katesi elementi kolobarja $\mathbb{Z}[i]$ 6.10

so asociirani $m+ni$

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

kateri so obrnljivi:

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

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

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

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

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

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

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

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

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

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

zaprtost za seštevanje, množenje, enota

za množenje:

$$(m+n\sqrt{d})(x+x\sqrt{d}) = mx+nyd+\sqrt{d}(nx+ym)$$

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

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

2) invertiranje

je tu

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

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

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

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

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

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

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

$$xy = 1 \Rightarrow N(xy) = N(1)$$
$$N(x)N(y) = 1$$
$$N(x) = \frac{1}{N(y)} \qquad N(y) \in \mathbb{Z} \wedge N(x) \in \mathbb{Z}$$
$$\Rightarrow N(y) \in \{\cancel{0}\,{-1}, 1\}$$
$$\Rightarrow N(x) \in \{-1, 1\}$$

6)

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

recimo da x razcepen in $N(x) = \pm p$ ab neobrnljiva

$$x = ab$$
$$N(x) = N(a)N(b) = \pm p \Rightarrow N(a) = 1 \vee N(b) =$$

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

5) ne prebe

Mora da je $N(a) \pm 1 \Rightarrow a$ obrnljiv.

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

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

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

$|d| \geq 1$

če je $b^2 > 1 \Rightarrow N > 1$

$\Rightarrow b = 0$

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

~~neomejeni~~ mnogoštevilnih

in vemo da sta različna to rešitve 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

$p \to$ nerazcepne

$N(7+8i) = 49 + 64 = \text{velik} = 113$ praštevilo

~~bi je praštevilo~~ Norma je 9

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

vsaj 2 morata biti 1

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

$\underline{N(x)} = \underline{n} \Rightarrow \underline{n}$ razcepna

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

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

$x | 2 \Leftrightarrow 2 = xy$ za nek y

$N(x \cdot y) = 4 \quad N(x)N(y) = 4$

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

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

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

$x = \pm 2$ so vse možnosti

$x = \pm 2i$

1)

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

$b = 1-3i$

$|a| = 9+16 = 25$

$|b| = 1+9 = 10$ $\quad$ fuyni deldely

$a = kb + r$

$\frac{a}{b} = \underset{\in \mathbb{Z}[i]}{k} + \frac{r}{b} \in \mathbb{Q}[i]$

$a = 3-4i$

$b = 1-3i$

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

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

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

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

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

2)

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

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

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

$\cancel{c \mid a}$ ~~...~~ $\Rightarrow$ ~~...~~ $\frac{a}{c}$, $d \mid a$, $d \mid b \Rightarrow 6 \cdot 2 \cdot 3$

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

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

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

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

$\Downarrow \qquad \Downarrow$

$x^2 = 3 \qquad x^2 = \times$

Tak nedotegne

3) UFD $\Rightarrow$ gcd obstaja

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

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

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

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

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

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

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

podobno $m_i < l_i \Rightarrow \forall i$

$c \mid d$

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

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

b) $\delta(a) \leq \delta(a\cdot b) \; \forall a,b \in K - \{0\}$

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

Vene da b velja

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

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

$$a = \left([q_1] + [q_2]\sqrt{-2}\right)b + \left(q_1 - [q_1] + (q_2 - [q_2])\sqrt{-2}\right)b$$

DN:

Naj bo $K[X]$ UFD

Potem ima polinom $n^{\epsilon K}$ enolično faktorizacijo

Torej je tud $K[\ldots]$ UFD

Naj bo K UFD

Naj bo $p(x)$ poljuben polinom

Razcepimo $p(x) = \prod_{k=1}^{r}\left(\sum_{i=1}^{n} a_{ik} X^{n}\right) =$

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

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g)$$

$$p \mid \mathrm{cont}(f,g) \Rightarrow \gcd(a_0 \ldots a_n) = p$$

$$fg = 0 \vee K/p[X]$$

$$\Rightarrow f = 0 \vee g = 0$$

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

$$\Rightarrow p \mid \mathrm{cont} f \vee p \mid \mathrm{cont} g$$

Recimo da f razcepen $F[X]$

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

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

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

$$= a \cdot \text{enolično}$$

enolični skupni delitelji

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

$\shortparallel$

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

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

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

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

$\Rightarrow \forall\, p(x) \ldots$ [illegible]

