CAYLEYEV IZREK ZA KOLOBARJE

Opomba: V grupah:

G grupa

$l_a : x \mapsto ax$

$\varphi : G \to Sym(G)$
$a \mapsto l_a$

M aditivna grupa

$End(M)$ = množica vseh endomorfizmov M

$End(M)$ je kolobar, če vpeljemo seštevanje po točkah in množenje kot komponiranje:

$(\varphi + \psi)(u) = \varphi(u) + \psi(u)$
$(\varphi \psi)(u) = \varphi(\psi(u))$

Izrek: Vsak kolobar lahko vložimo v kolobar endomorfizmov neke aditivne grupe.

Dokaz: K kolobar

$a \in K$

$$l_a : K \to K$$
$$x \mapsto ax$$

$$l_a(x+y) \overset{\text{dist.}}{=} l_a(x) + l_a(y)$$

$$\Rightarrow l_a \in End(K)$$

$$\varphi : K \to End(K)$$
$$a \mapsto l_a$$

$$\varphi(a+b) = l_{a+b} \overset{\text{dist.}}{=} l_a + l_b = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = l_{ab} \overset{\text{asoc.}}{=} l_a \circ l_b = \varphi(a)\varphi(b)$$

$$\varphi(1) = 1 = id_K$$

$$\Rightarrow \varphi \text{ homomorfizem}$$

$$a \in \ker\varphi \Leftrightarrow l_a = 0 \Leftrightarrow ax = 0 \ \forall x \Leftrightarrow a = 0 \quad (x=1)$$

$$\Rightarrow \varphi \text{ injektiven}$$

A algebra nad F

V vektorski prostor nad F

$End_F(V)$ = algebra vseh endomorfizmov V

Na podoben način dokažemo:

Izrek: Vsako algebro nad F lahko vložimo v algebro endomorfizmov nekega vektorskega prostora nad F.

$\dim A = n < \infty$:

$$A \to End_F(A) \cong M_n(F)$$

Posledica: Vsako končnorazsežno algebro A nad F lahko vložimo v algebro $n \times n$ matrik nad F za nek n.

Primer: Naj bo A konč. raz. alg. nad F. Ali A lahko vsebuje taka elementa s, t, da je $st - ts = 1$.

Lahko gledamo, ali obstajata taki matriki S, T, da velja $ST - TS = I$.

$$\begin{array}{ccc} sl(ST-TS) & = & sl(I) \\ \| & & \| \\ 0 & & n \end{array}$$

Če je $\operatorname{char} F = 0$, je to protislovje.

DEFINICIJA MODULA

Definicija: Naj bo K kolobar. Množica M, skupaj z zunanjo binarno operacijo $(a, u) \mapsto au$ na $K \times M$ v M in notranjo binarno operacijo $(u, v) \mapsto u + v$ na $M \times M$ v M je modul nad K (ali K-modul), če velja:

1) $(M, +)$ je Abelova grupa

2) $(a+b)u = au + bu \quad \forall a, b \in K \quad \forall u \in M$

3) $a(u+v) = au + av \quad \forall a \in K \quad \forall u, v \in M$

4) $(ab)u = a(bu)$ $\quad \forall a,b \in K \ \forall u \in M$

5) $1 \cdot u = u$ $\quad \forall u \in M$

Operaciji $(a,u) \mapsto au$ pravimo množenje s skalarji ali modulsko množenje.

Opomba: Če je K polje, je to vektorski prostor.

Opomba: Pojem K-modula M je ekvivalenten pojmu homomorfizma kolobarjev $K \to End(M)$.

Naj bo M K-modul. Definirajmo $\varphi : K \to End(M)$ s predpisom $\varphi(a)(u) := au$. To je homomorfizem.

Obratno, če je $\varphi : K \to End(M)$ homomorfizem, postane M K-modul, če definiramo $au := \varphi(a)(u)$.

Opomba: Definirali smo levi K-modul.

Desni K-modul definiramo podobno, le namesto $(a,u) \mapsto au$ uporabljamo $(u,a) \mapsto ua$ in ustrezno prilagodimo pogoje:

$u(a+b) = ua + ub$
$(u+v)a = ua + va$
$u(ab) = (ua)b$
$u \cdot 1 = u$

M levi K-modul, K komutativen

$ua := au$

$\Rightarrow$ M desni K-modul

Odslej: modul = levi modul

Primer: Če je $K = F$ polje, je F-modul vektorski prostor nad F.

Primer: Vsaka aditivna grupa M je $\mathbb{Z}$-modul, če definiramo:

$$mu = \underbrace{u + \dots + u}_{n}$$

$$(-n)u = n(-u)$$

$$0u = 0$$

Primer: Vsak kolobar K postane modul nad samim seboj, če definiramo au kot običajni produkt a in u v K.

Primer: Naj bo I levi ideal K. I je K-modul, če ima au, $a \in K$, $u \in I$, običajen pomen.

Primer: Naj bo K podkolobar K'. Če au, $a \in K$, $u \in K'$, označuje množenje v K', je K' K-modul.

Primer: $K = M_n(F)$
$M = F^n$

Au = običajno množenje matrike z vektorjem

Primer: Trivialni ali ničelni modul: $\{0\}$

OSNOVNI POJMI TEORIJE MODULOV

PODMODULI

Definicija: Podmodul modula je podmnožica, ki je za isti operaciji sama modul:

Če je $N \subseteq M$, je N podmodul, če velja:

- N je podgrupa za $+$: $u, v \in N \Rightarrow u - v \in N$
- $KN \subseteq N$

Primer: V vektorski prostor nad F

podmodul = podprostor

Primer: $\mathbb{Z}$-modul (aditivna grupa)

podmodul = podgrupa

Primer: K-modul K

podmodul = levi ideal

Če sta N_1, N_2 podmodula, sta $N_1 \cap N_2$ in $N_1 + N_2 = \{u_1 + u_2 ; u_i \in N_i\}$ tudi podmodula.

$\{0\}$ in M sta vedno podmodula M. Če sta to tudi edina podmodula M in $M \neq \{0\}$, rečemo, da je M enostaven modul.

Primer: Vektorski prostor V enostaven kot modul $\Leftrightarrow \dim V = 1$

Primer: Aditivna grupa G enostavna kot $\mathbb{Z}$-modul $\Leftrightarrow G \cong \mathbb{Z}_p$

Primer: $K = M_n(F)$
$M = F^n$

$N \leq F^n$

$N \neq \{0\}$, $0 \neq u \in N$

$Au \in N \quad \forall A \in M_n(F)$

$\{Au;\ A \in M_n(F)\} = F^n$

$\Rightarrow M$ je enostaven $M_n(F)$-modul

HOMOMORFIZMI MODULOV

M, N K-modula

Definicija: $\varphi : M \to N$ je homomorfizem K-modulov, če velja:

- $\varphi(u+v) = \varphi(u) + \varphi(v) \quad \forall u, v \in M$
- $\varphi(au) = a\varphi(u) \quad \forall a \in K \ \forall u \in M$

Ekvivalentno: $\varphi(au + bv) = a\varphi(u) + b\varphi(v)$

Rečemo jim tudi K-linearne preslikave.

