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

$\mathbb{Z}[i] = \{ m+ni ; \ m,n \in \mathbb{Z} \}$

x, y asociirana $\Leftrightarrow$ $x = n \cdot y$, n obrnljiv element

Obrnljivi v $\mathbb{Z}[i]$:

$(m+ni)(k+li) = 1$

$mk + (ml + nk)i - nl = 1$

$mk - nl = 1$ $\qquad$ $ml + nk = 0$

$mk + \frac{n^2k}{m} = 1$ $\qquad$ $ml = -nk$

$m^2k + n^2k = m$ $\qquad$ $l = -\frac{nk}{m}$

$\Rightarrow k = \frac{m}{m^2+n^2} \in \mathbb{Z}$

$l = \frac{n}{m^2+n^2} \in \mathbb{Z}$

Kdaj je $\left|\frac{m}{m^2+n^2}\right| \geq 1$?

$|m| \geq m^2+n^2 \geq m^2$

$\Rightarrow m \in \{-1, 0, 1\}$

$n \in \{-1, 0, 1\}$

$\pm 1 \pm i$: $k = \frac{\pm 1}{1+1} = \frac{1}{2}$ //

$\Rightarrow$ i) $m = 0,\ n = \pm 1$

ii) $m = \pm 1,\ n = 0$

$\Rightarrow 1, -1, i, -i$

Asociirani elementi $m + ni$:

$m + ni$
$-m - ni$
$mi - n$
$mi + n$

$d \in \mathbb{Z}$

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

$\mathbb{Q}(\sqrt{d}) = \{q + r\sqrt{d};\ q, r \in \mathbb{Q}\}$

---

2) Pokaži:

a) $\mathbb{Z}[\sqrt{d}]$ je podkolobar $\mathbb{Q}$

Zaprtost za množenje:

$(m + n\sqrt{d})(a + b\sqrt{d}) = ma + (mb + na)\sqrt{d} + nbd =$

$= ma + nbcd + (mb + na)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

Zaprtost za seštevanje:

Očitna

Enota: 1

b) $\mathbb{Q}(\sqrt{d})$ je podpolje $\mathbb{Q}$, generirano z $\mathbb{Z}[\sqrt{d}]$

Podpolje, generirano z $\mathbb{Z}[\sqrt{d}] = \{xy^{-1};\ x, y \overset{\neq 0}{\in} \mathbb{Z}[\sqrt{d}]\} = P$

$\mathbb{Q}(\sqrt{d}) \subseteq P$

$$q + r\sqrt{d} = \frac{q_1}{q_2} + \frac{r_1\sqrt{d}}{r_2} = \frac{q_1 r_2 + r_1 q_2 \sqrt{d}}{q_2 \cdot r_2} \quad \checkmark$$

$P \subseteq \mathbb{Q}(\sqrt{d})$

$$(m + n\sqrt{d})(k + l\sqrt{d})^{-1} = \frac{(m + n\sqrt{d}) \cdot (k - l\sqrt{d})}{(k + l\sqrt{d}) \cdot (k - l\sqrt{d})} = \frac{mk - lm\sqrt{d} + nk\sqrt{d} - nld}{k^2 - l^2 d} \quad \checkmark$$

Avtomorfizmi $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, d ni popoln kvadrat:

id

$\sigma: \sqrt{d} \to -\sqrt{d}$

$x \in \mathbb{Q}(\sqrt{d})$: $N(x) = x \cdot \sigma(x)$

$x \in \mathbb{Q}(i)$: $N(m + ni) = (m + ni)(m - ni) = m^2 + n^2$

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

2) Pokaži:

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

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

d) Element $x \in \mathbb{Z}[\sqrt{d}]$ je obrnljiv natanko tedaj, ko je $N(x) = \pm 1$.

($\Rightarrow$) x obrnljiv

$\Rightarrow \quad x x^{-1} = 1$

$\Rightarrow N(x x^{-1}) = N(1)$

$N(x)\,N(x^{-1}) \quad 1$

$N(x) \in \mathbb{Z}, \quad N(x^{-1}) \in \mathbb{Z}$

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

($\Leftarrow$) $N(x) = \pm 1$

$x\,\sigma(x) = \pm 1$

$x = m + n\sqrt{d} \quad \in \mathbb{Z}[\sqrt{d}]$
$\sigma(x) = m - n\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

$x\,\sigma(x) = 1 : \quad x^{-1} = \sigma(x)$
$x\,\sigma(x) = -1 : \quad x^{-1} = -\sigma(x)$

e) Iz $N(x) = \pm p$, kjer je p praštevilo, sledi, da je x nerazcepen.

