PRIRODNO-MATEMATIČKI FAKULTET
UNIVERZITETA U BEOGRADU

Gojko Kalajdžić

O PRSTENIMA HERMITSKOG TIPA I MODULIMA NAD NJIMA

(DOKTORSKA DISERTACIJA)

BEOGRAD, 1982.

SADRŽAJ

PREDGOVOR

Mnogi problemi u *LINEARNOJ ALGEBRI* (kao i matematici uopšte) su u uskoj vezi sa problemom *svodjenja* matrica nad odredjenim prstenom A na matrice nekog posebnog tipa. *KAPLANSKY* [*1*] definiše desni (odnosno levi) *HERMITSKI PRSTEN* kao svaki prsten A sa svojstvom da za svaku matricu M formata 1×2 (odnosno 2×1) postoji *inverzibilna* matrica $P\in M_2(A)$ takva da je matrica MP (odnosno PM) trougaona. Zahtevom da u toj definiciji umesto uslova "inverzibilnosti" matrica P zadovoljava neki drugi uslov (na primer, da je proizvod elementarnih matrica, i sl.), dobijamo neku drugu klasu prstena "hermitskog tipa". Tako, na primer, uz simboliku i terminologiju iz *IV* poglavlja, svaki (desni) euklidski, glavnoidealski, neterovski domen je hermitski (zdesna) u odnosu na hermitski niz $\mathcal{E}(A_n)$, $U(A_n)$, $R(A_n)$ respektivno. Osim *IV* poglavlja, u kome je reč o prstenima hermitskog tipa uopšte, preostala poglavlja se odnose na problematiku u vezi sa euklidskim prstenima i modulima.

U *I*, §*1* definiše se Σ-euklidska valuacija $\Phi: M\to W$ desnog A-modula M, koja se u slučaju da je $M=A$ komutativan prsten i $\Sigma=A^c$ podudara sa pojmom euklidske valuacije prstena A u smislu *SAMUEL* [*1*]. Pri tome je W bilo koji dobro uredjen skup. Ako *tip* dobro uredjenog skupa $\phi(M)$ nije veći od ω, za valuaciju ϕ kažemo da je *konačna*. Prema *V*, *T.1-3*, prsten $M_2(Z)$ je euklidski, ali prema *V*, *T.1-10* nema nijednu konačnu euklidsku valuaciju. Prsten $2Z$ nije euklidski (*II*, *Primer 1-1*), ali je to slučaj sa $2Z$ kao desnim Z-modulom. Drugi paragraf prvog poglavlja posvećen je euklidskim valuacijama prstena koje zadovoljavaju neke posebne uslove (*str. 14*). Pri tome se sva tvrdjenja odnose na *nekomutativne* prstene. Važne su *Teoreme 2-2* i *2-3* koje omogućuju "detaljniju" karakterizaciju prstena koji imaju bar jednu euklidsku valuaciju koja zadovoljava neke od uslova (M), (T), (N), (Z). Ako *konačna* euklidska valuacija ϕ domena A zadovoljava uslove (M) i (L), tada je uz simboliku *Teoreme 2-7* domen

A oblika $K[X,f,\delta]$ (*JACOBSON*[*1*], *COHN*[*1*]). *Teoremama 2-6, 2-7* i *2-8* taj problem je rešen u opštem slučaju (i kada valuacija ϕ nije konačna), i to pod pretpostavkom da ϕ zadovoljava samo uslov (*M*). Poslednjim dvema *Teoremama 2-9, 2-10* opisani su svi domeni koji imaju bar jednu konačnu euklidsku valuaciju koja zadovoljava uslov (*T*) i neki od uslova (*N*) i (*Z*). *Korolarom 2-2* data je jedna karakterizacija klase domena koji su ili tela, ili su izomorfni prstenu *Z*.

U drugom poglavlju, razvijajući jednu ideju iz *SAMUEL*[*1*], uvodi se pojam Σ-euklidskih razreda i Σ-euklidskog jezgra proizvoljnog (desnog) modula nad nekim prstenom. Na *Primerima 1-1* i *1-2* ilustrovan je i jedan postupak za ispitivanje (leve, desne) euklidnosti nekog prstena, kao i za odredjivanje njegove minimalne euklidske valuacije (u slučaju da je euklidski). *Primer 1-2* pokazuje da postoji desni euklidski prsten koji nije euklidski (pa čak ni glavnoidealski) sleva. *Teoremom 1-09* data je zavisnost $(G\times H)$-euklidskih razreda konačnog stepena proizvoda *M* desnih modula *U* i *V* u funkciji od *G*-euklidskih i *H*-euklidskih razreda samih modula *U* i *V*. Prema *Korolaru 1-2* klasa euklidskih modula je "zatvorena u odnosu na proizvod", a prema *Korolaru 1-3* euklidski modul ne mora da ima i konačnu euklidsku valuaciju. Preostalim tvrdjenjima date su neke osobine vezane za euklidske razrede i jezgro nekog modula *M* i njegove podmodule. Tako, na primer, ako je *L* desni, ali ne i levi ideal desnog euklidskog prstena *A* (*V*, *Primer 1-2*), tada je prema *Teoremi 1-7* desni *A*-modul A/L euklidski, dok se o količničkom prstenu A/L čak ne može ni govoriti (jer ideal *L* nije obostran).

Prvi paragraf trećeg poglavlja posvećen je problemu "euklidnosti" lokalizacije A_S prstena *A* na nekom njegovom denominatoru *SCA*. *Teoremom 1-1* dat je uzajamni odnos izmedju euklidskih razreda prstena A_S i *A*, dok se *Teoremom 1-3* daju neki dovoljni uslovi pod kojima je prsten A_S euklidski zdesna. *Teorema 1-4* je uopštenje jednog rezultata iz *SAMUEL* [*1*] (koji se dobije iz *Teoreme 1-4* u slučaju da je prsten *B* komutativan i $f=1_B$, $\delta=0$). *Teorema 1-5* predstavlja uopštenje "stava o razlaganju racionalnih funkcija nad prstenom $A=K[X]$" na slučaj bilo kog (desnog) euklidskog prstena *A*. Drugi paragraf je posvećen problematici u vezi sa "euklidnošću" direktnog proizvoda i sume euklidskih prstena, i uopšte projektivnog i induktivnog limesa "odgovarajuće familije" u kategoriji *EUC* (*I*, *Def. 1-4*) euklidskih parova. Glavni rezultati su dati *Teoremama 2-1, 2-2, 2-3* i *2-5*.

U *IV* poglavlju uvodi se pojam *hermitskog niza* nad datim prstenom *A* (*Definicija 1-1*), a zatim i pojam (desnog, levog) *hermitskog prstena* u odnosu na neki hermitski niz (*Definicija 1-3*). *Teoreme 1-1, 1-2, 1-9* su uopštenja odgovarajućih tvrdjenja iz *KAPLANSKY* [*1*]. Ostali važniji rezultati su dati *Lemom 1-4* i *Teoremama 1-3, 1-4* i *1-8*.

Najzad, *V* poglavlje je posvećeno matricama sa elementima iz nekog euklidskog prstena, tačnije prstenima $M_n(A)$ kvadratnih matrica reda n nad datim euklidskim prstenom A. Uz terminologiju iz *I*, *Definicija 1-1*, u *SANOV*[*1*] je dokazano da ako *komutativan* domen A ima *konačnu* euklidsku valuaciju ϕ koja zadovoljava uslov (*N*), prsten $M_n(A)$ je Γ-euklidski i sleva i zdesna. U slučaju da je prsten $A=K$ polje, taj rezultat postaje trivijalnim, jer je tada u prstenu $M_n(K)$ svaki regularan element nužno jednota. U *Teoremi 1-3* je (i pod slabijim pretpostavkama za valuaciju ϕ) prvo dokazano da je prsten $M_n(A)$ euklidski, a u *Teoremi 1-4* da je i Γ-euklidski. Slično tvrdjenje važi ako je prsten A nekomutativan i prost ili valuacioni (*Teoreme 1-5* i *1-6*). Prema *Teoremi 1-7* to važi za svaki komutativan prsten koji ima euklidsku valuaciju koja zadovoljava uslov kancelacije (*Definicija 1-2*). Dalje, u *Teoremi 1-8* je dokazano da je prsten $M_n(A)$ Γ-euklidski i u slučaju nekomutativnog domena A sa bar jednom euklidskom valuacijom koja zadovoljava uslov (*N*) ili (*M*). Uz to je prsten $M_2(A)$ i euklidski (*Teorema 1-9*). Najzad, prema *Teoremi 1-10*, ako domen A nije telo, tada za $n>1$ prsten $M_n(A)$ ne može imati konačnu euklidsku valuaciju.

Ukoliko se ne kaže izričito drugačije, svi prsteni o kojima bude bilo reči imaće jedinicu *1* i bar dva člana. Za element a prstena A kažemo da je (leva, desna) *jednota* ako ima (desni, levi) *inverz*. Skupove svih (levih, desnih) jednota prstena A označavaćemo "redom" sa $U_l(A)$, $U_d(A)$ i $U(A)$. Slično, sa

(0) $$\Delta = R_d(A), \qquad \Lambda = R_l(A), \qquad \Gamma = R(A),$$

označavaćemo redom skupove svih (desnih, levih) *regularnih* elemenata a prstena A. Ako je G aditivni grupoid sa neutralom 0 i $\Sigma \subset G$, tada ćemo sa Σ^0 označavati *razliku* $\Sigma-\{0\}$, a sa Σ_0 *zbir* $\Sigma\cup\{0\}$. Kao i obično, sa $A[X]$ ćemo označavati prsten polinoma po X sa koeficijentima iz A, a sa $M_{mn}(A)$ ili A_{mn} skup svih matrica formata $m\times n$ nad prstenom A.

I

O EUKLIDSKIM VALUACIJAMA MODULA I PRSTENA

Uz raniji dogovor o simbolici, u ovom poglavlju, ukoliko ne kažemo drugačije, A će nam označavati proizvoljan prsten sa jedinicom u kome je $0 \neq 1$, Σ neprazan podskup od A^0, i W dobro uredjen skup. Pri tome je $\Sigma^0 = \Sigma - \{0\}$ i $\Sigma_0 = \Sigma \cup \{0\}$ za proizvoljan podskup Σ od A. Posebno će biti čest slučaj kada je Σ neki od skupova A^0, $\Delta = R_d(A)$, $\Lambda = R_l(A)$, $\Gamma = R(A)$.

1. EUKLIDSKA VALUACIJA PRSTENA. EUKLIDSKI PAR

DEFINICIJA 1-1

Ako je M desni modul nad prstenom A i $\Sigma \subset M^0$, tada pod Σ-EUKLIDSKOM VALUACIJOM modula M podrazumevamo svako preslikavanje $\phi: M \to W$ toga modula u bilo koji dobro uredjen skup W sa sledeća dva svojstva:

E0. *$\phi(0)$ je minimalni član skupa W;*

E1. *Za svako $a \in M$ i $b \in \Sigma$ postoje $q \in A$ i $r \in \Sigma_0$ takvi da je*

$$a = bq + r, \qquad \phi(r) < \phi(b). \tag{1}$$

Za Σ-euklidsku valuaciju ϕ desnog A-modula M kažemo da je PRIRODNA ako zadovoljava uslov

E2. $\phi(ma) \geqslant \phi(m)$ $\qquad (m \in M,\ a \in A,\ ma \in \Sigma)$.

Pod DESNOM (levom) Σ-EUKLIDSKOM VALUACIJOM prstena A podrazumevamo Σ-euklidsku valuaciju desnog (levog) A-modula A. Ako je ϕ i leva i desna (prirodna) Σ-euklidska valuacija prstena A, tada kažemo samo da je ϕ (prirodna) Σ-EUKLIDSKA valuacija toga prstena.

Neka je simbolika iz prethodne Definicije 1-1. Tada q i r zovemo *KOLIČNIKOM* i *OSTATKOM* pri ϕ-*deljenju* a sa b. Za valuaciju ϕ kažemo da je *KONAČNA* ako *ordinal* koji "odgovara" dobro uredjenom skupu $\phi(\Sigma)$ nije veći od ω. U suprotnom za valuaciju ϕ kažemo da je *TRANSFINITNA*. Posle ćemo videti da postoje prsteni koji imaju bar jednu *transfinitnu*, ali ne i *konačnu* Σ-euklidsku valuaciju.

Ako u uslovu *EI* modul M zamenimo nekim njegovim podskupom S, tada govorimo o Σ-euklidskoj valuaciji ϕ skupa S. Dalje, ako je $\Sigma = M^0$, tada kažemo samo da je ϕ *EUKLIDSKA* valuacija (desnog) A-modula M (što se u slučaju komutativnog prstena A i za $M = A$ podudara sa pojmom *euklidske valuacije* u smislu *P. SAMUEL* [*1*]).

Ako je $M = A$ i Σ skup svih (*levih, desnih*) regularnih elemenata iz A, tada kažemo da je ϕ Γ-*EUKLIDSKA* (Λ-*EUKLIDSKA*, Δ-*EUKLIDSKA*) valuacija prstena A. Posle ćemo dokazati da postoje prsteni koji imaju bar jednu desnu, ali ne i levu Γ-euklidsku valuaciju.

PRIMER 1-1. (α) *Preslikavanje* $\nu: Z \to N_0$ *dato sa* $\nu(m) = |m|$, $m \in Z$, *je jedna prirodna euklidska valuacija prstena* Z. *Jasno je da za dato* $a \in Z$ *i* $b \in Z^0$ *količnik* q *i ostatak* r *pri* ν-*deljenju* a *sa* b *ne moraju biti odredjeni jednoznačno. Pri tome je* ν *i* N-*euklidska valuacija prstena* Z.

Restrikcija od ν *na* $2Z$ *nije ni euklidska ni* $2N$-*euklidska valuacija prstena* $2Z$, *ali je i jedno i drugo za desni* Z-*modul* $2Z$. *Ako je* $\phi: Z \to N_0$ *preslikavanje dato sa* $\phi(3) = 6$, $\phi(m) = |m|$ $(m \neq 3)$, *tada je* ϕ *euklidska valuacija prstena* Z *koja nije prirodna.*

(β) *Ako je* K *polje i* $W = \{-\infty\} \cup N_0$, *tada je sa* $\sigma(P) = st(P)$ $(P \in A)$ *definisana jedna prirodna euklidska valuacija* $\sigma: A \to W$ *prstena* $A = K[X]$ (*koju ćemo zvati STEPENOM valuacijom*). *Ako je* $n \in N$ *i* $\Sigma = K^n[X]$, *tada je* σ Σ-*euklidska valuacija na svakom podskupu* S *od* $K[X]$.

(γ) *Ako je* $\Sigma = U_l(A)$ *skup svih levih jednota prstena* A, *tada je sa* $\delta(a) = 1$ $(a \in \Sigma)$, $\delta(a) = 0$ $(a \in A - \Sigma)$ *definisana jedna KONSTANTNA desna* Σ-*euklidska valuacija prstena* A.

Posebno, svako polje (telo) ima bar jednu konstantnu desnu (levu) euklidsku valuaciju. Opštije od toga, za proizvoljno telo K *i prirodan broj* $n \in N$, *prsten* $K_n = M_n(K)$ *ima bar jednu (levu, desnu)* Γ-*euklidsku*

valuaciju. Jedna od njih je data sa $\psi(M) = 1$, odnosno $\psi(M) = 0$, već prema tome da li je matrica $M \in M_n(K)$ regularna ili singularna.

(6) Ako je $M_n(Z)$ prsten kvadratnih matrica reda n nad prstenom Z, tada je sa $\psi(M) = |\det M|$, $M \in M_n(Z)$, definisana jedna Γ-euklidska valuacija $\psi: M_n(Z) \to N_0$ prstena $M_n(Z)$ (koji je za $n > 1$ i nekomutativan i sa deliteljima nule). Pri tome ψ nije i euklidska valuacija prstena $M_n(Z)$. To je poseban slučaj jednog opštijeg tvrdjenja o kome će kasnije biti više reči. □

TEOREMA 1-1

Preslikavanje $\phi: A \to W$ zadovoljava uslov E1 ako i samo ako za svako $a \in A$ i svako $b \in \Sigma$ postoji bar jedno $c \in A$ takvo da je $a - bc \in \Sigma_0$ i

$$\phi(a-bc) < \mathrm{Max}(\phi a, \phi b). \tag{2}$$

DOKAZ. Jasno je da je uslov potreban. Dokažimo da je i dovoljan. Neka je $a \in A$ i $b \in \Sigma$. Kako za bar jedno $c \in A$ važi $a - bc \in \Sigma_0$, skup $B = (a + bA) \cap \Sigma_0$ nije prazan. Otuda je $\phi(B)$ neprazan podskup dobro uredjenog skupa W, pa ima minimalni član α. Pri tome je $\alpha = \phi(r)$ za neko $r \in B$, to jest za neko r oblika $r = a - bq \in \Sigma_0$.

Kako je $\phi(a-bq) = \min \phi(B)$, (2) važi za $c = q$. Pretpostavimo da je $\phi(r) = \phi(a-bq) \geq \phi(b)$. Kako za neko $c_0 \in A$ važi $\phi(r - bc_0) < \max(\phi r, \phi b)$, biće $\phi(r - bc_0) < \phi(r)$ sa $r - bc_0 \in \Sigma_0$. Uz to je $r - bc_0 = a - bq - bc_0 = a - bq_0$, i prema tome $r - bc_0 \in B$. Medjutim, to nije moguće jer je ϕr minimalni član skupa $\phi(B)$ i $\phi(r - bc_0) < \phi(r)$. Otuda i tvrdjenje. □

TEOREMA 1-2

Ako je $\phi: A \to W$ desna Σ-euklidska valuacija prstena A sa jedinicom i $\phi_0: A \to W$ preslikavanje definisano sa

$$\phi_0(a) = \begin{cases} \phi(0), & a \in A - \Sigma, \\ \mathrm{Min}\, \phi(aA \cap \Sigma), & a \in \Sigma, \end{cases} \tag{3}$$

tada je ϕ_0 jedna prirodna desna Σ-euklidska valuacija prstena A. Pri tome je $\phi_0(a) \leq \phi(a)$ $(a \in A)$.

DOKAZ. Pre svega, preslikavanje ϕ_0 je dobro definisano. Naime, prsten A ima jedinicu pa za $a \in \Sigma$ važi $a \in aA \cap \Sigma$. To znači da je $\phi(aA \cap \Sigma)$ neprazan podskup dobro uredjenog skupa W, i dakle ima minimalni član. Jasno je da preslikavanje ϕ_0 zadovoljava uslov *E0*. Dokažimo da ϕ_0 zadovoljava i uslov *E1*. Neka je $a \in A$ i $b \in \Sigma$. Prema *(3)* postoji bar jedno $c \in A$ za koje važi $\phi_0(b) = \phi(bc)$ i $bc \in \Sigma$. Kako je ϕ desna Σ-euklidska valuacija prstena A, postoje $q \in A$ i $r \in \Sigma_0$ takvi da je

$$a = bc \cdot q + r, \qquad \phi(r) < \phi(bc). \tag{4}$$

Uz to je $\phi_0(0) = \phi(0)$, $\phi_0(x) = \min \phi(xA \cap \Sigma) \leq \phi(x)$ $(x \in \Sigma)$, pa za $q_0 = cq$ iz *(4)* sledi $a = bq_0 + r$, $\phi_0(r) < \phi_0(b)$, što upravo znači da valuacija ϕ_0 zadovoljava uslov *E1*.

Najzad, dokažimo da ϕ_0 zadovoljava i uslov *E2*, to jest da za svako $a, b \in A$ iz $ab \in \Sigma$ sledi $\phi_0(ab) \geq \phi_0(a)$. Za $a \in A - \Sigma$ to sledi neposredno, jer je $\phi(0) = \min W$. Ako je $a \in \Sigma$, biće $(abA \cap \Sigma) \subset (aA \cap \Sigma)$, pa prema *(3)* imamo $\phi_0(ab) = \min \phi(abA \cap \Sigma) \geq \min \phi(aA \cap \Sigma) = \phi_0(a)$. □

TEOREMA 1-3

Ako je ψ prirodna i ϕ bilo koja desna Σ-euklidska valuacija prstena A, tada za svako $a, b, ab \in \Sigma$ važi:

(α) $\phi(0) < \phi(a)$,

(β) $\psi(ab) = \psi(a) \iff abA = aA$,

(γ) $\phi(a) = \min \phi(\Sigma) \Rightarrow a \in U_l(A)$,

(δ) $\psi(a) = \min \psi(\Sigma) \iff a \in U_l(A)$.

DOKAZ. (α) Neka je $\phi(c)$ $(c \in \Sigma)$ minimalni član skupa $\phi(\Sigma)$. Iz $c \in \Sigma$ sledi da postoje $q \in A$ i $r \in \Sigma_0$ takvi da je $0 = cq + r$ sa $\phi(r) < \phi(c)$. Pri tom je $\phi(r) < \phi(c)$ i $\phi(c) = \min \phi(\Sigma)$, pa mora biti $r = 0$. Otuda je $\phi 0 < \phi c$, a time i $\phi(0) < \phi(a)$ (za svako $a \in \Sigma$).

(β) Neka je $\psi(ab) = \psi(a)$. Kako je $ab \in \Sigma$, postoje $q \in A$ i $r \in \Sigma_0$ takvi da je $a = ab \cdot q + r$ sa $\psi(r) < \psi(ab)$, tj. $ac = r$ sa $c = 1 - bq$, $\psi(r) < \psi(a)$. Uz to je valuacija ψ prirodna, pa $ac = r \in \Sigma$ daje $\psi(r) = \psi(ac) \geq \psi(a)$, što se kosi sa $\psi(r) < \psi(a)$. Dakle je $r = 0$, to jest $a = abq$. Otuda je $aA \subset abA$, a time i $abA = aA$.

Obratno, ako je $aA = abA$, tada za neko $q \in A$ važi $a = abq$, pa kako je valuacija ψ prirodna i $ab \cdot q = a \in \Sigma$, biće $\psi(a) = \psi(ab \cdot q) \geqslant \psi(ab)$, što sa $\psi(ab) \geqslant \psi(a)$ daje $\psi(ab) = \psi(a)$.

(γ) Iz $a \in \Sigma$ sledi da za neko $q \in A$ i $r \in \Sigma_0$ važi $1 = aq + r$, $\phi(r) < \phi(a)$. Kako je $\phi(a) = \min \phi(\Sigma)$, $\phi(r) < \phi(a)$ i $r \in \Sigma_0$, mora biti $r = 0$, tj. $1 = aq$, a time i $a \in U_\ell(A)$.

(δ) S obzirom na (γ) treba još dokazati da iz $a \in U_\ell(A)$ sledi da je $\psi(a) = \min \psi(\Sigma)$. Zaista, kako je $a \in U_\ell(A)$, biće $ac = 1$ za neko $c \in A$, pa za svako $b \in \Sigma$ važi $\psi(b) = \psi(acb) \geqslant \psi(a)$. Otuda i tvrdjenje. □

Ako je $\Sigma = R_\ell(A)$, tada uz prethodnu simboliku važi $\psi(ab) = \psi(a)$ ako i samo ako je $b \in U(A)$. Naime, s obzirom na (β) dovoljno je dokazati da je $aA = abA$ akko je $b \in U(A)$. Jasno je da iz $b \in U(A)$ sledi $aA = abA$. Ako je $aA = abA$ biće $a = abq$ za neko $q \in A$. Kako je $a \in R_\ell(A)$, iz $a(1 - bq) = 0$ sledi $bq = 1$. Sada $bq = 1$ daje $bqb = b$, to jest $b(qb - 1) = 0$, pa kako je i $b \in R_\ell(A)$, mora biti $qb = 1$, a time i $b \in U(A)$. To važi i za $\Sigma = A^0$ ako su svi desni delitelji nule prstena A u njegovom radikalu J. Naime, u tom slučaju iz $a(1 - bq) = 0$ sledi $1 - bq \in J$, a time i $b \in U(A)$.

Ako prsten A (*sa jedinicom*) ima bar jednu desnu Σ-euklidsku valuaciju, tada iz (γ) sledi da Σ sadrži bar jednu levu jednotu prstena A. To ne mora da važi ako prsten A nema jedinicu, kao što to pokazuje primer $\mathbb{Z}$-modula $A = 2\mathbb{Z}$ i skupa $\Sigma = \{2\}$. Ukoliko ne kažemo drugačije, ubuduće ćemo podrazumevati da, u slučaju desne Σ-euklidske valuacije prstena A, skup Σ sadrži sve leve jednote toga prstena, to jest da je $U_\ell(A) \subset \Sigma$.

TEOREMA 1-4

Neka je F familija svih desnih Σ-euklidskih valuacija prstena A sa istim kodomenom W. Ako familija F nije prazna, tada je sa

$$\mu(a) = \min \{\phi(a) : \phi \in F\} \qquad (a \in A) \tag{5}$$

definisana jedna prirodna desna Σ-euklidska valuacija prstena A sa kodomenom W. Pri tome je $\mu(a) \leqslant \phi(a)$ $(a \in \Sigma, \phi \in F)$, kao i $\mu(a) = 0$ za $a \in A - \Sigma$ $(\text{sa } 0 = \min W)$.

DOKAZ. Pre svega, za svako $a \in A$ skup $\{\phi(a) : \phi \in F\}$ je neprazan podskup

dobro uredjenog skupa W, pa je preslikavanje μ dobro definisano. Ako je $\phi \in F$ i ϕ_0 Σ-euklidska valuacija o kojoj je reč u *Teoremi 1-2*, biće $\phi_0 \in F$ i $\phi_0(a) = \phi_0(0) = \min W$ $(a \in A-\Sigma)$. Otuda je i $\mu(a) = \mu(0) = \min W$ $(a \in A-\Sigma)$, pa μ zadovoljava uslov *E0*.

Dokažimo da μ zadovoljava i uslov *E1*. Neka je $a \in A$, $b \in \Sigma$, i označimo sa ψ element familije F za koji je $\psi(b) = \min_{\phi} \phi(b)$. Tada je $\mu(b) = \psi(b)$. Kako valuacija ψ zadovoljava uslov *E1*, postoje $q \in A$ i $r \in \Sigma_0$ takvi da je $a = bq+r$ sa $\psi(r) < \psi(b)$. Uz to je $\mu(r) \leqslant \psi(r)$ i $\mu(b) = \psi(b)$, i prema tome $a = bq+r$ sa $\mu(r) < \mu(b)$, što upravo znači da μ zadovoljava i uslov *E1*.

Najzad, uz simboliku iz *Teoreme 1-2* postoji prirodna Σ-euklidska valuacija $\mu_0 \in F$ takva da je $\mu_0 a \leqslant \mu a$ za svako $a \in A$. Medjutim, prema (5) je $\mu a \leqslant \mu_0 a$ $(a \in A)$, pa je $\mu_0 = \mu$. Otuda i tvrdjenje. □

DEFINICIJA 1-2

Ako prsten A ima bar jednu (levu, desnu) Σ-euklidsku valuaciju sa kodomenom W, tada prirodnu (levu, desnu) Σ-euklidsku valuaciju μ o kojoj je reč u Teoremi 1-4 zovemo MINIMALNOM *(levom, desnom) Σ-euklidskom valuacijom prstena A (sa kodomenom W).*

Kasnije ćemo dokazati da je "stepena" valuacija σ prstena $A = K[X]$, o kojoj je bilo reči u *Primeru 1-1* pod (γ), upravo njegova minimalna euklidska valuacija sa kodomenom $\{-\infty\} \cup N_0$, i da je minimalna euklidska valuacija prstena Z data sa: $\mu(m) = \min\{n \in N_0 : 2^n > |m|\}$ $(m \in Z)$.

DEFINICIJA 1-3

Pod (desnim) Σ-EUKLIDSKIM PRSTENOM podrazumevamo svaki prsten koji ima bar jednu (desnu) Σ-euklidsku valuaciju.