$\ker\varphi = \{u \in M;\ \varphi(u) = 0\} \leq M$
$\mathrm{Im}\varphi = \{\varphi(u);\ u \in M\} \leq N$

$\ker\varphi = \{0\} \Leftrightarrow \varphi$ injektivna

$M \cong N \Leftrightarrow$ Obstaja izomorfizem M in N

Primer: $K = F$:

Homomorfizmi so običajne linearne preslikave

Primer: $K = \mathbb{Z}$:

Homomorfizmi so aditivne preslikave, torej homomorfizmi aditivnih grup

Primer: I levi ideal K:

$u_0 \in I$

$\varphi : I \to I$
$u \mapsto u u_0$

φ endomorfizem K-modula I

KOLOBARJI ENDOMORFIZMOV

$End_K(M)$ = množica vseh endomorfizmov K-modula M

Postane kolobar, če vpeljemo:

$(\varphi + \psi)(u) = \varphi(u) + \psi(u)$
$(\varphi\psi)(u) = \varphi(\psi(u))$

Schurova lema:

Če je M enostaven K-modul, je kolobar $End_K(M)$ obseg.

Dokaz: $0 \neq \varphi \in End_K(M)$

$\ker\varphi$, $\mathrm{Im}\varphi$ podmodula

$\Rightarrow \ker\varphi = \{0\}$, $\mathrm{Im}\varphi = M$

$\Rightarrow \varphi$ bijekcija $\Rightarrow \varphi$ obrnljiv element $\mathrm{End}_K(M)$

KVOCIENTNI MODULI

M K-modul
N podmodul

$M/N := \{u+N \,;\, u \in M\}$

$(u+N)+(v+N) := (u+v)+N$
$a(u+N) := au+N$

~ Dobro definirano

$\Rightarrow M/N$ postane K-modul, kvocientni/faktorski modul

Primer: $K = F$:

Kvocientni vektorski prostori

Primer: $K = \mathbb{Z}$:

Kvocientna grupa

Primer: I levi ideal K:

$K/I := \{a+I \,;\, a \in K\}$

$$(a+I)+(b+I) = (a+b)+I$$
$$a(b+I) = ab+I$$

To pa ni isto kot običajno!

Izrek o izomorfizmu:

$$\varphi : M \to N$$

$$\Rightarrow M/\ker\varphi \cong \operatorname{Im}\varphi$$

DIREKTNE VSOTE MODULOV

$M_1, \dots, M_s$ K-moduli

Množica $M_1 \times \dots \times M_s$ postane K-modul, če definiramo:

$$(u_1, \dots, u_s) + (v_1, \dots, v_s) := (u_1 + v_1, \dots, u_s + v_s)$$
$$a(u_1, \dots, u_s) := (au_1, \dots, au_s)$$

Imenujemo ga direktna vsota modulov $M_1, \dots, M_s$.

Oznaka: $M_1 \oplus \dots \oplus M_s$

Natančneje, to je zunanja direktna vsota.

Naj bo zdaj M modul in $N_1, \dots, N_s$ njegovi podmoduli. Če velja:

i) $M = N_1 + \dots + N_s$

ii) $N_i \cap (N_1 + \dots + N_{i-1} + N_{i+1} + \dots + N_s) = \{0\} \quad \forall i$

potem M imenujemo notranja direktna vsota modulov $N_1, \dots, N_s$.

Ekvivalentno lahko (ii) predstavimo kot:

ii') $v_1 + v_2 + \dots + v_s = 0$, $v_i \in V_i \Rightarrow v_i = 0$

Če je M notranja direktna vsota $N_1, \dots, N_s$, je M izomorfen zunanji direktni vsoti $N_1, \dots, N_s$. Izomorfizem je podan s samoumevnim predpisom:

$$v_1 + \dots + v_s \mapsto (v_1, \dots, v_s)$$

Obe označujemo z $N_1 \oplus \dots \oplus N_s$.

Naj bo N podmodul M. Rečemo, da je N direktni sumand, če obstaja tak podmodul N', da je $M = N \oplus N'$.

Primer: $K = F$:

Vsi podprostori so direktni sumandi

Primer: $K = \mathbb{Z}$:

$M = \mathbb{Z}$

Podmoduli (podgrupe) so $n\mathbb{Z}$, $n \in \mathbb{N} \cup \{0\}$

Direktna sumanda sta le $\{0\}$ in $\mathbb{Z}$, sicer $n\mathbb{Z} \cap m\mathbb{Z} \neq \{0\}$

GENERATORJI MODULOV

M K-modul

$a \in M$

$Ku = \{au ; a \in K\}$ je podmodul M, ki vsebuje u, in je najmanjši podmodul, ki vsebuje u. Rečemo, da je Ku generiran z u.

Podmodul, generiran z enim elementom, se imenuje ciklični podmodul.

Primer: $K = F$:

1. razsežni podprostori in $\{0\}$

Primer: $K = \mathbb{Z}$:

Ciklični podmoduli so ciklične podgrupe

Primer: K komutativen kolobar:

Ciklični podmoduli K-modula K so glavni ideali

Primer: I levi ideal K:

$K/I = \{a+I ; a \in K\}$

$a+I = a(1+I)$

K/I je ciklični modul, generiran z $1+I$

Naj bo $X \subseteq M$. Podmodul, generiran z X, je množica vseh linearnih kombinacij $a_1u_1 + \ldots + a_mu_m$, $m \in \mathbb{N}$, $a_i \in K$, $u_i \in X$.

Če je podmodul, generiran z X, cel M, rečemo, da X generira M.

Rečemo, da je M končno generiran, če je generiran s kako končno množico:

$M = Ku_1 + \ldots + Ku_s$

PROSTI MODULI

Definicija: Podmnožica B K-modula M je **linearno neodvisna**, če za vse različne $e_1, \dots, e_s \in B$ in vse $a_1, \dots, a_s \in K$ iz $a_1e_1 + \dots + a_se_s = 0$ sledi $a_1 = \dots = a_s = 0$.

Če je B linearno neodvisna in generira M, je **baza** modula M.

Opomba: Če je B baza M, za vsak $u \in M$ obstajajo $e_1, \dots, e_s \in B$, da je $u = a_1e_1 + \dots + a_se_s$, kjer so $a_i \in K$ enolično določeni.

Pišemo: $u = \sum_i a_i e_i$ (končno mnogo a_i neničelnih)

Primer: $K = F$:

Vsi vektorski prostori imajo bazo

Primer: $K = \mathbb{Z}$, G končna Abelova grupa:

$u \in G$

$\{u\}$ ni linearno neodvisna, saj je $n \cdot u = 0$ $(n = |G|)$

Edina lin. neodvisna množica je prazna množica

$\Rightarrow$ Baze ni

Primer: $K = \mathbb{Z}$, $G = \mathbb{Z}$:

Bazi sta $\{1\}$, $\{-1\}$

Definicija: Modul, ki ima bazo, se imenuje **prosti moduli**.

Primer: Vsak vektorski prostor je prost.

Primer: Če je K kolobar, je $\overbrace{K \oplus \dots \oplus K}^{s \text{ krat}} = K^s$ prosti K-modul, npr. z bazo $\{(1,0\dots,0), \dots, (0,\dots,0,1)\}$.

Definicija: *Prosta abelova grupa* je abelova grupa, ki je kot $\mathbb{Z}$-modul prost.

Primer: $\mathbb{Z}^s = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$

Opomba: Če obstaja baza z n elementi, ni nujno res, da je tudi vsaka druga množica z n elementi baza.

Opomba: Podmodul prostega modula ni nujno prost:

Vsak kolobar K je prost kot K-modul (baza je $\{1\}$). Podmoduli so levi ideali, ki niso nujno prosti:

$K = \mathbb{Z}_4$ prost kot K-modul
$2K = \{0, 2\}$ pa nima nobene lin. neodvisne množice $(2 \cdot 2 = 0)$

Opomba: Lahko se zgodi, da je $K^s \cong K^t$ in $s \neq t$ (če K ni komutativen). Z drugimi besedami, baze imajo lahko različno kardinalnost.