Recimo, da je x razcepen.

$x = yz$, y, z nista obrnljiva

$\Rightarrow N(x), N(y) \notin \{-1, +1\}$

$\pm p = N(x) = N(y)N(z)$

---

3) Če je $d < -1$, sta 1 in -1 edina obrnljiva elementa v $\mathbb{Z}[\sqrt{d}]$.

$N(n + m\sqrt{d}) = n^2 - d m^2 = \pm 1$

$\Rightarrow m = 0$

$\Rightarrow |n| = 1$

$\Rightarrow n = \pm 1$

---

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

$N(1+i) = (1+i)(1-i) = 2$ praštevilo ☺

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

$N(3) = 9$ ni praštevilo ☹

Denimo, da je 3 razcepen.

$3 = x \cdot y \quad / N$

$9 = N(3) = N(x)\,N(y)$

x, y nista obrnljiva

$\Rightarrow N(x), N(y)$ nista ± 1

$\Rightarrow N(x), N(y) = \pm 3$

$N(n+mi) = n^2 + m^2 = \pm 3$

$\exists x : N(x) = p \Rightarrow p$ razcepen v $\mathbb{Z}[\sqrt{d}]$

---

praštevilo p razcepno v $\mathbb{Z}[\sqrt{d}] \Leftrightarrow p = m^2 - dn^2$

---

5) Poišči vse delitelje elementa 2 v $\mathbb{Z}[i]$.

$x \mid 2 \Leftrightarrow 2 = x \cdot y$ za nek y

$N(2) = N(x)\,N(y)$

$4 = N(x)\,N(y)$

·) $N(x) = \pm 1, \quad N(y) = \pm 4$

$\Rightarrow x$ obrnljiv

• $N(x) = \pm 2$, $N(y) = \pm 2$

$N(n+mi) = n^2 + m^2 = \pm 2$

$n, m = \pm 1$

$x = \pm 1 \pm i$

• $N(x) = \pm 4$, $N(y) = \pm 1$

$\Rightarrow x = \pm 2, \pm 2i$

13.10.

1) Določi gcd $a = 3+4i$, $b = 1-3i$ v kolobarju $\mathbb{Z}[i]$.

stopnja $\sigma = n^2 + m^2$ (norma)

$a = k \cdot b + r \quad / : b$

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

$\frac{a}{b} = \frac{(3-4i)(1+3i)}{(1-3i)(1+3i)} = \frac{15+5i}{10} = \frac{3}{2} + \frac{1}{2}i \approx (2+i) + (-\frac{1}{2} - \frac{1}{2}i)$

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

$(-\frac{1}{2} - \frac{1}{2}i)b = -2+i \in \mathbb{Z}[i]$ ✓

$\sigma(b) = 9+1 = 10$
$\sigma(-2+i) = 4+1 = 5$

$\frac{1-3i}{-2+i} = \frac{-(1-3i)(2+i)}{4+1} = \frac{-5+5i}{5} = -1+i$

$\Rightarrow a = (2+i)b + (-2+i)$
$b = (-1+i)(-2+i) + 0$

Razširjev Evklidov algoritem:

$a = (2+i)(-1+i)(-2+i) + (-2+i) = (-2+i)[(2+i)(-1+i)+1]$

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

$\frac{a}{-2+i} = (2+i)\cdot\frac{b}{-2+i} + 1$

$1 = \frac{a}{-2+i} - (2+i)\cdot\frac{b}{-2+i}$

$\Rightarrow gcd = -2+i$

---

2) Pokaži, da elementa $a = 6$ in $b = 2+2\sqrt{-5}$ kolobarja $\mathbb{Z}[\sqrt{-5}]$ nimata največjega skupnega delitelja.