Ako je ϕ (desna) Σ-euklidska valuacija prstena A, tada uredjen par (A, ϕ) zovemo (desnim) Σ-EUKLIDSKIM PAROM.

Ako je A *(desni)* Σ-euklidski prsten, tada za $\Sigma = A^0$ kažemo samo da je A *(desni)* euklidski prsten, dok za $\Sigma = R(A), R_\ell(A), R_d(A)$ kažemo da je prsten A Γ-euklidski, odnosno Λ-euklidski, odnosno Δ-euklidski. □

TEOREMA 1-5

Neka je A desni Σ-euklidski prsten Ako desni ideal I prstena A ima neprazan presek Π sa skupom Σ, tada je I = aA za neko a∈Σ. Posebno, ako je Σ=A°, tada je u prstenu A svaki desni ideal glavni.

Svaka dva elementa a∈A i b∈Σ imaju najveći zajednicki levi delitelj c koji pripada skupu Σ. Pri tome postoje p,q iz A takvi da je

$$ap + bq = c. \tag{6}$$

DOKAZ. Neka je ϕ desna Σ-euklidska valuacija prstena A. Iz $\Pi \neq \Theta$ sledi da za neko $a \in \Sigma$ važi $\phi(a) = min\,\phi(\Pi)$. Kako $a \in \Sigma$, za svako $c \in I$ postoji $q \in A$ i $r \in \Sigma_0$ takvi da je $c = aq + r$, $\phi(r) < \phi(a)$. Iz $a \in I$ sledi $aq \in I$, što sa $c \in I$ daje $r = c - aq \in I$. Uz to je $\phi(r) < \phi(a)$, pa ne može biti $r \in \Sigma$. To znači da mora biti $r=0$, to jest $c = aq$, i prema tome $I = aA$.

Kako je $I = aA + bA$ desni ideal prstena A koji sadrži element b iz Σ, prema dokazanom delu tvrdjenja postoji $c \in \Sigma$ za koje je $I = cA$. Otuda je $aA + bA = cA$, što sa $c \in cA$ znači da za neko p,q iz A važi *(6)*. Preostali deo tvrdjenja sledi neposredno. □

LEMA 1-1

Neka je ϕ prirodna (desna) Σ-euklidska valuacija prstena A čiji su svi desni delitelji nule u njegovom radikalu $J(A)$. Ako za neko $x \in A$ vazi $\phi(x) > \phi(1)$, $x^n \in \Sigma$ $(n \in N)$, tada niz $\phi(x^n)$ $(n \in N)$ strogo raste.

Analogno tvrdjenje važi i za proizvoljan prsten A ako x nije levi delitelj nule.

DOKAZ. Pretpostavimo da za neko $n \in N$ važi $\phi(x^n) \geq \phi(x^{n+1})$. Tada postoje $q \in A$ i $r \in \Sigma_0$ takvi da je $x^n = x^{n+1}q + r$, $\phi r < \phi x^n$. Dokažimo da mora biti $r=0$. Naime, kako je valuacija ϕ prirodna, iz $r \in \Sigma$ i $r = x^n(1-xq)$ sledi $\phi r \geq \phi x^n$, što je u suprotnosti sa učinjenom pretpostavkom. Sada iz $x^n \in \Sigma$ i $r=0$ sledi da je $1-xq$ desni delitelj nule u prstenu A, pa pripada njegovom radikalu $J(A)$. Otuda je $x \in U(A)$. Medjutim, to nije moguće jer iz $xy = 1$ sledi $\phi 1 \geq \phi x$, što se kosi sa $\phi x > \phi 1$.

Slično se dokazuje i drugi deo tvrdjenja. Naime, tada iz $x^n \in R_\ell(A)$ i $x^n(1-xq) = 0$ sledi $1 = xq$, a time i $\phi 1 \geq \phi x$. Tu je posebno važan slučaj kada je $\Sigma = R_\ell(A)$ ili $\Sigma = \Gamma$. □

DEFINICIJA 1-4

Pod MORFIZMOM (desnog) euklidskog para (A,ϕ) *u (desni) euklidski par* (B,ψ) *podrazumevamo svaki uredjen par* (f,h), *pri čemu je* $f:A\to B$ *morfizam u kategoriji ANN i* h *monomorfizam dobro uredjenog skupa* $\phi(A)$ *u dobro uredjen skup* $\psi(B)$, *takav da je* $\psi\circ f = h\circ\phi$.

Ako je uz to f *izomorfizam, tada kažemo da je par* (f,h) *IZOMORFIZAM (desnog) euklidskog para* (A,ϕ) *na par* (B,ψ), *kao i da je euklidski par* (B,ψ) *IZOMORFAN euklidskom paru* (A,ϕ).

Ako su $(f,u)\colon (A,\phi)\to(B,\psi)$ i $(g,v)\colon (B,\psi)\to(C,\eta)$ dva morfizma medju (desnim) euklidskim parovima, tada se neposredno proverava da je i njihova "kompozicija" $(g\circ f,\ v\circ u)$ morfizam euklidskog para (A,ϕ) u euklidski par (C,η). Otuda se na prirodan način može definisati jedna *kategorija* čiji su objekti euklidski parovi, a morfizmi su "odredjeni" prethodnom *Definicijom 1-4*. Zvaćemo je *KATEGORIJOM EUKLIDSKIH PRSTENA* i označavati sa *EUC*. Naravno da kategorija *EUC* nije podkategorija kategorije *ANN*.

TEOREMA 1-6

Neka je A *prsten,* $h:W\to W'$ *monomorfizam dobro uredjenog skupa* W *u dobro uredjen skup* W' *i* $\phi:A\to W$ *preslikavanje skupa* A *u* W. *Tada je* (A,ϕ) *desni euklidski par akko je to i* $(A,\ h\circ\phi)$.

Ako je uz to $f:B\to A$ *izomorfizam prstena* B *na* A, *tada je par* (A,ϕ) *euklidski ako i samo ako je to slučaj sa parom* $(B,\ \phi\circ f)$.

DOKAZ. Kako je $h:W\to W'$ monomorfizam, za $r\in A$ i $b\in A^0$ važi $\phi(r)<\phi(b)$ ako i samo ako je $h(\phi(r)) < h(\phi(b))$, to jest akko je $(h\circ\phi)(r)\ (h\circ\phi)(b)$, pa se neposredno zaključuje da je (A,ϕ) desni euklidski par ako i samo ako je to slučaj sa parom $(A,\ h\circ\phi)$.

Dokažimo sada drugi deo tvrdjenja. Neka je prvo (A,ϕ) euklidski par i $a\in B$, $b\in B^0$. Tada je $f(b)\in A^0$, pa postoje $q_0\in A$ i $r_0\in A$ takvi da je $f(a) = f(b)q_0 + r_0$, $\phi(r_0) < \phi(f(b))$, to jest $f(a) = f(b)f(q)+f(r)$, i prema tome $f(a) = f(bq+r)$ sa $q = f(q)$, $r = f(r)$. Uz to je f izomorfizam pa mora biti $a = bq+r$, što sa $(\phi\circ f)(r) < (\phi\circ f)(b)$ upravo znači da je i $(B,\phi\circ f)$ desni euklidski par. Obratno, ako je (B,ψ) $(\psi = \phi\circ f)$ euklidski par, tada iz dokazanog dela tvrdjenja sledi da je i $(A,\ \psi\circ f^{-1})$ euklidski par. □

Ako je σ stepena valuacija prstena $K[X]$, tada je sa $\phi(a) = 2^{\sigma(a)}$ $(a \in K[X])$ definisana jedna euklidska valuacija $\phi: K[X] \to N_0$ prstena $K[X]$ koja zadovoljava uslov $\phi(ab) = \phi(a)\phi(b)$. Slično, sa $\psi(a) = \ell n|m|$ $(m \neq 0)$ i $\psi(0)=0$ je definisana jedna euklidska valuacija $\psi: Z \to W$ prstena Z koja zadovoljava uslov $\psi(ab) = \psi(a) + \psi(b)$, pri čemu je $W = \{\ell n(n): \ n \in N\}$.

LEMA 1-2

Ako su (A,ϕ) i (B,ψ) izomorfni (desni) euklidski parovi, tada je valuacija ψ prirodna akko je to slučaj sa valuacijom ϕ.

DOKAZ. Neka je valuacija ϕ prirodna i (f,h) izomorfizam euklidskog para (A,ϕ) na par (B,ψ). Tada za svako $a \in B$ i $b, ab \in B^0$ postoje $x, y \in A$ takvi da je $a = f(x)$, $b = f(y)$, $xy \in A$. Pri tome je valuacija ϕ prirodna, pa važi $\phi(xy) \geq \phi(x)$, a time i $h\big(\phi(xy)\big) \geq h\big(\phi(x)\big)$, što sa $\psi \circ f = h \circ \phi$ daje $\psi(ab) = (\psi \circ f)(xy) = (h \circ \phi)(xy) = h\big(\phi(xy)\big) \geq h\big(\phi(x)\big) = \psi\big(f(x)\big)$, i prema tome $\psi(ab) \geq \psi(a)$. Otuda i tvrdjenje. □

TEOREMA 1-7

Ako su $\phi: A \to W$ i $\psi: B \to V$ minimalne desne euklidske valuacije prstena A i B, tada su desni euklidski parovi (A,ϕ) i (B,ψ) izomorfni ako i samo ako je to slučaj sa prstenima A i B.

DOKAZ. Neka je $f: A \to B$ izomorfizam prstena A na prsten B. Skupovi $\phi(A)$ i $\psi(B)$ su dobro uredjeni pa postoji monomorfizam h bar jednog od njih na početni interval drugog. Neka je, na primer, $h: \phi(A) \to \psi(B)$, pri čemu je $h\big(\phi(A)\big)$ početni interval skupa $\psi(B)$. Prema *Teoremi 1-6* preslikavanje $(h \circ \phi \circ f^{-1}): B \to V$ je desna euklidska valuacija prstena B. Kako je $\psi: B \to V$ minimalna desna euklidska valuacija prstena B, biće $\big(h \circ \phi \circ f^{-1}\big)(b) \geq \psi(b)$, pa stavljajući $f^{-1}(b) = a$ dobijamo

$$(7) \qquad (h \circ \phi)(a) \geq (\psi \circ f)(a) \qquad (a \in A).$$

Dalje je $B = \{f(a): \ a \in A\}$, pa iz (7) sledi da za svako $\beta \in \psi(B)$ postoji bar jedno $a \in A$ takvo da je (*) $\beta < h\big(\phi(a)\big)$, a time i $\beta \in h\big(\phi(A)\big)$, jer je $h\big(\phi(A)\big)$ početni interval skupa $\psi(B)$. Otuda je $h\big(\phi(A)\big) = \psi(B)$. To upravo znači da je h surjekcija, a time i bijekcija. Otuda, zamenjujući u (7)

a sa $f(a)$ i h,ϕ,ψ,f redom sa h^{-1},ψ,ϕ,f^{-1}, dobijamo da za svako a iz A važi $(\psi\circ f)(a) \geqslant (h\circ\phi)(a)$, što uporedjeno sa (7) daje $h\circ\phi = \psi\circ f$, pa je (f,h) izomorfizam euklidskog para (A,ϕ) na euklidski par (B,ψ). Otuda i tvrdjenje. □

Iz poslednja tri tvrdjenja sledi da se u izučavanju Σ-euklidskih parova možemo ograničiti na euklidske parove (A,ϕ) kod kojih je kodomen valuacije ϕ dobro uredjen skup oblika $W = \{0,1,..,\omega,\omega+1,..,\eta\}$, pri čemu je $\eta = \eta(A)$ "dovoljno veliki" *ordinal*. U tom slučaju sa W_0 označavaćemo uniju $\{-\infty\} \cup W$, gde je $-\infty < \alpha$ za svako $\alpha \in W$. Ubuduće, ukoliko ne kažemo izričito drugačije, W i W_0 imaće prethodna značenja.

2. O EUKLIDSKIM VALUACIJAMA SA NEKIM SPECIFIČNIM SVOJSTVIMA

Euklidske valuacije prstena često imaju i neka specifična svojstva koja karakterišu neke dobro poznate klase (euklidskih) prstena. Posebno su česti i važni primeri euklidskih valuacija $\phi: A \to W$ koje zadovoljavaju neke od sledećih uslova:

$$(Z) \qquad \phi(a) = \phi(b) \iff (\exists e \in A^*)(a = be),$$

$$(N) \qquad \phi(ab) = \phi(a)\phi(b),$$

$$(T) \qquad \phi(a+b) \leqslant \phi(a) + \phi(b),$$

$$(M) \qquad \phi(a+b) \leqslant \mathrm{Max}\{\phi(a), \phi(b)\},$$

$$(V) \qquad \phi(a+b) \geqslant \mathrm{Min}\{\phi(a); \phi(b)\} \qquad (a+b \neq 0)$$

$(a,b \in A)$, gde je $A^* = U(A)$. Uz to se o uslovima (M) i (V) može govoriti i u slučaju proizvoljnog dobro uredjenog skupa W. Operacije o kojima je reč na desnim stranama relacija iz uslova (T) i (N) su obično sabiranje i množenje ordinala. Ako je kodomen valuacije ϕ skup $W_0 = \{-\infty\} \cup W$, tada po dogovoru stavljamo $(-\infty)+\alpha = \alpha+(-\infty) = -\infty$ i $(-\infty)\alpha = \alpha(-\infty) = -\infty$ $(\alpha \in W_0)$.

U ovom paragrafu biće reči upravo o prstenima koji imaju bar jednu euklidsku valuaciju koja zadovoljava neke od uslova (M)-(Z). Pri tom se u vezi sa prethodnim uslovima često pojavljuju i uslovi:

(L) $\phi(ab) = \phi(a) + \phi(b)$,

(P) $\phi(a) \geq \phi(b) \quad \Rightarrow \quad \phi(a+b) = \phi(a)$,

(S) $\phi(a) = \phi(b) \quad \Leftrightarrow \quad (\exists e \in A^*)(a = be \ \vee \ \phi(a-be) < \phi(a))$.

Tako, na primer, stepena euklidska valuacija ∂ prstena $A = K[X]$ od svih prethodnih uslova (Z)-(S) ne zadovoljava jedino uslove (N), (Z) i (V). S druge strane, euklidska valuacija $\phi: K[X] \to N_0$ data sa $\phi(a) = 2^{\partial(a)}$ zadovoljava sve prethodne uslove izuzev (Z), (V) i (L). To posebno znači da prsten $K[X]$ ima bar jednu euklidsku valuaciju koja zadovoljava uslov *norme*, to jest uslov (N).

Od uslova (Z)-(S) standardna euklidska valuacija $\nu: Z \to N_0$ prstena Z zadovoljava samo tri: (T), (N), (Z), dok minimalna euklidska valuacija μ prstena Z zadovoljava jedino uslov (T). Kasnije ćemo dokazati da prsten Z nema nijednu euklidsku valuaciju koja zadovoljava neki od uslova (M), (P), (S), (V).

Ako je $n>1$ i ψ (desna) Γ-euklidska valuacija prstena $A = M_n(Z)$ data sa $\psi(M) = |\det M|$, $M \in A$, neposredno se proverava da valuacija ψ od svih prethodnih uslova zadovoljava jedino uslov (N). Posle ćemo dokazati da slično tvrdjenje važi i za prsten $M_n(A)$, pri čemu je A bilo koji domen sa bar jednom euklidskom valuacijom $\phi: A \to W$ koja zadovoljava uslov *norme*.

Primećujemo da svaki od (desnih) Γ-euklidskih prstena $M_n(Z)$ i $K[X]$ ima bar jednu (desnu) Γ-euklidsku valuaciju koja zadovoljava uslov (N). To važi i za svaki "poznati" (desni) Γ-euklidski prsten. U vezi sa tim prirodno se nameće problem:

Da li svaki (desni) Γ-euklidski prsten ima bar jednu Γ-euklidsku valuaciju koja zadovoljava uslov norme?

Jasno je da uslov (M) povlači uslov (T). Ako prsten A ima bar jednu desnu euklidsku valuaciju ϕ koja zadovoljava uslov (Z) ili (N), tada je A oblast celih. Svaka valuacija koja zadovoljava uslov (N) je *prirodna*.

TEOREMA 2-1

Za svaku prirodnu (desnu) euklidsku valuaciju $\phi: A \to W$ oblasti celih A uslovi (M), (P) i (S) su ekvivalentni.

DOKAZ. Dokažimo prvo implikaciju (M) => (P). Kako je A domen i valuacija ϕ prirodna, za $a,b \in A$ važi $\phi(be) = \phi(b)$ akko je $e \in U(A)$. Neka za $a,b \in A$ važi $\phi(a) \geq \phi(b)$. Tada je $\phi(-b) = \phi(b \cdot -1) = \phi(b)$, pa $\phi(a) \geq \phi(b)$ i uslov (M) daju $\phi(a+b) \leq \phi(a)$, $\phi(a) = \phi(a+b-b) \leq Max\left(\phi(a+b), \phi(b)\right) = \phi(a+b)$, a time i $\phi(a+b) = \phi(a)$, što upravo znači da valuacija ϕ zadovoljava uslov (P).

Dokažimo sada da uslov (P) povlači uslov (S). Pretpostavimo prvo da za $a,b \in A$ važi $\phi(a) = \phi(b)$. Ako je $b=0$ tada prema *Teoremi 1-3* mora biti i $a=0$, a time i $a = b \cdot 1$. Ako je $b \neq 0$, tada postoje e i r iz A takvi da je $a = be+r$, $\phi(r) < \phi(b)$. Otuda je i $\phi(a) > \phi(r)$, pa kako ϕ zadovoljava uslov (P), imamo $\phi(a) = \phi(a-r) = \phi(be)$, a time i $\phi(be) = \phi(b)$. To posebno znači da je $e \in U(A)$, pa je $\phi(a-be) < \phi(a)$ sa $e \in U(A)$. Obratno, pretpostavimo sada da za neko $a,b \in A$ i $e \in U(A)$ važi $\phi(a-be) < \phi(a)$. Tada uslov (P) daje $\phi(be) = \phi\left(a+(be-a)\right) = \phi(a)$. Uz to je $\phi(be) = \phi(b)$, i prema tome $\phi(a) = \phi(b)$.

Najzad, dokažimo da važi i implikacija (S) => (M). Pretpostavimo da za neko $a,b \in A$ važi $\phi(a+b) > \phi(a)$. Tada, za $c=a+b$, iz $\phi(c-b \cdot 1) < \phi(c)$ i uslova (S) sledi $\phi(a+b) = \phi(b)$, i prema tome $\phi(a+b) \leq Max\left(\phi a, \phi b\right)$. Otuda i tvrdjenje u celini. □

TEOREMA 2-2

(α) Ako prirodna (desna) euklidska valuacija $\phi: A \to W$ nekog domena A zadovoljava uslov (M), tada je $K = U_0(A)$.

(β) Ako desna euklidska valuacija $\phi: A \to W$ prstena A zadovoljava uslove (T) i (N), tada ϕ zadovoljava i uslov (M) ako i samo ako je $K = U_0(A)$ podtelo prstena A.

DOKAZ. (α) Dokažimo prvo da je $K = \{a \in A: \ \phi(a) \leq \phi(1)\}$. Jasno je da za $a \in K$ važi $\phi(a) \leq \phi(1)$, kao i da je $\phi(a) = \phi(1 \cdot a) \geq \phi(1)$ za svako $a \neq 0$. Ako za neko $a \in A$ važi $\phi a = \phi(1)$, postoje $q,r \in A$ takvi da je $1 = aq+r$, $\phi(r) < \phi(1)$. Otuda je $r=0$, to jest $1=aq$, a time i $a \in K$. Kako valuacija ϕ zadovoljava uslov (M), za svako $a,b \in K$ biće $\phi(a-b) \leq Max\left(\phi(a), \phi(b)\right) \leq \phi(1)$, što sa prethodnim daje $a-b \in K$. Uz to je $K^* = U(A)$ multiplikativna podgrupa od A

pa je K podtelo prstena A.

(β) Pre svega, iz pretpostavke da ϕ zadovoljava uslov (N) sledi da je valuacija ϕ prirodna, da je A domen i da je $\phi(0)=0$, $\phi(1)=1$. Ako ϕ zadovoljava i uslov (M), tada iz upravo dokazanog dela tvrdjenja sledi da je uslov potreban. Dokažimo da je i dovoljan, tj. da iz pretpostavke da je K podtelo prstena A sledi da za svako $a,b\in A$ važi

$$(1)\qquad \phi(a)\leqslant\phi(b) \quad\Rightarrow\quad \phi(a+b)\leqslant\phi(b).$$

Dokaz implikacije (1) izvešćemo (transfinitnom) indukcijom po $\phi(a)$ ($a\in A^0$). Neka je prvo $\phi(a)=1$, i dakle $a\in U(A)$. Kako ϕ zadovoljava uslov (N), imamo $\phi(a+b)=\phi\left(a(1+a^{-1}b)\right)=\phi(a)\cdot\phi(1+c)$, pri čemu je $c=a^{-1}b$, a time i $\phi(c)=\phi(a^{-1})\phi(b)=\phi(b)$. Otuda se za $\phi(a)=1$ tvrdjenje svodi na $1\leqslant\phi(c) \Rightarrow \phi(1+c)\leqslant\phi(c)$, $c\in A$. Kako je K telo, biće $1+\cdots+1=n1\in K$ za svaki prirodan broj n, a time i $\phi(n1)<1$ za svako $n\in N$. Uz to 1 komutira sa svakim elementom $c\in A$, pa kako ϕ zadovoljava uslove (T) i (N), imamo da za svako $n\in N$ i $c\in A^0$ važi:

$$\begin{aligned}(2)\qquad \left(\phi(1+c)\right)^n &= \phi\left((1+c)^n\right)=\phi\left(\Sigma\binom{n}{k}c^k\right)\\ &\leqslant \Sigma\phi\left(\binom{n}{k}\cdot 1\right)\phi(c^k)\\ &\leqslant \Sigma\left(\phi(c)\right)^k.\end{aligned}$$

Stavimo $\phi(c)=\beta$. Kako je $c\neq 0$ biće $\beta\geqslant 1$. Iz (2) sledi da za svako $c\in A^0$ za koje je $\beta<\omega$ važi

$$(3)\qquad \phi(1+c)\leqslant\begin{cases}(1+n)^{1/n} & (\beta=1),\\ \left(\dfrac{\beta^{n+1}-1}{\beta-1}\right)^{1/n} & (\beta>1).\end{cases}$$

Kako (3) važi za svako $n\in N$, puštajući da $n\to\infty$ dobijamo $\phi(1+c)\leqslant\beta$, što sa prethodnim zaključcima daje $\phi(a+b)\leqslant\phi(b)$ za svako $a\in K$ i svako $b\in A$ za koje je $1\leqslant\phi(b)=\phi(c)<\omega$. Ako je $\phi(b)=\beta\geqslant\omega$, biće $1+\beta=\beta$, pa uslov (T) direktno daje $\phi(a+b)\leqslant\phi(a)+\phi(b)=1+\beta=\beta=\phi(b)$. Otuda i tvrdjenje za $a,b\in A$, $\phi(a)\leqslant 1$.

Pretpostavimo sada da (1) važi za svako $a\in A$ za koje je $\phi a<\alpha$ ($\alpha>1$

fiksiran ordinal iz W), pa dokažimo da važi i za svako eventualno $a \in A^0$ takvo da je $\phi(a) = min(\phi(c):\ c \in A,\ \phi c \geqslant \alpha)$. Kako je $a \neq 0$, postoje q i r iz A takvi da je $b = aq+r$, $\phi(r) < \phi(a)$. Otuda je $a+b = r+c$ sa $c=a(1+q)$ i $\phi(r) < \phi(a)$. Ako je $1+q=0$ biće $a+b=r$, a time i $\phi(a+b) = \phi(r) < \phi(a)$. Ako je $1+q \neq 0$, tada uslov (N) daje $\phi(c) = \phi(a)\cdot\phi(1+q) \geqslant \phi(a) > \phi(r)$. Uz to, iz $\phi(r) < \phi(a)$ sledi $\phi(r) < \alpha$, pa na osnovu induktivne pretpostavke imamo da je $\phi(r+c) \leqslant \phi(c)$, a time i

$$(4) \qquad \phi(a+b) \leqslant \phi(a)\phi(1+q).$$

Slučaj $q=0$ se apsolvira neposredno. Ako je $\phi(q) \geqslant 1$, prema dokazanom delu tvrdjenja važi $\phi(1+q) \leqslant \phi(q)$, pa uslov (N) daje

$$(5) \qquad \phi(a)\phi(1+q) \leqslant \phi(a)\phi(q) = \phi(aq) = \phi(b-r).$$

Kako je $\phi(-r) = \phi(r) < \alpha \leqslant \phi(b)$, na osnovu induktivne pretpostavke imamo $\phi(b-r) \leqslant \phi(b)$, što sa prethodnim relacijama daje $\phi(a+b) \leqslant \phi(b)$. Otuda i tvrdjenje u celini. □

TEOREMA 2-3

Ako (desna) euklidska valuacija $\phi: A \to W$ prstena A zadovoljava uslov (N), tada valuacija ϕ zadovoljava i uslov (T) ako i samo ako važi

$$(M_2) \qquad \phi(a+b) \leqslant 2\cdot Max(\phi a, \phi b) \qquad (a,b \in A).$$

DOKAZ. Kako ϕ zadovoljava uslov (N), biće valuacija ϕ prirodna, A domen i $\phi(0)=0$, $\phi(1)=1$. Jasno je da je uslov potreban. Dokažimo da je uslov i dovoljan. S obzirom na uslov (M_2), indukcijom po r dobijamo da za svaki prirodan broj m oblika $m = 2^r$ i proizvoljne elemente $a_1,\ldots,a_m$ iz A važi (*) $\phi(a_1+\cdots+a_m) \leqslant 2^r\cdot Max(\phi a_\nu)$. Ako je n proizvoljan prirodan broj i r najmanji ceo broj za koji je $2^r > n$, to jest $2^{r-1} \leqslant n < 2^r$, tada za $a_\nu = 0$ $(n < \nu \leqslant m)$ iz (*) sledi

$$(6) \qquad \phi(a_1+\cdots+a_m) \leqslant 2n\cdot Max(\phi a_\nu),$$

jer je $2^r \leqslant 2n$. Za proizvoljne elemente a,b prstena A i prirodan broj n oblika $n = 2^r-1$ označimo sa C_ν $(0 \leqslant \nu \leqslant n)$ sumu od $\binom{n}{\nu}$ sabiraka $C_{\nu k}$, pri

čemu je svaki od $C_{\nu k}$-ova, $1 \leqslant k \leqslant \binom{n}{\nu}$, proizvod od n faktora među kojima je ν a-ova i $n-\nu$ b-ova. Kako valuacija ϕ zadovoljava uslov (N), biće

$$(7) \qquad \phi(C_{\nu k}) = (\phi(a))^{\nu} (\phi(b))^{n-\nu}, \qquad 1 \leqslant k \leqslant \binom{n}{\nu},$$

za svako $a,b \in A$ za koje je $\phi a, \phi b < \omega$, odnosno $\phi(a) = 1$. S druge strane je $(a+b)^n = C_0 + \cdots + C_n$, pa na osnovu uslova (N) i relacija (6) i (7) jedno za drugim imamo:

$$\begin{aligned} (8) \qquad (\phi(a+b))^n &= \phi((a+b)^n) = \phi(C_0 + \cdots + C_n) \\ &\leqslant 2^r \cdot \operatorname{Max} \phi(C_\nu) < 2^r \Sigma \phi(C_\nu) \\ &\leqslant 2^r \cdot \Sigma \left(2 \binom{n}{\nu} \cdot (\phi a)^{\nu} (\phi b)^{n-\nu}\right) \\ &= 2^{r+1} (\phi a + \phi b)^n, \end{aligned}$$

I prema tome

$$(9) \qquad \phi(a+b) \leqslant 2^s (\phi a + \phi b), \qquad s = (r+1)/n.$$

Kako je $n = 2^r - 1$, biće $s \to \infty$ $(r \to \infty)$, pa puštajući u (9) da $r \to \infty$ dobijamo da za svako $a,b \in A$ za koje je $\phi a = 1$ ili $\phi a, \phi b < \omega$ važi

$$(10) \qquad \phi(a+b) \leqslant \phi(a) + \phi(b).$$

Otuda i tvrdjenje u slučaju da je valuacija ϕ konačna, tj. ako za svako $a \in A$ važi $\phi(a) < \omega$. Ako valuacija ϕ nije konačna, neka je $\alpha > 1$ fiksiran ordinal iz $\phi(A)$. Pretpostavimo da (10) važi za svako $a,b \in A$, $\phi a < \alpha$, pa dokažimo da važi i za svako $a,b \in A$, $\phi(a) = \alpha$. Pri tome je slučaj $\alpha = 1$ već apsolviran.