Naj bo B množica in K kolobar. Ali obstaja kak prost modul nad K, ki ima bazo B?

$B = \{e_1, \dots, e_s\}$

Označimo množico vseh formalnih linearnih kombinacij $a_1 e_1 + \dots + a_n e_n$, $a_i \in K$, in vpeljemo seštevanje in množenje s skalarjem po "komponentah" e_i.

Če je B poljubna množica, vpeljemo formalne vsote $\sum a_s e_s$, kjer je le končno mnogo a_s neničelnih, in spet vpeljemo operaciji po komponentah:

$$\sum a_s e_s + \sum b_s e_s := \sum (a_s + b_s) e_s$$
$$a \sum a_s e_s := \sum a a_s e_s$$

Izrek: Za vsako množico B obstaja K-modul z bazo B.

Izrek: Naj bo M prosti K-modul z bazo B in N poljuben K-modul. Vsako funkcijo $f: B \to N$ lahko enolično razširimo do homomorfizma $\varphi: M \to N$.

Dokaz: $\varphi(\sum_{e \in B} a_e e) = \sum_{e \in B} a_e f(e)$

Opomba: To pove, da so prosti moduli prosti objekti v kategoriji K-modulov.

Posledica: Vsak modul je homomorfna slika prostega modula.

Dokaz: Vzemimo modul N. Naj bo $B \subseteq N$, ki generira N. Izrek pove, da obstaja prosti modul M z bazo B. Vzemimo preslikavo $f: B \to N$, $f(e) = e$. Po izreku obstaja $\varphi: M \to N$, $\varphi(e) = e$. Torej $\operatorname{Im} \varphi = N$.

$N \cong M/L$, $L = \ker \varphi$

Definicija: Modul nad obsegom D imenujemo vektorski prostor nad D.

Primer: $\mathbb{H}^s = \mathbb{H} \oplus \dots \oplus \mathbb{H}$ je vektorski prostor nad $\mathbb{H}$.

Zornova lema:

$S \neq \emptyset$, $\leq$ delna urejenost

Vsaka veriga V ima zgornjo mejo $\Rightarrow$ S ima maks. element

Izrek: Vsaka linearno neodvisna podmnožica vektorskega prostora V nad obsegom D je vsebovana v kakšni bazi.

Dokaz: T lin. neodv. podmn. V

$\mathcal{S}$:= množica vseh lin. neodv. podmn. V, ki vsebujejo T

$T \in \mathcal{S} \Rightarrow \mathcal{S} \neq \emptyset$

$\mathcal{S}$ delno uredimo z inkluzijo

$\mathcal{V}$ veriga v $\mathcal{S}$

$Z := \bigcup_{A \in \mathcal{V}} A$

$Z \in \mathcal{S} \Leftrightarrow Z$ lin. neodvisna in vsebuje T

Očitno $T \in Z$

Naj bodo $z_1, \dots, z_n \in Z$

$z_1 \in A_1, A_1 \in \mathcal{V}$

$\vdots$

$z_n \in A_n, A_n \in \mathcal{V}$

$A_1 \subseteq A_2$ ali $A_2 \subseteq A_1$

Npr: $A_1 \supseteq A_i$

$z_1, \dots, z_n \in A_1$ lin neodvisna

$\Rightarrow Z_i$ lin. neodvisni

$\Rightarrow Z$ zgornja meja V

Zornova lema $\Rightarrow \mathcal{Y}$ ima maks. element B

B je lin. neodvisna in $T \subseteq B$

Vzemimo $v \in V$

$v \in B \Rightarrow v = 1 \cdot v \Rightarrow v$ lin. kombo. elem. iz B

Torej $v \notin B$

Zaradi maksimalnosti $B \cup \{v\} \notin \mathcal{Y}$, torej $B \cup \{v\}$ ni lin. neodv.

$\Rightarrow$ Vsebuje neko končno lin. odv. množico $\{b_1, \dots, b_m, v\}$, $b_i \in B$

$\Rightarrow a_1 b_1 + \dots + a_m b_m + a_0 v = 0$ za neke $a_i \in D$, ne vse 0

Očitno $a_0 \neq 0$, ker so b_i neodvisni

$\Rightarrow v = -a_0^{-1} a_1 b_1 - \dots - a_0^{-1} a_m b_m$

($a_0^{-1} \in K$, $a_0^{-1} \in D$)

Posledica: Vsak vektorski prostor ima bazo.

Dokaz: $T \neq \emptyset$

EKSAKTNA ZAPOREDJA

Definicija: Naj bodo $M_0, M_1, \dots, M_s$ moduli. Zaporedje homomorfizmov

$$M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_s} M_s$$

je **eksaktno**, če je $\operatorname{Im}\varphi_i = \operatorname{Ker}\varphi_{i+1}$ za $i = 0, 1, \dots, s-1$.

Primer: $0 \to L \xrightarrow{\varphi} M$ je eksaktno, kadar je φ injektiven.

Primer: $M \xrightarrow{\psi} N \to 0$ je eksaktno, kadar je ψ surjektiven

Primer: $0 \to L \xrightarrow{\varphi} M \to 0$ je eksaktno, kadar je φ izomorfizem.

Primer: $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$

φ inj.
ψ surj.
$\operatorname{Im}\varphi = \operatorname{Ker}\varphi$

$\Rightarrow \psi\varphi = 0$

To je **kratko eksaktno zaporedje**.

Primer: Naj bo L podmodul M.

$$0 \to L \xrightarrow{\iota_L} M \xrightarrow{\pi} M/L \to 0$$

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

$L \cong \operatorname{Im}\varphi$
$N \cong M/\operatorname{Ker}\psi = M/\operatorname{Im}\varphi$

Primer: $0 \to L \xrightarrow{\iota_L} L \oplus N \xrightarrow{\pi_N} N \to 0$

$i_L(t) = (t,0)$
$\pi_N(t,v) = v$

Definicija: Kratko eksaktno zaporedje $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ imenujemo **razpadno kratko eksaktno zaporedje**, če obstaja tak izomorfizem $\sigma: M \to L \oplus N$, da naslednji diagram komutira:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \sigma} & & \downarrow & & \\ 0 & \longrightarrow & L & \longrightarrow & L \oplus N & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

Med drugim $M \cong L \oplus N$.

$N \subseteq M$ direktni sumand $\Leftrightarrow \exists L \subseteq M: M = L \oplus N$

$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ k.e.z. $\Leftrightarrow$ φ inj., ψ surj., $\operatorname{Im}\varphi = \operatorname{Ker}\psi$ ($\psi\varphi = 0$)

Primer: $0 \to L \to M \to M/L \to 0$

$L \cong \operatorname{Im}\varphi = \operatorname{Ker}\psi$

$N \cong M/\operatorname{Im}\varphi$

Primer: $0 \to L \to L \oplus N \to N \to 0$

$M \dots u$
$N \dots v$
$L \dots t$

$t \overset{i_L}{\mapsto} (t,0)$, $(t,v) \overset{\pi_N}{\mapsto} v$

Opomba: Razpadno k.e.z.:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \sigma & & \downarrow & & \\ 0 & \longrightarrow & L & \longrightarrow & L \oplus N & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

$\sigma\varphi = i_L$

$\pi_N \sigma = \psi$, $\pi_N = \psi\sigma^{-1}$

$M \cong L \oplus N$

$\sigma(\varphi(t)) = (t, 0)$

$\psi(\sigma^{-1}(t, v)) = v$

Izrek: Za k.e.z. $0 \to L \underset{\varphi'}{\overset{\varphi}{\rightleftarrows}} M \underset{\psi'}{\overset{\psi}{\rightleftarrows}} N \to 0$ so naslednji pogoji ekvivalentni:

i) Zaporedje je razpadno

ii) Obstaja homomorfizem $\varphi' : M \to L$, da je $\varphi'\varphi = id_L$

iii) Obstaja homomorfizem $\psi' : N \to M$, da je $\psi\psi' = id_N$

Dokaz: (ii) $\Rightarrow$ (i)

$\sigma(u) = (\varphi'(u), \psi(u))$

σ homomorfizem

σ injektiven

$u \in \ker\sigma \Rightarrow \varphi'(u) = 0,\ \psi(u) = 0$

$u \in \ker\psi = \operatorname{Im}\varphi \Rightarrow u = \varphi(t)$ za nek $t \in L$

$$\Rightarrow \varphi'(\varphi(t)) = 0 \Rightarrow u = 0$$
$$\| \quad t$$

σ surjektiven.