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

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

$\exists b \quad ab = 1$

(a) je ideal $\quad (a) = \{af \,;\, f \in K[x]\}$

20.10

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

$1+\sqrt{3}$ nerazcepen

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

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

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

če bi bila 1 bi bila obrnljiva

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

$b=0$

$a^2 = \pm 2$ nedosegljivo

Ni praelement

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

Vsak element deli svojo normo

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

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

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

$N(k) = \pm 1$

$\Rightarrow k = \pm 1$

Domača naloga

1)

$$\omega = \frac{(1+\sqrt{-19})}{2} \qquad \mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$$

$$N(a+b\omega) = |a+b\omega|^2 = a^2+ab+5b^2$$

2 in 3 nerazcepna

$N(2) = 4$

$2 = ab$; a, b neobr. $\Rightarrow N(a) = N(b) = 2$

$a =: a+b\omega$

$N(a) = a^2+ab+5b^2 = 2$

$b \neq 0 \Rightarrow 5b^2 > 2 \Rightarrow N(a) > 2$ ↯

$N(3) = 9 \qquad 9 = x \cdot y \qquad 9 = 3 \cdot 3 \Rightarrow N(x) = N(y) = 3$

$N(x) = 3 \qquad x = a+b\omega$

$a^2+ab+5b^2 = 3$

$b \neq 0 \Rightarrow 5b^2 > 3 \Rightarrow N(x) > 3$ ↯

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

$a^2+ab+5b^2 = 1$

$b \neq 0 \Rightarrow 5b^2 > 1$ ↯ $\Rightarrow b = 0$

$a^2 = 1 \Rightarrow a \in \{1, -1\} \Rightarrow x \in \{1, -1\}$

Moduli

$K = \{$zgornje trikotne matrike nad $F\}$

$M = \begin{bmatrix} F \\ F \end{bmatrix}$ je levi K-modul

iščemo podmodule od M

$KM \subseteq M$

$N = \{\lambda \begin{bmatrix} u \\ v \end{bmatrix} ; \lambda \in F\}$ za $u, v \in F$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot \lambda \begin{bmatrix} u \\ v \end{bmatrix} = \lambda \begin{bmatrix} au+bv \\ cv \end{bmatrix} \in N$$

$$\lambda au + \lambda bv = \mu u$$
$$\lambda cv = \mu v \quad \Rightarrow \quad \lambda c = \mu$$

$$\lambda au + \lambda bv = \lambda cu$$
$$au - cu + bv = 0$$
$$bv = (c-a)u$$

DN naprej

$\mathbb{Z}[\omega]$ ni evklidski

$(\exists\, \delta : \mathbb{Z}[\omega] - \{0\} \to \mathbb{N} \cup \{0\})$

$\omega = gx + r \Rightarrow r \in \{1, -1, 0\}$

$r = 0 \Rightarrow \omega = gx \Rightarrow x$ asociiran z ω

$N(x) = N(\omega) = 5$

$2 = g'x \pm 1 \Rightarrow x \in \{\pm 2, \pm 3\} \Rightarrow N(x) \in \{4, 9\}$ $\times$

$r = 1 \Rightarrow \omega = gx + 1$

$-1 + \omega = gx \Rightarrow 1 - 1 + 5 = N(g)N(x) = 5$

$N(x) = 5$ $\times$

$r = 1 \Rightarrow 1 + \omega = gx \Rightarrow 7 = N(g)N(x) \Rightarrow N(x) = 7$ $\times$

$\mathbb{Z}[\omega]$ je glavni

$$\left(\forall \alpha \in \mathbb{C} - \mathbb{Z}[\omega] . \exists p, g \in \mathbb{Z}[\omega] . \ 0 < |p\alpha - g| < 1\right)$$
$$\Longrightarrow \mathbb{Z}[\omega] \text{ glavni kolobar}$$

Naj bo I poljuben ideal. Naj bo $b \in I$ tak da

$\forall x \in I . \ N(x) \geq N(b)$

Naj bo $a \in I$ poljuben $\quad \alpha = \frac{a}{b} \quad a = \alpha b$

$\alpha \in \mathbb{Z}[\omega] \Rightarrow b | a$ za $\forall a \in I \Longrightarrow I = (b)$

$\alpha \notin \mathbb{Z}[\omega]$ in $\{p \text{ a } g\} \Longrightarrow 0 < |p\frac{a}{b} - g|^2 < 1 \quad / \cdot |b|$

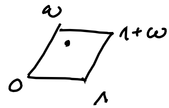
$$0 < |\underbrace{pa}_{\in I} - \underbrace{gb}_{\in I}|^2 < |b|^2 \quad \times$$

$\forall \alpha \in \mathbb{C} - \mathbb{Z}[\omega] \ \exists \rho, g \in \mathbb{Z}[\omega] . \ 0 < |\rho\alpha - g| < 1$