Neka je prvo $\alpha < \omega$. Ne umanjujući opštost možemo pretpostaviti da je $\phi(a) \leqslant \phi(b)$. Prema dokazanom delu tvrdjenja (10) važi za $\phi(b) < \omega$. Zato pretpostavimo da je $\phi(b) \geqslant \omega$, i neka je $b = aq + r$, $\phi(r) < \phi(a)$. Pri tom je $\phi(r) < \alpha < \omega$, pa na osnovu induktivne pretpostavke, za $c = a(1+q)$, imamo (*) $\phi(a+b) = \phi(r+c) \leqslant \phi(r) + \phi(c)$. Iz istih razloga je $\phi(b-r) \leqslant \phi(r) + \phi(b)$ i $\phi(1+q) \leqslant 1 + \phi q$. Uz to je $\phi(r) + \phi(b) = \phi(b)$ (jer je $\phi(r) < \omega$ i $\phi(b) \geqslant \omega$), i prema tome $\phi(c) = \phi(a)\phi(1+q) \leqslant \phi(a) + \phi(a)\phi(q) = \phi(a) + \phi(aq)$, što sa

$aq = b-r$, (*) i prethodnim zaključkom $\phi(r)+\phi(b) = \phi(b)$ daje

$$(11)\qquad \begin{aligned} \phi(a+b) &\leqslant \phi(r) + \big(\phi(a) + \phi(b-r)\big) \\ &\leqslant \phi(r) + \big(\phi a + (\phi r + \phi b]\big) \\ &= \phi(r) + \big(\phi a + \phi b\big) \\ &= \phi(a) + \phi(b) \end{aligned}$$

(jer je $\phi a + \phi b \geqslant \omega$ i $\phi r < \omega$). Time je dokazano da relacija (10) važi za svako $a,b \in A$ za koje je $\phi(a) < \omega$ ili $\phi(b) < \omega$.

Neka je sada $\alpha \geqslant \omega$. Ako je $\phi(c) = Min\{\phi(c): c \in A, \ \phi(c) \geqslant \omega\}$, tada postoje p,q,r,s iz A takvi da je $a = cp+r$, $b = cq+s$ sa $\phi r, \phi s < \omega \leqslant \phi c$, pa prema dokazanom delu tvrdjenja imamo prvo $\phi(r+s) \leqslant \phi(r)+\phi(s) < \omega$ a zatim i $\phi(a+b) \leqslant \phi(r+s) + \phi(cp+cq)$. Slučaj $p+q=0$ se lako apsolvira. Za $p+q \neq 0$ je $\phi(cp+cq) = \phi(c)\phi(p+q) \geqslant \omega$, i dakle $\phi(a+b) \leqslant \phi(c)\phi(p+q)$. S druge strane iz $\phi(c)\phi(p) = \phi(cp) = \phi(a-r) \leqslant \phi(r)+\phi(a) \leqslant \phi(a)$ sledi $\phi(p) \leqslant \phi(a)$, pa na osnovu induktivne pretpostavke važi $\phi(p+q) \leqslant \phi(p)+\phi(q)$, a time i

$$(12)\qquad \begin{aligned} \phi(a+b) &\leqslant \phi(c)\big(\phi(p) + \phi(q)\big) \leqslant \phi(c)\phi(p) + \phi(c)\phi(q) \\ &= \phi(cp) + \phi(cq) = \phi(a-r) + \phi(b-s) \\ &\leqslant \big(\phi r + \phi a\big) + \big(\phi s + \phi b\big) \\ &= \phi(a) + \phi(b), \end{aligned}$$

jer je $\phi a, \phi b \geqslant \omega$ i $\phi r, \phi s < \omega$. Prema tome, (10) važi i za svako $a,b \in A$ za koje je $\phi(a) = \alpha$. Otuda i tvrdjenje u celini. (Analogno tvrdjenje važi i ako se uslov (M_2) zameni uslovom (M_k) $\phi(a+b) \leqslant k \cdot Max\{\phi a, \phi b\}$ $(a,b \in A)$, gde je $k > 1$ bilo koji prirodan broj.) □

Svako telo A ima bar jednu (desnu) euklidsku valuaciju $\phi: A \to W$ koja je konstantna na skupu A^0. Pri tome važi i obrnuto tvrdjenje. Naime, ako je $\phi(a) = \phi(1)$ $(a \in A^0)$, tada za svako $a \in A^0$ postoje $q,r \in A_0$ takvi da je $1 = aq+r$, $\phi(r) < \phi(a)$. Otuda je $r=0$, to jest $1=aq$, i dakle $a \in U_\ell(A)$. Kako to važi za svako $a \in A^0$, biće $A^0 = U(A)$, pa je A telo. To ne mora da važi ako je ϕ desna Γ-euklidska valuacija prstena A. Tako, na primer, ako je K polje i $\psi: M_n(K) \to N_0$ preslikavanje definisano sa $\psi(0)=0$, $\psi(M)=1$ $(M \neq 0)$, tada je ψ desna Γ-euklidska valuacija prstena $A=M_n(K)$ koja je konstantna

na skupu A^0, ali za $n>1$ prsten A nije telo. Iz *Leme 1-1* sledi da slično svojstvo ima i svaki konačan prsten koji nije telo.

Prema tome, ako prsten A nije telo, tada za svaku (desnu) euklidsku valuaciju $\phi:A\to W$ prstena A postoji bar jedan element $x\in A$ takav da je $\phi(x)>\phi(1)$. Pri tome x nije (leva) jednota prstena A.

Ako je $\phi:A\to W$ (desna) Σ-euklidska valuacija prstena A i $a\in\Sigma$, tada je jednoznačno odredjen najmanji ordinal $\alpha\in W$ takav da je $\alpha\geqslant\phi(a^n)$ za svako $n\in N$ za koje je $a^n\in\Sigma$. Označavaćemo ga sa $\phi(a^\omega)$. Drugim rečima, za svako $a\in\Sigma$ po definiciji je

$$\phi(a^\omega) = Sup\{\phi(a^n):\ n\in N,\ a^n\in\Sigma\}, \tag{13}$$

a u vezi sa tim i

$$A(a,\phi) = \{c\in A:\ \phi(c)<\phi(a^\omega)\}. \tag{14}$$

Tako, na primer, ako je $\Sigma=\Gamma$ i ako za neko $x\in\Gamma$ važi $\phi(x)>\phi(1)$, tada prema *Lemi 1-1* niz $\phi(x^n)$ $(n\in N)$ strogo raste, pa za svako takvo x važi $\phi(x^\omega)\geqslant\omega$. Ako je uz to valuacija ϕ konačna, biće $\phi(a)<\phi(x^\omega)$ za svako a iz A, i prema tome $A(x,\phi)=A$. Tu je posebno važan slučaj kada je $\phi(x)$ najmanji ordinal iz W koji je veći od $\phi(1)$. Kasnije ćemo dokazati da u slučaju transfinitne euklidske valuacije ϕ ne mora da postoji $x\in A$ koje ima prethodna dva svojstva.

LEMA 2-1

Ako (desna) euklidska valuacija ϕ prstena A zadovoljava uslov (N) i bilo koji od uslova (T) i (M), tada je $A(x,\phi)$ potprsten prstena A za svako $x\in A$ za koje je $\phi(x)>\phi(1)$.

DOKAZ. Iz pretpostavke da ϕ zadovoljava uslov (N) sledi da je A domen i da je valuacija ϕ prirodna. Otuda iz $\phi(x)>\phi(1)$ sledi $\phi(x^\omega)\geqslant\omega$. Neka su a,b proizvoljni elementi skupa $A(x,\phi)$. Tada postoje $m,n\in N$ takvi da je $\phi(a)\leqslant\phi(x^m)$, $\phi(b)\leqslant\phi(x^n)$. Uz to valuacija ϕ zadovoljava uslov (N) pa je $\phi(ab)=\phi(a)\phi(b)\leqslant\phi(x^m)\phi(x^n)=\phi(x^mx^n)=\phi(x^{m+n})<\phi(x^\omega)$, i prema tome $ab\in A(x,\phi)$. Ako valuacija ϕ zadovoljava i uslov (T), tada je (za $m\geqslant n$):

$$(15)\qquad \phi(a+b) \leqslant \phi(a)+\phi(b) \leqslant \phi(x^m)+\phi(x^n) \leqslant \phi(x^m)\phi(x^n) = \phi(x^{m+n}) < \phi(x^{\omega}),$$

a time i $a+b\in A(x,\phi)$, što sa prethodnim upravo znači da je $A(x,\phi)$ jedan potprsten prstena A. Naravno, ako (dobro uredjen) skup $\phi(A)$ zadovoljava uslov kofinalnosti, tada je $A(x,\phi)=A$. □

TEOREMA 2-4

Neka je $\phi: A\to W$ desna euklidska valuacija domena A koji nije telo, $K=U_0(A)$, i x bilo koji element iz $A-K$ takav da je $\phi(x)$ najmanji ordinal iz W koji je veći od $\phi(1)$.

(α) Ako ϕ zadovoljava uslove (N) i (T), tada se svaki element $a\in A$ može predstaviti u obliku

$$(16)\qquad a = x^n\alpha_n + \cdots + x\alpha_1 + \alpha_0 \qquad (\alpha_\nu\in K,\ 0\leqslant\nu\leqslant n).$$

Pri tome $a=0$ ima tačno jedan rastav oblika (16) To važi i za svako a iz A ako je K podtelo prstena A.

(β) Ako je valuacija ϕ prirodna i ako zadovoljava uslov (M), tada svako a iz $A(x,\phi)$ ima tačno jedan rastav oblika (16).

DOKAZ. (α) Pre svega, ϕ zadovoljava uslov *(N)* pa je valuacija ϕ prirodna i važi $\phi(0)=0$ i $\phi(1)=1$. Dokaz ćemo izvesti transfinitnom indukcijom po $\phi(a)$. Jasno je da svako $a\in A$ za koje je $\phi(a)\leqslant 1$, to jest svako $a\in K$ ima rastav oblika *(16)*. Pretpostavimo da tvrdjenje važi za svako b iz A za koje je $\phi(b)<\alpha$ ($\alpha>1$ fiksiran ordinal iz W), i neka je $a\in A$ proizvoljan element iz A takav da je $\phi(a)=\alpha$. Tada za neko $b,\alpha_0\in A$ važi

$$(17)\qquad a = xb+\alpha_0, \qquad \phi(\alpha_0)<\phi(x).$$

Iz $\phi(\alpha_0)<\phi(x)$ sledi $\phi(\alpha_0)\leqslant 1$, a time i $\alpha_0\in K$. Kako valuacija ϕ zadovoljava uslove *(N)* i *(T)*, biće $\phi(xb)=\phi(a-\alpha_0)\leqslant\phi(\alpha_0)+\phi(a)\leqslant 1+\alpha$, i prema tome (*) $\phi(x)\phi(b)\leqslant 1+\alpha$. Ako bi bilo $\phi(b)>\alpha$, tada bi iz $\phi(x)>\phi(1)=1$ sledilo $\phi(x)\phi(b)\geqslant(1+1)\alpha=\alpha+\alpha>1+\alpha$, što se kosi sa (*). Otuda je $\phi(b)<\alpha$, pa na

osnovu induktivne pretpostavke b ima rastav oblika *(16)*. To znači da za neko $n\in N$ i $\alpha_\nu\in K$ $(1\leqslant\nu\leqslant n)$ važi $b = x^{n-1}\alpha_n+\cdots+x\alpha_1+\alpha_0$, što zamenjeno u *(17)* daje *(16)*, a time i prvi deo tvrdjenja. Za dokaz preostalog dela tvrdjenja dokažimo prvo da za svako $n\in N$ i $\alpha_\nu\in K$ $(0\leqslant\nu\leqslant n)$ važi

$$\phi(\alpha_0+\cdots+x^n\alpha_n) < \phi(x^{n+1}). \tag{18}$$

Zaista, ako je K telo, tada prema *Teoremi 2-2* valuacija ϕ zadovoljava i uslov *(M)*, pa *(18)* sledi neposredno, jer niz $\phi(x^n)$ strogo raste. Ako K nije telo, tada za neko $a,b\in K$ važi $a+b\notin K$, a time i $\phi(a+b)>1$, što sa $\phi(a+b)\leqslant\phi(a)+\phi(b)$ daje $\phi(a+b)=2$. Kako je $\phi(x) = \mathit{Min}\,\phi(A-K)$, mora biti i $\phi(x)=2$, pa imamo

$$\begin{aligned}\phi(\alpha_0+\cdots+x^n\alpha_n) &\leqslant 1+\phi(x)+\cdots+\phi(x^n)\\ &= 1+2+\cdots+2^n\\ &< 2^{n+1},\end{aligned} \tag{19}$$

a time i tvrdjenje. Dokažimo sada da za $a=0$ iz *(16)* sledi $\alpha_\nu=0$ $(0\leqslant\nu\leqslant n)$. Naime, ako je $\alpha_n\neq0$ biće $\phi(\alpha_n)=1$, i dakle $\phi(-x^n\alpha_n)=\phi(x^n)$. Uz to za $a=0$ iz *(16)* sledi $-x^n\alpha_n = \Sigma x^\nu\alpha_\nu$ $(0\leqslant\nu\leqslant n)$, pa *(18)* daje $\phi(-x^n\alpha_n) < \phi(x^n)$, što je u suprotnosti sa prethodnim zaključkom. Otuda je $\alpha_n=0$, i slično $\alpha_\nu=0$ $(0\leqslant\nu\leqslant n)$.

Najzad, ako je K telo i $a=\alpha_0+\cdots+x^n\alpha_n$ i $a=\beta_0+\cdots+x^n\beta_n$ rastavi od a oblika *(16)*, biće i $\lambda_\nu=\alpha_\nu-\beta_\nu$ $(0\leqslant\nu\leqslant n)$ elementi tela K, pa kako je $0=a-a=\lambda_0+\cdots+x^n\lambda_n$, prema dokazanom delu tvrdjenja imamo $\lambda_\nu=0$, a time i $\alpha_\nu=\beta_\nu$ $(0\leqslant\nu\leqslant n)$. Otuda i tvrdjenje.

(β) Za svako $a\neq0$ iz $A(x,\phi)$ postoji tačno jedan ceo broj $n\in N_0$ za koji važi (*) $\phi(x^n)\leqslant\phi(a)<\phi(x^{n+1})$. Označimo ga sa $\sigma(a)$. Kako je jasno da svako $a\in K$ ima rastav oblika *(16)*, pretpostavimo da tvrdjenje važi i za svako $a\in A(x,\phi)$ za koje je $\sigma(a)<n$ ($n>1$ zadat prirodan broj), i neka je $a\in A$, $\sigma(a)=n$. Tada postoje $c,b\in A$ takvi da je

$$a = x^nc+b, \qquad \phi(b)<\phi(x^n)\leqslant\phi(a). \tag{20}$$

Dokažimo da je $c\in K$. Naime, ako je $c=xq+r$, $\phi(r)<\phi(x)$, biće prvo $r\in K$, a zatim i $\phi(x^nr)\leqslant\phi(x^n)$ (jer je valuacija ϕ prirodna). Kako valuacija ϕ

zadovoljava uslov *(M)*, mora biti $q=0$. Naime, u suprotnom bi iz *(20)*, za $c = xq+r$, sledilo

$$\phi(x^{n+1}) \leqslant \phi(x^{n+1}q) = \phi(a-x^n r-b) \leqslant \phi(a), \tag{21}$$

što je u suprotnosti sa (*). Otuda je $c = r \in K$. Dalje, iz $\phi b < \phi x^n$ sledi $\sigma(a) < n$, pa na osnovu induktivne pretpostavke postoje α_ν $(0 \leqslant \nu \leqslant n)$ iz K takvi da je $b = \Sigma x^\nu \alpha_\nu$, što zamenjeno u *(20)* daje *(16)* (sa $\alpha_n = c$). Dokaz preostalog dela tvrdjenja je analogan dokazu poslednjeg dela tvrdjenja pod (α). □

KOROLAR 2-1

Neka je simbolika iz Teoreme 2-4 pod (β). Tada je $V = A(x,\phi)$ desni vektorski prostor nad telom K i $\{1,x,x^2,..\}$ je jedna njegova baza.

DOKAZ. To je neposredna posledica prethodne teoreme. Posle ćemo dokazati da $A(x,\phi)$ ne mora biti i levi vektorski prostor nad telom K (naravno, u odnosu na operacije iz A). □

Neka je simbolika iz prethodne teoreme. Ako valuacija ϕ zadovoljava uslove *(N)* i *(T)*, tada rastav *(16)* ne mora biti jednoznačan za svako a iz A, kao što to pokazuje primer prstena Z sa $\phi = \nu$. S druge strane, ako ϕ zadovoljava uslov *(M)*, tada ne mora svako a iz A imati rastav oblika *(16)*, to jest ne mora biti $A(x,\phi) = A$. Naravno, ako ϕ zadovoljava i uslov *norme*, tada prema (α) važi $A(x,\phi) = A$. Štaviše, ako je $A(x,\phi) = A$ i ako ϕ zadovoljava uslov *(M)*, tada prsten A ima bar jednu (desnu) euklidsku valuaciju koja pored uslova *(M)* zadovoljava i uslov *(N)* (o čemu će biti reči kasnije).

Ako $a \in A$ ima tačno jedan rastav oblika *(16)*, zvaćemo ga *POLINOMSKIM* (preciznije: *desnim polinomskim*) *RASTAVOM* od a po x, i označavati sa a_x ili $a(x)$. Ako je uz to $a = \alpha_0 + \cdots + x^n\alpha_n$ sa $\alpha_n \neq 0$, tada ćemo ceo broj n zvati *STEPENOM* od a po x i označavati sa $\sigma(a)$. Za $a=0$ po definiciji ćemo stavljati $\sigma(0) = -\infty$. Posebno je važan slučaj kada se $A(x,\phi)$ podudara sa prstenom A.

U nekoliko narednih tvrdjenja biće reči o prstenima koji imaju bar jednu (desnu) euklidsku valuaciju koja zadovoljava uslov (*M*). Takav je,

na primer, svaki od prstena $K[X]$, pri čemu je K proizvoljno telo. Ako je σ stepena valuacija prstena $K[X]$, tada su, za svako $a\in A$ i $b\in A^0$, ostatak i količnik pri σ-deljenju polinoma a polinomom b odredjeni jednoznačno. U vezi sa tim imamo sledeće tvrdjenje.

TEOREMA 2-5

Neka je ϕ prirodna (desna) euklidska valuacija prstena A. Da bi za svako $a\in A$ i $b\in A^0$ ostatak r pri ϕ-deljenju a sa b bio odredjen jednoznačno, treba i dosta je da valuacija ϕ zadovoljava uslov (M).

DOKAZ. Dokažimo prvo da je uslov potreban. Pretpostavimo da za neko a,b iz A važi (*) $\phi(a-b) > Max(\phi a, \phi b)$. Tada je $c = a-b \neq 0$, pa kako prsten A ima *jedinicu*, biće

$$(22)\qquad a = c\cdot 0 + a, \quad \phi a < \phi c; \qquad a = c\cdot 1 + b, \quad \phi b < \phi c.$$

To znači da su a i b ostaci pri ϕ-deljenju elementa a sa $c\in A^0$, pa kako je taj ostatak (za dato a i c) odredjen jednoznačno, mora biti $a=b$, što je u suprotnosti sa (*). Prema tome, (*) ne važi ni za jedno $a,b\in A$, pa valuacija ϕ zadovoljava uslov (M).

Dokažimo sada da je uslov i dovoljan. Neka je $a = bq_\nu + r_\nu$, $\phi r_\nu < \phi b$ $(\nu=1,2)$, i stavimo $q=q_1-q_2$, $r=r_2-r_1$. Tada je $r = bq$. Kako je valuacija ϕ prirodna, iz $r\neq 0$ sledi $\phi(r) = \phi(bq) \geqslant \phi(b)$. S druge strane, ϕ zadovoljava uslov (M), pa imamo

$$(23)\qquad \phi(r) = \phi(r_2-r_1) \leqslant Max(\phi r_1, \phi r_2) < \phi(b),$$

što je u suprotnosti sa prethodnim zaključkom. Dakle, mora biti $r = 0$, a time i $r_1 = r_2$. Pri tome, ako b nije (levi) delitelj nule, iz $0=bq$ sledi da je i $q_1 = q_2$. Otuda i tvrdjenje u celini. □

Prethodno tvrdjenje ne važi za svaku prirodnu Σ-euklidsku valuaciju ϕ prstena A. Tako, na primer, ako je $A=Z$, $\Sigma=N$ i $\phi=\nu$ standardna *norma* na prstenu Z, tada je ϕ prirodna Σ-euklidska valuacija toga prstena, i za svako $m\in A$ i $n\in\Sigma$ postoji tačno jedno $q\in A$ i tačno jedno $r\in\Sigma_0$ takvi da je $m = nq + r$, $\phi(r) < \phi(n)$. S druge strane, jasno je da ϕ ne zadovoljava

uslov (*M*). U vezi sa tim i *Teoremom 2-4* pod (α) primetimo da za $x=2$ i $L=\{a\in\Sigma_0:\ \phi a\leqslant\phi 1\}=\{0,1\}$ svaki ceo broj m ima tačno jedan rastav u obliku polinoma po x sa koeficijentima iz skupa L (za $m>0$), odnosno iz skupa $-L$ (za $m<0$).

LEMA 2-2

Ako prirodna desna euklidska valuacija $\phi:A\to W_0$ domena A zadovoljava uslov (M), tada za svako $a,b\in A$ i $c\in A^*$ važi implikacija

$$\phi(a)<\phi(b) \quad\Rightarrow\quad \phi(ca)<\phi(cb). \tag{24}$$

DOKAZ. Dokaz ćemo izvesti transfinitnom indukcijom po $\alpha=\phi(a)$. Jasno je da *(24)* važi za $a=0$ i svako $b\in A$ i $c\in A^0$. Pretpostavimo da *(24)* važi za svako $a\in A$ za koje je $\phi(a)<\alpha$ ($\alpha>0$ zadat ordinal iz W_0), i neka su a,b i c proizvoljni elementi iz A takvi da je $\phi(a)=\alpha$, $\phi(a)<\phi(b)$, $c\neq 0$. Dokažimo da je tada i $\phi(ca)<\phi(cb)$. Pre svega, postoje $q,r\in A$ takvi da je $b=aq+r$, $\phi r<\phi a$. Kako je $\phi(r)<\alpha$, na osnovu induktivne pretpostavke biće i $\phi(cr)<\phi(ca)$, što sa prethodnim daje

$$cb=caq+cr, \qquad \phi(cr)<\phi(ca). \tag{25}$$

Uz to mora biti $q\neq 0$ (jer bi u suprotnom bilo $\phi b<\phi a$). Prema *Teoremi 2-1* valuacija ϕ zadovoljava i uslov (*P*). Kako je valuacija ϕ i prirodna, iz $\phi(caq)>\phi(ca)>\phi(cr)$ sledi $\phi(caq+cr)=\phi(caq)$, pa na osnovu *(25)* imamo

$$\phi(cb)=\phi(caq+cr)=\phi(caq)>\phi(ca). \tag{26}$$

Ako bi bilo $\phi(cb)=\phi(ca)$, tada bi iz $\phi(caq)=\phi(ca)$ sledilo $q\in U(A)$, a time i $\phi(b)=\phi(aq+r)=\phi(aq)=\phi(a)$, što je u suprotnosti sa učinjenom pretpostavkom $\phi a<\phi b$. Prema tome, iz *(26)* sledi $\phi(cb)>\phi(ca)$, pa imamo i samo tvrdjenje. □

Ako je $\phi:A\to W_0$ desna euklidska valuacija domena A, tada je, prema *Teoremi 2-2*, $U_0(A)$ podtelo prstena A. Označavaćemo ga sa K. Pri tome je $K=\{a\in A:\ \phi a\leqslant\phi 1\}$. Ako je $A\neq K$, u nekoliko narednih *tvrdjenja* sa x ćemo označavati bilo koji element iz A takav da je $\phi(x)=\min\phi(A-K)$. U tom

slučaju skup $A(x,\phi)$ označavaćemo i sa V. Prema *Korolaru 2-1* $V=A(x,\phi)$ je desni K-vektorski prostor (u odnosu na operacije prstena A) i svaki element $a\in V$ ima tačno jedan desni polinomski rastav po x oblika

$$a = \alpha_0 + x\alpha_1 + \cdots + x^n\alpha_n , \tag{27}$$

pri čemu su α_ν-ovi iz K, $\alpha_n \neq 0$ za $a \neq 0$. Posle ćemo dokazati da je V i potprsten prstena A. Ako je $K[X]$ prsten polinoma po X sa koeficijentima iz tela K, neposredno se proverava da je sa

$$F(\alpha_0 + x\alpha_1 + \cdots + x^n\alpha_n) = \alpha_0 + X\alpha_1 + \cdots + X^n\alpha_n \tag{28}$$

definisan jedan izomorfizam F desnog K-vektorskog prostora $V=A(x,\phi)$ na desni K-vektorski prostor $K[X]$. Medjutim, preslikavanje F ne mora biti izomorfizam prstena $A(x,\phi)$ na prsten $K[X]$. Naime, ne mora za svako a,b iz $A(x,\phi)$ da važi

$$F(ab) = F(a)F(b), \tag{29}$$

to jest, desni polinomski rastav proizvoda ab po x ne mora biti jednak "polinomskom" proizvodu desnih polinomskih rastava od a i b po x. To će biti slučaj ako i samo ako x komutira sa svakom jednotom prstena A. □

LEMA 2-3

Neka je $\phi: A \to W$ prirodna desna euklidska valuacija domena A koja zadovoljava uslov (M) i stavimo $K = U_0(A)$, $V = A[x,\phi]$. Ako je $A \neq K$ i x bilo koji element iz A takav da je $\phi(x) = \min \phi(A-K)$, tada je sa $\sigma(0) = -\infty$ i

$$\sigma(a) = \max\{n\in N_0 : \phi a \geq \phi x^n\} \qquad (a \in V^0,\ x^0 = 1) \tag{30}$$

definisana prirodna euklidska valuacija $\sigma: A \to W$ na podskupu $A[x,\phi)$ desnog A-modula A, koja takodje zadovoljava uslov (M).