$(t,v) \in L \oplus N$

$\exists u \in M: (t,v) = \sigma(u) = (\varphi'(u), \psi(u))$

$\varphi'(u) = t, \quad \psi(u) = v$

$\sigma\varphi = i_2$

ψ surj. $\Rightarrow \exists u_0 \in M: \psi(u_0) = v$

$\psi(u_0 + \varphi(l)) = v \quad \forall l \in L$

Poiščimo l, da $\varphi'(u_0 + \varphi(l)) = t$.

$\varphi'(u_0) + l = t$

$l := t - \varphi'(u_0)$

$\sigma(\varphi(t)) = (\varphi'(\varphi(t)), \psi(\varphi(t))) = (t, 0)$

$\pi_N \sigma = \psi$

$\pi_N(\sigma(u)) = \pi_N(\varphi'(u), \psi(u)) = \psi(u)$

(iii) $\Rightarrow$ (i)

$\sigma' : L \oplus N \to M$
$(t,v) \mapsto \varphi(t) + \psi'(v)$

σ^{-1} homomorfizem

σ^{-1} injektiven

$(t,v) \in \ker \sigma^{-1} \Rightarrow \varphi(t) + \psi'(v) = 0$

$\Rightarrow \psi\varphi(t) + \psi\psi'(v) = 0 \Rightarrow v = 0$

($\psi\varphi(t) = 0$, $\psi\psi'(v) = v$)

$\Rightarrow \varphi(t) = 0 \overset{\varphi \text{ inj.}}{\Rightarrow} t = 0$

σ^{-1} surjektiven

$u \in M : u = \varphi(t) + \psi'(v)$

$\psi(u) = 0 + v \Rightarrow v = \psi(u)$

$u = \varphi(t) + \psi'(\psi(u))$

$\varphi(t) = u - \psi'(\psi(u))$

$u - \psi'(\psi(u)) \in \operatorname{Im}\varphi = \ker\psi$

$\psi(u - \psi'(\psi(u))) = \psi(u) - \psi(u) = 0$

$\sigma := \sigma^{-1-1}$

$\varphi(t) = \sigma(t,0)$

✓

$\psi(\sigma^{-1}(t,v)) = v$

$$\psi(\sigma^{-1}(t,v)) = \psi(\varphi(t)+\psi'(v)) = v$$

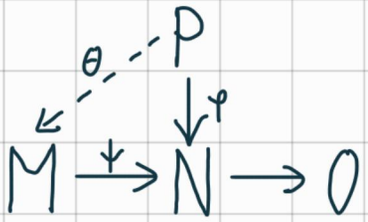
(i) $\Rightarrow$ (ii), (iii)

$\sigma: M \to L \oplus N$

$\varphi' := \pi_L \sigma$

$\psi' := \sigma^{-1} i_N$

PROJEKTIVNI MODULI



Definicija: Modul P je projektiven, če za vsak homomorfizem $\varphi: P \to N$ in vsak epimorfizem $\psi: M \to N$ obstaja tak homomorfizem $\theta: P \to M$, da je $\psi\theta = \varphi$.

Lema: Vsak prosti modul je projektiven.

Dokaz: Naj bo P prost.



P ima bazo B.

$e \in B: \quad \varphi(e) = \psi(u_e) \quad \forall u_e \in M$

$\theta(e) := u_e$

θ je z delovanjem na bazi enolično določen.

$\psi\theta = \varphi$

Izrek: Za modul P so naslednje trditve ekvivalentne:

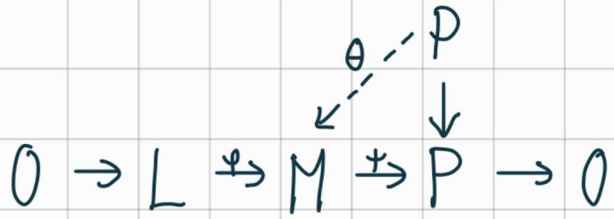
i) P je projektivni modul.

ii) Vsako kratko eksaktno zaporedje $0 \to L \overset{\varphi}{\to} M \overset{\psi}{\to} P \to 0$ razpade.

iii) Obstaja tak modul L, da je $L \oplus P$ prost.

Dokaz: (i) $\Rightarrow$ (ii)

P projektiven



$\psi\theta = id_P$

(ii) $\Rightarrow$ (iii)

Vsak modul, tudi P je homomorfna slika prostega modula M.

$0 \to L \xrightarrow{id_L} M \overset{\psi}{\to} P \to 0$

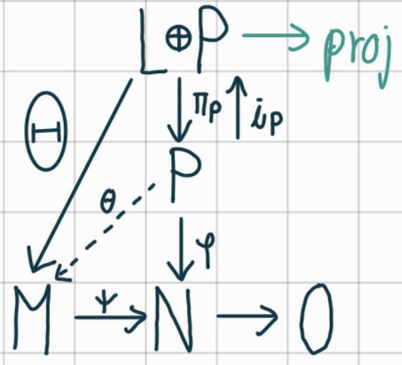
$L := \ker \psi$

Ker to k.e.z. razpade, je $M \cong L \oplus P$.

M je prost, torej je $L \oplus P$ tudi prost.

(iii) $\Rightarrow$ (i)

$L \oplus P$ je prost za neki L.



$\Theta := \Theta i_P$

$\psi \Theta = \varphi$

$$\psi\Theta = \psi \Theta i_P = \varphi \pi_P i_P = \varphi \, id_P = \varphi$$

Primer: K je prost K-modul.

Naj bo K komutativen in naj obstaja $e = e^2 \notin \{0,1\}$.

$P := eK = \{ex ; x \in K\}$ je podmodul (ideal).

$1-e \in K \Rightarrow (1-e) \cdot ex = 0$ (v P)

$\{ex\}$ nikoli ni lin. neodvisen.

Torej je P projektivni modul kot direktni sumand prostega, ki ni prost:

$$K = \underset{\| \; eK}{P} \oplus \underset{\| \; (1-e)K}{L}$$

Primer: K_1, K_2 komutativna kolobarja

$$K := K_1 \times K_2$$

$$e = (1,0)$$

$$K = \underset{\| \; P}{eK} \oplus (1-e)K$$

$$x = ex + (1-e)x$$

$$e \cdot / \; ex = (1-e)y \Rightarrow ex = 0$$

TENZORSKI PRODUKTI MODULOV

$M \otimes N$

M, N K-modula,
K komutativen

Vzemimo prosti modul, ki ima $M \times N$ za bazo.
Označimo ga $\mathcal{F} = \mathcal{F}_{M,N}$.