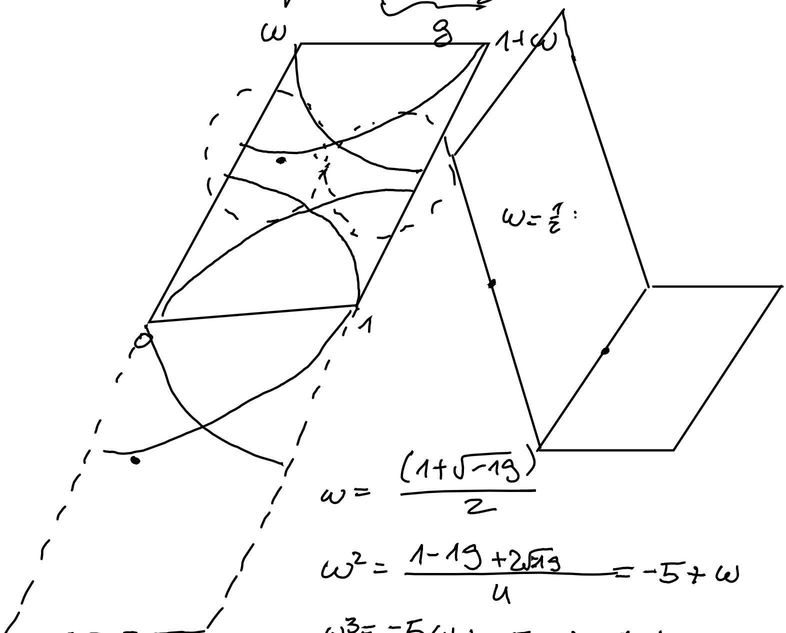
$\alpha \in \mathbb{C} - \mathbb{Z}[\omega]$ poljuben

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

$\beta = \alpha - (m + \omega n) \quad \beta \in$



$\rho\alpha - g = \rho\beta + \underbrace{\rho(\ldots) - g}$



$$\omega = \frac{(1+\sqrt{-19})}{2}$$

$$\omega^2 = \frac{1 - 19 + 2\sqrt{-19}}{4} = -5 + \omega$$

$$\omega^3 = -5\omega + -5 + \omega = -5 - 4\omega$$

DM ze teorie:

$d = 4k+1$

$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 = 4(2-k)$

$b^2 = 1$:

$a^2 - 4k - 1$

$a = 3$

$8 - 4k = 4(2-k)$

$b^2 = 1$

$a^2 = 9$

$$\{(x-1)p(x)\} = \{\sum a_n = 0\}$$

Tiote je ideal

$$\sum_{n=0}^{k} a_n x^n$$

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 : (x-1) = a_n x^{n-1}$$

$$- a_n x^n + a_n x^{n-1} \qquad \cancel{+a_n}$$

$$(a_n + a_{n-1}) x^{n-1} + \dots + a_0$$

kdgtv pd 2x ven očegta

ind prelp.

$$ax - a = a(x-1)$$ ✓

Besoin de g_i $\exists$ B $\{f_1 \ldots f_g\}$

tout élément de espace

$g_1 f_1 + \ldots + g_n f_n$

$\sqrt{f_1^2 + \ldots + f_n^2}$

$\sqrt{g_1^2 f_1^2 + \ldots + g_n^2 f_n^2} \leq \sqrt{\max(g_1 \ldots)} \sqrt{f_1^2 + \ldots + f_n^2}$

$= h_1 f_1 + \ldots + h_n f_n$

$M = {}_{\mathbb{Z}}\mathbb{Z}_{12}$

$\mathbb{Z}_2 = \{0, 6\}$ enostavni
$\mathbb{Z}_3 = \{0, 4, 8\}$ enostavne
$\mathbb{Z}_4 = \{0, 3, 6, 9\} \supseteq \mathbb{Z}_2$
$\mathbb{Z}_6 = \{0, 2, 4, 6, 8, 10\} \supseteq \mathbb{Z}_2, \mathbb{Z}_3$

3) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_{12})$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_3, \mathbb{Z}_4)$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_{12}, \mathbb{Z}_{12})$

$\mathbb{Z} \longrightarrow \mathbb{Z}_{12}$
$0 \longmapsto 0$ 1 natanko določi
$1 \longmapsto$ karkoli $\Rightarrow$ imamo 12 homomorfizmov

$$\boxed{\begin{array}{l} K \text{ kolobar, } {}_K M \text{ modul} \Rightarrow \\ \mathrm{Hom}(K, M) = \{x \longmapsto xm : m \in M\} \cong {}_K M \end{array}}$$

$\mathbb{Z}_3 \to \mathbb{Z}_4$
$0 \longmapsto 0$

1.	2.	3.
$1 \longmapsto 1$	$1 \longmapsto 2$	$n \longmapsto 0$
$2 \longmapsto 2$	$2 \longmapsto 1$	
$3 \longmapsto 0$	$3 \longmapsto 0$	
$4 \longmapsto 1$	$4 \longmapsto 2$	