DOKAZ. Jasno je da je preslikavanje σ dobro definisano. Kako svako a iz V^0 ima tačno jedan rastav oblika *(27)* sa $\alpha_n \neq 0$, biće $\phi(a) = \phi(x^n)$, što uporedjeno sa *(30)* znači da je $\sigma(a)$ upravo "stepen" desnog polinomskog

rastava $a(x)$ od a po x (sa koeficijentima iz K). Neka je $h:\sigma(V)\to\phi(V)$ preslikavanje definisano sa: $h(-\infty)=\phi(0)$, $h(n)=\phi(x^n)$ $(n\neq-\infty)$. Tada za svako $a\in V^*$ dato sa *(27)* važi

$$\phi(a)=\phi(x^n)=h(n)=[h\circ\sigma](a), \tag{31}$$

pa je $\psi=h\circ\sigma$, pri čemu je ψ restrikcija od ϕ na V. To posebno znači da je h surjekcija. Kako prema *Lemi 1-1* niz $\phi(x^n)$, $n\in N$, strogo raste, biće to slučaj i sa funkcijom h, što sa prethodnim znači da je h izomorfizam dobro uredjenog skupa $\sigma(V)$ na dobro uredjen skup $\phi(V)$. Uz to je $\psi=h\circ\sigma$, pa kako je ψ prirodna desna euklidska valuacija na V, prema *Teoremi 1-6* biće to slučaj i sa σ. Najzad, iz $\psi=h\circ\sigma$ neposredno sledi da (zajedno sa valuacijom ψ) uslov (M) zadovoljava i valuacija σ. □

TEOREMA 2-6

Neka je simbolika iz prethodne Leme 2-3, ψ restrikcija valuacije ϕ na skup $V=A(x,\phi)$ i ∂ stepena valuacija prstena $K[x]$.

(α) Skup V je potprsten prstena A i desni euklidski parovi (V,ψ) i (V,σ) su izomorfni. Uz to valuacija σ zadovoljava i uslov (L).

(β) Ako x komutira sa svakom jednotom prstena A, tada je euklidski par (V,ψ) izomorfan euklidskom paru $(K[x],\partial)$.

(γ) Ako je prsten A komutativan, tada je $V=A$ i euklidski par (A,ϕ) je izomorfan euklidskom paru $(K[x],\partial)$.

DOKAZ. (α) Dokažimo prvo da je $\phi(ux)=\phi(x)$ za svaku jednotu u prstena A. Naime, kako je $ux\neq0$, iz $\phi(ux)<\phi(x)$ bi sledilo da je $ux\in K$, a time i $x\in K^*$, što je suprotno pretpostavci. Dakle je $\phi(ux)\geq\phi(x)$ za svako u iz K^*. Neka je $v=u^{-1}$. Ako bi bilo $\phi(ux)>\phi(x)$, tada bi prema *Lemi 2-2* bilo i $\phi(vux)>\phi(vx)$, to jest $\phi(x)>\phi(vx)$, što je u suprotnosti sa prethodnim zaključkom. Prema tome, mora biti $\phi(ux)=\phi(x)$ za svaku jednotu u prstena A. To posebno znači da je $ux\in V$ za svako $u\in K$. Otuda, ako je $\sigma(ux)=n$, biće $\phi(ux)=\phi(x^n)$, a time i $\phi(x^n)=\phi(x)$. Kako je valuacija ϕ prirodna, iz poslednje jednakosti sledi $n=1$, i prema tome $ux=x\alpha+\beta$ za neke elemente $\alpha,\beta\in K$. Na osnovu toga, indukcijom po r zaključujemo da za svako $u\in K$ i prirodan broj r važi (*) $ux^r\in V$, pa postoje δ_V-ovi iz

K takvi da je $ux^r = x^r\xi_r + \cdots + x\xi_1 + \xi_0$. Otuda, ako su $a = x^m\alpha_m + \cdots + \alpha_0$ i $b = x^n\beta_n + \cdots + \beta_0$ elementi iz V, biće $ab = x^s\lambda_s + \cdots + \lambda_0$ za neke λ_ν-ove iz K, pa je $ab \in V$, a time i V potprsten prstena A. Pri tome je $s = m+n$, to jest $\sigma(ab) = \sigma a + \sigma b$ $(a,b \in V)$, pa σ zadovoljava i uslov (L). Preostali deo tvrdjenja sledi neposredno iz *Leme 2-3*, jer je $\psi = h\circ\sigma$.

(β) Prema upravo dokazanom delu tvrdjenja, desni euklidski parovi (V,ψ) i (V,σ) su izomorfni. S druge strane, kako x komutira sa svakim elementom iz K, preslikavanje $F: A(x,\phi) \to K[X]$ dato sa *(28)* zadovoljava i *(29)*, pa je F izomorfizam prstena V na prsten $K[X]$. Uz to je $\sigma = \partial\circ F$, pa je desni euklidski par (V,σ), a time i par (V,ψ) izomorfan (desnom) euklidskom paru $(K[X],\partial)$.

(γ) S obzirom na (β), tvrdjenje će biti dokazano ako dokažemo da je $V = A$. Pretpostavimo da je $A \neq V$ i neka je y bilo koji element prstena A takav da je $\phi(y) = \min\phi(A-V)$. Tada postoje $a,b \in A$ za koje je

$$y = xa + b, \qquad \phi(b) < \phi(x). \tag{32}$$

Iz $\phi(a) < \phi(y)$ sledi $a \in V$, a time i $y = xa+b \in V$ (jer je V potprsten od A i $x,a,b \in V$), što je u suprotnosti sa učinjenom pretpostavkom. Otuda je $\phi(a) \geqslant \phi(y)$. S druge strane imamo $\phi(a) \leqslant \phi(ax) = \phi(xa) = \phi(y-b) \leqslant \phi(y)$, pa je $\phi(a) = \phi(y)$. Neka je $a = yq+c$, $\phi(c) < \phi(y)$. Tada iz *(32)* sledi da je $y(1-xq) = xc+b$ (jer je prsten A komutativan). Uz to je $1 \neq xq$, pa kako je valuacija ϕ prirodna, biće

$$\phi(xc+b) = \phi\big(y(1-cq)\big) \geqslant \phi(y). \tag{33}$$

Medjutim, to nije moguće jer je V potprsten od A pa iz $x,b,c \in V$ sleduje da mora biti $xc+b \in V$, a time i $\phi(xc+b) < \phi(y)$. Otuda i tvrdjenje. □

Neka je simbolika iz prethodne *teoreme*. Ako je ϕ i leva prirodna euklidska valuacija prstena A, slično kao pri dokazu tvrdjenja pod (γ) (jer za neko $q,c \in A$ važi i $a = qy+c$, $\phi c < \phi y$) zaključujemo da i tada važi $A = A(x,\phi)$, ali prsten A ne mora biti izomorfan prstenu $K[X]$.

Posebno, ako domen A ima bar jednu prirodnu *EUKLIDSKU* valuaciju ϕ koja zadovoljava uslov (M), tada A ima i bar jednu *KONAČNU* euklidsku

valuaciju σ koja zadovoljava uslove (M) i (L). Uz to je $\tau = 2^{\sigma}$ konačna euklidska valuacija prstena A koja zadovoljava uslove (M) i (N).

Odredimo sada pobliže strukturu prstena $V = A(x,\phi)$. Kao što smo već konstatovali prilikom dokaza *Teoreme 2-6*, za svako $u \in K$ postoje a_u i b_u iz K takvi da je

$$(34) \qquad ux = xa_u + b_u, \qquad \phi(b_u) < \phi(x).$$

Pri tome su a_u i b_u odredjeni jednoznačno sa u. Posebno je $a_u = 0$ ako i samo ako je $u=0$. Otuda su sa *(34)* i

$$(35) \qquad f(u) = a_u, \qquad \delta(u) = b_u, \qquad (u \in K)$$

definisana dva preslikavanja $f:K \to K$ i $\delta:K \to K$. Odredimo neka važnija svojstva tih preslikavanja. Pre svega je $f(K^*)$ K^*. Nadalje, za svako $u,v \in K$ je $(u+v)x = ux + vx$, $(uv)x = u(vx)$, pa na osnovu *(34)* imamo da je $xa_{u+v} + b_{u+v} = (xa_u + b_u) + (xa_v + b_v)$, $xa_{uv} + b_{uv} = xa_ua_v + b_ua_v + ub_v$, i prema tome

$$(36) \qquad f(u+v) = f(u) + (v), \qquad f(uv) = f(u)f(v),$$

$$(37) \qquad \delta(u+v) = \delta(u) + \delta(v), \qquad \delta(uv) = \delta(u)f(v) + u\delta(v).$$

Otuda je f endomorfizam tela K, dok *(37)* upravo znači da je δ takozvano (desno) *f-diferenciranje* tela K. Pri tome je $\delta(1) = 0$, $Ker(f) = \{0\}$, pa je f monomorfizam tela K.

S obzirom na *(34)* i *(35)*, potprsten $V = A(x,\phi)$ domena A je potpuno odredjen telom K, elementom x i preslikavanjima f i δ. Zato ga možemo označiti sa $K[x,f,\delta]$. Prema tome, svaki element iz $K[x,f,\delta]$ ima tačno jedan desni polinomski rastav po x sa koeficijentima iz K, i za svako u iz K važi $ux = xf(u) + \delta(u)$.

Uopšte, ako je A proizvoljan domen, $f:A \to A$ i $\delta:A \to A$ monomorfizam i desno f-diferenciranje domena A, i X *neodredjena*, tada postoji domen B koji sadrži X, kome je A potprsten, u kome svaki član ima tačno jedan desni polinomski rastav po X sa koeficijentima iz A, i pri čemu za svako $a \in A$ važi:

(38) $$aX = Xf(a) + \delta(a) .$$

Označavaćemo ga sa $B = A[X,f,\delta]$ i zvati *PRSTENOM* (f,δ)*-POLINOMA* po X sa koeficijentima iz A (*Ore*, [1]). Ako je $f=1_A$, odnosno $\delta=0$, pisaćemo samo $B=A[X,\delta]$, odnosno $B=A[X,f]$. Jasno je da se prsten $A[X,1_A,0]$ podudara sa prstenom $A[X]$ svih polinoma po X sa koeficijentima iz A. Kasnije ćemo dokazati da je $A[X,f,\delta]$ desni euklidski prsten akko je A telo, kao i da je taj prsten euklidski i sleva akko je f automorfizam tela A. Otuda i naredno tvrdjenje.

TEOREMA 2-7

Neka je simbolika iz Teoreme 2-6. Tada postoje monomorfizam $\varphi:K\to K$ i desno φ-diferenciranje $\delta:K\to K$ tela K takvi da je desni euklidski par (V,ψ) izomorfan desnom euklidskom paru (B,∂), gde je $B=K[X,f,\delta]$ i ∂ stepena valuacija prstena $K[X,f,\delta]$.

DOKAZ. Pre svega, V je potprsten prstena A i desni euklidski par (V,ψ) je izomorfan paru (V,σ). Uz to je $\psi = h\circ\sigma$. Već smo dokazali da pod datim pretpostavkama postoje monomorfizam f i (desno) f-diferenciranje δ tela K takvi da je $V=K[x,f,\delta]$. Uporedjujući *(34)* i *(35)* sa *(38)* neposredno zaključujemo da je preslikavanje F dato sa *(28)* izomorfizam domena V na domen $K[X,f,\delta]$, kao i da je $\sigma = \partial\circ F$. Otuda i tvrdjenje. □

Podsetimo se da smo sa $A(a,\phi)$ označili skup svih elemenata $c\in A$ za koje je $\phi(c) < \phi(a^{(n)})$, to jest $\phi(c) < \phi(a^n)$ za bar jedno $n\in N$. Uz simboliku i pretpostavke *Leme 2-3*, $V=A(x,\phi)$ je potprsten od A čija je struktura pobliže odredjena *Teoremama 2-6* i *2-7*. Ako, pri tome, i za element $z\in A$ važi $\phi(z) = \min \phi(A-K)$, tada je $A(z,\phi)=A(x,\phi)$. Otuda je $A(x,\phi)$ najmanji potprsten od A koji sadrži K i seče skup $\{a\in A:\ \phi a = \min \phi(A-K)\}$. Posle ćemo videti na primeru da $V=A(x,\phi)$ može biti pravi potprsten domena A.

Ako je $A\neq V$ dokazaćemo da se može sprovesti analogno rasudjivanje kao u dokazima prethodnih tvrdjenja zamenjujući u njima K sa V a x bilo kojim elementom $y\in A$ za koji je $\phi(y) = \min \phi(A-V)$. Ako je $A(y,\phi)$ pravi potprsten prstena A, proces možemo opet ponoviti, itd. Pri tom je jasno da važi $A(x,\phi) = \{c\in A:\ \phi c < \phi y\}$. Ako je $a\in A^0$ i $G_a = \{c\in A:\ \phi c<\phi a\}$, tada

je G_a podgrupa grupe $(A,+)$ za svako $a\in A^0$, ali G_a ne mora biti potprsten prstena A. Uz prethodnu simboliku to važi, npr., za $a\in\{1,x,y\}$. U vezi sa tim dokažimo prvo sledeće tvrdjenje.

LEMA 2-4

Neka je $\phi:A\to W_0$ prirodna desna euklidska valuacija domena A koja zadovoljava uslov (M) i x bilo koji element iz A-K takav da je $B=\{b\in A:\ \phi b<\phi x\}$ potprsten prstena A. Tada je $A(x,\phi)$ potprsten od A i a pripada skupu $A(x,\phi)$ akko ima tačno jedan rastav oblika

$$a=x^n a_n+\cdots+xa_1+a_0 \qquad (a_\nu\in B). \tag{39}$$

DOKAZ. Stavimo $V=A(x,\phi)$ i dokažimo prvo da svako $a\in V$ ima (bar jedan) rastav oblika *(39)*. Jasno je da to važi za $a\in B$. Ako je $a\in V-B$, tada za neki prirodan broj n važi (*) $\phi(x^n)\leqslant\phi(a)<\phi(x^{n+1})$. Uz to postoje c i a_0 iz A takvi da je $a=xc+a_0$, $\phi a_0<\phi x$. Kako ϕ zadovoljava uslov (M), iz $\phi a_0<\phi x\leqslant\phi a$ sledi (**) $\phi(xc)=\phi(a-a_0)=\phi(a)$, kao i $a_0\in B$. Ako dokažemo da je $\phi(c)<\phi(x^n)$, tvrdjenje će slediti neposredno indukcijom po n za koje važi (*). Neka je $c=x^nq+r$, $\phi(r)<\phi(x^n)$. Ako je $q\neq 0$ biće

$$\phi(x^{n+1}q)\geqslant\phi(x^{n+1})>\phi(a) \tag{40}$$

S druge strane, na osnovu *Leme 2-2* iz $\phi(r)<\phi(x^n)$ sledi $\phi(xr)<\phi(x^{n+1})$ pa kako valuacija ϕ zadovoljava i uslov (P), množeći jednakost $c=x^nq+r$ sleva sa x jedno za drugim imamo

$$\phi(xc)=\phi(x^{n+1}q+xr)=\phi(x^{n+1}q)\geqslant\phi(x^{n+1}), \tag{41}$$

to jest $\phi(xc)>\phi(a)$, što je u suprotnosti sa (**). Dakle je $q=0$, a time i $\phi(c)=\phi(r)<\phi(x^n)$. Otuda c ima rastav oblika *(39)*, pa iz $a=xc+a_0$ i $a_0\in B$ sledi da to svojstvo ima i a.

Ako je $m,n\in N_0$, tada za $m>n$ i proizvoljne elemente $p\in B^0$ i $q\in B$ važi $\phi(x^{m-n}p)\geqslant\phi(x)>\phi(q)$, a time i $\phi(x^mp)>\phi(x^nq)$ (*Lema 2-2*). Uz to ϕ zadovoljava uslov (P) pa za svako a oblika *(39)* važi $\phi(a)=\phi(x^na_n)$. To posebno znači da u *(39)* za $a=0$ svi a_ν-ovi moraju biti nule. Neka za a dato sa *(39)* važi i $a=x^nb_n+\cdots+b_0$ za neke b_ν-ove iz B. Ako stavimo

$c_\nu = a_\nu - b_\nu$, biće $0 = x^n c_n + \cdots + c_0$. No, kako je B potprsten od A, zajedno sa a_ν-ovima i b_ν-ovima biće i c_ν-ovi iz B, pa iz poslednje jednakosti sledi da mora biti $c_\nu = 0$, a time i $a_\nu = b_\nu$ za svako ν.

S druge strane, kako za $c \in B$ važi $\phi(c) < \phi(x)$, na osnovu *Leme 2-2* zaključujemo da je $\phi(x^n c) < \phi(x^{n+1})$ za svako $c \in B$ i $n \in N_0$. Otuda za svako $a \in A$ oblika *(39)* važi $\phi(a) = \phi(x^n a_n) < \phi(x^{n+1})$, i dakle $a \in A(x,\phi)$. Prema tome, $A(x,\phi)$ je upravo skup svih elemenata prstena A koji imaju (tačno jedan) desni polinomski rastav po x sa koeficijentima iz prstena B. Uz to je $A(x,\phi)$ desni B-modul u kome je $\{1,x,x^2,..\}$ jedna baza.

Najzad, dokažimo da je $V = A(x,\phi)$ potprsten prstena A, to jest da za svako $a,b \in V$ važi i $ab \in V$. Neka je prvo $a \in B$, $b = x^n$ $(n \in N)$ i stavimo $x = aq + r$, $\phi r < \phi a$. Tada je $\phi(x) = \phi(aq)$. Ako je $\phi(q) > \phi(x)$, prema *Lemi 2-2* biće $\phi(x) = \phi(aq) > \phi(ax)$, i dakle $ax \in V$. U slučaju da je $\phi q = \phi x$ stavimo $q = xu + s$, $\phi s < \phi x$. Iz $\phi(q) = \phi(x) > \phi(s)$ sledi $u \neq 0$, pa je $\phi(xu) \geq \phi(s)$, a time i $\phi(q) = \phi(xu)$, što sa $\phi(q) = \phi(x)$ daje $\phi(xu) = \phi(x)$. To znači da je u jednota prstena A, pa kako iz $\phi(s) < \phi(x)$ sledi $\phi(as) < \phi(ax) \leq \phi(axu)$ (*Lema 2-2*), biće

$$\phi(x) = \phi(aq) = \phi(axu + as) = \phi(axu) = \phi(ax), \tag{42}$$

i prema tome $ax \in V$. Na kraju, ako bi bilo $\phi q < \phi x$, i dakle $q \in B$, tada bi zajedno sa $a,q,r \in B$ bilo i $x = aq + r \in B$ (jer je B potprsten od A), što je u suprotnosti sa $x \in A-B$. Dakle je $ax \in V$ za svako $a \in B$. Pretpostavimo da za svaki prirodan broj $m < n$ važi $ax^m \in V$. Prema dokazanom delu tvrdjenje iz $ax \in V$ sledi da za neke a_ν-ove iz B važi $ax = x^k a_k + \cdots + a_0$, a time i

$$ax^n = (ax)x^m = x^k(a_k x^m) + \cdots + (a_0 x^m), \tag{43}$$

pri čemu je $m = n-1$. Kako je $a_\nu x^m \in V$, svaki od elemenata $a_\nu x^m$ ima desni polinomski rastav po x sa koeficijentima iz B, pa iz *(43)* sledi da to svojstvo ima i ax^n, što sa već dokazanim delom tvrdjenja daje $ax^n \in V$.

Neka su sada a i b proizvoljni elementi iz V. Tada za neke a_ν-ove i b_ν-ove iz B važi $a = x^m a_m + \cdots + a_0$, $b = x^n b_n + \cdots + b_0$, pa je ab suma od konačno mnogo sabiraka oblika $x^\nu(px^\kappa)q$ sa $p,q \in B$. Kako uz to svaki od px^κ-ova ima desni polinomski rastav po x sa koeficijentima iz B, biće to slučaj i sa ab. Otuda i tvrdjenje u celini. □

Neka je simbolika iz prethodne *Leme 2-4*. Dokazujući poslednji deo te *Leme* dokazali smo i da za svako $u \in B$ važi (*) $\phi(ux) \leqslant \phi(x)$. Stavimo $ux = xq+r$, $\phi r < \phi x$. Tada za $q \neq 0$ važi $\phi(x) = \phi(ux) = \phi(xq)$, pa q mora biti jednota prstena A. Otuda za svako $u \in B$ postoje (jednoznačno odredjeni) elementi $a_u \in K$ i $b_u \in B$ takvi da je

$$ux = xa_u + b_u. \tag{44}$$

To posebno znači da su sa *(44)* i $f(u) = a_u$, $\delta(u) = b_u$ $(u \in B)$ definisana dva preslikavanja $f: B \to B$ i $\delta: B \to B$. Slično kao u slučaju kada je $B = K$ zaključujemo da je f endomorfizam a δ desno f-diferenciranje prstena B pa je $A(x,\phi) = B[x,f,\delta]$. Pri tome je $f(B^0) \subset K$.

Medjutim, ostaje otvoreno pitanje da li f mora biti injekcija, to jest da li za neko $u \in B^0$ može biti $\phi(ux) < \phi(x)$. Jasno je da za $u \in K^0$ ne može biti $\phi(ux) < \phi(x)$, jer bi za $vu = 1$ bilo $\phi(x) = \phi(vux) < \phi(vx)$, što je u suprotnosti sa (*). Otuda je $K \cap Ker(f) = \{0\}$, pa je f monomorfizam za $B = K$ (što je dokazano i ranije). To važi i za svaki od potprstena B prstena A (uz simboliku *Leme 2-4*) ako je valuacija ϕ *prirodna* i sleva, to jest ako zadovoljava i uslov

$$\phi(ab) \geqslant \phi(b) \qquad (a \in A^0,\ b \in A). \tag{Ω}$$

Naime, tada za $u \in B^0$ važi $\phi(ux) > \phi(x)$, što sa (*) daje $\phi(ux) = \phi(x)$, pa u *(44)* mora biti $a_u \neq 0$ za svako $u \neq 0$. Otuda je $Ker(f) = \{0\}$, što i znači da je f monomorfizam prstena B.

Naravno da se uslovom (Ω) ne zahteva da valuacija ϕ bude euklidska i sleva. Inače, uslov (Ω) zadovoljava svaka desna euklidska valuacija ϕ koja zadovoljava neki od uslova *(N)* i *(L)*. Uz to može biti $\phi(ab) = \phi(b)$ i u slučaju kada a nije jednota prstena A (jer valuacija ϕ ne mora biti euklidska i sleva).

Ako se u *Lemi 2-4* element x zameni nekim drugim elementom $z \in A$ za koji je $\phi(z) = \phi(x)$, neposredno se proverava da je $A(z,\phi) = A(x,\phi)$. Ako je pri tom $z = xe+r$, $\phi(r) < \phi(x)$, biće $e \in K^0$ i $A(z,\phi) = K[z,g,\zeta]$, gde je $g = fe$, $\zeta = \delta e + 1_B r$. Jasno je da je g injekcija akko je to slučaj i sa f. Ako f nije injekcija tada se $r \in B$ ne može izabrati tako da je $\zeta = 0$, jer bi tada za neko $u \in B^0$ bilo $uz = 0$.

Označimo sa F familiju svih potprstena B prstena A takvih da za bar jedno $x=x(B)$ važi $B=\{a\in A:\ \phi a<\phi x\}$. Prema *Lemi 2-4* za svako $B\in F$ i $x=x(B)$ prsten $A(x,\phi)$ se ili podudara sa A, ili pripada familiji F. Ako je G lanac u (F,C), tada je unija B svih članova iz G potprsten od A za koji važi $B=A$ ili $B\in F$. Ako prsten A nije telo, tada je $X\in F$, pa u tom slučaju familija F nije prazna.

Uz prethodnu simboliku označimo sa $\tau=\tau(A,\phi)$ *tip* dobro uredjenog skupa $\phi(A^0)$ i za svaki ordinal $\alpha<\tau$ definišimo potprsten A_α prstena A na sledeći način:

(0) $A_0=K$, i dakle $A_0\in F$;

(α) Pretpostavimo da su *skupovi* A_β $(\beta<\alpha)$ već definisani i neka je $B_\alpha=\cup_{\beta<\alpha}A_\alpha$. Ako je $B_\alpha=A$ stavimo $A_\alpha=A$. Ako je $B_\alpha\neq A$ i x_α bilo koji element iz $A-B_\alpha$ za koji je $\phi(x_\alpha)=\min\phi(A-B_\alpha)$, sa A_α označimo *skup* $A(x_\alpha,\phi)$.

Naime, na osnovu *Leme 2-4* i prethodnih "komentara", transfinitnom indukcijom po α $(0\leqslant\alpha\leqslant\tau)$ neposredno zaključujemo da je A_α potprsten od A za svako α. Pri tome je τ tip od $\phi(A^0)$, pa mora biti $A_\tau=A$. Označimo sa $\eta=\eta(A,\phi)$ najmanji ordinal za koji je $A_\eta=A$. Tada je $G=\{A_\alpha:\ \alpha\leqslant\eta\}$ jedan lanac u (F,C). Uz to je i $B_\alpha\in F$ za $1<\alpha<\eta$. Ako i za z_α iz $A_\alpha-B_\alpha$ važi $\phi(z_\alpha)=\min\phi(A-B_\alpha)$, tada je $A(x_\alpha,\phi)=A(z_\alpha,\phi)$, što upravo znači da je "lanac" G potpuno odredjen domenom A i valuacijom ϕ. Inače, ako je $A_\alpha=A(x_\alpha,\phi)$, na osnovu prethodnih zaključaka postoje endomorfizam f_α i desno f_α-diferenciranje δ_α domena B_α takvi da je

$$A_\alpha=B_\alpha[x_\alpha,f_\alpha,\delta_\alpha]. \tag{45}$$

Pri tome je $f_\alpha(B_\alpha)\subset K$ za svako $\alpha\leqslant\eta$. Ako uz to ϕ zadovoljava i uslov (Ω), tada je f_α monomorfizam, a time i $f_\alpha(B_\alpha^0)\subset K^0$ za svako $\alpha\leqslant\eta$. Neka je $H=\{\alpha:\ 1\leqslant\alpha\leqslant\eta\}$ i T skup svih preslikavanja $\theta:H\to N_0$ sa svojstvom da za najviše konačno mnogo ordinala α važi $\theta(\alpha)\neq 0$, i označimo sa E skup svih "monoma" oblika

$$x[\theta]=x_\eta^{m_\eta}\cdots x_\alpha^{m_\alpha}\cdots x_1^{m_1},\qquad \theta(\alpha)=m_\alpha\ \ (\alpha\in H), \tag{46}$$

sa $\theta\in T$, to jest $E=\{x[\theta]:\ \theta\in T\}$. Tada je skup E baza desnog vektorskog prostora A nad telom K. Naime, za svako $a\in A^0$ postoji tačno jedno $\alpha<\eta$

za koje je $a \in A_\alpha - B_\alpha$. Ako je $\alpha > 0$, tada postoje (jednoznačno odredjeni) a_ν-ovi iz B_α takvi da je (*) $a = x_\alpha^n a_n + \cdots + a_0$ sa $a_n \neq 0$. Iz definicije skupa B_α sledi da za neko $\beta < \alpha$ svi a_ν-ovi pripadaju A_β, pa (indukcijom po α) neposredno zaključujemo da je E desna K-generatrisa od A. Slično se dokazuje da je skup E i K-linearno nezavisan zdesna u A.

Prema tome, svako $a \in A$ može se (na tačno jedan način) pretstaviti kao desna K-linearna kombinacija "monoma" $x[\theta]$ oblika *(46)*. Za $a \in A - K$ označimo sa $x[\theta_a]$ "vodeći monom" u toj linearnoj kombinaciji. Ako je $a \in K^0$ stavimo $\theta_a = 0$ i $x[\theta_a] = 1$. Neposredno se zaključuje da za a dato sa (*) vodeći monom $x[\theta_a]$ ima oblik

$$x[\theta_a] = x_\alpha^n \cdot\cdot x_\gamma^k, \tag{47}$$

pri čemu su ordinali $\alpha > \cdots > \gamma$ i prirodni brojevi $n, \ldots, k \in N$ jednoznačno odredjeni sa a. Pri tome je $a = x[\theta_a]e + b$ za neku jednotu e i neko b iz A takvo da je $\phi(b) < \phi(a) = \phi\left(x[\theta_a]\right)$. Neka je $\sigma: A \to T_0$ preslikavanje definisano sa

$$\sigma(a) = \begin{cases} -\infty, & a = 0 \\ \theta_a, & a \in A^0, \end{cases} \tag{48}$$

gde je $T_0 = \{-\infty\} \cup T$. Skup T je dobro uredjen u odnosu na relaciju "$<$" datu sa: $\theta < \zeta$ akko je $\theta = \zeta$ ili za neki ordinal $\beta < \eta$ važi $\theta(\beta) < \zeta(\beta)$ sa $\theta(\alpha) = \zeta(\alpha)$ za svako eventualno $\alpha > \beta$. U narednoj teoremi dokazaćemo da je $\sigma: A \to T_0$ jedna prirodna desna euklidska valuacija prstena A koja takodje zadovoljava uslov *(M)*.

