Kateri elementi kolobarja $\mathbb{Z}[i]$ so asociirani: $m+ni$

$x = u(m+ni) = um + uni$

kateri so deljivi:

$(x+yi)(a+bi) = 1$

$xa - yb + i(ay+xb) = 1$

$ay + xb = 0 \quad xa - yb = 1$

$x = \frac{-ay}{b} \quad -\frac{a^2y}{b} - yb = 1$

$-\frac{y}{b}(a^2+b^2) = 1$

$y = \frac{-b}{a^2+b^2}$

$x = \frac{a}{a^2+b^2} \quad |a| \leq |a^2| \Rightarrow$

$a^2+b^2 \in \{0,1\} \Rightarrow a^2+b^2 = 1$

$\Rightarrow a \in \{0,1\}$
$b \in \{0,1\}$ deljivi $\{1,-1,i,-i\}$

asoc: $\{m+ni, -m-ni, n-mi, -n+mi\}$

$d \in \mathbb{Z}$

$\mathbb{Z}[\sqrt{d}] = \{ m + n\sqrt{d} ;\ m, n \in \mathbb{Z} \}$

1) Pokaži $\mathbb{Z}[\sqrt{d}]$ je podkolobar $\mathbb{C}$

2) Množica $\mathbb{Q}[\sqrt{d}] = \{ q + r\sqrt{d} ;\ q, r \in \mathbb{Q} \}$ je podpolje $\mathbb{C}$ generirano z $\mathbb{Z}[\sqrt{d}]$

---

1) $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{C}$

zaprtost za seštevanje, množenje, enote

za množenje:

$$(m + n\sqrt{d})(x + y\sqrt{d}) = mx + nyd + \sqrt{d}(ny + xm)$$

enota $= 1 = 1 + 0 \cdot \sqrt{d}$

sešteva: $(m + n\sqrt{d}) - (x + y\sqrt{d}) = (m - x) + (n - y)\sqrt{d}$

2) inverzi

$$\frac{m + n\sqrt{d}}{x + y\sqrt{d}} = \frac{(m + n\sqrt{d})(x - y\sqrt{d})}{x^2 - y^2 d} = \frac{c}{\quad} + \frac{e}{\quad}\sqrt{d}$$

(ja tu)

Avtomorfizmi $\mathbb{Z}[\sqrt{d}] = \{ id ;\ \sigma \}$, $\sqrt{d} \mapsto -\sqrt{d}$

Norma $N(x) = x\sigma(x)$

$N(q + r\sqrt{d}) = (q + r\sqrt{d})(q - r\sqrt{d}) = q^2 - r^2 d$

3) $\forall x,y \in \mathbb{Z}[\sqrt{a}]: N(xy) = N(x)N(y)$

$N(x,y) = xy\sigma(xy) = xy\sigma(x)\sigma(y) = x\sigma(x)y\sigma(y)$

$= N(x) \cdot N(y)$

4) $x \in \mathbb{Z}[\sqrt{a}]$ je obrnljiv $\Leftrightarrow N(x) = \pm 1$

$xy = 1 \Rightarrow N(xy) = N(1)$

$N(x)N(y) = 1$

$N(x) = \frac{1}{N(y)}$ $\quad N(y) \in \mathbb{Z} \wedge N(x) \in \mathbb{Z}$

$\Rightarrow N(y) \in \{\frac{1}{2}, 1\}$

$\Rightarrow N(x) \in \{-1, 1\}$

5) $p \in \mathbb{P}$; $N(x) = \pm p \Rightarrow x$ nerazcepen

in $N(x) = \pm p$

recimo da x razcepen ab nekoliko

$x = ab$

$N(x) = N(a)N(b) \overset{!}{=} p \Rightarrow N(a) = 1 \vee N(b) =$

4) $\Leftarrow N(x) = 1$, $x\sigma(x) \neq 1 \Rightarrow x^{-1} \neq \sigma(x)$

5) nepraz
mamo da je $N(x) \pm 1 \Rightarrow a$ obrnljiv.