$\mathbb{Z}_{12} \mapsto \mathbb{Z}_{12}$
$0 \longmapsto 0$
$1 \longmapsto a$
$n \longmapsto na \mod 12$

K kolobar. K enostaven $\iff$ K obseg

$\Rightarrow$ Recimo da je enostaven, $a \in K$ poljuben

a obrnljiv

$Ka = K \Rightarrow \exists k \in K.\ ka = 1$

$\Leftarrow$ M podkolobar ima

Vaje za nazaj

1 Naloga M K-modul $M \neq \{0\}$ enostaven $\Leftrightarrow M = Km$ $\forall m \in M$

Naj bo M enostaven. Edina podmodula sta $\{0\}$ in M

$\Rightarrow$ Naj bo $m \in M$ poljuben $\underline{Km \text{ je podmodul}}$

$\alpha, \beta \in K$ $\quad \alpha k m - \beta h m = (\alpha k - \beta h) m \in Km$

$\Leftarrow$ $M = Km$ za $\forall m \in M$.

Naj bo N podmodul.

$\forall n \in N$. $Kn = M$ torej $N = M$

2. naloga

levi: K modul ${}_K M$ enostaven $\Leftrightarrow M \cong {}^K\!/_{{}_K I}$, kjer je ${}_K I \leq K$ maksimalen levi ideal

$\Rightarrow$ Naj bo M enostaven, $a \in M$

$\varphi: K \longrightarrow M$ $\qquad$ φ surjektiven po prejšnji nalogi

$k \mapsto ka$

$\ker\varphi = \underbrace{\{k;\ ka = 0\} = {}_K I}$ maksimalen

$I \subsetneq J \subsetneq K$ $\qquad$ $\varphi_*(J) = M \Rightarrow m = ja$ $\forall m$

$\qquad\qquad\qquad\qquad\qquad\Rightarrow j = ja \Rightarrow j(1-a) = 0$

$K \longrightarrow M$ $\qquad$ $0 \subsetneq \varphi_*(J) \subsetneq M$ (ker $J \neq \ker\varphi$) $\quad \cancel{\longrightarrow}$ $\quad 1-a \in \ker\varphi$

$J \xrightarrow{sur} \varphi_*(J)$ $\qquad\qquad\qquad\qquad\Rightarrow 1-a \in J$

$\qquad\qquad\qquad\qquad\qquad\qquad (1-a)+a = 1 \in J$

$I \longrightarrow 0$ $\qquad \Longrightarrow J = I \vee J = K$ $\qquad \Rightarrow J = K$ $\times$

$\Leftarrow$ Naj bo ${}_K M \cong {}^K\!/_{{}_K I}$; I maksimalen levi ideal

$0 < N < M$ $\qquad \varphi$ surj

$\uparrow \quad \uparrow \quad \uparrow$

$I < J < K$ $\qquad J = \varphi^*(N)$

$N \subseteq \varphi_*(J) = \varphi_*(\varphi^*(N)) \Longrightarrow \varphi_*(J) = N$

$K/I \longrightarrow M$ $\qquad\qquad \varphi: K \longrightarrow M$

$1 + I \mapsto e \in M - \{0\}$ $\quad\Longrightarrow\quad k \mapsto ke$

$x + I = x(1+I) \mapsto xe$

$\underline{M \text{ enostaven}}$ $\qquad \underline{I = J} \vee \underline{J = K}$

$I < J_2 < J_1 < K$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$0 < \varphi_*(J_2) = \varphi_*(J_1) < M$ $\qquad /:\varphi(J_2)$

$0 = \dfrac{\varphi_*(J_1)}{\varphi_*(J_2)} < M/\varphi(J_2)$

??

Tene nelo ge
espanta

Od zadnjič:

$$\mathrm{End}(M \oplus N) \cong \begin{bmatrix} \mathrm{End}(M) & \mathrm{Hom}(N,M) \\ \mathrm{Hom}(M,N) & \mathrm{End}(N) \end{bmatrix}$$

1) določi kolobarje endomorfizmov $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_2 \oplus \mathbb{Z}_3)$, $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_6 \oplus \mathbb{Z}_3)$

$$\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_2 \oplus \mathbb{Z}_3) = \begin{bmatrix} \mathrm{End}\,\mathbb{Z}_2 & \mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_2) \\ \mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_3) & \mathrm{End}\,\mathbb{Z}_3 \end{bmatrix}$$

$\mathrm{End}\,\mathbb{Z}_2$: $0 \mapsto 0,\ 1 \mapsto 1$; $1 \mapsto 0,\ 0 \mapsto 1$ $\cong \mathbb{Z}_2$