Ako je $a \in A^0$ i $x[\theta_a]$ vodeći monom od a dat sa *(47)*, tada ordinal $\partial(a) = \phi(x_\alpha)n + \cdots + \phi(x_\gamma)k$ zovemo *STEPENOM* od a po $\{x_\alpha : \alpha < \eta\}$. Drugim rečima, za svako $a \in A^0$ po dogovoru stavljamo

$$\partial(a) = \Sigma_{\eta > \alpha}\, \phi(x_\alpha)\theta_a(\alpha). \tag{49}$$

Time je sa $\partial(0) = -\infty$ i *(49)* definisano jedno preslikavanje prstena A u izvestan dobro uredjen skup $\bar{W}_0$. Ako je $\eta = 1$ tada je $\partial = \sigma$ upravo stepena valuacija prstena $A = K[x, f, \delta]$. Može se dokazati da je ∂ prirodna desna euklidska valuacija prstena A i za $\eta = 2$. To važi i u opštem slučaju ako

su ordinali $\phi(x_\alpha)$ oblika ω^λ $(\lambda>0)$, što će sigurno biti ako valuacija ϕ zadovoljava i uslov (L) $\phi(ab)=\phi a+\phi b$ $(a,b\in A)$. Ako valuacija ϕ zadovoljava uslov (M), tada se bez teškoća proverava da uslov (Ω), a time i uslov (L), povlači uslov

$$(\Omega_0) \qquad \phi(a^\omega)<\phi(b) \quad \Rightarrow \quad \phi(ab)=\phi(b) \qquad (a,b\in A^0),$$

to jest $(\forall n\in N)(\phi a^n<\phi b) \Rightarrow \phi(ab)=\phi(b)$ $(a,b\in A^0)$. Pri tom je jasno da i iz uslova (Ω_0) sledi da je svaki od endomorfizama f_α prstena B_α o kojima je reč u *(45)* monomorfizam za koji važi $f_\alpha(B_\alpha^0)\subset K^0$ za svako α.

TEOREMA 2-8

Ako je $\phi:A\to W_0$ prirodna desna euklidska valuacija domena A koja zadovoljava uslov (M), tada uz prethodnu simboliku vazi:

(α) Postoji ordinal $\eta=\eta(A,\phi)$, familija elemenata x_α $(1\leqslant\alpha\leqslant\eta)$ i lanac potprstena A_α $(\alpha<\eta)$ prstena A takvi da za $B_\alpha=\cup_{\beta<\alpha}A_\beta$ vazi

$$(50) \qquad A_\alpha=A(x_\alpha,\phi), \quad A=\cup_{\alpha<\eta}A_\alpha, \quad B_\alpha=\{a\in A:\ \phi a<\phi x_\alpha\}.$$

(β) Za $1\leqslant\alpha<\eta$ postoje endomorfizam f_α i desno f_α-diferenciranje δ_α prstena B_α takvi da je $A_\alpha=B_\alpha[x_\alpha,f_\alpha,\delta_\alpha]$ i $f_\alpha(B_\alpha)\subset K$. Ako uz to valuacija ϕ zadovoljava i uslov (Ω_0), tada je f_α $(\alpha<\eta)$ injekcija.

(γ) Skup E svih monoma $x[\theta]$ $(\theta\in T)$ oblika (46) je baza desnog vektorskog prostora A nad telom K. Preslikavanje $\sigma:A\to T_0$ definisano sa (48) je desna euklidska valuacija prstena A, i desni euklidski parovi (A,ϕ) i (A,σ) su izomorfni. Ako valuacija ϕ zadovoljava i uslov (Ω_0), tada σ zadovoljava uslov $(\bar{I})$ $\sigma(ab)\leqslant\sigma a+\sigma b$ $(a,b\in A)$.

(δ) Ako je $\eta\leqslant 2$, tada je sa (49) definisana jedna desna euklidska valuacija $\partial:A\to\bar{W}_0$ prstena A koja zadovoljava uslov (L). Uz to su desni euklidski parovi (A,ϕ) i (A,∂) izomorfni. To vazi i za svaki ordinal η ako ϕ zadovoljava i uslov (L_0) $\phi(ab)\geqslant\phi a+\phi b$ $(a,b\in A^0)$.

DOKAZ. Treba još jedino dokazati tvrdjenja pod (γ) i (δ). Jasno je da je svaki element iz T oblika θ_a za neko $a\in A^0$, i dakle $\sigma(A)=T_0$. Kako

je E baza desnog K-vektorskog prostora A, za svako $a \in A^0$ vodeći monom $x[\theta_a]$ od a je odredjen jednoznačno. Uz to je $\phi(a) = \phi\left(x[\theta_a]\right)$, pa je sa

$$h(\theta_a) = \phi(a) \qquad (a \in A^0) \tag{51}$$

i $h(0) = \phi(0)$ definisano jedno preslikavanje $h: \Gamma_0 \to W_0$. Kako je pri tom $\theta_a = \sigma(a)$ $(a \in A^0)$, biće (*) $\phi = h \circ \sigma$. Dokažimo da h strogo raste, tj. da iz $\theta_a < \theta_c$ sledi $\phi\left(x[\theta_a]\right) < \phi\left(x[\theta_c]\right)$. Zaista, $\theta_a < \theta_c$ znači da za neko $\beta < \eta$ važi $\theta_a(\beta) < \theta_c(\beta)$, $\theta_a(\alpha) = \theta_c(\alpha)$ $(\alpha > \beta)$. Stavimo $\theta_a(\beta) = m$, $\theta_c(\beta) = n$. Iz $m > n$ sledi da za neki ordinal $x > 0$ važi $n = m + x$. Nadalje, kako je $\theta_a(\alpha) = \theta_c(\alpha)$ za $\alpha > \beta$, to za neko b, u, v iz A važi

$$x[\theta_a] = b x_\beta^m u, \qquad x[\theta_c] = b x_\beta^n v, \tag{52}$$

sa $\phi(u), \phi(v) < \phi(x_\beta)$. Sada iz $x > 0$ i $\phi(u) < \phi(x_\beta) < \phi(x_\beta^x v)$ sledi da mora biti (*Lema 2-2*)

$$\phi\left(b x_\beta^m \cdot u\right) < \phi\left(b x_\beta^m \cdot x_\beta^x v\right), \tag{53}$$

što sa $n = m + x$ i *(51)* upravo znači da je $h(\theta_a) < h(\theta_c)$, tj. da funkcija h strogo raste. Uz to je $\phi = h \circ \sigma$, pa su (na osnovu *Teoreme 1-6*) euklidski parovi (A, ϕ) i (A, σ) izomorfni.

Neka sada valuacija ϕ zadovoljava i uslov (Ω_0). To posebno znači da za svako $a \in B_\alpha$ i $n > 0$ važi $\phi(a x_\alpha^n) = \phi(x_\alpha^n)$. Na osnovu toga neposredno se proverava da je vodeći monom od ab jednak vodećem monomu proizvoda vodećih monoma od a i b. Uz to je jasno da za svaki monom $a = x[\theta]$ dat sa *(46)* važi (*) $\sigma(a) = \Sigma_{\eta > \alpha}\, \sigma(x_\alpha^{m_\alpha})$.

Dokažimo prvo da $(\tilde{\Sigma})$ važi za svako $a \in A$ oblika $a = x_\alpha^m$ i bilo koje b iz A. Neka je $x[\theta_b] = x_\beta^n \cdot\cdot x_\gamma^k$ $(\beta > \cdot\cdot > \gamma)$ vodeći monom od $b \in A^0$. Tada je $\phi(ab) = \phi\, x_\alpha^m x_\beta^n \cdot\cdot x_\gamma^k$. Na osnovu toga i (*) za $\alpha \geq \beta$ imamo

$$\begin{aligned} \sigma(ab) &= \sigma(x_\alpha^m) + \sigma(x_\beta^n) + \cdot\cdot + \sigma(x_\gamma^k) \\ &= \sigma(a) + \sigma(b). \end{aligned} \tag{54}$$

Ako je $\alpha < \beta$ biće $a = x_\alpha^m \in B_\beta$, pa je $\phi(ab) = \phi(b)$, a time i $\sigma(ab) = \sigma(b)$ (jer je $\phi = h \circ \sigma$ i h injekcija). Prema tome, $(\tilde{\Sigma})$ važi za svako a oblika

x_α^m i proizvoljno $b\in A$. To posebno znači da relacija $(\bar{L})$ važi za svako $a\in A_0$ i $b\in A$. Neka je $\alpha>0$ zadat ordinal i pretpostavimo da $(\bar{L})$ važi za svako $a\in B_\alpha$ i $b\in A$, pa dokažimo da važi i za svako $a\in A_\alpha-B_\alpha$ i $b\in A$. Iz $a\in A_\alpha-B_\alpha$ sledi da je vodeći monom od a oblika $x[\theta_a]=x^m c$ za neko c iz B_α. Pri tome je $\sigma(a)=\sigma(x_\alpha^m)+\sigma(c)$. Označimo sa $z=x[\theta_b]$ vodeći monom od b. Tada je $\sigma(b)=\sigma(z)$. Uz to ab i $x_\alpha^m cz$ imaju iste vodeće monome pa je $\sigma(ab)=\sigma(x_\alpha^m cz)$. Kako je $c\in B_\alpha$, na osnovu induktivne pretpostavke važi $\sigma(cz)\leqslant\sigma(c)+\sigma(z)$, pa prema dokazanom delu tvrdjenja imamo da je

$$\sigma(ab)=\sigma(x_\alpha^m cz)\leqslant\sigma(x_\alpha^m)+\sigma(cz)\leqslant\sigma(x_\alpha^m)+\sigma(c)+\sigma(z)\,, \tag{55}$$

i prema tome $\sigma(ab)\leqslant\sigma a+\sigma b$. Otuda i tvrdjenje. Pri tome u $(\bar{L})$ ne mora da važi jednakost. Tako, na primer, ako je $\eta>2$, tada iz $\phi(x_1)<\phi(x_2)$ sledi $\phi(x_1x_2)=\phi(x_2)$, a time i $\sigma(x_1x_2)=\sigma(x_2)=(0,1)<\sigma(x_1)+\sigma(x_2)$.

Najzad, dokažimo i tvrdjenje pod (δ). Neka je $v=x_\beta^{n_\beta}\cdot\cdot x_1^{n_1}$ vodeći monom nekog elementa $b\in A^0$. Tada za proizvoljne ordinale $\alpha>\beta>\cdot\cdot>1$ važi $v\in B_\alpha$, pa kako ϕ zadovoljava uslov (L_0) biće

$$\phi(x_\alpha)>\phi(v)\geqslant(\phi x_\beta)n_\beta+\cdot\cdot+(\phi x_1)n_1\,. \tag{56}$$

Na osnovu toga neposredno se zaključuje da preslikavanje $g:\sigma(A)\to\partial(A)$ definisano sa $g(\theta)=\Sigma_{\eta>\alpha}\phi(x_\alpha)\theta(\alpha)$ $(\theta\in T)$, $g(-\infty)=-\infty$, strogo raste. Kako smo već dokazali da je σ desna euklidska valuacija prstena A, iz $\partial=g\circ\sigma$ i *Teoreme 1-6* sledi da je to slučaj i sa ∂, kao i da su desni euklidski parovi (A,σ) i (A,∂) izomorfni. Dalje, vodeći monom u svakog elementa $a\in A^0$ može se pretstaviti u obliku $u=wc$, pri čemu je $c\in B^0$ i

$$w=x_\eta^{m_\eta}\cdot\cdot x_\beta^{m_\beta}\,, \tag{57}$$

uz mogućnost da je $m_\beta=0$. Kako iz $c\in B_\beta$ sledi $\phi(cx_\beta)\leqslant\phi(x_\beta)$, a iz (L_0) $\phi(cx_\beta)\geqslant\phi c+\phi x_\beta\geqslant\phi x_\beta$, biće $\phi(cx_\beta)=\phi(x_\beta)$, pa za neko $e\in K^0$ i $r\in B_\beta$ važi $cx_\beta=x_\beta e+r$. Otuda je v vodeći monom i od cv, pa iz *(57)* i $u=wc$ sledi da je $x[\theta_{uv}]=wv$. Jasno je da je tada $(**)$ $\partial(ab)=\partial(uv)=\partial w+\partial v$, to jest $\partial(ab)=\partial(w)+\partial(v)$. S druge strane, iz (56) sledi da za svako $b\in B_\alpha$ važi $\partial(b)\leqslant\phi(b)<\phi(x_\alpha)$, pa je $\partial c+\phi x_\beta\leqslant\phi c+\phi x_\beta\leqslant\phi(cx_\beta)=\phi x_\beta$, i prema tome $\partial c+\partial v=\partial v$ (jer je ∂v oblika $\phi x_\beta+\lambda$). Na osnovu toga imamo da je

$\partial u + \partial v = \partial w + \partial c + \partial v = \partial w + \partial v$, što uporedjeno sa (**) daje $\partial(ab) = \partial a + \partial b$ $(a,b \in A)$, pa ∂ zadovoljava i uslov (Σ). Otuda i tvrdjenje u celini. □

U vezi sa prethodnom *teoremom* prirodno se nameće pitanje da li za svaki ordinal $\lambda > 0$ postoji desni euklidski par (A,ϕ) sa svojstvom da za $\lambda = \eta$ važe tvrdjenja pod (α) i (β). Neka je $\eta > 0$ proizvoljan ordinal, D domen, $X = \{X_\alpha : 1 \leqslant \alpha < \eta\}$ uredjena familija *neodredjenih* i $\{A_\alpha : 0 \leqslant \alpha < \eta\}$ lanac prstena "oblika":

(0) $A_0 = D$,

(α) Ako je $B_\alpha = \cup_{\beta<\alpha} A_\beta$, tada je $A_\alpha = B_\alpha[X_\alpha, f_\alpha, \delta_\alpha]$, gde su, kao i obično, f_α i δ_α endomorfizam i desno f_α-diferenciranje prstena B_α. ¤

Stavimo $A = A_\eta$, $F = \{f_\alpha : 1 \leqslant \alpha < \eta\}$ i $\Phi = \{\delta_\alpha : 1 \leqslant \alpha < \eta\}$. Tada sam prsten A zovemo *PRSTENOM* (F,Φ)*-POLINOMA* po X sa koeficijentima u D. Možemo ga označiti sa $A = D[X,F,\Phi]$. Ako je $\Phi = 0$, tada je u prstenu $D[X,F]$ svaki desni ideal glavni ako i samo ako je u prstenu $D = A_0$ svaki desni ideal glavni i ako za svako $1 \leqslant \alpha < \eta$ važi $f_\alpha(B_\alpha^0) \subset U(D)$ (*JATEGAONKAR*, [1]). Ako je uz to D telo i $f_\alpha(B_\alpha^0) \subset D^0$ za $\alpha < \eta$, tada je sa (48) definisana jedna desna euklidska valuacija σ prstena $A = D[X,F,0]$. S druge strane, prema *JATEGAONKAR*, [1], *Teorema 3-1*, za svako telo K i ordinal η postoji telo D kome je K podtelo i za koje, uz prethodnu simboliku, važi $f_\alpha(B_\alpha^0) \subset D^0$ $(\alpha < \eta)$, što sa prethodnim daje potvrdan odgovor na postavljeno pitanje.

Inače, klasa prstena tipa $D[X,F,\Phi]$ je izvor mnogih važnih primera i kontraprimera u teoriji nekomutativnih prstena. Tako, na primer, uz prethodnu simboliku, za svaki ordinal $\eta > 0$ postoji desni glavnoidealski domen $A = D[X,F]$ takav da za njegov Jacobson-ov radikal J važi $J^\eta \neq \{0\}$ (*JATEGAONKAR*, [1], *1969*), što predstavlja negativan odgovor na poznatu Jacobson-ovu hipotezu da za radikal J proizvoljnog desnog neterovskog domena važi $J^\omega = \{0\}$. Pri tome potenciju J^α definišemo induktivno po α sa $J^1 = J$, $J^\alpha = J^\beta \cdot J$ za $\alpha = \beta + 1$, i $J^\alpha = \cap_{\beta<\alpha} J^\beta$ ako je α granični ordinal. Štaviše, tu D može biti i telo pa na osnovu prethodnog zaključujemo da Jacobson-ova hipoteza ne važi ni za desne euklidske domene.

Poslednjim trima *teoremama* su opisani svi domeni A koji imaju bar jednu desnu euklidsku valuaciju $\phi : A \to W_0$ koja zadovoljava uslov (M). Pri tome W može biti bilo koji dobro uredjen skup. Slučaj kada je $W = N_0$ i

pod pretpostavkom da valuacija ¢ uz uslov (*M*) zadovoljava i uslov (*L*) razmatrali su *JACOBSON* [*1*], i nezavisno *COHN* [*1*]. Uz simboliku *Teorema 2-7* i *2-8*, pod tim pretpostavkama važi $A = A(x,\phi)$, $\phi = \partial$ i $\eta = 1$. Dalje, ako je valuacija ϕ euklidska i sleva, tada je ona *konačna*, i dakle $\eta = 1$. To posebno važi ako je domen A komutativan. □

Razmotrimo sada pobliže klasu svih prstena A koji imaju bar jednu desnu euklidsku valuaciju $\phi: A \to W$ koja zadovoljava uslov (*T*) i neki od uslova (*N*) i (*Z*). Pri tome ćemo se prvo ograničiti na slučaj kada je kodomen valuacije ϕ skup N_0. Prema tome, u nekoliko narednih tvrdjenja ϕ će nam označavati desnu euklidsku valuaciju nekog prstena A, čiji je kodomen N_0 i koja zadovoljava uslov

(*T*) $$\phi(a+b) \leqslant \phi(a) + \phi(b) \qquad (a,b \in A).$$

Klasa N_0 svih prstena A koji imaju bar jednu desnu euklidsku valuaciju $\phi: A \to N_0$ koja zadovoljava uslove (*T*) i (*N*) sadrži klasu M_0 svih domena A sa bar jednom konačnom desnom euklidskom valuacijom koja zadovoljava uslov (*M*). Naime, prema *Teoremi 2-7* svaki domen A iz M_0 ima bar jednu desnu euklidsku valuaciju ∂ koja uz uslov (*M*) zadovoljava i uslov (*L*), pa tada valuacija $\psi = 2^{\partial}$ zadovoljava uslove (*T*) i (*N*). Dalje, sa ν ćemo označavati standardnu euklidsku valuaciju prstena Z.

TEOREMA 2-9

Ako je $\phi: A \to N_0$ desna euklidska valuacija prstena A koja zadovoljava uslove (T) i (N), tada za $K = V_0(A)$ važi:

(α) Ako je K podtelo prstena A, tada je ili $A = K$, ili je, za neki monomorfizam f i desno f-diferenciranje ∂ tela K, desni euklidski par (A,ϕ) izomorfan desnom euklidskom paru (B,∂), gde je ∂ stepena valuacija prstena $B = K[X,f,\delta]$.

(β) Ako K nije podtelo od A, tada je (desni) euklidski par (A,ϕ) izomorfan euklidskom paru (Z,ν).

DOKAZ. (α) Pre svega, iz pretpostavke da ϕ zadovoljava uslov (*N*) sledi

da je A domen, da je valuacija ϕ prirodna, kao i da je $\phi 1 = 1$. Uz to je K podtelo domena A, pa na osnovu *Teoreme 2-2* valuacija ϕ zadovoljava i uslov (M). Otuda su zadovoljene pretpostavke *Teoreme 2-7*. Kako je pri tome valuacija ϕ konačna, biće $A(x,\phi) = A$, pa tvrdjenje sledi direktno iz pomenute *Teoreme 2-7*.

(β) Kako K nije podtelo prstena A, zbir $u+v$ bar dve jednote $u,v \in K$ prstena A nije u K. Otuda je $\phi(u+v) > 1$, što sa $\phi(u+v) \leqslant \phi u + \phi v = 1+1 = 2$ daje $\phi(u+v) = 2$. Kako za $e = u^{-1}v \in K$ važi $u+v = u(1+e)$, i kako uz to ϕ zadovoljava uslov (N), biće $2 = \phi(u+v) = \phi(u)\phi(1+e) = \phi(1+e)$. To posebno znači da za bar jednu jednotu $e \in K^0$ važi $\phi(e) = 2$. Za takvo $e \in K$ stavimo

$$a = 1+e, \qquad b = 1-e, \qquad c = 1+e^2. \tag{58}$$

Tada iz $\phi(a) = 2$ sledi $\phi(a^2) = \phi(a)\phi(a) = 4$, $\phi(c) \leqslant \phi(1) + \phi(e^2) = 2$. Kako je $a^2 = c + 2e$, biće $\phi(a^2) = \phi(c+2e) \leqslant \phi(c) + \phi(2\cdot e)$, što sa prethodnim i $\phi(2e) = \phi(e+e) \leqslant 2$ daje $\phi(c) = 2$, $\phi(2e) = 2$. Dalje, za svako $u \in K^0$ važi $2\cdot u = 2ev$ sa $v = e^{-1}u$, pa je $\phi(2u) = \phi(2e)\phi(v)$, i prema tome

$$\phi(2u) = 2, \qquad (u \in K^0). \tag{59}$$

Posebno je $\phi(1+1) = \phi(2\cdot 1) = 2$, i dakle $1+1 \neq 0$, a time i $1 \neq -1$. Dokažimo da su 1 i -1 jedine jednote prstena A. U tu svrhu, za proizvoljno $e \in K^0$ označimo sa a,b,c elemente iz A date sa *(58)*. Tada iz $ab = 1-e^2$ sledi $\phi(a)\phi(b) = \phi(ab) = \phi(1-e^2) \leqslant 2$, i dakle $\phi a \leqslant 2$ ili $\phi b \leqslant 2$. Dokažimo da je $a=0$ ili $b=0$. Zaista, ako bi bilo $\phi a = \phi b = 1$, tada bi iz $a^2-b^2 = (2\cdot 1)^2 e$ i *(59)* sledilo

$$4 = \phi(4e) = \phi(e^2-b^2) \leqslant \phi a^2 + \phi b^2 = 2, \tag{60}$$

što je nemoguće. Pretpostavimo zato da je $\phi a = 2$. U tom slučaju mora biti $\phi b \leqslant 1$. S druge strane, iz $a^2 = c+2e$ sledi $4 \leqslant \phi c + 2$, što sa $\phi c \leqslant 2$ daje $\phi c = 2$. Kako je $abc = 1-e^4$, biće $(\phi a)(\phi b)(\phi c) = \phi(1-e^4) \leqslant 2$, što sa $\phi a = 2$ i $\phi c = 2$ daje $4\phi(b) \leqslant 2$, i prema tome $b = 0$. Slično iz $\phi b = 2$ sledi da je $a=0$. Na osnovu toga i *(58)* zaključujemo da za svaku jednotu e prstena A važi $e = 1$ *ili* $e = -1$, i dakle

$$K^0 = \{-1,1\}, \qquad K = \{-1,0,1\}. \tag{61}$$

Dokažimo sada da za svaki prirodan broj n važi $\phi(n\cdot 1)=n$. Za $n=2$ to smo već dokazali. Pretpostavimo da tvrdjenje važi za svaki prirodan broj $<n$ ($n>1$ zadat prirodan broj) pa dokažimo da važi i za n. U slučaju da je $n=pq$ složen broj biće $n\cdot 1=(p\cdot 1)(q\cdot 1)$, pa zbog $p<n$ i $q<n$ važi $\phi(n\cdot 1)=\phi(p\cdot 1)\phi(q\cdot 1)=pq=n$.

Neka je sada $n>2$ prost broj i pretpostavimo da je $\phi(n\cdot 1)\neq n$. Tada za neke prirodne brojeve $p,q<n$ važi $n-1=2p$ i $n+1=2q$. Uz dogovor da $m\in N$ u prstenu A ima značenje sume $m\cdot 1$ od m jedinica, na osnovu induktivne pretpostavke iz $p,q<n$ sledi $\phi(p)=p$, $\phi(q)=q$. Dalje, jasno je da $p\cdot 1$ i $q\cdot 1$ pripadaju centru prstena A, pa u prstenu A važi $n^2-1=4pq$. Uz to je $\phi 4=(\phi 2)(\phi 2)=4$ i $\phi(n\cdot 1)=\phi(1+\cdots+1)<n$, što sa prethodnim daje

$$(62)\qquad (\phi 4)(\phi p)(\phi q)=\phi(n^2-1)\leq 1+\phi n^2<1+(n-1)^2,$$

to jest $4pq=n^2-1<1+(n-1)^2$ (u prstenu Z), a to nije moguće. Dakle je $\phi(n\cdot 1)=n$ za svaki prirodan broj n, a time i $\phi(m\cdot 1)=|m|$ $(m\in Z)$. Otuda je prsten A karakteristike 0.

Najzad, dokažimo da je svaki element $a\in A$ oblika $m\cdot 1$ za neki ceo broj m. Štaviše, ako je $\phi a=n$ tada je $a=n1$ ili $a=(-n)1$. Zaista, za $n=1$ tvrdjenje sledi iz (61). Neka je $n>1$ fiksiran prirodan broj i pretpostavimo da tvrdjenje važi za svako $a\in A$ takvo da je $\phi a<n$. Uz to je $n\cdot 1\neq 0$, pa postoje $q,r\in A$ takvi da je

$$(63)\qquad a=(n\cdot 1)q+r,\qquad \phi(r)<\phi(n1)=n.$$

Kako je $\phi r=s<n$, prema induktivnoj pretpostavci je $r=s1$ ili $r=-s1$. S druge strane, u prstenu A važi $\phi(nq)=(\phi n)(\phi q)=n(\phi q)$, pa $nq=a-r$ daje $n(\phi q)=\phi(a-r)\leq \phi a+\phi r=n+s$, i dakle

$$(64)\qquad n(\phi q-1)\leq s.$$

Kako je $s<n$, iz (64) sledi da mora biti $\phi q\leq 1$. Pri tome ne može biti $\phi q=0$, jer bi tada iz $q=0$ sledilo $a=r$, i dakle $\phi a=n>\phi r$, što se kosi sa (63). Otuda je $\phi q=1$, pa iz (64) i $s=\phi r$ sledi da je $r=0$. Dalje, iz $\phi q=1$ sledi $q\in K^0$, pa na osnovu (61) imamo $q=1$ ili $q=-1$, što zajedno sa $r=0$ i (63) daje $a=n\cdot 1$ ili $a=-n\cdot 1$, za čime se i išlo. To znači da je sa $F(m)=m\cdot 1$ $(m\in Z)$ definisan jedan izomorfizam F prstena Z na prsten

A. Kako je uz to $\phi \circ F = \nu$, biće i (desni) euklidski par (A,ϕ) izomorfan euklidskom paru (Z,ν). Otuda i tvrdjenje u celini. □

TEOREMA 2-10

Neka je $\phi: A \to N_0$ prirodna desna euklidska valuacija prstena A koja zadovoljava uslove (I) i (Z). Ako je $\phi 1 = 1$ i $K = U_0(A)$, tada važi:

(α) Ako K nije podtelo od A, tada je (desni) euklidski par (A,ϕ) izomorfan euklidskom paru (Z,ν).

(β) Ako je K podtelo od A sa bar tri elementa, tada je $A = K$ telo.

(γ) Ako je K dvočlano podtelo prstena A, a valuacija ϕ prirodna i sleva, tada je ili $A = K$, ili je prsten A izomorfan prstenu $B = K[X]$. Pri tome euklidski parovi (A,ϕ) i (B,∂) nisu izomorfni.