Naj bo $\mathcal{N} = \mathcal{N}_{M,N}$ njegov podmodul, generiran z elementi oblike

$(au + a'u', v) - a(u,v) - a'(u',v)$,
$(u, av + a'v') - a(u,v) - a'(u,v')$,

kjer $a, a' \in K$, $u, u' \in M$, $v, v' \in N$.

Definicija: Tenzorski produkt modulov M in N je modul $\mathcal{F}/\mathcal{N}$.

Oznaka: $M \otimes N \quad (= M \otimes_K N)$

Definicija: Preslikava $\phi : M \times N \to L$ je bilinearna, če je linearna v vsakem argumentu:

$$\phi(au + a'u', v) = a\phi(u, v) + a'\phi(u', v)$$
$$\phi(u, av + a'v') = a\phi(u, v) + a'\phi(u, v')$$

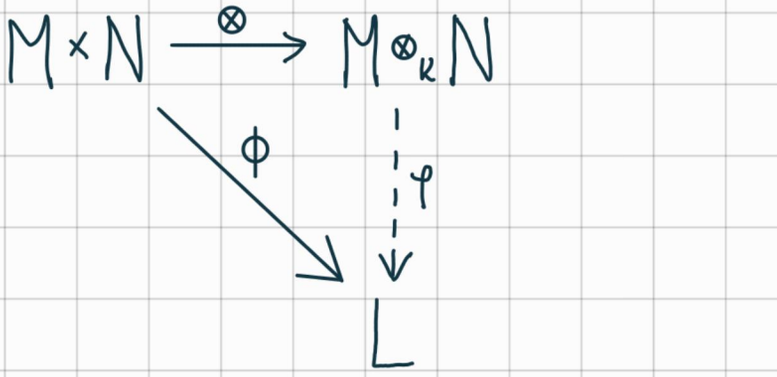
Primer: Skalarni produkt, vektorski produkt v $\mathbb{R}^3$, produkt v algebri, produkt matrik $M_{m,n}(F) \times M_{n,p}(F) \to M_{m,p}(F)$ ...

Izrek (univerzalna lastnost tenzorskega produkta):

Za vsaka modula M in N nad komutativnim kolobarjem K obstaja taka bilinearna preslikava $M \times N \to M \otimes_K N$, $(u, v) \mapsto u \otimes v$, za katero velja:

Za vsako bilinearno preslikavo $\phi : M \times N \to L$ obstaja natanko določena linearna preslikava $\varphi : M \otimes N \to L$, da velja $\varphi(u \otimes v) = \phi(u, v)$ za vse $u \in M$, $v \in N$.

S to lastnostjo je tenzorski produkt do izomorfizma natančno določen.



Dokaz: Vpeljimo $u \otimes v := (u, v) + \mathcal{N}$.

$(au+a'u', v) - a(u,v) - a'(u',v) \in W$

$\Leftrightarrow (au+a'u', v) + W = a((u,v)+W) + a'((u',v)+W)$

$\Leftrightarrow (au+a'u') \otimes v = a(u \otimes v) + a'(u' \otimes v)$

Podobno vpeljemo linearnost $\otimes$ v drugem argumentu.

$\phi: M \times N \to L$ bilinearna preslikava

$\mathcal{F}$ je prosti modul z bazo $M \times N$.

Zato lahko ϕ razširimo do linearne preslikave $F: \mathcal{F} \to L$.

$\Rightarrow F((u,v)) = \phi(u,v)$

Ker je ϕ bilinearna, $\ker F$ vsebuje W:

$F((au+a'u', v) - a(u,v) - a'(u',v)) = F(,) - aF(,) - a'F(,)$

$= \phi(au+a'u', v) - a\phi(u,v) - a'\phi(u',v) = 0$

Zato je $\varphi: M \otimes N \to L$, $x+W \mapsto F(x)$ dobro definirana:

$x+W = y+W \Rightarrow x-y \in W \Rightarrow F(x-y) = 0 \Rightarrow F(x) = F(y)$

F linearna $\Rightarrow \varphi$ linearna

$\varphi(u \otimes v) = \varphi((u,v)+W) = F((u,v)) = \phi(u,v)$

Vsak element v $\mathcal{F}$ je linearna kombinacija baznih elementov (u,v). Zato je vsak element v $M \otimes N$ $(= \mathcal{F}/V)$ enak linearni kombinaciji elementov $u \otimes v$.

Vsak element je oblike:

$$a_1(u_1 \otimes v_1) + \ldots + a_n(u_n \otimes v_n) =$$

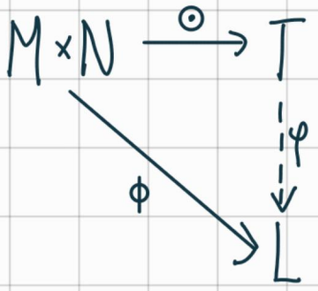
$$= (a_1 u_1 \otimes v_1) + \ldots + (a_n u_n \otimes v_n)$$

Vsak element v $M \otimes N$ je vsota $u \otimes v$.

Od tod jasno sledi enoličnost preslikave φ.

Dokažimo še enoličnost:

Naj bo T še en modul z enako lastnostjo:



Ker je $\odot$ bilinearna preslikava, obstaja linearna preslikava $\varphi : M \otimes N \to T$, da je $\varphi(u \otimes v) = u \odot v$.

Analogno obstaja linearna preslikava $\psi : T \to M \otimes N$, da je $\psi(u \odot v) = u \otimes v$.

$$(\psi\varphi)(u \otimes v) = u \otimes v \Rightarrow \psi\varphi = id_{M \otimes N}$$

$$(\varphi\psi)(u \odot v) = u \odot v \Rightarrow \varphi\psi = id_T$$

$$\Rightarrow M \otimes N \cong T$$

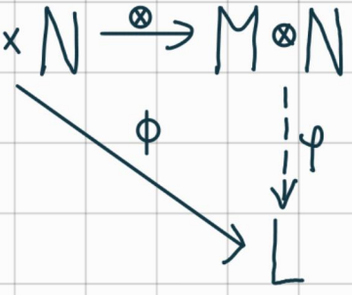
Opomba: „Praktična" definicija tenzorskega produkta:

i) Za vsaka $u \in M$ in $v \in N$ obstaja $u \otimes v \in M \otimes N$.
Pravimo mu enostavni tenzor.

Vsak element v $M \otimes N$ je vsota enostavnih tenzorjev.

ii) $(u+u') \otimes v = u \otimes v + u' \otimes v$
$u \otimes (v+v') = u \otimes v + u \otimes v'$
$(au) \otimes v = u \otimes (av) = a(u \otimes v)$

$(\Rightarrow 0 \otimes v = u \otimes 0 = 0)$

iii)


$\varphi(u \otimes v) := \phi(u, v)$

$\varphi(\sum u_i \otimes v_i) = \sum \phi(u_i, v_i)$

Sporočilo izreka je, da je ta preslikava dobro definirana.

Tenzorski produkt linearnih preslikav:

$\varphi : M \to M'$, $\psi : N \to N'$ linearna preslikava

$M \times N \longrightarrow M' \otimes N'$ je bilinearna.
$(u, v) \longmapsto \varphi(u) \otimes \psi(v)$

Zato obstaja linearna preslikava $\varphi \otimes \psi$ z lastnostjo:

$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$

Imenujemo jo tenzorski produkt linearnih preslikav φ in ψ.