Želimo najti dva delitelja c_1, c_2, $c_i | a$, $c_i | b$, ki ne moreta deliti nobenega tretjega delitelja d, $d|a$, $d|b$.

Opomba: $a' = 3$, $b' = 1+\sqrt{-5}$ pa imata gcd 1

$c_1 = 2$
$c_2 = 1+\sqrt{-5}$ $\qquad ((1+\sqrt{-5})(1-\sqrt{-5}) = 6)$

Denimo: $c_1 c_2 | d$

$\Rightarrow N(c_1)\,N(c_2) \mid N(d)$
$\quad\;\; 4 \quad\; 6$
$\Rightarrow 12 | N(d)$

$N(\gcd(a,b)) \mid \gcd(N(a), N(b))$

$\Rightarrow N(d) \mid \gcd(36,24) = 12 = x^2 + 5y^2$ (1 ali 2)

$x^2 \neq 11$, $x^2+5 \neq 11$

Kolobar z enolično faktorizacijo (UFD):

$\forall a \neq 0 : a = p_1 \cdots p_n$, p_i nerazcepni, "enolično"

Kdaj gcd obstaja?

- evklidski : evklidov algoritem
- glavni (nk) : $\gcd(a,b) = (a,b)$
- UFD (nk)

---

3) Če je K UFD, pokaži, da gcd vedno obstaja.

$a = p_1^{k_1} \cdots p_n^{k_n} \cdot \cancel{u}$ (obrnljiva)

$b = p_1^{l_1} \cdots p_n^{l_n} \cdot \cancel{v}$

Dovolimo: $l_i, k_i = 0$

$d = \gcd(a,b) := p_1^{m_1} \cdots p_n^{m_n}$

$m_i := \min\{l_i, k_i\}$

Očitno: $d \mid a$, $d \mid b$

$c = p_1^{r_1} \cdots p_n^{r_n} \cdot q_1 \cdots q_m$

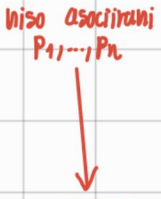
$c \mid a$

$\Leftrightarrow a = c \cdot \alpha$

$\Leftrightarrow p_1^{k_1} \cdots p_n^{k_n} = p_1^{r_1} \cdots p_n^{r_n} \cdot \underbrace{q_1 \cdots q_m}_{\alpha} \cdot s_1 \cdots s_{\bar{s}}$

$c \mid b$

$\Leftrightarrow b = c \cdot \beta$



$\Leftrightarrow p_1^{l_1} \cdots p_n^{l_n} = p_1^{r_1} \cdots p_n^{r_n} \cdot \underbrace{q_1 \cdots q_m}_{\beta} \cdot t_1 \cdots t_{\bar{t}}$

$\Rightarrow m = 0$ (q_i ne nastopajo)

$r_i \leq k_i$
$r_i \leq l_i$

$\Rightarrow r_i \leq m_i$

$\Rightarrow c = p_1^{r_1} \cdots p_n^{r_n}$, $r_i \leq m_i$

$\Rightarrow c \mid d$ ✓

---

4) Pokaži, da je $\mathbb{Z}[\sqrt{-2}]$ evklidski.

$\sigma(m + n\sqrt{-2}) = m^2 + 2n^2$ $(\sigma(a) = N(a))$

$\frac{a}{b} = q_1 + q_2 \sqrt{-2}$

$a = ([q_1] + [q_2]\sqrt{-2})b + \underbrace{((q_1 - [q_1]) + (q_2 - [q_2])\sqrt{-2})b}_{r}$

$\delta(r) = N(r) = \underbrace{N(\dots + \dots \sqrt{-2})}_{3/4} \cdot N(b) < \delta(b) = N(b)$

$(\dots)^2 + 2(\dots)^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4}$

20.10.

DN1) $K[X]$ UFD $\Rightarrow$ K UFD

$K[X]^* = \{$konstantni polinomi, obrnljive konstante iz $K\}$

Faktorizirano ga v $K[X]$, isti razcep tudi v K

Neničeln element $K[X]$ produkt nerazcepnih.