$d < -1 \Rightarrow 1, -1$ sta edina obrnljiva v $\mathbb{Z}[\sqrt{d}]$

x obrnljiv $\Rightarrow N(x) N(y) = \pm 1$

$N(a+b\sqrt{d}) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2 d = a^2 + b^2 |d|$

$|d| > 1$

če je $b^2 > 1 \Rightarrow N > 1$

$\Rightarrow b = 0$

a^2 mora biti $1 \Rightarrow a = \pm 1$ sta edini

~~mmmm~~ najmanjši

in vemo da sta različna to re je ke je rezultat

Pokaži da so $1+i$, $7+8i$, 3 nerazcepni v $\mathbb{Z}[i]$

Recimo da so razcepni

$1+i = x y \quad N(xy) = x\sigma(x) y\sigma(y) = 2$

praštevilo

$p \to$ nerazcepno

$N(7+8i) = 49 + 64 =$ velik $= 113$ praštevilo

~~nje praštevilo~~ Norma je 9

$3 = xy \quad N(xy) = x\sigma(x) y\sigma(y) = 9$

vsaj 2 morata biti 1

~~$x\sigma(x)$~~ $N(x) = N(\sigma(x)) = \sigma(x)\sigma\sigma(x) = x\sigma(x)$

$N(x) = n \Rightarrow n$ razcepna

$N(x) = n = x\sigma(x)$

6) Poiščimo vse delitelje elementa $2 \in \mathbb{Z}[i]$

$x \mid 2 \Leftrightarrow 2 = xy$ za neki y

$N(xy) = N(2) = 4 \qquad N(x)N(y) = 4$

$x\sigma(x)\,y\sigma(y) = 4 = 2 \cdot 2 = xy\sigma(xy) = 2\sigma(xy)$

$\Rightarrow \sigma(xy) = 2 = \sigma(x)\sigma(y) \Rightarrow$

$N(x) = 2 \qquad x = \pm 1 \pm i$

$x = \pm 2$ ... use možnosti

$x = \pm 2i$

1)

$a = 3+4i$ $\quad \delta = m^2+n^2$

$b = 1-3i$ $\quad |a| = 9+16 = 25$

$|b| = 1+9 = 10$ $\quad$ nyilvánvaló

$a = kb + r$

$\frac{a}{b} = k + \frac{r}{b}$

$\in \mathbb{Z}[i]$ $\quad \in \mathbb{R}[i]$

$a = 3-4i$

$b = 1-3i$

$\frac{a}{b} = \frac{(3-4i)(1+3i)}{10} = \frac{3+12+i(9-4)}{10} = 1 + \frac{1}{2} + \frac{1}{2}i$

$\frac{1}{2}(1+i)(1-3i) = \frac{1}{2}(1+3+i(1-3)) = 2-i$

$a = b + 2-i \qquad / : (2-i)$

$\frac{a}{2-i} = \frac{b}{2-i} + 1 \qquad \Rightarrow$

$\frac{a}{2-i} - \frac{b}{2-i} = 1 \quad \Rightarrow \quad a-b = 2-i$

2)

$a = 6$ $\qquad \mathbb{Z}[\sqrt{-5}]$

$b = 2 + 2\sqrt{-5}$

$c = 2 \xRightarrow{N(a) = 36} \frac{6}{2} = 3 \quad N(b) = 4 + 4 \cdot 5 = 4 \cdot 6 \quad \frac{b}{2} = 1 + \sqrt{5}$

$c \mid a \quad \Rightarrow \frac{a}{c} \ldots, \ d \mid a,\ d \mid b \Rightarrow 6 \cdot 2 \cdot 3$

$\delta(c) = 1 + 5 = 6$

$6 \cdot 2 \cdot 3 = 6^2 \qquad 6 \cdot 2 \cdot 3 = 6 \cdot 4$

$N(\gcd(a,b)) = \gcd(N(a), N(b)) = \gcd(36, 24) = 12 = x^2 + 5y^2$

$y^2 \in \{1, 2\}$

$\Downarrow \qquad \Downarrow$

$x^2 = 23 \qquad x^2 = 2$ ✗

Tak nedostopa

3) UFD ⇒ gcd dobrze

$a = \prod_{i \in I} p_i^{k_i}$

$b = \prod_{i \in I} p_i^{l_i}$

$d = \gcd(a,b) = \prod_{i \in I} p_i^{\min\{k_i, l_i\}}$

$d \mid a \wedge d \mid b$

Niech $c = \prod_{i \in I} p_i^{m_i}$ $\quad c \mid a \wedge c \mid b$

$a = c\alpha \quad \alpha = \prod p_i^{n_i}$

$a = \prod p_i^{n_i + m_i} = \prod p_i^{k_i} \Rightarrow m_i \le k_i$

podobnie $m_i \le l_i \Rightarrow$ itd.