$\boxed{\text{Splošno: } \mathrm{End}\,\mathbb{Z}_p \cong \mathbb{Z}_p}$ $\Rightarrow \mathbb{Z}_3 \cong \mathbb{Z}_3$

$1 \mapsto$ red elementa 3 ne obstaja in

$$\mathrm{End}(\mathbb{Z}_2 \oplus \mathbb{Z}_3) \cong \begin{bmatrix} \mathbb{Z}_2 & 0 \\ 0 & \mathbb{Z}_3 \end{bmatrix} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$$

$\mathrm{End}(\mathbb{Z}_6 \oplus \mathbb{Z}_3)$: $\mathrm{End}(\mathrm{End}(\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_3) =$

$$= \begin{bmatrix} \mathrm{End}(\mathbb{Z}_2 \oplus \mathbb{Z}_3) & \mathrm{Hom} \\ \mathrm{Hom} & \mathrm{End}\,\mathbb{Z}_3 \end{bmatrix} = \begin{bmatrix} \mathbb{Z}_6 & \mathrm{Hom} \\ \mathrm{Hom} & \mathbb{Z}_3 \end{bmatrix}$$

$$\mathrm{Hom}(\mathbb{Z}_6, \mathbb{Z}_3) \cong_{\mathbb{Z}} \mathrm{Hom}(\mathbb{Z}_2 \oplus \mathbb{Z}_3, \mathbb{Z}_3) \cong$$

$$\cong \underbrace{\mathrm{Hom}(\mathbb{Z}_2, \mathbb{Z}_3)}_{0} \oplus \mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_3) \cong \mathbb{Z}_3$$

$$\mathrm{End}(\mathbb{Z}_6 \oplus \mathbb{Z}_3) = \begin{bmatrix} \mathbb{Z}_6 & \mathbb{Z}_3 \\ \mathbb{Z}_3 & \mathbb{Z}_3 \end{bmatrix}$$

$1 \mapsto 2$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix} \overset{?}{=} \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$$ se ne izide

$x \mapsto (2, x \bmod \mathbb{Z}_3)$

$$\begin{bmatrix} 0 & \mathbb{Z}_3 \to \mathbb{Z}_2 \oplus \mathbb{Z}_3 \to \mathbb{Z}_6 \\ & 1 \mapsto (1,0) \mapsto 4 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \mathbb{Z}_6 \to \mathbb{Z}_2 + \mathbb{Z}_3 \to \mathbb{Z}_3 & \\ (1,0) \mapsto 2 & 0 \\ x \mapsto 2x \bmod 3 & \end{bmatrix}$$

$$= \begin{bmatrix} x \mapsto 2x \mapsto (2x \bmod 3, 0) = 4x \\ \cancel{2 \mapsto \ldots} \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$$

$\updownarrow\ \mathbb{Z}_6 \to \mathbb{Z}_3$ $\qquad \updownarrow$

$$\begin{bmatrix} 0 & x \mapsto 4x \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ x \mapsto 2x & 0 \end{bmatrix} \begin{bmatrix} x \mapsto 8x & 0 \\ 0 & 0 \end{bmatrix}$$

$\mathbb{Z}_3 \to \mathbb{Z}_6$

k $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_6$ $\qquad$ $\mathbb{Z}_6 \longrightarrow \mathbb{Z}_3$

$1 =$ $1 \mapsto (1,0) \longrightarrow 4$ $\qquad$ $k =$ $1 \mapsto k \bmod 3$

$2 =$ $1 \mapsto (2,0) \mapsto 2$

$k =$ $1 \mapsto (k,0) \mapsto \ldots$

Hitreje:

$$\mathbb{Z}_{18} = \mathbb{Z}_6 \oplus \mathbb{Z}_3 = \mathbb{Z}_2 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_3)$$

$$\operatorname{End}(\mathbb{Z}_6 \oplus \mathbb{Z}_3) = \begin{bmatrix} \mathbb{Z}_2 & \operatorname{Hom}(\mathbb{Z}_3 \oplus \mathbb{Z}_3, \mathbb{Z}_2) \\ \operatorname{Hom}(\mathbb{Z}_2, \mathbb{Z}_3 \oplus \mathbb{Z}_3) & \operatorname{End}(\mathbb{Z}_3 \oplus \mathbb{Z}_3) \end{bmatrix} =$$

$$\operatorname{Hom}(\mathbb{Z}_2, \mathbb{Z}_3 \oplus \mathbb{Z}_3) = \operatorname{Hom}(\mathbb{Z}_2, \mathbb{Z}_3) \oplus \operatorname{Hom}(\mathbb{Z}_2, \mathbb{Z}_3)$$