$(\varphi_1 + \varphi_2) \otimes \psi = \varphi_1 \otimes \psi + \varphi_2 \otimes \psi$
$\varphi \otimes (\psi_1 + \psi_2) = \varphi \otimes \psi_1 + \varphi \otimes \psi_2$
$a\varphi \otimes \psi = \varphi \otimes a\psi = a(\varphi \otimes \psi)$
$(\varphi_1 \otimes \varphi_2)(\psi_1 \otimes \psi_2) = \varphi_1\psi_1 \otimes \varphi_2\psi_2$

φ, ψ izomorfizma $\Rightarrow \varphi \otimes \psi$ bijekcija in $(\varphi \otimes \psi)^{-1} = \varphi^{-1} \otimes \psi^{-1}$

Izrek: Naj bodo M, N, R moduli. Potem velja:

a) $M \otimes N \cong N \otimes M$

b) $(M \otimes N) \otimes R \cong M \otimes (N \otimes R)$

c) $(M \oplus N) \otimes R \cong (M \otimes R) \oplus (N \otimes R)$

d) $M \otimes K \cong M$

c') $R \otimes (M \oplus N) \cong (R \otimes M) \oplus (R \otimes N)$

d') $K \otimes M \cong M$

Dokaz: a) $M \times N \to N \otimes M$ je bilinearna.
$(u, v) \mapsto v \otimes u$

Zato obstaja linearna preslikava $u \otimes v \overset{\varphi}{\mapsto} v \otimes u$.

Analogno obstaja linearna preslikava $v \otimes u \overset{\psi}{\mapsto} u \otimes v$.

Preslikavi sta si očitno inverzni.

d) $u \otimes a \mapsto au$

$u \mapsto u \otimes 1$

b) Radi bi videli, da je $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$ dobro definirana linearna preslikava. Analogno definirana linearna preslikava $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$ bo njen inverz.

Fiksirano $w \in R$.

$(u, v) \mapsto u \otimes (v \otimes w)$ je bilinearna, zato obstaja linearna preslikava $u \otimes v \overset{\alpha}{\longmapsto} u \otimes (v \otimes w)$.

$\alpha(\sum u_i \otimes v_i) = \sum u_i \otimes (v_i \otimes w)$

Zato lahko definiramo linearno preslikavo
$\phi : (M \otimes N) \times R \to M \otimes (N \otimes R)$:

$\phi(\sum u_i \otimes v_i, w) = \sum u_i \otimes (v_i \otimes w)$

Nato spet uporabimo univerzalno lastnost.

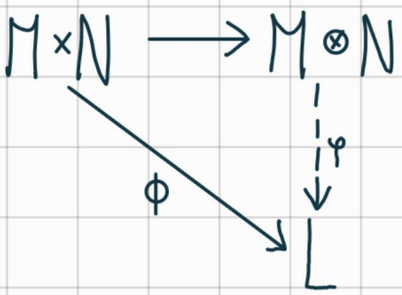
Povzetek: M, N K-modula

$M \otimes_K N = M \otimes N$

$\sum u_i \otimes v_i, \quad u_i \in M, \ v_i \in N$

$\otimes : (u, v) \mapsto u \otimes v$ bilinearna

$$(u_1 + u_2) \otimes v = u_1 \otimes v + u_2 \otimes v$$
$$u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2$$
$$a(u \otimes v) = (au) \otimes v = u \otimes (av)$$



$$\varphi(u \otimes v) = \phi(u, v)$$

$$M \otimes N \cong N \otimes M$$
$$(M \otimes N) \otimes R \cong M \otimes (N \otimes R)$$
$$M \otimes (N \oplus R) \cong M \otimes N \oplus M \otimes R$$
$$M \otimes K \cong M$$

$$M^{\otimes n} = \underbrace{M \otimes \dots \otimes M}_{n\text{-krat}}$$

TENZORSKI PRODUKTI PROSTIH MODULOV

Primer: $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathbb{Z}_2 = ?$

$$u \otimes v = (3u - 2u) \otimes v = -2u \otimes v = -u \otimes 2v = 0$$

$$\Rightarrow \mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathbb{Z}_2 = \{0\}$$

Izrek: Naj bo M prost K-modul z bazo $\{e_i \mid i \in I\}$ in N poljuben K-modul. Potem vsak element v $M \otimes N$ lahko enoličino zapišemo kot $\sum_i e_i \otimes v_i$, kjer je le končno mnogo $v_i \in N$ neničelnih.

Dokaz: Obstoj:

$u \in M, v \in N$

$$u \otimes v = \sum_i^K a_i e_i \otimes v = \sum_i e_i \otimes (a_i v)$$

Ker je vsak element iz $M \otimes N$ vsota enostavnih tenzorjev, je res vsak element oblike $\sum_i e_i \otimes v_i$.

Enoličnost:

$$\forall \sum e_i \otimes v_i = 0 \Rightarrow v_i = 0$$

Izberimo $i_0 \in I$.

Če uspemo najti tako linearno preslikavo $\varphi: M \otimes N \to N$, da bo $\varphi(e_i \otimes v_i) = 0$ za vse $i \neq i_0$ in $\varphi(e_i \otimes v_{i_0}) = v_{i_0}$, potem bo sledilo $0 = \varphi(0) = \varphi(\sum_i e_i \otimes v_i) = \sum_i \varphi(e_i \otimes v_i) = v_{i_0}$.

Izberimo lin. preslikavo $\varphi_0: M \to K$, $\varphi_0(e_i) = 0$, $i \neq i_0$ in $\varphi_0(e_{i_0}) = 1$ (obstaja, ker je $\{e_i\}$ baza).

$$\begin{aligned} \Phi: M \times N &\to N \\ (u, v) &\mapsto \varphi_0(u) v \end{aligned}$$

Φ je bilinearna, zato obstaja linearna $\varphi: M \otimes N \to N$:

$$\varphi(u \otimes v) = \Phi(u, v)$$

$$\varphi(e_i \otimes v_i) = \varphi_0(e_i) v_i = \begin{cases} v_{i_0} & ; i = i_0 \\ 0 & ; \text{sicer} \end{cases}$$

Opomba: Podobno velja, če je N prost z bazo $\{f_j\}$, so elementi $M \otimes N$ oblike $\sum_j u_j \otimes f_j$.

Izrek: Naj bo M prosti K-modul z bazo $\{e_i\}$ in N prosti K-modul z bazo $\{f_j\}$. Potem je $M \otimes N$ prosti K-modul z bazo $\{e_i \otimes f_j \; ; \; i \in I, j \in J\}$.

Dokaz: Vsak element v $M \otimes N$ je oblike:

$$\sum_i e_i \otimes v_i = \sum_i e_i \otimes \Big(\sum_j \overset{K}{a_{ij}} f_j\Big) = \sum_i \sum_j a_{ij} (e_i \otimes f_j)$$

Linearna neodvisnost:

$$0 = \sum_{i,j} a_{ij} (e_i \otimes f_j) = \sum_i e_i \otimes \Big(\sum_j a_{ij} f_j\Big)$$

$$\Rightarrow \sum_j a_{ij} f_j = 0 \quad \forall i$$

$$\overset{\{f_j\} \text{ bazni}}{\Rightarrow} a_{ij} = 0$$

Posledica: Če je U vektorski prostor nad F z bazo $\{e_i \; ; \; i \in I\}$ in V vektorski prostor nad F z bazo $\{f_j \; ; \; j \in J\}$, je $U \otimes V$ vektorski prostor nad F z bazo $\{e_i \otimes f_j \; ; \; i \in I, j \in J\}$.