$c \mid d$

$\mathbb{Z}[\sqrt{-2}]$ euklidisch

a) $\forall a,b$ $b\neq 0$ $\exists q,r$ eind. $a=qb+r$ $\wedge r=0 \vee \delta(r)<\delta(b)$

b) $\delta(a)\leq\delta(a,b)$ $\forall a,b\neq 0$ $\{a\}$

$\delta: m+\sqrt{-2}n = m^2+2n^2$

Norm der b reelle

$a,b\in\mathbb{Z}[\sqrt{-2}]$ gesucht $a=x+\sqrt{-2}y$ $b=m+\sqrt{-2}n$

$$\frac{a}{b}=z_1+z_2\sqrt{-2}$$

$$a=\left([z_1]+[z_2]\sqrt{-2}\right)b+\left(z_1-[z_1]+(z_2-[z_2])\sqrt{-2}\right)b$$

DN:

Naj bo $K[x]$ UFD

Potem ima polinem $n^{\in K}$ enolično faktorizacijo

Sledi je tud $K[x][x]$ UFD

Naj bo K UFD

Naj bo $p \in K$ poljuben prim

Razcepim prod: $\prod_{k=1}^{r}\left(\sum_{i=1}^{n} a_{ik}x^n\right) =$

$= \prod_{k=1}^{r}\left(a_{nk}x^n + \dots + a_{0k}\right) = x^{nr}\left(\prod_{k=1}^{r} a_{nk}\right) + \dots$

$cont(fg) = cont(f)cont(g)$

$p \mid cont(f,g) \Rightarrow gcd(a_0, \dots, a_n) = p$

$fg = 0 \text{ v } K/p[x]$

$\Rightarrow p = 0 \text{ V } g = 0$

$(ax+b)(cx+d) = acx^2 + x(cb+ad) + bd$

$\Rightarrow p \mid cont f \text{ V } p \mid cont g$

Recimo da f razcepen $F[X]$

potem lahko zapišemo $af = p(x)q(x) \in K[X]$

Najprej skrajšamo $\mathrm{cont}(af)$ ker $af = pq$ / cont

$$\mathrm{cont}(af) = \mathrm{cont}(q)\,\mathrm{cont}(p) = a\,\mathrm{cont}f$$

$$= a \cdot \text{enolično}$$

enolično skupaj delitelji

$$a \mid \mathrm{cont}(pq) \Rightarrow \frac{p}{x} \cdot \frac{q}{y} = \frac{fa}{a} = f$$

$$\Vert$$

$$\underbrace{x}_{\mid p}\,\underbrace{y}_{\mid q}$$

$$f \mid pq \Rightarrow f \mid p \vee f \mid q$$

$kf = pq \quad \mathrm{cont}f\,\mathrm{cont}k = \mathrm{cont}\,p\,\mathrm{cont}q$

pq imata razcep $\Rightarrow f \mid p \vee f \mid q$

$\Rightarrow \forall\, p_i(x) \ldots$ pušča

2) $K[X]$ glavni ideal $\Leftrightarrow$ K je polje

$a \in K - \{0\}$

$\exists b \quad ab = 1$

(a) je ideal $(a) = \{af : f \in K[X]\}$

1) $1+\sqrt{-3}$ nerazcepen v $\mathbb{Z}[\sqrt{-3}]$, ampak ni praelement

$1+\sqrt{3}$ nerazcepen

Recimo da je $(1+\sqrt{-3}) = \alpha \cdot \beta$

$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) = 1+3 = 4$

$N(\alpha) = N(\beta) = \pm 2$

ce bi bila 1 bi bila obrnljiva

$N(a+\sqrt{-3}b) = a^2 + 3b^2 = \pm 2$

$b = 0$

$a^2 = \pm 2$ neobstaja

Ni praelement

~~$(a+b\sqrt{-3})(1+\sqrt{-3}) = a + b\sqrt{-3} + a\sqrt{-3} - b =$~~

Vsak element deli svojo norma

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$

$(1+\sqrt{-3}) \nmid 2$

Recimo da $k(1+\sqrt{-3}) = 2$ $\quad N(2) = 4 \Rightarrow$

$N(k) = \pm 1$

$\Rightarrow k = \pm 1$