$$= \begin{bmatrix} \mathbb{Z}_2 & 0 \\ 0 & \begin{bmatrix} \mathbb{Z}_3 & \mathbb{Z}_3 \\ \mathbb{Z}_3 & \mathbb{Z}_3 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \mathbb{Z}_2 & 0 & 0 \\ 0 & \mathbb{Z}_3 & \mathbb{Z}_3 \\ 0 & \mathbb{Z}_3 & \mathbb{Z}_3 \end{bmatrix} \cong$$

$$\cong \mathbb{Z}_2 \oplus M_2(\mathbb{Z}_3)$$

Bimoduli

$K^{op} = \{ x^{op} \mid x \in K \}$ $\quad x^{op} \cdot y^{op} = (yx)^{op}$

Grupe: $G \cong G^{op}$
$x^{op} = x^{-1}$

${}_K M \cong M_{K^{op}}$ vsak levi modul lahko predstavimo kot desni K modul

Bimodul je ${}_K M_S$, povezuje pa ga asociativnostni zakon
K, S kolobarja ${}_K M$ je levi K-modul
M_S je desni S-modul

$x \in K$, $y \in S$

$m \in M$ $\quad \underbrace{(x \cdot m)}_{\in M} y = x (m \cdot y)$

Primeri

1) ${}_K K_K$ je bimodul

2) ${}_K M_{K^{op}}$ ni bimodul (razen če K komut.

$m \cdot x^{op} := xm$ $\quad$ $x(m y^{op}) = xym$
$\qquad\qquad\qquad\qquad \parallel$
$\qquad\qquad\qquad (xm) y^{op} = yxm$

3) ${}_K M_{\mathrm{End}(M)^{op}}$ je bimodul

$(xm)\varphi^{op} = \varphi(xm) = x\varphi(m) = x(m\varphi^{op})$

2) Naj bosta ${}_K M_S$ in ${}_K N_R$ bimodula (K, S, R kolobarji)

Premisli, da imajo homomorfizmi: $M \to N$ naravno strukturo (S, R)-bimodula ← homomorfizmi kot levih K-modulov

Zgubi strukturo K modula

$${}_S \mathrm{Hom}(M,N)_R$$

$$s \in S \quad s\varphi := m \mapsto \varphi(ms)$$

$$r \in R \quad \varphi r := m \mapsto \varphi(m) r$$

Hom(M,N) je levi S modul

$$(s+t)\varphi = (m \mapsto \varphi(m(s+t))) = (m \mapsto \varphi(ms) + m \mapsto \varphi(mt)) = s\varphi + t\varphi$$

$$\varphi(m(s+t)) = \varphi(ms) + \varphi(mt)$$

$$1 \cdot \varphi = (m \mapsto \varphi(m)) = \varphi$$

$$s(\varphi + \psi) = \checkmark$$

Vm. $(st)\varphi\,(m) = \varphi(mst) = \varphi((ms)t) =$

$$= (t\varphi)(ms) = s(t\varphi(m)) = s(t\varphi)(m)$$

ali je to vredu $\quad (t\varphi)(xm) = x((t\varphi)(m))$

$$(t\varphi)(xm) = \varphi((xm)t) = \varphi(x(mt)) = x\varphi(mt)$$

Podobno za desni R modul

$$s(\varphi r)(m) = (\varphi r)(ms) = \varphi(ms) r = (s\varphi(m)) r$$

Lev K-modul ${}_K M$. Dual je $M^*_K = \mathrm{Hom}(\cancel{{}_K}M, \cancel{{}_K}K_K)$

Ker je domena bimodul, je tudi M^*_K desni K modul

Funkcional

$$M = \begin{bmatrix} F \\ F \end{bmatrix}$$

3) Določi $\left({}_{M_2(F)} M\right)^*$

$$M^*_{M_2(F)} = \mathrm{Hom}\left({}_{M_2(F)}M, M_2(F)_{M_2(F)}\right) \cong$$

$$\begin{bmatrix} F & F \\ F & F \end{bmatrix} \cong \begin{bmatrix} F & 0 \\ F & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & F \\ 0 & F \end{bmatrix} \cong M \oplus M$$

$$\cong \mathrm{Hom}(M, M \oplus M) = \mathrm{End}(M) \oplus \mathrm{End}(M) \cong F^2$$

To sta obsega (Shurova lema)

$M = \begin{bmatrix} F \\ F \end{bmatrix}$ $\quad M \overset{?}{=} [F\ F]$

$K = \begin{bmatrix} F & F \\ F & F \end{bmatrix}$ $\quad K \cong M \oplus M$ vrstica + vrstica

$\begin{bmatrix} 0 & F \\ 0 & F \end{bmatrix} \oplus \begin{bmatrix} F & 0 \\ F & 0 \end{bmatrix}$

struktura desnega K-modula

$M^* = \mathrm{Hom}(M,K)_K \cong \mathrm{Hom}(M,M) \oplus \mathrm{Hom}(M,M) \cong F \oplus F$

ni desni k modul.