Če sta U, V končnorazsežna, je $\dim_F (U \otimes V) = \dim_F U \cdot \dim_F V$.

Primer: V vektorski prostor nad F
$v \in V, \; f \in V^*$

$$v \otimes f : V \to V$$

$$(v \otimes f)(u) := f(u) v$$

Primer: $\sum u_i \otimes v_i = 0 \overset{u_i \text{ lin. neodv.}}{\Rightarrow} v_i = 0$

$$u_1 \otimes v_1 + \ldots + u_m \otimes v_m = u_1' \otimes v_1' + \ldots + u_n' \otimes v_n'$$

u_i lin. neodv. $\Rightarrow v_i \in \mathrm{Lin}\{v_1', \ldots, v_n'\}$

TENZORSKI PRODUKT ALGEBER

Algebra nad poljem F:

- vek. prost. nad F
- kolobar
- $a(xy) = (ax)y = x(ay) \quad \forall x,y \in A \quad \forall a \in F$

Splošneje: Algebra nad komutativnim kolobarjem K

- K-modul
- kolobar
- -||-

Primer: Vsak kolobar je algebra nad $\mathbb{Z}$.

Primer: Vsak kolobar je algebra nad $Z(K)$.

Primer: $K \subseteq C$ komutativen kolobar

$\Rightarrow C$ je K-algebra (množenje s skalarji je kar dano množenje)

Izrek: Naj bosta A in B K-algebri. Potem K-modul $A \otimes B$ postane K-algebra, če vpeljemo še množenje s predpisom:

$$(u \otimes v) \cdot (z \otimes w) = uz \otimes vw$$

Opomba: Prava definicija množenja je:

$$\left(\sum_i u_i \otimes v_j\right) \cdot \left(\sum_j z_j \otimes w_j\right) = \sum_{i,j} u_i z_j \otimes v_i w_j$$

Dokaz: Problem je dobra definiranost množenja.

$\rho_z(x) = xz$ je K-linearna preslikava na vsaki algebri

$z \in A$, $w \in B$

$\rho_z \otimes \rho_w : A \otimes B \to A \otimes B$

$\phi : A \times B \to End(A \otimes B)$
$(z, w) \mapsto \rho_z \otimes \rho_w$

ϕ bilinearna

$\Rightarrow \exists \varphi : A \otimes B \to End_K(A \otimes B)$ linearna
$(z \otimes w) \mapsto \rho_z \otimes \rho_w$

Definirano množenje na $A \otimes B$ s predpisom:

$r \cdot s = \varphi(s)(r)$

Posebej:

$(u \otimes v) \cdot (z \otimes w) = \varphi(z \otimes w)(u \otimes v) =$

$= (\rho_z \otimes \rho_w)(u \otimes v) = uz \otimes vw$

Produkt je torej tudi bilinearen:

$(ar + a'r')s = a(rs) + a'(r's)$
$r(\dots) = \dots$

Asociativnost sledi iz definicije.

Enota je $1 \otimes 1$.

Izrek: Za K-algebre A, B, C velja:

a) $A \otimes B \cong B \otimes A$
b) $A \otimes (B \otimes C) \cong (A \otimes B) \otimes C$
c) $(A \times B) \otimes C \cong (A \otimes C) \times (B \otimes C)$
d) $A \otimes K \cong A$

Dokaz: Enak kot za module.

Primer: $K[X]$ je kolobar in celo K-algebra:

$$a(a_0 + a_1 X + \ldots + a_n X^n) := aa_0 + aa_1 X + \ldots + aa_n X^n$$

A naj bo K-algebra.

$A[X]$ je spet K-algebra.

$A \otimes K[X] \cong A[X]$

$K[X]$ je prosti K-modul $\{1, X, X^2, \ldots\}$.

Elementi v $A \otimes K[X]$ so torej oblike:

$$\sum_{i \geq 0} a_i \otimes X^i$$

Preslikava $\sum a_i \otimes X^i \mapsto \sum a_i X^i$ je izomorfizem.

Primer: Naj bo A poljubna K-algebra.

Kolobar $M_n(K)$ je K-algebra, če definirano:

$$a\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = \begin{bmatrix} aa_{11} & \cdots & aa_{1n} \\ \vdots & & \vdots \\ aa_{n1} & \cdots & aa_{nn} \end{bmatrix}$$

Zato lahko definiramo $M_n(K) \otimes A \cong M_n(A)$.

Pokažimo, da je vsak element v tenzorskem produktu $M_n(K) \otimes A$ oblike $\sum_{i,j=1}^{n} E_{ij} \otimes a_{ij}$ za enolične $a_{ij} \in A$.

Vpeljimo $\varphi : M_n(K) \otimes A \to M_n(A)$:

$$\varphi\left(\sum_{i,j} E_{ij} \otimes a_{ij}\right) := \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

$$\varphi(E_{ij} \otimes a) = a E_{ij}$$

$$\varphi(E_{ij} \otimes a \cdot E_{kl} \otimes v) = \varphi(\delta_{jk} E_{il} \otimes av) = \delta_{jk}\, av\, E_{il}$$

$$\varphi(\cdots)\varphi(\cdots) = a E_{ij} \cdot v E_{kl} = \delta_{jk}\, av\, E_{il} \quad //$$

Konkreten primer:

$$M_m(K) \otimes M_n(K) \cong M_m(M_n(K)) \cong M_{mn}(K)$$

Ta izomorfizem element $S \in M_m(K)$, $T \in M_n(K)$ preslika:

$$S \otimes T = \sum_i \sum_j s_{ij} E_{ij} \otimes T = \sum_i \sum_j E_{ij} \otimes s_{ij} T$$

$$\longmapsto \begin{bmatrix} s_{11}T & \cdots & s_{1m}T \\ \vdots & & \vdots \\ s_{m1}T & \cdots & s_{mm}T \end{bmatrix} =: S \otimes T$$

RAZŠIRITEV SKALARJEV

Naj bo A realna končno-dimenzionalna algebra.

Naj bo $\{e_1, \dots, e_n\}$ njena baza.

$$e_i e_j = \sum_k \alpha_{ijk} e_k, \quad \alpha_{ijk} \in \mathbb{R} \qquad (*)$$

$A_{\mathbb{C}}$ naj bo kompleksen prostor z bazo $\{e_1, \dots, e_n\}$, množenje pa naj bo določeno z isto formulo $(*)$.

Primer: $M_n(\mathbb{R})_{\mathbb{C}} \cong M_n(\mathbb{C})$

Primer: $\mathbb{H}_{\mathbb{C}} \cong M_2(\mathbb{C})$

$$\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k, \quad \lambda_i \in \mathbb{C}$$

$$(1 - i\underline{i})(1 + i\underline{i}) = 1 - i^2 \underline{i}^2 = 0$$

Nimamo pa več obzega, ker imamo delitelje niča ...

K, C komutativna kolobarja

$\alpha : K \to C$ homomorfizem

M K-modul

C postane K-modul, če definiramo:

$$kc := \alpha(k)c$$

$$(k_1 k_2)c = \alpha(k_1 k_2)c = \alpha(k_1)\alpha(k_2)c = \alpha(k_1) \cdot k_2 c = k_1(k_2 c)$$

Zato lahko definiramo K-modul:

$M_C := C \otimes M$

Opomba: M_C je odvisen od α!

Ta K-modul postane C-modul, če definiramo:

$c(d \otimes u) = cd \otimes u$

To je dobro definirano:

$$\ell_c : C \to C$$
$$d \mapsto cd$$

ℓ_c je K-linearna.

