax + by} = 0$

$$a^{-1} \cdot 0 = 0$$

$$N(a) = 1$$

$$N(a) = a^{-1} = 1$$

$$\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$$

(3)  $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$



$$\begin{cases} nb = -a^2y + b^2yd = -N(\alpha)y \\ 0 = ay + bx \end{cases}$$

$$\|c \quad \|N(0) \quad N(\alpha)/n \quad \|c \quad N(\alpha)/b \quad \|c \quad N(\alpha)/nb$$

$$a^2 + b^2 \downarrow = N(\alpha)/b \quad \|c$$

$$\Downarrow$$

$$N(\alpha)/a$$

$$\Downarrow$$

$$2 | N(\alpha) | \alpha$$

$\Downarrow$

.  $\alpha$   $\in$   $\langle \alpha \rangle$   $\cap \mathbb{Z}$   $\neq \emptyset$

$$\langle \alpha \rangle \cap \mathbb{Z} = \mathbb{Z} N(\alpha)$$

$N(\alpha) \in \langle \alpha \rangle$   $\cap \mathbb{Z}$   $\neq \emptyset$   $\Rightarrow$   $\langle \alpha \rangle \cap \mathbb{Z} \neq \emptyset$

$\alpha/n$   $\in \langle \alpha \rangle \cap \mathbb{Z}$

$$\mathbb{Z} N(\alpha) \subseteq \langle \alpha \rangle \cap \mathbb{Z}$$

$$\exists c \cdot n \in \langle \alpha \rangle \cap \mathbb{Z}$$

$$n \in \mathbb{Z} \cdot N(\alpha)$$

$\|c$

$\alpha/n$   $\in \langle \alpha \rangle \cap \mathbb{Z}$   
 $\Rightarrow$   $\langle \alpha \rangle \cap \mathbb{Z} \neq \emptyset$

$\mathbb{Z}N$

~~XXXXXXXXXX~~

$\sigma_d$   $\in \mathbb{Z}N$   $\Rightarrow$   $\sigma_d \in \mathbb{Z}N$   $\Rightarrow$   $\sigma_d \in \mathbb{Z}N$   $\Rightarrow$   $\sigma_d \in \mathbb{Z}N$

$$\{ \overline{a+bi} \} = \{ a-bi \}$$

$$\sigma_d / I = \{ a+bi \} = \{ \overline{a+bi} \} \quad a, b \in \mathbb{Z}, n \in \mathbb{N}$$

$\sigma_d \in \mathbb{Z}N$



$(a|b)=1 \Leftrightarrow \exists a+bi \in \mathbb{Z} \text{ s.t. } a+bi \mid b \Rightarrow a+bi \in R \Rightarrow \exists k \in \mathbb{Z} \text{ s.t. } a+bi = kb$

$|N(a)| = |R/Ra|$

$\mathbb{Z}/a\mathbb{Z} \cong \mathbb{Z} + R_a / R_a \cong \mathbb{Z} / a\mathbb{Z}$  (isomorphism)

$\mathbb{Z}/a\mathbb{Z} \cong \mathbb{Z} + R_a / R_a \xrightarrow{\cong} R/Ra$

$N \leq |R/Ra|$

(Note:  $N \leq |R/Ra|$  is a consequence of the isomorphism)

$(b|a) = (b|a^2 - b^2) = (a|b) = 1$

$(a|a) = 1$

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

□  $\Rightarrow$  (by induction)

Proposition: If  $a \in R$  and  $(a|a)=1$ , then  $(a|b)=1$  for all  $b \in R$ .

$\alpha = a + bi \mid a + bi \Rightarrow \alpha \mid \alpha^2 = (a+bi)^2 = a^2 - b^2 + 2abi$

$(a|b)=1$

$N(a) = N(\alpha) \cdot N(\alpha') = c^2 \cdot |R/Ra| = |R/Ra| \cdot |R/Ra| = |R/Ra|^2$



עקרונות (מבוא-מקדים)

$\exists c: b=ac \Leftrightarrow a|b$   
 (עבור  $a, b \in \mathbb{Z}$  ו- $a \neq 0$ )  
 $2 \cdot \frac{3}{2} = 3 \Leftrightarrow 2|3$  לא נכון

עקרון השלישי: אם  $a|b$  ו- $a|c$  אז  $a|b \pm c$   
 אם  $a|b$  ו- $a|c$  אז  $a|kb \pm kc$  לכל  $k \in \mathbb{Z}$

עקרון הרביעי: אם  $a|b$  ו- $b|c$  אז  $a|c$   
 $\langle a \rangle = \langle b \rangle \Leftrightarrow a|b$  ו- $b|a$

עקרון החמישי: אם  $a|bc$  ו- $a$  אי-מעריכי  $b$  אז  $a|c$   
 (עבור  $a, b, c \in \mathbb{Z}$  ו- $a \neq 0$ )

מערכות  
 (1)  $\mathbb{Z} \rightarrow \mathbb{Z}$  הומומורפיזם

(2)  $X \in F[x]$  ו- $X = f(x) \cdot g(x)$   
 $\deg X = 1$   
 $= \deg f(x) + \deg g(x)$

אם  $\deg f = 0$  ו- $\deg g = 0$  אז  $f, g \in F$   
 כלומר  $f$  ו- $g$  הם קבועים

(3)  $x^2 + 1 \in \mathbb{R}[x]$  אי-מעריכי- $\mathbb{R}$   
 $x^2 + 1 \in \mathbb{C}[x]$  מעריכי- $\mathbb{C}$

(4)  $2 \in \mathbb{Z}[i]$  אי-מעריכי- $\mathbb{Z}[i]$   
 $2 = (1+i)(1-i)$  כן מעריכי- $\mathbb{C}$   
 $2 = N(1+i) \neq 2$  (אם  $N$  הוא נורמה)

$\mathbb{Z} \setminus \mathbb{Z} \neq \emptyset$   
 $\downarrow$   
 קבוצת שארית

(1)  $\rightarrow$

$\alpha = a$

$\sqrt{2} \in \mathbb{R}$



מטרה:  $a \mid b$  אם ורק אם  $a \mid b$

תוצאה:  $a \mid b$  ורק אם  $a \mid b$  ורק אם  $a \mid b$

$a \mid b$  ורק אם  $a \mid b$  ורק אם  $a \mid b$

מטרה:  $a \mid b$  ורק אם  $a \mid b$  ורק אם  $a \mid b$

הוכחה

נניח  $a \mid b$  ונראה ש  $a \mid b$

$a \mid b$  ורק אם  $a \mid b$

$$N(y + \sqrt{b}) = 0 = N(x) \cdot N(y)$$

$$N(x) = \pm 2, \pm 3 \quad (-)$$

$$N(x) = a^2 - 10b^2 \equiv 0 \pmod{10}$$

אם  $a \equiv 0 \pmod{10}$  אז  $a = 10k$  ונראה ש  $a \mid b$

אם  $a \not\equiv 0 \pmod{10}$  אז  $a \equiv \pm 1, \pm 3, \pm 7, \pm 9 \pmod{10}$  ונראה ש  $a \mid b$



$a/b - 1$   $\in$   $\mathbb{R}$   $\Rightarrow$   $a/b \in \mathbb{R} + 1$   $\Rightarrow$   $a/b \in \mathbb{R}$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$

$a/b \in \mathbb{R} \Rightarrow a/b \in \mathbb{R} + 1$