Izgubimo strukturo modula

(*) $F \cong \mathrm{Hom}(M,M) = \mathrm{End}\, M$

End(M) obseg, če M enostaven

$F \cong \mathrm{End}(M)$

2-dim vek prostor

$\supseteq$ V posebnem: $\varphi \in \mathrm{Hom}_K(M,M) \leq \mathrm{Hom}_F(M,M) \cong M_2(F)$

$\varphi(Ax) = A\varphi(x)$ $\quad \varphi = B \Rightarrow$

$BAx = ABx$ za $\forall A \in K$ $\forall x \in M$ $\Rightarrow BA = AB$ $\forall A \in K$.

$B \in Z(M_2(F)) = F \cdot I$ diagonalne matrike $\cong_F$

$\subseteq$ očitno

(**) M^*_K tej $(F \oplus F)_K$

$\varphi \in \mathrm{Hom}(M,K)$

$\varphi(m) = (\varphi_1(m), \varphi_2(m)) = \left(\varphi(m) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \varphi(m) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$

stolpci

$\varphi(m) = \left[\varphi_1(m) \,\vdots\, \varphi_2(m)\right]$

$\varphi(Am) = \left[\varphi_1(Am) \,\vdots\, \varphi_2(Am)\right]$

$A\varphi(m) = \left[A\varphi_1(m) \,\vdots\, A\varphi_2(m)\right]$ $\quad \varphi_{1,2}$ skalarne večkratnika identitete

$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ $\quad \varphi \cdot A \overset{v\, M^*}{=} (m \longmapsto \varphi(m) \cdot A)$ dano po definiciji

$[\varphi_1, \varphi_2] \cdot A = \varphi_1 a + \varphi_2 b + \varphi_1 c + \varphi_2 d = \varphi_1(a+c) + \varphi_2(b+d)$

kako sklepamo dalje

$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ $\quad \varphi(m) = [\varphi_1(m), \varphi_2(m)]$ * $\quad m = \begin{bmatrix} x \\ y \end{bmatrix}$

skalarji

$= [\lambda_1 m \ \ \lambda_2 m] = \begin{bmatrix} \lambda_1 x & \lambda_2 x \\ \lambda_1 y & \lambda_2 y \end{bmatrix}$

$\varphi(m) \cdot A = \begin{bmatrix} a\lambda_1 x + b\lambda_2 x & c\lambda_1 x + d\lambda_2 x \\ a\lambda_1 x + b\lambda_2 y & c\lambda_1 y + d\lambda_2 y \end{bmatrix} =$

$= \begin{bmatrix} x(a\lambda_1 + b\lambda_2) & x(c\lambda_1 + d\lambda_2) \\ y(a\lambda_1 + b\lambda_2) & y(c\lambda_1 + d\lambda_2) \end{bmatrix}$

$\varphi = [\lambda_1\ \lambda_2]$ $\quad \varphi \cdot A = [\lambda_1 a + \lambda_2 b, \ c\lambda_1 + d\lambda_2]$

Lažje: $\quad F \oplus F \to \mathrm{Hom}(M,K)$

$[\lambda, \mu] \longmapsto \left(\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} x \\ y \end{bmatrix} [\lambda, \mu]\right)$

$(\varphi \cdot A)\begin{bmatrix} x \\ y \end{bmatrix} = \left(\underbrace{\begin{bmatrix} x \\ y \end{bmatrix} [\lambda, \mu]}_{\varphi}\right) A = \begin{bmatrix} x \\ y \end{bmatrix} ([\lambda, \mu] A)$

1) Določi dual ${}_{\mathbb{Z}}\mathbb{Z}_n^*$

$= \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}) = 0$

$1 \mapsto x \qquad \mathrm{red}\, 1 \mid \mathrm{red}\, x \Rightarrow x = 0$

2) K cel kolobar (brez del. niča, komut)

za ${}_K M$ K-modul definiramo

$\mathrm{tor}(M) - \{m \in M ;\ xm = 0,\ x \in K - \{0\}\}$

$\mathrm{tor}\left(\bigoplus_{n=2}^{\infty} \mathbb{Z}_n\right) = \bigoplus_{n=2}^{\infty} \mathbb{Z}_n$; amak ne obstaja element, ki bi uničil vse