DOKAZ. (α) Pre svega, iz uslova (Z) sledi da je A oblast celih. Kako K nije podtelo prstena A, za bar dve jednote $u, v \in K^0$ važi $u+v \notin K$, što sa $\phi(u+v) \leqslant \phi u + \phi v = 2$ daje $\phi(u+v) = 2$. Stavimo $e = vu^{-1}$ i

$$a = 1+e, \qquad b = 1-e, \qquad c = 1+e^2. \tag{65}$$

Tada je $\phi b \leqslant 2$, $\phi c \leqslant 2$ i $2 = \phi(u+v) = \phi\big((1+e)u\big) = \phi(1+e) = \phi a$. Dokažimo da je $\phi(2e) = 2$. Svakako je $\phi(2e) = \phi(e+e) \leqslant 2$. Dalje, iz $\phi(2e) = 0$ sledi da je $2e = 0$, i dakle $a^2 = 1+e^2$, a time i $\phi a^2 \leqslant 2$. No, to nije moguće jer zbog $\phi a > \phi 1$ niz ϕa^n $(n \in N)$ strogo raste (*Lema 1-1*) pa je $\phi a^2 > \phi a = 2$. Dakle je $\phi(2e) > 1$. Dokažimo da ne može biti ni $\phi(2e) = 1$. Naime, u suprotnom bi iz $a^2 = c+2e$ i $\phi a^2 > 2$ sledilo

$$3 \leqslant \phi a^2 = \phi(c+2e) \leqslant 1+\phi c, \tag{66}$$

što sa $\phi c < 2$ daje $\phi c = 2$. Kako je $acb = 1-e^4$, biće $\phi(acb) \leqslant \phi 1 + \phi e^4 = 2$ (jer je i $e^4 \in K^0$). Ako bi bilo $\phi(acb) = 1 = \phi(1)$, tada prema uslovu (Z) za neko $u \in K^0$ važi $acb = 1 \cdot u$, a time i $a \in K^0$, što je u suprotnosti sa $\phi a = 2$. Slično iz $\phi(acb) = 2 = \phi(a)$ sledi da za neko $u \in K^0$ važi $acb = au$, a time i $cb = u$, to jest $c \in K^0$, što se kosi sa $\phi c = 2$. Najzad, ako bi bilo $\phi(acb) = 0$, to jest $acb = 0$, tada bi iz $ac \neq 0$ sledilo $b = 0$, a time i $e = 1$. Medjutim, to nije moguće jer bi tada bilo $2 = \phi a = \phi(1+1) = \phi(2 \cdot 1)$,

što je suprotno učinjenoj pretpostavci $\phi(2e)=1$. Prema tome, za uočenu jednotu $e\in K^0$ važi $\phi(2e)=2$.

Dokažimo da je $\phi(2u)=2$ za sveko $u\in K^0$. Naime, ako je $v=u^{-1}e$ biće i $v\in K^0$, pa uslov (z) daje $\phi(2u)=\phi(2uv)=\phi(2e)=2$. To posebno znači da za $x=1+1=2\cdot 1$ važi $\phi x=2=\min\phi(A-K)$. Dokažimo da mora biti $\phi x^2=4$. Zaista, prvo je $\phi x^2=\phi(4\cdot 1)=\phi(1+1+1+1)<4$, što zajedno sa $\phi x^2>\phi x=2$ daje $\phi x^2\geqslant 3$. Otuda je $\phi x^2=4$ ili $\phi x^2=3$. Sddruge strane, uz dogovor da u prstenu A umesto $m1$ pišemo samo m, imamo da je $x^2=4$. Pri tome je $\phi(3)\leqslant 3$. Kako iz $\phi 3\leqslant 1$ sledi $\phi x^2=\phi 4=\phi(3+1)\leqslant 1+1=2$, zaključujemo da mora biti $\phi 3\geqslant 2$. No, ako bi bilo $\phi 3=2=\phi 2$, tada bi, prema uslovu (z), postojala jednota $u\in K^0$ takva da je $3=2u$, to jest $1=x(u-1)$, što nije moguće jer $x\in K^0$. Dakle je $\phi(3\cdot 1)=3$. Analogno zaključujemo da ne može biti $\phi 4=3=\phi 3$, pa je $\phi x^2=4$.

Dokažimo sada da je $K^0=\{-1,1\}$, to jest da prsten A ima samo dve jednote. Pre svega, iz $1+1=2\cdot 1\neq 0$ sledi da je $-1\neq 1$. Za proizvoljno e iz K^0 stavimo: $a=1+e$, $b=1-e$, $c=1+e^2$. Dokazaćemo da je $a=0$ v $b=0$, a time i $e=-1$ ili $e=1$. Naime, prvo je $\phi a\leqslant 2$, $\phi b\leqslant 2$, $\phi c\leqslant 2$. Kako je još

$$\phi(a^2-b^2)=\phi(4e)=\phi(4\cdot 1)=4, \tag{67}$$

kao i $\phi(a^2-b^2)\leqslant \phi a^2+\phi b^2$, zaključujemo da ne može biti $\phi a=\phi b=1$. Ako je $\phi a=\phi b=2$, tada prema uslovu (z) za neko $u\in K^0$ važi $b=au$, a time i $1-e^2=ab=a^2u$. To znači da je $\phi a^2=\phi(a^2u)=\phi(1-e^2)<2$, što je nemoguće jer iz $\phi a=2>\phi 1$ sledi $\phi a^2>\phi a=2$. Najzad, pretpostavimo da je $\phi a=2$ i $\phi b>1$. Tada za neko $u\in K^0$ važi $a=2u$, pa je $\phi a^2=\phi(4u^2)=\phi(4\cdot 1)=4$ i prema tome

$$4=\phi a^2=\phi(c+2e)\leqslant \phi c+\phi(2e)=2+\phi c. \tag{68}$$

Otuda je $\phi c\geqslant 2$, a time i $\phi c=2$. S druge strane je $\phi(acb)=\phi(1-e^4)\leqslant 2$. Iz $\phi(acb)=2=\phi a$ i uslova (z) sledi da za bar jednu jednotu $u\in K^0$ važi $acb=au$, to jest $cb=u$, i dakle $c\in K^0$, što se kosi sa $\phi c=2$. Slično iz $\phi(acb)=1$ sledi $1\geqslant\phi a$, što je u suprotnosti sa $\phi a=2$. Otuda sledi da mora biti $\phi(acb)=0$, to jest $acb=0$, pa $ac\neq 0$ daje $b=0$, a samim tim i $e=1$. Slično iz $\phi a\leqslant 1$ i $\phi b=2$ sledi da je $e=-1$, pa je $K^0=\{-1,1\}$.

Prsten A je karakteristike $p=0$. Naime, prvo iz $2\cdot 1\neq 0$ sledi da

je $p \neq 2$. Pretpostavimo da je $p>2$. Tada je $x = 1+1 = 1^p + 1^p = (1+1)^p = x^p$, tj. $x^s \cdot x = 1$ (sa $s=p-2$), i dakle $x \in K^0$, a to nije. Dakle je $p=0$. Otuda u prstenu A za svaki ceo broj m važi $m1 = 0 \iff m = 0$.

Dalje, prema uslovu (Z) za $m,n \in Z$ je $\phi(m1) = \phi(n1)$ akko je $m1 = nu$ za neku jednotu $u \in K^0$, i dakle akko je $m1=n1$ ili $m1=-n1$, što zajedno sa prethodnim daje $\phi(m1) = \phi(n1) \iff (m=n \vee m=-n)$. Dokažimo da za svaki prirodan broj n važi (**) $\phi(n1) = n$. Za $n=1,2$ to je već dokazano. Pretpostavimo da tvrdjenje važi za svaki prirodan broj $<n$ ($n>2$ fiksiran prirodan broj). Kako je $\phi(n1) = \phi(1+\cdots+1) \leqslant n$, iz $\phi(n1) \neq n$ sledi da je $\phi(n1) \leqslant n-1$. Stavimo $\phi(n1) = k$. Tada je $k<n$, pa važi $\phi(k1) = k$. Otuda je $\phi(n1) = \phi(k1)$, a time i $n=k$, što je u suprotnosti sa $k<n$. Prema tome, ne može biti $\phi(n1) < n$, pa je $\phi(n1) = n$. Jasno je da tada za svaki ceo broj m važi $\phi(m1) = |m|$.

Najzad, neka je a proizvoljan element prstena A i stavimo $\phi a = n$. Kako je i $\phi(n1) = n$, biće $\phi(a) = \phi(n1)$, pa za neku jednotu $u \in K^0$ prstena A važi $a = nu$, i dakle $a = n1$ ili $a = -n1$. Otuda je sa $F(m) = m1$ $(m \in Z)$ definisan jedan izomorfizam F prstena Z na prsten A. Kako uz to važi i $\phi \circ F = \nu$, biće i (desni) euklidski parovi (Z,ν) i (A,ϕ) izomorfni. Otuda i tvrdjenje.

(β) Neka je sada K podtelo prstena A sa bar tri člana. To posebno znači da prsten A ima bar dve različite jednote, na primer 1 i e. Ako je $A = K$ stvar je gotova. Zato pretpostavimo da je $A \neq K$ i označimo sa x bilo koji element iz A takav da je $\phi x = \min \phi(A-K)$. Kako ϕ zadovoljava uslov (T) biće (*) $\phi(1+x) \leqslant 1 + \phi x$.

Pretpostavimo da je $\phi(1+x) = \phi(x)$. Tada, prema uslovu (Z), za neku jednotu $u \in K^0$ važi $1+x=xu$, to jest $x(u-1) = 1$, i dakle $x \in K^0$, što je u suprotnosti sa $x \in A-K$. Dalje, iz $\phi(1+x) < \phi(x)$ sledi $\phi(1+x) \leqslant \phi(1)$, to jest $1+x \in K$, što nije moguće jer bi tada bilo i $x \in K$. Prema tome mora biti $\phi(1+x) \geqslant \phi(x)$, što sa (*) daje $\phi(1+x) = 1 + \phi x$. Jasno je da se tu x može zameniti sa xv za proizvoljno $v \in K^0$. Otuda za $u \in K^0$ i $v = u^{-1}$ važi

$$\phi(u+x) = \phi\big((1+xv)u\big) = \phi(1+xv) = 1+\phi(xv), \tag{69}$$

i dakle (**) $\phi(u+x) = 1 + \phi x$ $(u \in K^0)$. Ako u (**) zamenimo $u=1$ i $u=e$ biće $\phi(1+x) = \phi(e+x)$, pa za neku jednotu $v \in K^0$ važi $e+x = (1+x)v$, što možemo

zapisati i u obliku $x(1-v)=v-e$. Pri tom iz $1\neq e$ sledi da ne može biti $v=1$, pa je $v-e\in K^0$. No, tada iz poslednje jednakosti sledi $x\in K^0$, što je u suprotnosti sa $x\in A-K$. Prema tome, mora biti $A-K=\Theta$, pa je A telo.

(γ) Pre svega, iz $K^0=\{1\}$ i uslova (Z) sledi da je ϕ injekcija, a iz $1+1=0$ da je karakteristika prstena A jednaka 2. Ako je $A=K$, stvar je gotova. Zato pretpostavimo da je $A\neq K$ i neka je x bilo koji element iz $A-K$ za koji je $\phi x=\min\phi(A-K)$. Tada je $\phi x>\phi 1=1$, pa niz ϕx^n $(n\in N)$ strogo raste. Slično kao u dokazu tvrdjenja pod (β) zaključujemo da je

$(*)$ $\phi(1+x)=1+\phi x$.

Dokažimo da svaki element $a\in A$ ima tačno jedan (desni) polinomski rastav $a=a_0+\cdots+x^n a_n$ po x sa koeficijentima iz K. Dokaz ćemo izvesti indukcijom po $n=\phi a$. Jasno je da to važi za $n<\phi x$. Zato pretpostavimo da tvrdjenje važi za svako $a\in A$ za koje je $\phi a<n$, gde je $n\geqslant\phi(x)$ zadat prirodan broj, i neka je a bilo koji član iz A takav da je $\phi a=n$. Tada za neko $c,r\in A$ važi $a=xc+r$, $\phi r<\phi x$. Iz $\phi r<\phi x$ sledi $r\in K$. Kako je uz to valuacija ϕ prirodna i sleva, biće

$$(70)\qquad \phi c\leqslant\phi(xc)=\phi(a-r)\leqslant\phi a+\phi r\leqslant 1+\phi a.$$

Pri tome ne može biti $\phi c=\phi(xc)$. Naime, u suprotnom bi bilo $c=xc$ (jer je ϕ injekcija), a time i $1=x$. Otuda je $\phi c\leqslant\phi(xc)<1+\phi a$, i prema tome $\phi c\leqslant\phi a$. Pretpostavimo da je $\phi c=\phi a$. Tada je $c=a$, što zajedno sa $a=xc+r$ daje $r=(1-x)a$, a time i $\phi r\geqslant\phi a$ Medjutim, to nije moguće jer je prema prethodnom $\phi r<\phi x\leqslant\phi a$. Dakle je $\phi c<\phi a$. To posebno znači da je $\phi c<n$, pa na osnovu induktivne pretpostavke c ima polinomski rastav traženog oblika. Jasno je da tada iz $a=xc+r$ i $r\in K$ sledi da to važi i za a. Uz to je K podtelo domena A i $x\in A-K$ pa se neposredno dokazuje da je skup $\{x^n:\ n\in N_0\}$ jedna baza desnog K-vektorskog prostora A. Otuda svako a iz A ima tačno jedan polinomski rastav po x sa koeficijentima u telu K.

Kako 1 komutira sa svakom potencijom od x, na osnovu prethodnog neposredno zaključujemo da je sa $F(a_0+\cdots+x^n a_n)=a_0+\cdots+X^n a_n$ definisan jedan izomorfizam F prstena A na prsten $B=K[X]$.

Medjutim, euklidski parovi (A,ϕ) i (B,∂) nisu izomorfni. Naime, u suprotnom bi postojao neki izomorfizam (f,h) euklidskog para (A,ϕ) na euklidski par (B,∂). To posebno znači da je $\partial\circ f=h\circ\phi$. Naravno, tu je f

izomorfizam prstena A na B, a h monomorfizam dobro uredjenog skupa ϕA na dobro uredjen skup ∂B. Kako x nije jednota u A, to ni $P=f(x)$ nije jednota u prstenu B, pa je $\partial(P)>0$. Otuda je $\partial(1+P)=\partial(P)$. Zamenjujući tu P sa $f(x)$ dobijamo $(\partial\circ f)(1+x)=(\partial\circ f)(x)$, što sa $\partial\circ f=h\circ\phi$ daje $(h\circ\phi)(1+x)=(h\circ\phi)(x)$, a time i $\phi(1+x)=\phi(x)$. Medjutim, to nije moguće jer iz (*) sledi $\phi(1+x)>\phi(x)$. Otuda i tvrdjenje u celini. □

Naredni *Primer 2-1* pokazuje da postoji euklidski par (A,ϕ) u kome važe uslovi tvrdjenja pod (γ) sa $A\neq K$. Pri tome, ostatak i količnik pri ϕ-deljenju u prstenu A nisu odredjeni jednoznačno. Tako, na primer, uz prethodnu simboliku imamo da je

$$(71)\qquad x^2=(x+1)(x+1)+1,\qquad x^2=(x+1)x+1,$$

sa $\phi 1<\phi(x+1)$ i $\phi x<1+\phi x=\phi(x+1)$. Ostaje otvoreno pitanje da li tvrdjenje pod (γ) važi i bez pretpostavke da je valuacija $\phi:A\to N_0$ prirodna i sleva, tj. da za $a\in A^0$ i $b\in A$ važi $\phi(ab)\geqslant\phi(b)$, a time i pitanje da li postoji desni nekomutativan euklidski par (A,ϕ) takav da je K dvočlano podtelo prstena A, a da valuacija $\phi:A\to N_0$ zadovoljava uslove (I) i (Z).

PRIMER 2-1. *Neka je $K=\{0,1\}$ dvočlano polje, $A=K[X]$ prsten polinoma po X sa koeficijentima iz K i $\phi:A\to N_0$ preslikavanje definisano sa*

$$(72)\qquad \phi(a_0+\cdots+X^n a_n)=a_0+\cdots+2^n a_n,$$

pri čemu a_i na desnoj strani u (72) treba shvatiti kao ceo broj 0 ili 1 već prema tome da li je $a_i=0$ ili $a_i=1$ u prstenu A. Tada je (A,ϕ) euklidski par koji zadovoljava uslove Teoreme 2-10 pod (γ). Zaista, ako je ∂ stepena valuacija prstena A, tada za svako $a\in A$ i $b\in A^0$ postoje q,r iz A takvi da je (*) $a=bq+r$, $\partial r<\partial b$. S druge strane je

$$(73)\qquad \phi(a_0+\cdots+X^n a_n)=1+\cdots+2^n<2^{n+1},$$

pa se neposredno proverava da $\partial r<\partial b$ povlači $\phi r<\phi b$, što sa (*) upravo znači da je i ϕ euklidska valuacija prstena A. Nadalje, svaki prirodan broj m se može na tačno jedan način pretstaviti u obliku $m=a_0+\cdots+2^n a_n$

sa $a_i \in \{0,1\}$. *Otuda je preslikavanje* ϕ *injekcija. Uz to je* $K^0 = \{1\}$, *pa valuacija* ϕ *zadovoljava uslov (Z). Najzad, ako su* $a = \Sigma a_i X^i$, $b = \Sigma b_i X^i$ $(0 \leqslant i \leqslant n,\ a_n \neq 0 \vee b_n \neq 0)$ *dva proizvoljna elementa iz prstena* $A = K[X]$, *biće*

$$a+b = c_0 + c_1 X + \cdots + c_n X^n, \tag{74}$$

sa $c_i = a_i + b_i$ $(0 \leqslant i \leqslant n)$. *Pri tome je* $c_i = 0$ *ili* $c_i = 1$ *već prema tome da li je* $a_i = b_i$ *ili* $a_i \neq b_i$, *pa u prstenu Z važi* $c_i \leqslant a_i + b_i$ $(0 \leqslant i \leqslant n)$. *Otuda je*

$$\begin{aligned} \phi(a+b) &= c_0 + 2c_1 + \cdots + 2^n c_n \\ &\leqslant (a_0+b_0) + \cdots + 2^n (a_n+b_n) \\ &= \left(a_0 + \cdots + 2^n a_n\right) + \left(b_0 + \cdots + 2^n b_n\right), \end{aligned} \tag{75}$$

to jest $\phi(a+b) \leqslant \phi(a) + \phi(b)$, *što upravo znači da euklidska valuacija* ϕ *zadovoljava i uslov (T). Otuda i tvrdjenje. U vezi sa tim primetimo da je sa* $\mu(0) = -\infty$ *i*

$$\mu(a) = \min \{n \in N_0 : \ \phi a < \phi X^n\} \qquad (a \in A^0) \tag{76}$$

definisana upravo stepena valuacija $\mu = \partial$ *prstena* $A = K[X]$. *Uopšte, ako je* (A,ϕ) *euklidski par koji zadovoljava uslove Teoreme 2-9 ili Teoreme 2-10, X bilo koji element iz A za koji je* $\phi X = \min \phi(A-K)$, *i ako prsten A nije telo, tada je sa (76) definisana jedna prirodna euklidska valuacija prstena A koja zadovoljava uslov (T), ali ne i uslov (Z). Posle ćemo dokazati da je* μ *upravo minimalna euklidska valuacija prstena A čiji je kodomen skup* $\{-\infty\} \cup N_0$. □

KOROLAR 2-2

Ako za prsten A *postoji bar jedno preslikavanje* $\phi : A \to N_0$ *koje zadovoljava uslove* (T), (N) *i* (Z), *tada je prsten* A *ili telo, ili je* (A,ϕ) *euklidski par izomorfan euklidskom paru* (Z,v).

DOKAZ. Iz $\phi(1) = \phi(0)$ i uslova (Z) sledi da za neku jednotu u prstena A važi $1 = 0u = 0$, što nije. Dakle je $\phi(1) \neq \phi(0)$, pa preslikavanje ϕ nije konstanta. Kako je uz to $\phi a = \phi(a1) = (\phi a)(\phi 1)$ za svako $a \in A$, mora biti

$\phi 1 = 1$. Dalje je $\phi 0 = \phi(0\cdot 0) = (\phi 0)(\phi 0)$, što sa $\phi 0 \neq \phi 1$ daje $\phi 0 = 0$, a time i $\phi a = 0$ akko je $a=0$. Sada iz uslova (N) neposredno sledi da je A domen. S druge strane, prema uslovu (Z) je $\phi a = \phi 1$ $(= 1)$ akko za neku jednotu u prstena A važi $a = 1u = u$. Otuda je $u \in A$ jednota u prstenu A ako i samo ako je $\phi a = 1$, a time i $K = \{a \in A: \phi a \leqslant 1\}$. Najzad, iz uslova (N) sledi da za $a,b \in A$ važi $\phi(ab) \geqslant \phi a, \phi b$, kao i da za $\phi a > 1$ niz ϕa^n $(n \in N)$ strogo raste. Posebno, ako je $A \neq K$ prsten A nije konačan.

Ako je K podtelo prstena A, tada je $A = K$. Naime, u slučaju da telo K ima bar tri člana, slično kao pri dokazu odgovarajućeg dela *Teoreme 2-10* zaključujemo da je $A-K = \Theta$. Neka je $K = \{0,1\}$ i pretpostavimo da je $A-K \neq \Theta$. Ako je $x \in A$ i $\phi x = min\, \phi(A-K)$, radeći analogno kao pri dokazu *Teoreme 2-10* pod (γ) dobijamo da je $\phi(1+x) = 1+\phi x$. Kako preslikavanje ϕ sada zadovoljava i uslov (N), iz poslednje jednakosti sledi prvo

$$(77) \qquad \phi\big((1+x)^2\big) = \big(\phi(1+x)\big)^2 = \big(1+\phi x\big)^2 = (1+n)^2,$$

a zatim i (jer ϕ zadovoljava i uslov *trougla*):

$$(78) \qquad \phi\big((1+x)^2\big) = \phi(1+x^2) \leqslant 1 + \phi(x^2) = 1+n^2,$$

pri čemu je stavljeno $\phi x = n$. To znači da mora biti $(1+n)^2 \leqslant 1+n^2$, i dakle $n=0$. Medjutim, to nije moguće jer je $x \in A-K$, a time i $\phi x > 1$. Prema tome, mora biti $A-K = \Theta$, to jest $A = K$.

Pretpostavimo sada da K nije podtelo prstena A. Radeći slično kao pri dokazu *Teoreme 2-9* zaključujemo da je $K^0 = \{-1,1\}$ sa $-1 \neq 1$, kao i da za svaki ceo broj m važi $\phi(m1) = |m|$. Otuda, ako je a proizvoljan član prstena A i $\phi a = n$, biće $\phi a = \phi(n1)$, pa uslov (Z) daje $a = n1$ *ili* $a = -n1$ (jer su -1 i 1 jedine jednote prstena A). Dakle je $A = \{m1: m \in Z\}$, pa je (A,ϕ) euklidski par izomorfan euklidskom paru (Z,ν). □

II

EUKLIDSKI RAZREDI I EUKLIDSKO JEZGRO MODULA

Uz prethodnu simboliku u ovom poglavlju sa M ćemo označavati desni modul nad prstenom A, a sam prsten A shvataćemo kao *desni* A-modul. Pod *valuacijom (ili vrednovanjem)* modula M podrazumevamo svako preslikavanje $\phi: M \to W$ toga modula u neki dobro uredjen skup W za koje je $\phi(0) = \min W$. Za podskup Σ modula M kažemo da je *euklidski* ako taj modul ima bar jednu Σ-euklidsku valuaciju. Po dogovoru i prazan skup Θ smatramo euklidskim podskupom modula M. Ako je $\phi: M \to W$ valuacija modula M, tada ćemo elemente dobro uredjenog skupa $\phi(M)$ označavati sa $0, 1, .., \omega, \omega+1, ..$ (naravno, ako ne postoji opasnost od zabune).

DEFINICIJA 1-1

Neka je $\phi: M \to W$ valuacija desnog A-modula M, α proizvoljan element iz $\phi(M)$ i Σ neprazan podskup od M^0. Ako je $\alpha > 0$, tada skup svih $b \in \Sigma$ takvih da za svako $a \in M$ postoje $q \in A$ i $r \in \Sigma_0$ za koje je

$$(1) \qquad a = bq + r, \qquad \phi r < \phi b \leq \alpha,$$

zovemo Σ_ϕ-EUKLIDSKIM RAZREDOM stepena α modula M i označavamo sa $\Sigma_\phi M_\alpha$. Za $\alpha = 0$ stavljamo $\Sigma_\phi M_0 = \{0\}$. Pod Σ_ϕ-EUKLIDSKIM JEZGROM modula M podrazumevamo uniju svih njegovih Σ_ϕ-euklidskih razreda stepena većeg od 0. Označavaćemo ga sa $\Sigma_\phi M^*$. U tom slučaju skup $\{0\} \cup \Sigma_\phi M^*$ zovemo Σ_ϕ-EUKLIDSKIM DELOM modula M i označavamo sa $\Sigma_\phi M^\circ$.

Uz prethodnu simboliku, razliku skupa Σ i Σ_ϕ-euklidskog jezgra modula M zvaćemo njegovim Σ_ϕ-*euklidskim DEFEKTOM*. Za dato $\alpha > 0$ iz $\phi(M)$ uniju svih

Σ_ϕ-euklidskih razreda $\Sigma_\phi M_\beta$ $(\beta<\alpha)$ modula M označavaćemo sa $\Sigma_\phi M^*_\alpha$ i zvati *izvodom* razreda $\Sigma_\phi M_\alpha$. Ako je $M=A$, tada govorimo o *desnim* Σ_ϕ-euklidskim razredima, jezgru, delu i defektu prstena A.

LEMA 1-1

Neka je $\phi: M \to W$ valuacija desnog A-modula M, Σ podskup od M^0, i F_ϕ familija svih podskupova S od Σ za koje je ϕ S-euklidska valuacija modula M. Tada, u odnosu na relaciju inkluzije, familija F_ϕ ima tačno jedan maksimalan član L, i to je upravo Σ_ϕ-euklidsko jezgro modula M.

DOKAZ. Pre svega, familija F_ϕ nije prazna jer sadrži, na primer, prazan skup Θ. Nadalje, ako je (S_i) $(i\in I)$ bilo koji lanac elemenata familije F_ϕ, neposredno se proverava da je i njihova unija $S = \cup_{i\in I} S_i$ član te familije (što posebno znači da je i Σ_ϕ-euklidsko jezgro $\Sigma_\phi M^*$ modula M član familije F_ϕ). Otuda, prema *Zornovoj lemi*, familija F_ϕ ima bar jedan maksimalan član L. Ako je $b\in L$ i $\phi(b)=\beta$, biće $b\in \Sigma_\phi M_\beta$, a time i $b\in \Sigma_\phi M^*$. S druge strane je i $\Sigma_\phi M^* \subset F_\phi$, pa iz $L\subset \Sigma_\phi M^*$ sledi da mora biti $\Sigma_\phi M^* = L$. Otuda i tvrdjenje. □

Ako je $\phi: M\to W$ valuacija A-modula M, $L=\Sigma_\phi M^*$ Σ_ϕ-euklidsko jezgro i $\&_L$ familija svih L-euklidskih valuacija modula M (sa istim kodomenom) tada je sa $\mu(a) = min\{\psi(a): \psi\in\&_L\}$ $(a\in\Sigma)$, $\mu a = 0$ $(a\in M-\Sigma)$, definisana *minimalna* L-euklidska valuacija modula M (*Teorema 1-2*). Uz to, za svako $b\in A$ i $a, ab\in\Sigma$ važi $\mu(ab)\geqslant\mu(a)$. Dalje, indukcijom po α, neposredno se zaključuje da za svako $\alpha\in\mu(M)$ važi $\Sigma_\psi M_\alpha \subset \Sigma_\mu M_\alpha$, $\Sigma_\psi M^* \subset \Sigma_\mu M^*$ $(\psi\in\&_L)$.