Naso definicijo lahko zapišemo takole:

$c \cdot y = (\ell_c \otimes id_M)(y) \quad \forall c \in C \quad \forall y \in M_C$

$c \otimes u = c(1 \otimes u)$

Modul M_C sestoji iz lin. kombinacij elementov $1 \otimes u$, $u \in M$.

M_C dobimo iz M z razširitvijo skalarjev (s K na C).

Primer: $\alpha : K \to C$, $\alpha(k) = k$, $K \leq C$

$M_C = C \otimes M$

Elementi so C-linearne kombinacije $1 \otimes u$, $u \in M$

Naj bo A K-algebra.

A_C je C-modul.

$C \otimes A$ je tudi K-algebra, saj sta C in A K-algebri.

Torej je A_C tudi C-algebra, če definiramo $c(d \otimes a) = cd \otimes a$.

Elementi so C-linearne kombinacije $1 \otimes e_j$, kjer so e_i elementi baze za A.

Baza za A_C je $\{1 \otimes e_i \,;\, i \in I\}$.

Če je množenje v K-algebri A določeno z $e_i e_j = \sum_k \alpha_{ijk} e_k$, je množenje v C-algebri A_C določeno z $(1 \otimes e_i)(1 \otimes e_j) = \sum \alpha_{ijk} (1 \otimes e_k)$.

Primer: K komutativen kolobar
I maksimalen ideal v K

$\Rightarrow K/I = C$ polje

$\alpha : K \to C$
$k \mapsto k + I$

Tako iz K-modula M dobimo vektorski prostor M_C nad C.

Izrek: Naj bo K komutativen kolobar. Potem iz $K^s \cong K^t$ sledi $s = t$.

Dokaz: Naj bo C polje iz primera.

Za $n \in \mathbb{N}$ definiramo $(K^n)_C$, ki je tudi vektorski prostor nad C z bazo $1 \otimes e_1, \ldots, 1 \otimes e_n$, če je $\{e_1, \ldots, e_n\}$ baza za K^n. Torej je $\dim_C (K)_C = n$.

$\Phi : K^s \to K^t$ izomorfizem K-modulov

$id_C \otimes \phi : (K^s)_C \to (K^t)_C$ K-linearna

Očitno je tudi C-linearna in bijektivna.

Ker sta to vektorska prostora, je $s = t$.

KONČNO GENERIRANE ABELOVE GRUPE

K cel kolobar
M K-modul

Definiramo: $tor(M) := \{u \in M ; \exists a \in K \setminus \{0\} : au = 0\}$

$tor(u)$ je podmodul

$u, v \in tor(M)$

$a \neq 0, au = 0$
$b \neq 0, bv = 0$

$\Rightarrow ab(u-v) = 0$

$\Rightarrow u - v \in tor(M)$

$k \in K$

$\Rightarrow a(ku) = k(au) = 0$

$\Rightarrow ku \in tor(M)$

M je torzijsko prost, če je $tor(M) = \{0\}$

$M/\mathrm{tor}(M)$ je torzijsko prost

$u + \mathrm{tor}(M) \in M/\mathrm{tor}(M)$
$a \in K \setminus \{0\}: a(u + \mathrm{tor}(M)) = 0$

$\Rightarrow au + \mathrm{tor}(M) = 0$

$\Rightarrow au \in \mathrm{tor}(M)$

$\Rightarrow \exists b \in K \setminus \{0\}: b(au) = 0$

$\Rightarrow (ba)u = 0$
$\neq 0$

$\Rightarrow u \in \mathrm{tor}(M)$

$\Rightarrow u + \mathrm{tor}(M) = 0$

Poseben primer: $K = \mathbb{Z}$

$\mathrm{tor}(G)$ = torzijska podgrupa Abelove grupe G

$G/\mathrm{tor}(G)$ torzijsko prosta (vsi neničelni elementi imajo neskončen red)

Končna $\Rightarrow$ Končno generirana

$|G| < \infty \Rightarrow G \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_r}, \quad n_i = p_i^{l_i}$

$\mathbb{Z} \oplus K \cong \mathbb{Z}^s \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \dots \oplus \mathbb{Z}_{p_m^{e_m}}$ končno gen. Ab. grupa

G Abelova grupa

$\mathrm{tor}(G) = \{g \in G;\ g \text{ ima končen red}\}$

G je **torzijsko prosta**, če je $\text{tor}(G) = \{0\}$

Lema: Končno generirana torzijsko prosta Abelova grupa je prosta.

Dokaz: Naj bo H končno gen. tor. prosta Abelova grupa. Denimo, da ni prosta.

Naj bo $m \in \mathbb{N}$ tak, da je H generirana z m elementi, ne pa manj.

Izmed vseh množic z m elementi, ki generirajo H, izberimo najmanjšo v naslednjem smislu:

$\{a_1, \dots, a_m\}$ generira H
$\exists k_1, \dots, k_m \in \mathbb{Z}: \sum_{i=1}^{m} k_i a_i = 0$, $\sum_{i=1}^{m} |k_i|$ minimalna
($\{b_1, \dots, b_m\}$ tudi generira H, $\sum_{i=1}^{m} l_i b_i = 0 \Rightarrow \sum |k_i| \leq \sum |l_i|$)

Ker je H tor. prosta, sta vsaj dva k_i različna od 0.

Naj bosta to k_1, k_2.

BSS: $|k_1| \geq |k_2| > 0$

$k_1 = q k_2 + r, \quad 0 < r < |k_2|$

$0 \leq |k_1 - q k_2| < |k_2|$

$0 = k_1 a_1 + k_2 a_2 + k_3 a_3 + \dots + k_m a_m$

$= (k_1 - q k_2) a_1 + k_2 (a_2 + q a_1) + k_3 a_3 + \dots + a_m k_m$

$|k_1 - q k_2| < |k_2| \leq |k_1|$

$\Rightarrow |k_1 - q k_2| + |k_2| + \dots + |k_m| < |k_1| + |k_2| + \dots + |k_m|$

Ker tudi $\{a_1, a_2 + 2a_1, a_3, \dots, a_m\}$ generira H, je to protislovje.

Izrek: Naj bo G končno generirana Abelova grupa. Potem je njena torzijska podgrupa T končna in $G \cong \mathbb{Z}^s \oplus T$ za nek enolično določeni $s \geq 0$.

Dokaz: G obravnavamo kot $\mathbb{Z}$-modul.

G k. g. $\Rightarrow$ G/T k. g.

G/T torzijsko prosta $\Rightarrow$ G/T prosta

$\Rightarrow G/T \cong \mathbb{Z}^s$ za nek določen $s > 0$

G/T prosti $\mathbb{Z}$-modul $\Rightarrow$ G/T projektiven

$\Rightarrow 0 \to T \to G \to G/T \to 0$ razpade

$\Rightarrow G \cong T \oplus G/T \cong T \oplus \mathbb{Z}^s$

T končna

$T \cong T \oplus \mathbb{Z}^s / \{0\} \oplus \mathbb{Z}^s$

$T \oplus \mathbb{Z}^s$ končno generirana

$\Rightarrow$ T končno generirana

Naj bo $\{t_1, \dots, t_r\}$ množica generatorjev T.

Vsi elementi T so tvoje oblike $m_1 t_1 + \dots + m_r t_r$, $m_i \in \mathbb{Z}$.

Vsak t_i ima končen red, zato je takih različnih zapisov le končno mnogo, torej je elementov tudi končno mnogo.

Posledica: Vsaka končno generirana Abelova grupa je izomorfna grupi $\mathbb{Z}^s \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{k_r}}$.