Dokaži da je $\mathrm{tor}(M) \leq M$ podmodul in

$\varphi : M \to N$

$\varphi_*(\mathrm{tor}(M)) \leq \mathrm{tor}(N)$

a) $xm = 0 \quad yn = 0 \qquad m, n \in M \quad x, y \in K$

$\underbrace{xy}_{\neq 0}(m+n) = xym + x\underbrace{yn}_{0} = yxm = 0$

$\alpha \in K \quad xm = 0$

$x\alpha m = \alpha x m = 0$

b) φ homomorfizem

$x\varphi(m) = \varphi(xm) = 0 \rightarrow m \in \mathrm{tor}(M) \Rightarrow \varphi(m) \in \mathrm{tor}(N)$

$\Rightarrow \varphi_*(\mathrm{tor}(M)) \leq \mathrm{tor}(N)$

je podmodul: $xy(\alpha\varphi(m) + \beta\varphi(n)) =$

$\alpha y \underbrace{\varphi(xm)}_{0} + \beta x \underbrace{\varphi(n)}_{0} = 0$

$\mathrm{tor}\left(M/\mathrm{tor}(M)\right) = 0$ DN

$$x(m + \mathrm{tor}M) = \underbrace{xm}_{} + \mathrm{tor}M$$

$= 0 \Rightarrow m \in \mathrm{tor}M \rightarrow m + \mathrm{tor}M = 0$

$\neq 0 \Rightarrow m \notin \mathrm{tor}M$

$$\text{3. } M \text{ je prost} \overset{K \text{ cel}}{\Rightarrow} tor(M)=0$$

$$\varphi : M \xrightarrow{\cong} \bigoplus_{i=I} K$$

$$\varphi(tor M) \leq tor(\bigoplus_{i=I} K)$$

φ inj $\Rightarrow$ dovolj je dokazat $tor(\bigoplus_{i=I} K)=0$

(Dovolj je inj vložitev, ne izomorfizem)

$$\bigoplus_{i\in I} K = \{(x_i)_{i\in I} \; ; x_i \in K \quad x_i = 0 \text{ za vse razen končno mnogo}\}$$

$$(x_1, x_2, \ldots \ldots x_i, \ldots)$$

$$(x_i)_{i\in I} \in tor(\bigoplus K)$$

ne velja za noben element različen od 0

$$y(x_i)_{i\in I} = (yx_i)_{i\in I} \Leftrightarrow \overset{0}{\overset{\#}{y}} x_i = 0 \; \forall i$$

$$\Rightarrow x_i = 0 \; \forall i$$

4) Ali je $\mathbb{Z}_n$ prost $\mathbb{Z}$-modul?

NE, ker ima torzijo

> Izrek: M končno generiran $\mathbb{Z}$-modul.
> M prost $\Leftrightarrow$ M torzijska prost

5) Pokaži

${}_{\mathbb{Z}}\mathbb{Q}$ ni prost $\mathbb{Z}$-modul

$\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$

$(cb)\frac{a}{b} - (ad)\frac{c}{d} = 0$ netrivialna linearna kombinacija

Ali je lahko baza $\Rightarrow$

$\mathbb{Q} = (\frac{a}{b})$ $\quad \frac{1}{b^2}$ ni oblike $\alpha \frac{a}{b}$

Ali je $(\mathbb{Q}^*, \cdot)$ prost $\mathbb{Z}$ modul

$-1 \in \mathbb{Q}^*$ $\quad (-1)(-1) = 1 \Rightarrow (-1) \in T(\mathbb{Q}^*)$

$\Rightarrow$ ima torzijo, torej ni prost

kaj pa $(\mathbb{Q}_+^*, \cdot)$

$\sum \left(\frac{a_i}{b_i}\right)^{n_i} > 0 \neq 0$

Eksaktna zaporedja

kratka ≡ kvocienti

$$0 \xrightarrow{0} L \xrightarrow{\varphi} M \xrightarrow{\psi} N \xrightarrow{0} 0$$

$\operatorname{im}\varphi = \ker\psi \quad \operatorname{im}\psi = \ker 0 = N$

$0 = \operatorname{im} 0 = \ker\varphi$

↖ ψ surjektivna

↖ φ injektivna

$$M/\varphi(L) \cong N$$

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0$$

$x \longmapsto 2x \qquad x \longmapsto x \bmod 2$

$-2x$

inj

↖ edina možna preslikava

$\ker\psi = 2\mathbb{Z} = \operatorname{im}\varphi$

↙ enotska krožnica

$$0 \xrightarrow{\text{inj}\checkmark} \mathbb{Z} \longrightarrow \mathbb{R} \longrightarrow \mathbb{T} \xrightarrow{\text{surj}\checkmark} 0$$

$n \longmapsto \boxed{\begin{matrix} n \\ x \end{matrix}} \begin{matrix} \longmapsto 1 \\ \longmapsto e^{2\pi i x} \end{matrix}$