TEOREMA 1-1

Neka je $\phi: M\to W$ valuacija, $L=\Sigma_\phi M^*$ Σ_ϕ-euklidsko jezgro A-modula M i $\alpha>0$ proizvoljan element iz $\phi(M)$. Ako je ϕ minimalna L-euklidska valuacija modula M, tada se Σ_ϕ-euklidski razred $R_\alpha = \Sigma_\phi M_\alpha$ modula M podudara sa skupom T_α svih $b\in\Sigma$ za koje je kanoničko preslikavanje (*) $f_\alpha: R^*_\alpha \to M/bA$ surjekcija $(R^*_\alpha = \cup_{\beta<\alpha} R_\beta)$.

DOKAZ. Neka je $b\in R_\alpha$. Tada za svako $a\in M$ postoje $q\in A$ i $r\in L_0$ takvi da

je $a = bq+r$, $\phi r < \phi b$. Kako je $r \in L_0$ i $\phi r < \phi b \leq \alpha$, biće $r \in R_\beta$ za neko $\beta < \alpha$, a time i $r \in R_\alpha^*$. Uz to je $a-r = bq \in bA$, to jest $a+bA = r+bA$, a to upravo znači da je preslikavanje f_α surjekcija. Otuda je $b \in T_\alpha$, a samim tim i $R_\alpha \subset T_\alpha$. Obratno, neka je sada b proizvoljan element iz T_α i pretpostavimo da je $\phi(b) > \alpha$. Tada je sa

$$(2) \qquad \psi(b) = \alpha, \qquad \psi(a) = \phi(a) \qquad (a \in M-\{b\}),$$

definisana jedna L-euklidska valuacija modula M. Zaista, kako je $\phi: M \to W$ L-euklidska valuacija modula M, za svako $a \in M$ i $c \in L$ postoje $q \in A$ i $r \in L_0$ takvi da je

$$(3) \qquad a = cq+r, \qquad \phi(r) < \phi(c).$$

Ako je tu $c \neq b$ i $r \neq b$, tada prema *(2)* i *(3)* imamo $a = cq+r$, $\phi r < \phi c$. Ako je $c = b$, tada iz $b \in T_\alpha$ sledi da je kanoničko preslikavanje $f_\alpha: R_\alpha^* \to M/bA$ surjekcija, pa za neko $s \in R_\alpha^*$, to jest za neko $s \in L_0$ za koje je $\phi(s) < \alpha$, važi $a+bA = s+bA$, i dakle $a = bq+s$ za neko $q \in A$ i $s \in L_0$. S druge strane je $\psi(s) = \phi(s) < \alpha$, što sa $\alpha = \psi b$ i $c = b$ daje $a = cq+r$, $\psi r < \psi c$. Najzad, ako je u *(3)* $r = b$, tada iz $\phi(b) > \alpha$ sledi

$$(4) \qquad \psi(r) = \alpha < \phi(r) < \phi(c) = \psi(c),$$

pa je ψ L-euklidska valuacija modula M. Uz to je $\psi(a) < \phi(a)$ $(a \in M)$, pa kako je ϕ minimalna L-euklidska valuacija modula M, biće $\psi = \phi$, a time i $\phi(b) = \psi(b) = \alpha$, što je suprotno učinjenoj pretpostavci $\phi b > \alpha$. Dakle je $T_\alpha \subset R_\alpha$, a samim tim i $R_\alpha = T_\alpha$. □

TEOREMA 1-2

Neka je M desni A-modul, Σ podskup od M^0, W dobro uredjen skup, i (T_α) $(\alpha \in W)$ familija podskupova od Σ_0 odredjena sa:

(0) $T_0 = \{0\}$,

(α) *Ako je $\alpha > 0$ i $T_\alpha^* = \cup_{\beta<\alpha} T_\beta$, tada je T_α skup svih elemenata $b \in \Sigma$ za koje je kanoničko preslikavanje $f_\alpha: T_\alpha^* \to M/bA$ surjekcija.*

Tada je $L = \cup_{\alpha>0} T_\alpha$ euklidski podskup od M, i sa $\phi a = 0$ $(a \in M-L)$ i

(5) $\qquad \phi(a) = min\{\alpha\in W:\ a\in T_\alpha\} \qquad (a\in L),$

je definisana minimalna L-euklidska valuacija $\phi: M\to W$ modula M. Uz to je T_α upravo Σ_ϕ-euklidski razred stepena α modula M. Ako je pri tome $|A| < |W|$, tada je $L = \Sigma M^*$ najveći euklidski podskup modula M koji je sadržan u datom skupu Σ.

DOKAZ. Neka je $a\in A$ i $b\in L$. Ako je $\phi b = \alpha$, biće $\alpha = min\{\beta:\ b\in T_\beta\}$ i $b\in T_\alpha$. Otuda je kanoničko preslikavanje $f_\alpha: T_\alpha^* \to M/bA$ surjekcija, pa postoji r iz T_α^* takvo da je $a+bA = r+bA$, i dakle $a = bq+r$ za neko $q\in A$. Nadalje, iz $r\in T_\alpha^*$ sledi da za neko $\beta<\alpha$ važi $r\in T_\beta$, pa prema *(5)* imamo $\phi(r) < \alpha = \phi b$, što sa $a = bq+r$ i $r\in L_0$ upravo znači da je ϕ jedna L-euklidska valuacija modula M.

Ako je $\mu: M\to W$ minimalna L-euklidska valuacija modula M, na osnovu *Teoreme 1-1* zaključujemo da je L_μ-euklidski razred stepena α modula M upravo skup T_α (za svako α iz W). Uz to je $\mu(a) = min\{\alpha:\ a\in T_\alpha\}$ $(a\in L)$ i $\mu(a) = 0$ $(a\in M-L)$, što uporedjeno sa *(5)* daje $\mu = \phi$.

Najzad, pretpostavimo da za neki podskup G od Σ, koji sadrži skup L, postoji bar jedna G-euklidska valuacija modula M, i neka je $\psi: M\to W$ minimalna medju njima. Tada slično prethodnom zaključujemo da za svako $a\in L$ važi $\psi(a) = \phi(a)$. Ako je $G\neq L$, neka je b bilo koji element iz $G-L$ za koji je $\psi(b) = min\,\psi(G-L)$. Za svako $a\in M$ postoje $q\in A$ i $r\in G_0$ takvi da je $a = bq+r$, $\psi r < \psi b$. S druge strane, iz $L\subset G$, $r\in G_0$ i

(6) $\qquad \psi(r) < \psi(b) = min\,\psi(G-L)$

sledi $r\in L_0$, i dakle $r\in T^*$ za neko $\alpha\in W$. Uz to je $a-r\in bA$, i prema tome $a+bA = r+bA$, pa je kanoničko preslikavanje $f_\alpha: T_\alpha^* \to M/bA$ surjekcija. To znači da je $b\in T$, a time i $b\in L$, što je suprotno učinjenoj pretpostavci $b\in G-L$. Dakle je $G = L$, pa je L najveći euklidski podskup modula M sadržan u datom skupu Σ. Otuda i tvrdjenje. □

LEMA 1-2

Neka je M desni A-modul i $\Sigma\subset M^0$. Tada familija $\mathfrak{E}_\Sigma$ svih euklidskih podskupova $S\subset\Sigma$ modula M, u odnosu na relaciju inkluzije, ima tačno jedan maksimalan član $L = \Sigma M^*$.

DOKAZ. Ako je W dobro uredjen skup za koji je $|A| < |W|$, tada za svaki euklidski podskup S od M^* postoji S-euklidska valuacija $\varphi: M \to W$ modula M za koju je $\varphi(M)$ početni interval skupa W (I, Teorema 1-6). Na osnovu Teoreme 1-2, familija $\mathcal{E}_\Sigma$ ima bar jedan maksimalan član $\Sigma = \Sigma M^*$. Neka je G bilo koji maksimalan član familije $\mathcal{E}_\Sigma$, φ minimalna Σ-euklidska valuacija i ψ minimalna G-euklidska valuacija modula M.

Ako je $R_\alpha = G_\psi M_\alpha$ $(\alpha \in W)$, tada je R_α upravo skup svih $b \in G$ za koje je kanoničko preslikavanje $R^* \to M/bA$ surjekcija. S druge strane, prema Teoremi 1-1, $T_\alpha = \Sigma_\varphi M_\alpha$ je skup svih elemenata $b \in \Sigma$ za koje je kanoničko preslikavanje $T^* \to M/bA$ surjekcija. Kako je uz to $G \subset \Sigma$, transfinitnom indukcijom po α neposredno zaključujemo da za svako $\alpha \in W$ važi $R_\alpha \subset T_\alpha$. Otuda je i $G_\psi M^* \subset \Sigma_\varphi M^*$, to jest $G \subset \Sigma$, i dakle $G = \Sigma$ (jer je G maksimalan član familije $\mathcal{E}_\Sigma$). □

Prema prethodnoj Lemi 1-2, za svaki podskup Σ od M^0 postoji tačno jedan maksimalan euklidski podskup $\Sigma \subset \Sigma$ modula M. Ako je uz to $\varphi: M \to W$ $(|A| < |W|)$ minimalna Σ-euklidska valuacija modula M, prema Teoremi 1-2 Σ_φ-euklidski razredi modula M su upravo skupovi T_α, i dakle su potpuno odredjeni podskupom Σ od M^0. Otuda i naredna

DEFINICIJA 1-2

Neka je M desni A-modul, Σ podskup od M^0, W dobro uredjen skup za koji je $|A| < |W|$, i (T_α) $(\alpha \in W)$ familija podskupova od Σ_0 data sa

(0) $T_0 = \{0\}$,

(α) Ako je $\alpha > 0$ i $T^*_\alpha = \cup_{\xi<\alpha} T_\xi$, tada je T_α skup svih elemenata $b \in \Sigma$ za koje je kanoničko preslikavanje $T^*_\alpha \to M/bA$ surjekcija.

Skup $T_\alpha = \Sigma M_\alpha$, odnosno $\Sigma M^* = \cup_{\alpha>0} T_\alpha$ zovemo Σ-EUKLIDSKIM RAZREDOM stepena α, odnosno Σ-EUKLIDSKIM JEZGROM modula M. Razliku $\Sigma - \Sigma M^*$ i uniju $\Sigma M' = \{0\} \cup \Sigma M^*$ redom zovemo Σ-euklidskim DEFEKTOM i DELOM modula M.

Ako je $\Sigma = M^0$, tada u prethodnim terminima i oznakama izostavljamo "Σ", pa govorimo o *euklidskim* razredima M_α, jezgru M^*, .. modula M. Ako je $M = A$, tada govorimo o *DESNIM* Σ-euklidskim razredima ΣA_α, jezgru ΣA^*, delu $\Sigma A'$ i defektu $\Sigma - \Sigma A$ prstena A.

Ako su $\phi: M \to W$ i $\psi: M \to W'$ minimalne Σ-euklidske valuacije modula M, tada su Σ-euklidski parovi (M,ϕ) i (M,ψ) izomorfni (*I*, *T.1-7*). Ako je $(1_M, h)$ odgovarajući izomorfizam, neposredno se proverava da za svako α iz $\phi(M)$ važi $\Sigma M_\alpha = \Sigma M_{h(\alpha)}$. Zato ćemo za skup indeksa Σ-euklidskih razreda modula M uzimati dobro uredjen skup "oblika" $W = \{0,1,..,\omega,..,\eta\}$ za koji je $|A| < |W|$. Jasno je da tada medju razredima ΣM_α $(\alpha \in W)$ mora biti jednakih (jer je $\Sigma M_\beta \subset \Sigma M_\alpha$ za $\beta<\alpha$). Ako je λ najmanji ordinal za koji je $\Sigma M_\alpha = \Sigma M_{\alpha+1}$, biće $\Sigma M_\alpha = \Sigma M_\lambda$ za svako $\alpha>\lambda$, a time i $\Sigma M_\lambda = \Sigma M^*$ sa

(7) $$\lambda = \min \{\alpha \in W: \ \Sigma M_\alpha = \Sigma M^*\}.$$

Ordinal $\lambda = \lambda(\Sigma, M)$ odredjen sa *(7)* zvaćemo Σ-euklidskim *STEPENOM* modula M i označavati sa $\partial(\Sigma M^*)$. U slučaju da je $\Sigma = M^0$ govorimo o *euklidskom stepenu* modula M, i umesto $\partial(\Sigma M^*)$ pišemo samo $\partial(M^*)$. Ako je $M = A$, tada se neposredno proverava da je $A_0 = \{0\}$ i $A_1 = U_\ell(A)$ (= skup svih levih jednota prstena A), a time i $\partial(A^*) \geq 1$. Posebno, prsten A je telo ako i samo ako je $\partial(A^*) = 1$. □

TEOREMA 1-3

Podskup Σ desnog A-modula M je euklidski ako i samo ako se podudara sa svojim euklidskim jezgrom ΣM^*. U tom slučaju je sa

(8) $$\mu(a) = \min \{\alpha \in W: \ a \in \Sigma M_\alpha\} \qquad (a \in \Sigma)$$

i $\mu(a) = 0$ $(a \in M - \Sigma)$ definisana jedna minimalna Σ-euklidska valuacija μ modula M.

DOKAZ. To je neposredna posledica prethodnih tvrdjenja. (Slučaj kada je $M = A$ komutativan prsten i $\Sigma = A^0$ razmatran je u *SAMUEL* [*1*]). □

LEMA 1-3

Neka je M desni A-modul, Σ neprazan podskup od M^0 i P PARCIJALNO uredjen skup u kome svaki opadajući lanac ima minimalni član. Ako postoji bar jedno preslikavanje $\phi: M \to P$ sa svojstvom da za svako a iz M i $b \in \Sigma^0$ postoje $q \in A$ i $r \in \Sigma_0$ takvi da je $a = bq + r$, $\phi 0 \leq \phi r < \phi b$, tada je Σ euklidski podskup modula M (*SAMUEL* [*1*]).

DOKAZ. Neka su $\mathcal{T}_\alpha$ $(\alpha \in W)$ Σ-euklidski razredi modula M i pretpostavimo da skup $S = \Sigma - \Sigma M^*$ nije prazan. Ako je $\Pi = \mathcal{P}(\Sigma)$, tada uredjen skup $(\Pi, \geqslant)$ zadovoljava uslove *Zornove leme*, pa ima (bar jedan) minimalan član, na primer β. Neka je b bilo koji element iz S za koji je $\varphi(b) = \beta$. Tada za svako $a \in M$ postoje $q \in A$ i $r \in \Sigma_0$ takvi da je $a = bq + r$, $\varphi 0 < \varphi r < \varphi b$. Kako je $r \in \Sigma_0$ i $\varphi r < \varphi b = \beta$, mora biti $r \in \Sigma M^*$, a time i $r \in \Sigma M_\alpha$ za neko α iz W. To znači da je $a - r \in bA$, pa je kanoničko preslikavanje $\mathcal{T}_\alpha^* \to M/bA$ surjekcija. Otuda je $b \in \mathcal{T}_\alpha$, a time i $b \in \Sigma M^*$, što je u suprotnosti sa ranije učinjenom pretpostavkom $b \in \Sigma - \Sigma M^*$. Prema tome mora biti $\Sigma = \Sigma M^*$, pa je Σ euklidski podskup modula M. □

PRIMER 1-1. (α) *Odredimo euklidske razrede prstena* Z, *a time i njegovu minimalnu euklidsku valuaciju. Za* $m < n$ *stavimo* $[m,n] = \{k \in Z: m \leqslant k \leqslant n\}$. *Jasno je da je* $Z_0 = \{0\}$ *i* $Z_1 = \{-1,1\}$. *Kako je* $Z_2^* = [-1,1]$, *biće:* $n \in Z_2$ *ako i samo ako je kanoničko preslikavanje* $Z_2^* \to Z/nZ$ *surjekcija, što je ekvivalentno sa tim da za svako* $m \in Z$ *ceo broj* n *deli neki od brojeva iz skupa* $\{m-1, m, m+1\}$. *Posebno, za* $m=2$ *dobijamo da* n *mora deliti bar jedan od brojeva* $1,2,3$. *Otuda je* $n \in [-3, 3]^0$, *i dakle* $Z_2 \subset [-3,3]^0$. *No, jasno je da svako* $n \in [-3,3]^0$ *deli bar jedan od brojeva* $m-1, m, m+1$ *(za svako* m *iz* Z*), pa je* $Z_2 = [-3,3]^0$, *to jest* $Z_2 = [1-2^2, 2^2-1]^0$.

Radeći slično prethodnom, indukcijom po n *zaključujemo da za svaki prirodan broj* n *važi* $Z_n = [1-2^n, 2^n-1]^0$. *Na osnovu toga i Teoreme 1-3 zaključujemo da je minimalna euklidska valuacija* $\mu: Z \to N_0$ *prstena* Z *data sa* $\mu(m) = \min\{n \in N_0: m \in Z_n\}$, *to jest*

$$\mu(m) = \min\{n \in N_0: \ 2^n > |m|\} \qquad (m \in Z). \tag{9}$$

Primetimo da je $\mu(m)$ *upravo broj cifara u dijadskom "zapisu" prirodnog broja* $|m|$. *Ako sa* $\partial(m)$ $(m \in Z^0)$ *označimo "stepen" polinomskog rastava prirodnog broja* $|m|$ *po 2, tada je* $\mu(m) = 1 + \partial(m)$ $(m \in Z^0)$.

(β) *Prsten* $M = 2Z$ *nije euklidski. Naime, neposredno se proverava da je* $M_1 = \Theta$, *i dakle* $M^* \neq M^0$. *Štaviše, prazan skup je jedini euklidski podskup prstena* M. *Medjutim,* $M = 2Z$ *jeste euklidski* Z*-modul. Naime, radeći slično kao pod* (α), *neposredno zaključujemo da je euklidski razred stepena* $n \in N$ *modula* M *dat sa* $M_n = 2Z \cap [1-2^n, 2^n-1]^0$, *a time i* $M^* = M^0$.

(γ) *Neka je K telo, f i δ monomorfizam i desno f-diferenciranje tela K, i* $A = K[X,f,\delta]$ *prsten desnih* (f,δ)*-polinoma po X sa koeficijentima iz K. Ako je* ∂ *stepena valuacija prstena A i* $P \in A$, $Q \in A^0$, *tada iz* $P|Q$ *sledi* $\partial(P) \leqslant \partial(Q)$, *pa radeći slično kao pod (α) zaključujemo da je* $A_n = K^n[X,f,\delta]$ *(= skup svih polinoma iz* A^0 *stepena* $<n$*) za svako* $n \in N$. *To posebno znači de je* $A^\bullet = \cup_{n>0} A_n = A^0$, *pa je (prema Teoremi 1-3) A desni euklidski prsten čija je minimalna euklidska valuacija* $\mu: A \to N_0$ *data sa* $\mu(0) = 0$ *i*

$$\mu(P) = 1 + \partial(P) \qquad (P \in A^0). \tag{10}$$

Ako za kodomen (euklidskih) valuacija prstena $A = K[X,f,\delta]$ *uzmemo skup* $W_0 = \{-\infty\} \cup N_0$, *tada je minimalna euklidska valuacija* $\mu: A \to W_0$ *prstena A upravo njegova stepena valuacija* ∂.

(δ) *Prsten* $Z[X]$ *nije euklidski. Opštije: Ako je K domen, tada je prsten* $A = K[X]$ *euklidski ako i samo ako je K telo. Zaista, prvo je* $A_0 = \{0\}$ *i* $A_1 = U(A) = U(K)$. *Ako je* $U(K) = K^0$ *biće K telo, i stvar je gotova. Zato pretpostavimo da je* $U(K) \neq K^0$, *i neka je c proizvoljan element iz* $K^0 - U(K)$. *Kako je* $b \in A_2$ *ako i samo ako je kanoničko preslikavanje skupa* $A_2^\bullet = U_0(K)$ *u skup* A/bA *surjekcija, biće* $b \in A_2$ *ako i samo ako za svako* $a \in A$ *element b deli bar jedan od elemenata a-u* $(u \in A^0)$ *u prstenu A. Posebno, za a=c dobijamo da za neko* $u \in U_0(K)$ *b mora deliti c-u. Pri tom iz* $c \in U_0(K)$ *sledi* $c-u \neq 0$, *i dakle* $\partial(b)=0$, *a time i* $b \in K$. *Dalje, kako b mora deliti i bar jedan od elemenata X-u* $(u \in A_2^\bullet)$, *to za neko* $p,q \in K$ *važi* $b(pX+q) = X-u$, *što sa* $b = 0$ *daje* $bp=1$. *To znači da je* $b \in U(A)$, *pa je* $A_2 = A_1 = U(K)$, *a time i* $A^\bullet = U(K) = A^0$. *Otuda i tvrdjenje.* □

PRIMER 1-2. *Neka je L bilo koje polje, K polje razlomaka nad prstenom* $L[X]$ *i A skup svih matrica oblika* $M_{a,b} = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ $(a,b \in K)$. *Dalje, za svako* $a = a(X)$ *iz A stavimo* $\tilde{a}(X) = a(X^2)$, *i neka je* $\bullet$ *binarna operacija na skupu A data sa*

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \cdot \begin{bmatrix} p & q \\ 0 & p \end{bmatrix} = \begin{bmatrix} ap & \tilde{a}q+bp \\ 0 & ap \end{bmatrix}. \tag{11}$$

Tada je $\mathcal{A} = (A,+,\cdot)$ *nekomutativan prsten sa deliteljima nule. Posle*

kraćeg računa dobijamo da su desni euklidski razredi prstena A dati sa $A_0 = \{0\}$, $A_1 = U(A) = \{M_{a,b}: a \in K^\circ, b \in K\}$, $A_2 = A^0 = A^\bullet$. *Otuda je prsten A euklidski zdesna, sa euklidskim stepenom* $\delta(A^\bullet) = 2$.

Medjutim, prsten A nije euklidski i sleva. Naime, ako njegov levi euklidski razred stepena α *označimo sa* ${}_\alpha A$, *tada je* ${}_0A = \{0\}$, ${}_1A = U(A)$. *Pretpostavimo da je* ${}_2A \neq {}_1A$, *i dakle* $v = M_{0,b} \in {}_2A$ *za neko* $b \in K$. *Tada za svako* $u = M_{0,a} \in A$ *postoje* $z = M_{p,q} \in A$ *i* $w = M_{r,s} \in {}^\bullet_2A = U_0(A)$ *za koje je* $u = zv+w$, *i dakle* $r=0$, $a = \tilde{p}b+s$. *No, kako je* $r=0$ *i* $w \in U_0(A)$, *mora biti i* $s=0$, *i prema tome* (*) $a = \tilde{p}b$. *Pri tome je* $\tilde{p} = p(X^2)$, *pa za* $a = X^2$ *iz* (*) *sledi da za neko* $f \in K$ *važi* $b = f(X^2)$. *Kako je b fiksirano, sada iz* $a = p(X^2)f(X^2)$ *sledi da je svako* $a \in K$ *oblika* $a = h(X^2)$ *za neko* $h \in K$. *No jasno je da to ne važi, na primer, za* $a = X$. *Dakle je* ${}_2A = {}_1A$, *to jest* ${}^\bullet A = {}_1A = A^0$, *pa prsten A nije euklidski sleva.*

Ako je $e = M_{0,1}$, *neposredno se proverava da je* $I = eA$ *(obostrani) ideal prstena A. Radeći slično prethodnom, nije teško zaključiti da ne postoji* $u = M_{a,b}$ *iz A za koje je* $I = Au$. *To posebno znači da u prstenu A levi ideal ne mora biti glavni. Prema tome, postoji prsten A koji je euklidski zdesna, ali ne i sleva. Opštije: U desnom euklidskom prstenu levi ideali ne moraju biti glavni.* □

TEOREMA 1-4

> *Neka je simbolika iz I, Teorema 2-8. Za svako* $\alpha < \eta$ *i* $\theta \in T$ *označimo sa* $R_\alpha(\theta)$ *skup svih "polinoma"* $a \in A^0_\alpha$ *za čije vodeće monome* $x[\theta_a]$ *važi* $\theta_a \leqslant \theta$. *Ako je* f_α *monomorfizam prstena* B_α *za svako* $\alpha < \eta$, *tada je* $\{R_\alpha(\theta): \theta \in T\}$ *upravo familija svih desnih euklidskih razreda prstena* A_α. *To posebno važi i za prsten* $A_\eta = A$.

Ovom prilikom nećemo navoditi dokaz prethodnog tvrdjenja. Napominjemo jedino da on "teče" transfinitnom indukcijom po α. Za $\alpha = 1$ tvrdjenje se svodi na *Primer 1-1* pod (γ). □

U nekoliko narednih tvrdjenja biće reči o "zavisnosti" euklidskih razreda količničkog modula M/L i proizvoda $U \times V$ dva desna A-modula U i V od euklidskih razreda samih A-modula M, U, V. Takodje će biti dokazano da euklidski modul ne mora imati i konačnu euklidsku valuaciju.

LEMA 1-4

Ako je desni A-modul M euklidski, onda je to slučaj i sa svakim njegovim podmodulom L. Pravi podmodul L desnog A-modula M ne može biti njegov euklidski podskup.

DOKAZ. Ako je $\phi: M \to W$ euklidska valuacija modula M, tada za svako $a \in L$ i $b \in L^0$ postoje $q \in A$ i $r \in M$ takvi da je $a = bq + r$, $\phi r < \phi b$. Kako je L podmodul od M, biće i $r = a - bq \in L$, pa je restrikcija ψ od ϕ na L jedna euklidska valuacija A-modula L. (Naravno da potprsten euklidskog prstena ne mora biti euklidski, kao što to pokazuje primer potprstena $2\mathbb{Z}$ prstena $\mathbb{Z}$.)

Pretpostavimo da je L euklidski podskup modula M i neka je $\phi: M \to W$ bilo koja L-euklidska valuacija. Kako je $L \neq \{0\}$, biće $b \in L$ za bar jedno $b \neq 0$. Tada za svako $a \in M$ postoje $q \in A$ i $r \in L$ takvi da je $a = bq + r$ sa $\phi r < \phi b$. Pri tome je L desni A-modul, pa $b, r \in L$ povlači $bq + r \in L$, a time i $a \in L$, to jest $M = L$, što je suprotno pretpostavci. □

TEOREMA 1-5

Neka je L podmodul desnog A-modula M, $\Sigma \subset M^0$, i za svaki podskup S od M stavimo $S/L = \{a+L: a \in S\}$. Ako je λ (Σ/L)-euklidski stepen modula M/L, tada za svaki ordinal $\alpha < \lambda$ važi

$$(12) \qquad (\Sigma M_\alpha)/L \subset (\Sigma/L)(M/L)_\alpha .$$

DOKAZ. Stavimo $\Pi = \Sigma/L$ i $\bar{a} = a + L$ $(a \in A)$. Za $\alpha = 0, 1$ (12) sledi neposredno. Neka je $\alpha > 1$ zadat ordinal $(\alpha < \lambda)$ i pretpostavimo da tvrdjenje važi za svaki ordinal $\beta < \alpha$. Tada iz $(\Sigma M_\beta)/L \subset (\Sigma/L)(M/L)_\beta$ $(\beta < \alpha)$ sledi

$$(13) \qquad (\cup_{\beta<\alpha} \Sigma M_\beta)/L \subset \cup_{\beta<\alpha} (\Sigma M_\beta/L) \subset \cup_{\beta<\alpha} \Pi (M/L)_\beta ,$$

i prema tome

$$(14) \qquad (\Sigma M_\alpha^*)/L \subset (\Sigma/L)(M/L)_\alpha^* .$$

Neka je $\bar{c} = c + L$ proizvoljan element iz $\Sigma M_\alpha/L$ sa $c \in \Sigma M_\alpha$. Za svako a iz A postoje $q \in A$ i $r \in \Sigma M_\alpha^*$ takvi da je $a = cq + r$. Tada je $a + L = (c+L)q + (r+L)$, to jest (*) $\bar{a} = \bar{c}q + \bar{r}$. Kako je $r \in \Sigma M_\alpha$, biće $\bar{r} \in \Sigma M_\alpha/L$, pa na osnovu *14*)

imamo $r \in (\Sigma/L)(M/L)^{*}_{\alpha}$, što sa (*) znači da je kanoničko preslikavanje

(15) $$(\Sigma/L)(M/L)^{*}_{\alpha} \to (M/L)/\hat{c}(M/L)$$

surjekcija. Otuda je $\hat{c} \in (\Sigma/L)(M/L)_{\alpha} \cup \{L\}$. Ako bi bilo $\hat{c} = L$, tada bi iz $\hat{a} = \hat{c}q + \hat{r}$ sledilo $\hat{a} = \hat{r} \in \Sigma M_{\alpha}/L$ $(a \in M/L)$, i dakle $M/L \subset (\Sigma/L)(M/L)^{*}_{\alpha}$, što je u suprotnosti sa $\alpha < \lambda$. Prema tome, mora biti $\hat{c} \in (\Sigma/L)(M/L)_{\alpha}$, a time i $(\Sigma M_{\alpha})/L \subset (\Sigma/L)(M/L)_{\alpha}$. Otuda i tvrdjenje. □

KOROLAR 1-1

Ako je L podmodul desnog A-modula M i Σ neprazan podskup od M^{0}, tada važi ($\Sigma M^{\cdot}$ označava Σ-euklidski deo modula M):

(16) $$(\Sigma M^{\cdot})/L \subset (\Sigma/L)(M/L)^{\cdot} \subset \Sigma/L ,$$

i ako je Σ euklidski podskup modula M, onda je takav i skup Σ/L u modulu M/L. Posebno, ako je modul M euklidski, onda je to slučaj i sa količničkim modulom M/L.