- $f(x)$ nerazcepen:

  ✓

- $f(x)$ razcepen:

  $f(x) = k(x)g(x)$

  - $\text{st}\, k(x), \text{st}\, g(x) < \text{st}\, f(x)$:

    Nadaljujemo z indukcijo

  - En ima stopnjo 0:

    BSS: $\text{st}\, k(x) = 0$

    $\Rightarrow k(x) \in K \Rightarrow k(x)$ produkt nerazcepnih v K

    $g(x) = k_2(x)\, g_2(x)$

    $\vdots$

$f(x) = k_1 k_2 \cdots k_n \cdot g_n(x)$

$a_m x^m + \ldots$ $\qquad$ $b_m x^m + \ldots$

Ali se to zaključi?

$a_m = k_1 k_2 \cdots k_n b_m \in K$ enolična faktorizacija

Proces se ustavi:

$g_n(x) = h_1(x) h_2(x)$

Praelementi so nerazcepni elementi

Vemo iz predavanj

Nerazcepni elementi so praelementi v UFD

Želimo: f nerazc. in $f \mid pq \Rightarrow f \mid p$ ali $f \mid q$

$f = p_1 \cdots p_n$ enolično

$f \in K[x]$ nerazcepen $\Rightarrow$ f praelement

Želimo: f nerazc. in $f \mid pq \Rightarrow f \mid p$ ali $f \mid q$

$f \in F[x]$ nerazcepen $\xrightarrow{F[x] \text{ UFD}}$ $f \in F[x]$ praelement

Velja: $f \mid pq \Rightarrow f \mid p \vee f \mid q \vee F[x]$

$kf = pq$

$f = \frac{pq}{k} = \frac{pq}{ab} = \frac{p}{a} \cdot \frac{q}{b}$ $\quad a \in K[x]$, $b \in K[x]$

$f \mid p$ v $F[x]$: $af = p$, $a \in F[x]$, $a = \frac{g(x)}{k}$ ($g(x) \in K[x]$, $k \in K$)

$g(x) f(x) = k\, p(x)$

$\operatorname{cont} g \cdot \operatorname{cont} f = k \cdot \operatorname{cont} p \in K$ ($k = p_1 \cdots p_n$)

Cilj: $k = 1$

- $p_i \mid \operatorname{cont} f$:

  f nerazcepen

  $f = p_i h(x) \Rightarrow f \sim p$ (p prim. $\Rightarrow f$ prim.)

- $p_i \mid \operatorname{cont} g$:

  $\operatorname{cont} g$ tuja s k

  $\times$

$\Rightarrow k$ je obrnljiv

$\Rightarrow a = \frac{g(x)}{k} \in K[x] \Rightarrow f \mid p$ tudi v $K[x]$ $(fa = p)$ (k obrnljiv)

$\Rightarrow K = F[x]$ UFD, $F[x][y] = F[x,y]$

DN2) $K[x]$ glavni $\Rightarrow$ $\forall x \in K \setminus \{0\} : \exists x^{-1}$

a obrnljiv $\Leftrightarrow (a) = K$

$(a, x) = (a')$

$\Rightarrow (a, X) = (f(X)) \overset{st>1}{\Rightarrow} a \in (f(X))$

$a' bX = X$

$\Rightarrow a'b = 1 \Rightarrow (a') = K[X]$

$(a, X) = K[X] = (1)$

$1 = k(\alpha a + \beta X) = (k_0 + k_1 X + \dots)[(\alpha_0 + \alpha_1 X + \dots)a + (\beta_0 + \beta_1 X + \dots)X]$

konst: $1 = (k_0 \cdot \alpha_0) \cdot u$

---

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

Nerazcepen:

Recimo, da je $1+\sqrt{-3}$ razcepen.

$1+\sqrt{-3} = \alpha \cdot \beta$

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

$N(\alpha) N(\beta) = 4$

$N(\alpha), N(\beta) \neq \pm 1$, ker nista obrnljiva

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

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

$\Rightarrow b = 0 \Rightarrow a^2 = 2 \Rightarrow$ ↯

Ni praelement:

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

Če bi bil praelement, bi delil 2.

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

$N(*) = \pm 1 \Rightarrow * \text{ obrnljiv} \Rightarrow * = \pm 1$

$\Rightarrow$ Ne obstaja

$\Rightarrow \mathbb{Z}[\sqrt{-3}]$ ni UFD