DOKAZ. To je neposredna posledica prethodne *Teoreme 1-5*. Ako je $M = A$ i L obostran ideal prstena A, tada je A/L i prsten. Pri tom "euklidnost" prstena A povlači euklidnost količničkog prstena A/L.

Ako je $f: M \to S$ morfizam u kategoriji Mod_{A} (odnosno ANN), tada važi $f(M) \cong M/L$, pri čemu je $L = Ker(f)$ podmodul modula M (odnosno obostran ideal prstena M). Otuda "euklidnost" modula (prstena) M povlači i "euklidnost njegove slike" $f(M)$ pri morfizmu f. □

TEOREMA 1-6

Desni A-modul M je euklidski ako i samo ako njegov euklidski deo $M^{\cdot}$ sadrži bar jedan maksimalan podmodul L modula M.

DOKAZ. Jasno je da je uslov potreban. Dokažimo da je i dovoljan. Neka je L maksimalan podmodul modula M za koji važi $L \subset M^{\cdot}$. Pretpostavimo da je $M \neq M^{\cdot}$ i neka je $a \in M - M^{\cdot}$. Iz $a \notin L$ sledi da podmodul $L + aA$ od M strogo sadrži maksimalan podmodul L od M, pa mora biti $L + aA = M$, što sa $L \subset M^{\cdot}$

daje $M = M' + aA$. Ako je $\eta = \partial(M^*)$ euklidski stepen modula M, biće $M' = M^*_\eta$, i dakle $M = M^*_\eta + aA$. To znači da je kanoničko preslikavanje $F: M^*_\eta \to M/aA$ surjekcija, pa je $a \in M_\eta$. Uz to je $M^* = M_\eta$, i prema tome $a \in M^*$. Medjutim, to je nemoguće jer je $a \in M - M'$. Dakle je $M' = M$. □

LEMA 1-5

Ako je L podmodul desnog A-modula M, i ako za bar jedan euklidski podskup Σ od M važi (*) $M = \Sigma_0 + L$, tada je A-modul M/L euklidski.

DOKAZ. Iz (*) sledi da je svako $a \in M$ oblika $a = b + c$ $(b \in \Sigma_0,\ x \in L)$, a time i $\bar{a} = a + L = b + L$ za neko $b \in \Sigma_0$. Otuda je $M/L \subset \Sigma_0/L \subset M'/L$, pa na osnovu *Korolara 1-1* zaključujemo da je $M/L = (M/L)'$. □

TEOREMA 1-7

Neka je L podmodul i Σ euklidski podskup desnog A-modula M. Ako L ima neprazan presek sa skupom Σ^0, tada je $L = cA$ za neko $c \in \Sigma^0$, i količnički modul M/L je euklidski.

DOKAZ. Kako je $\Sigma^0 \cap L \neq \Theta$, biće $\Sigma M_\alpha \cap L \neq \Theta$ za bar jedan ordinal $\alpha > 0$. Neka je $\alpha > 0$ najmanji ordinal za koji je $\Sigma M_\alpha \cap L \neq \Theta$ i c bilo koji element iz $\Sigma M_\alpha \cap L$. Zbog $\alpha > 0$ mora biti $c \neq 0$, pa iz $c \in \Sigma M_\alpha$ sledi da za svako $a \in M$ postoji $q \in A$ takvo da je $a - cq \in \Sigma M^*_\alpha$, to jest $a - cq = 0$ *ili* $a - cq \in \Sigma M_\beta$ za neko $\beta < \alpha$. To posebno važi za svako $a \in L$. Kako je L podmodul modula M, iz $a, c \in L$ sledi $a - cq \in L$, pa zbog $\beta < \alpha$ ne može biti $a - cq \in \Sigma M_\beta$. Dakle, za svako $a \in L$ postoji $q \in A$ za koje je $a - cq = 0$, pa je $L \subset cA$. Kako je uz to $c \in L$, biće $L = cA$ sa $c \in \Sigma^0$, čime je dokazan prvi deo tvrdjenja. Dalje, iz $a - cq \in \Sigma M^*_\alpha$ sledi da za $cq = b$ i neko $r \in \Sigma_0$ važi $a = b + r$, i prema tome $M = \Sigma_0 + L$, pa drugi deo tvrdjenja sledi iz *Leme 1-5*. □

LEMA 1-6

Ako je Σ euklidski podskup desnog A-modula M, tada za svako a iz $M - \Sigma^0$ važi $aA \cap \Sigma^0 = \Theta$, a time i $aA \subset M - \Sigma^0$.

DOKAZ. Pretpostavimo da skup $aA \cap \Sigma^0$ nije prazan i neka je $b \in aA \cap \Sigma^0$. Tada za neko $c \in A$ važi $b = ac$. Dalje, iz $b \in \Sigma^0$ sledi da je $b \in \Sigma M_\alpha$ za bar

jedan ordinal $\alpha<\eta$, gde je $\eta=\vartheta(\Sigma^0)$. To posebno znači da je kanoničko preslikavanje $\Sigma M_\alpha \to M/ac\mathcal{A}$ surjekcija, pa je to slučaj i sa kanoničkim preslikavanjem $\Sigma M_\alpha \to M/a\mathcal{A}$. Otuda je $a\in\Sigma M_\alpha$, i dakle $a\in\Sigma^0$, što se kosi sa $a\in M-\Sigma^0$. □

TEOREMA 1-8

Ako je M desni A-modul i L bilo koji maksimalan element familije svih podmodula od M koji su sadržani u skupu $M-M^*$, tada je modul M/L euklidski.

DOKAZ. Pretpostavimo da modul M/L nije euklidski. Tada skup $M/L-(M/L)^*$ nije prazan. Neka je $\bar{a}=a+L$ bilo koji od njegovih elemenata. Iz $a+L\neq L$ sledi $a\in L$. Prema *Lemi 1-6* je $(a+L)(M/L)\subset(M/L)-(M/L)^*$. Kako je uz to $M^*/L\subset(M/L)^*$ (*Korolar 1-1*), biće

$$(a+L)(M/L)\subset(M/L-M^*/L)\cup\{L\}. \tag{17}$$

Pretpostavimo da skup $(aA+L)\cap M^*$ nije prazan i neka je $b=ac+x$ bilo koji njegov član. Tada je $b+L=ac+L=(a+L)c$ $(c\in A)$, i dakle $\bar{b}\in\bar{a}A$. Uz to, iz $b\in M^*$ sledi $\bar{b}\in M^*/L$, pa prema *(17)* mora biti $\bar{b}=L$, to jest $b\in L$, a time i $b\in M-M^*$, što je u suprotnosti sa $b\in M^*$.

Prema tome mora biti $(aA+L)\cap M^*=\Theta$. Otuda je $aA+L$ podmodul modula M koji je sadržan u skupu $M-M^*$ i koji sadrži podmodul L. No, kako je L maksimalan član familije svih podmodula od M koji su sadržani u $M-M^*$, mora biti $aA+L=L$, a time i $a\in L$, što je u suprotnosti sa $a\in L$. Dakle je $M/L=(M/L)^*$, pa je modul M/L euklidski. □

Ako je $M=A$ i L desni ideal prstena A, tada je pod pretpostavkama prethodne teoreme A-modul A/L euklidski. Ako je uz to ideal L obostran, tada je A/L i desni euklidski prsten, tj. euklidski (A/L)-modul.

Količnički modul M/L može biti euklidski i za neki podmodul L od M koji je sadržan u $M-M^*$, i koji nije maksimalan član u *familiji* $\mathcal{K}$ svih takvih podmodula modula M. Tako, na primer, ako je $M=A=Z[X]$ i $L=(X)$, biće $A^*=\{-1,1\}$ i $L\subset A-A^*$. Pri tome je prsten A/L izomorfan euklidskom prstenu Z pa je i sam euklidski. S druge strane, iz $A^*\subset U(A)$ sledi da su maksimalni članovi familije $\mathcal{K}$ upravo maksimalni ideali prstena A, pa

kako A/I nije polje, I nije maksimalan ideal prstena A, a samim tim ni maksimalan član familije $\mathcal{H}$.

TEOREMA 1-9

Ako su U i V desni moduli nad prstenima A i B respektivno, $G \subset U^0$ i $H \subset V^0$ euklidski skupovi, $M = U \times V$ desni modul nad prstenom $C = A \times B$ i $\Sigma = G \times H$, tada važi

$$\Sigma M_\nu = \cup_{\alpha,\beta} (GU_\alpha \times HV_\beta) \qquad (0 < \nu < \omega), \tag{17}$$

pri čemu se sabiranje vrši po $\alpha, \beta > 0$ za koje je $\alpha+\beta \leq \nu+1$, i Σ je euklidski podskup modula M. Ako je uz to modul V euklidski, tada je i $G \times V$ euklidski podskup modula $M = U \times V$.

DOKAZ. Jasno je da je $M_1 = GU_1 \times HV_1$, pa *(17)* važi za $\nu=1$. Pretpostavimo da *(17)* važi za svako $\nu < \eta$ (η zadat prirodan broj) pa dokažimo da važi i za $\nu = \eta$. Neka su $\alpha, \beta > 0$ takvi da je $\alpha+\beta \leq \eta+1$. Ako je $(a,b) \in GU_\alpha \times HV_\beta$, to jest $a \in GU_\alpha$ i $b \in HV_\beta$, tada za svako $x \in U$ i $y \in V$ postoje $p \in A$, $q \in B$ i $r \in GU_\alpha^*$, $s \in HV_\beta^*$ takvi da je $x = ap+r$ i $y = bq+s$, tj.:

$$(x,y) = (a,b)(p,q) + (r,s), \tag{18}$$

gde je (r,s) iz $GU_\alpha^* \times HV_\beta^*$. Ako je $(r=0$ i $s=0)$ *ili* $(r \neq 0$ i $s \neq 0)$, tada prema induktivnoj pretpostavci važi $(r,s) \in \Sigma M_\eta^*$, a time i $(a,b) \in \Sigma M_\eta$ (jer je $(\alpha-1)+(\beta-1) < \eta$). Zato pretpostavimo da je, na primer, $r=0$ i $s=0$. U tom slučaju *(18)* možemo pretstaviti u obliku

$$(x,y) = (a,b)(p-1,q) + (a,s). \tag{19}$$

Pri tome je $(a,s) \in GU_\alpha \times HV_\beta^*$, a time i $(a,s) \in GU_\alpha \times HV_\gamma$ za neki prirodan broj $\gamma < \beta$. Uz to je $\alpha+\gamma < \alpha+\beta$, tj. $\alpha+\gamma \leq (\eta-1)+1$, pa na osnovu induktivne pretpostavke imamo $(a,s) \in \Sigma M_{\eta-1}$, i dakle $(a,b) \in \Sigma M_\eta$. Prema tome, za svako (x,y) iz M postoje $(p\ q) \in C$ i $(r,s) \in \Sigma M_\eta^*$ takvi da važi *(18)*, pa je $(a,b) \in \Sigma M_\eta$, a samim time i (*) $\cup_{\alpha,\beta} (GU_\alpha \times HV_\beta) \subset \Sigma M_\eta$ $(\alpha, \beta > 0,\ \alpha+\beta < \eta+1)$.

Neka je sada (a,b) proizvoljan element iz ΣM_η. To posebno znači da za svako $(x,y) \in M$ postoje $(p,q) \in C$ i $(r,s) \in \Sigma M_\eta^*$ takvi da važi *(18)*.

Iz $(r,s)\in\Sigma M_\eta^*$ sledi da je $(r,s)=(0,0)$ *ili* $(r,s)\in\Sigma M_\theta$ za neko $0<\theta<\eta$. Kako prema induktivnoj pretpostavci *(17)* važi za svako $\nu<\eta$, imamo da je $(r,s)=(0,0)$ *ili* $(r,s)\in GU_\alpha\times HV_\beta$ za neko $\alpha,\beta>0$, $\alpha+\beta\leqslant\theta+1\leqslant\eta$. Uz to iz $\alpha<\eta$ i $\beta<\eta$ sledi $r\in GU_\eta^*$, $s\in HV_\eta^*$. S druge strane, prema *(18)*, za svako $x\in U$ i $y\in V$ je $x=ap+r$ i $y=bq+s$, što sa prethodnim daje $a\in GU_\eta^*$, $b\in HV_\eta^*$, to jest $(a,b)\in GU_\eta\times HV_\eta$, a time i (**) $\Sigma M_\eta\subset GU_\eta\times HV_\eta$.

Pretpostavimo da za neko $\alpha,\beta>0$, za koje je $\alpha+\beta>\eta+1$, postoje a iz $GU_\alpha-GU_\alpha^*$ i b iz $HV_\beta-HV_\beta^*$ takvi da je $(a,b)\in\Sigma M_\eta$. Tada za svako (x,y) iz M postoje $(p,q)\in C$ i $(r,s)\in\Sigma M_\eta^*$ takvi da važi *(18)*, a time i

$$x=ap+r,\qquad y=bq+s, \tag{20}$$

sa $(r,s)=(0,0)$ *ili* $(r,s)\in\Sigma M_\lambda$ za neko $0<\lambda<\eta$. Kako je $\alpha+\beta>\eta+1$ biće $\alpha>1$ ili $\beta>1$. Neka je, na primer, $\beta>1$ i označimo sa Y skup svih y iz V koji nisu oblika bq. Iz $\beta>1$ sledi $b\in HV_1$, pa skup Y nije prazan. Za svako x iz U i y iz Y u *(18)* mora biti $(r,s)\neq(0,0)$, i dakle $(r,s)\in\Sigma M_\lambda$. Kako je $0<\lambda<\eta$, na osnovu induktivne pretpostavke postoje prirodni brojevi m i n takvi da je $m+n\leqslant\lambda+1$ i $(r,s)\in GU_m\times HV_n$, tj. $r\in GU_m$ i $s\in HV_n$. Uz to možemo pretpostaviti da su $m=m(x,y)$ i $n=n(x,y)$ najmanji ordinali sa tim svojstvom. U tom slučaju je $m\leqslant\alpha$ i $n\leqslant\beta$.

Neka je $\gamma=\eta-1$. Tada, zbog $b\in HV_\beta-HV_\beta^*$, za bar jedno $y\in Y$ odgovarajuće n nije manje od γ (jer bi u suprotnom bilo $b\in HV_\gamma$ sa $\gamma<\beta$, što se kosi sa učinjenom pretpostavkom). Za $y\in Y$ i $x=0$ iz *(18)* i $s\neq0$ sledi da je $r=a(-q)\neq0$, pa kako $r\in GU_m$, mora biti i $a\in GU_m$. S druge strane je $a\in GU_m-GU_n$, pa je $m>\alpha$, što sa $m\leqslant\alpha$ daje $m=\alpha$. Otuda za $x=0$ i $y\in Y$ za koje je $n=n(0,y)\geqslant\gamma$ važi

$$m+n+1\geqslant\alpha+\gamma+1=\alpha+\beta>\eta+1. \tag{21}$$

Medjutim, to nije moguće jer za neko $\lambda<\eta$ važi $m+n\leqslant\lambda+1$, i prema tome $m+n+1\leqslant\eta+1$. Dakle, ako je $(a,b)\in\Sigma M_\eta$, prema (**) je $a\in GU_\eta$, $b\in HV_\eta$. Ako su α i β najmanji prirodni brojevi za koje je $a\in GU_\alpha$ i $b\in HV_\beta$, tada je $\alpha+\beta\leqslant\eta+1$, i dakle $\Sigma M_\eta\subset\cup_{\alpha,\beta}(GU_\alpha\times HV_\beta)$ $(\alpha,\beta>0,\ \alpha+\beta\leqslant\eta+1)$, što sa (*) daje jednakost *(17)* za $\nu=\eta$.

Neka su $\lambda=\partial(G)$ i $\eta=\partial(H)$ euklidski stepeni skupova G i H. Ako su λ i η prirodni brojevi i $\tau=\lambda+\eta$, tada na osnovu jednakosti *(17)* imamo:

(22) $$\Sigma M^* \supset \cup_{0<\nu<\tau} \Sigma M_\nu = \cup_{\alpha,\beta} (GU_\alpha \times HV_\beta) = (\cup_{\alpha>0} GU_\alpha) \times (\cup_{\beta>0} HV_\beta),$$

a time i $\Sigma M^* = G\times H = \Sigma$, pa je $\Sigma = G\times H$ euklidski podskup modula M. Dokažimo da to važi i ako su λ i η proizvoljni ordinali. Neka je $\phi: U \to W$ minimalna G-euklidska valuacija modula U i $\psi: V \to W$ minimalna H-euklidska valuacija modula V. Tada je preslikavanje $\delta: M \to W$ W modula $M = U\times V$ u dobro uredjen skup $W\times W$ (sa lekslografskim uredjenjem) definisano sa

(23) $$\delta(a,b) = (\phi a, \psi b), \qquad (a,b) \in M,$$

jedna Σ-euklidska valuacija modula M. Zaista, neka je $(a,b) \in \Sigma$, i dakle $a \in G$ i $b \in H$. Tada za svako $x \in U$, $y \in V$ postoje $p \in A$, $q \in B$ i $r \in G_0$, $s \in H_0$ za koje je $x = ap + r$ i $y = bq + s$, a time i

(24) $$(x,y) = (a,b)(p,q) + (r,s).$$

sa $\phi r < \phi a$ i $\psi s < \psi b$. Ako je $(r,s) = (0,0)$ ili $(r \neq 0 \quad s \neq 0)$, biće $(r,s) \in \Sigma_0$ sa $\delta(r,s) < \delta(a,b)$, i stvar je u redu. Ako je, npr., $r = 0$ i $s \neq 0$, tada je $\delta(r,s) < \delta(a,b)$, ali nije $(r,s) \in \Sigma_0$. No, zbog $r = 0$, (24) možemo izraziti i sa $(x,y) = (a,b)(p-1,q) + (a,s)$, pri čemu je, kako $(a,s) \in \Sigma_0$, tako i $\delta(a,s) < \delta(a,b)$. Sličan zaključak imamo i u slučaju da je $r \neq 0$ i $s = 0$, pa je $(a,b) \in \Sigma M^*$, a time i $\Sigma \subset \Sigma M^*$, što sa $\Sigma M^* \subset \Sigma$ daje $\Sigma M^* = \Sigma$.

Najzad, dokažimo da je za $H = V - \{0\}$ i skup $L = G\times H_0 = G\times V$ euklidski u modulu M. Neka je $\vec{W}$ ordinalna suma dobro uredjenih skupova $W\times W$ i W^0 (u kojoj je $W\times W$ početni interval) i $\zeta: M \to \vec{W}$ valuacija koja se na skupu $M - \{(a,0): a \in G\}$ podudara sa prethodnom valuacijom δ, dok je

(25) $$\zeta(a,0) = \phi(a), \qquad (a,0) \in G\times\{0\}.$$

Prema upravo dokazanom delu tvrdjenja skup $\Sigma = G\times H = G\times V^0$ je euklidski u modulu M, pa kako je $L = (G\times\{0\}) \cup \Sigma$, treba još dokazati da za svako $a \in G$ važi $(a,0) \in LM^*$. Zaista, iz "euklidnosti" skupa G u modulu U sledi da za svako $(x,y) \in M$ postoje $(p,q) \in C$ i $(r,s) \in G_0\times V$ takvi da je

(26) $$(x,y) = (a,0)(p,q) + (r,s)$$

sa $\phi r < \phi a$. Pri tome mora biti $s = y$. Ako je $(r,s) = (0,0)$ ili $r \neq 0$, tada je

$\zeta(r,s) < \zeta(a,0)$ sa $(r,s) \in \Sigma_0$ (jer je $R_0 = \{0\}$. U slučaju da je $s \neq 0$ i $r=0$ jednakost (26) možemo zapisati u obliku $(x,y) = (a,0)(p-1,q) + (a,s)$, i pri tome važi $(a,s) \in \Sigma_0$ sa $\zeta(a,s) < \zeta(a,0)$. Otuda $(a,0) \in \Sigma M^*$, a time i samo tvrdjenje. □

KOROLAR 1-2

Ako su desni A-modul U i B-modul V euklidski, onda je to slučaj i sa desnim modulom $M = U \times V$ nad prstenom $C = A \times B$.

DOKAZ. Prema *Teoremi 1-9* skup $U_0 \times V$ je euklidski u modulu M. Neka je μ minimalna Σ-euklidska valuacija modula M i $\eta = \partial(\Sigma M^*)$ euklidski stepen skupa $\Sigma = U_0 \times V$. Ako je ψ minimalna euklidska valuacija modula V, tada je sa $\theta(u) = \mu(u)$ $(u \in \Sigma_0)$ i

$$\theta(0,b) = \eta + \psi b, \qquad u = (0,b) \in M - \Sigma_0, \tag{27}$$

definisana jedna euklidska valuacija θ modula M. Kako se preslikavanje θ podudara sa Σ-euklidskom valuacijom μ modula M na skupu Σ, treba još dokazati da za svako $(x,y) \in M$ i $(0,b) \in M - \Sigma_0$ postoje $(p,q) \in C$ i (r,s) iz M takvi da je

$$(x,y) = (0,b)(p,q) + (r,s), \tag{28}$$

sa $\theta(r,s) < \theta(0,b)$. Pri tome mora biti $r=x$. Zaista, kako je ψ euklidska valuacija modula V, postoje $q \in B$ i $s \in V$ za koje je $y = bq+s$, $\psi s < \psi b$, to jest za koje važi (28) sa $\psi s < \psi b$. S druge strane, prema (27) je

$$\theta(0,s) = \eta + \psi s < \eta + \psi b = \theta(0,b), \tag{29}$$

što sa $\theta(r,s) < \theta(0,s)$ daje $\theta(r,s) < \theta(0,b)$, pa je θ euklidska valuacija modula M (koja ne mora biti minimalna). Otuda i tvrdjenje. □

Neka je simbolika iz prethodne *Teoreme 1-9*. Zavisnost euklidskih razreda ΣM_ω skupa $\Sigma = G \times H$ od euklidskih razreda GU_α i HV_ξ skupova G i H u opštem slučaju je dosta nepregledna. Ako je $\omega \leq \lambda, \eta$, može se dokazati da je $\Sigma M_\omega = (GU_\omega \times HV_\omega) \cup (GU_\omega \times HV_1) \cup (GU_1 \times HV_\omega)$. Posebno, ako je $G = U^0$ i

$H = V^0$, tada za $\lambda,\eta \geq \omega$ euklidski stepen skupa $\Sigma = U^0 \times V^0$ nije konačan. Uz to je i $L = U^0 \times V$ euklidski podskup modula M, i neposredno se zaključuje da je (*) $LM_\nu = \Sigma M_\nu$ $(0 < \nu < \omega)$. S druge strane, kako za svako $a \neq 0$ važi $(a,0) \in L - \Sigma_0$, stepen L-euklidskog razreda modula M kome "pripada" $(a,0)$ ne može biti konačan. To posebno znači da je euklidski stepen skupa L^0 veći od ω, pa na osnovu *Teoreme 1-3* zaključujemo da *minimalna* (a time ni bilo koja druga) L-euklidska valuacija modula M nije konačna. Otuda i naredni

KOROLAR 1-3

Postoji euklidski modul M čija minimalna euklidska valuacija nije konačna. Posebno, postoji KOMUTATIVAN euklidski prsten koji nema nijednu konačnu euklidsku valuaciju. □

Kako za proizvoljne prstene A i B važi $R(A \times B) = R(A) \times R(B)$, iz *Th. 1-9* sledi da Γ-euklidnost prstena A i B povlači Γ-euklidnost njihovog proizvoda $A \times B$. Pri tome, ako su minimalne Γ-euklidske valuacije prstena A i B konačne, onda je to slučaj i sa minimalnom Γ-euklidskom valuacijom prstena $A \times B$. Jasno je da to važi i u slučaju kada se "Γ" zameni sa Δ, odnosno Λ. Neposredno se zaključuje da to važi i za svaki proizvod od konačno mnogo Γ-euklidskih prstena. □

III

LOKALIZACIJA. PROIZVOD I DIREKTNA SUMA EUKLIDSKIH PRSTENA

1. O LOKALIZACIJI I EUKLIDNOSTI PRSTENA

Neka su A i B proizvoljni prsteni i S neprazan podskup od A. Tada za morfizam $f:A\to B$ kažemo da je *S-invertibilan* ako je $f(S)\subset U(B)$, to jest ako elemente skupa S prevodi u jednote prstena B. Za svaki prsten A i neprazan podskup S od A postoji prsten A_S sa, tzv., *univerzalnim S-invertibilnim* morfizmom $h:A\to A_S$, tj. sa svojstvom da za svaki prsten B i S-invertibilni morfizam $f:A\to B$ postoji tačno jedan morfizam $u:A_S\to B$ takav da je $f=u\,h$. Sam prsten A_S zovemo *univerzalnim S-invertibilnim prstenom* prstena A. Pri tome je posebno važan slučaj kada je S *desni IMENITELJ ili DENOMINATOR* prstena A, tj. *multiplikativan* podskup od A (i dakle $1\in S$) koji zadovoljava sledeća dva uslova:

D1. $aS\cap xA\neq\emptyset$ $(a\in A,\ x\in S)$,

D2. *Ako za $a\in A$ i $x\in S$ važi $ax=0$, tada za neko $y\in S$ važi i $ya=0$.*

Slično se definiše i *levi denominator* prstena A. Za prsten A kažemo da zadovoljava *desni Ore-ov* uslov ako važi $D1$ za $S=P(A)$. Ako je S desni denominator u prstenu S, tada je sa

$$(1)\qquad (a,x)\sim(b,y) \iff (\exists\, u,v\in A)(au=bv \wedge xu=yv\in S)$$

definisana jedna relacija ekvivalencije na skupu $A\times S$. Označimo sa a/x klasu ekvivalencije relacije $\sim$ kojoj pripada par (a,x). Uobičajeno je da se odgovarajući količnički skup $A\times S/\sim$ označava sa $A[S^{-1}]=AS^{-1}$, i dakle (*) $AS^{-1}=\{a/x:\ a\in A,\ x\in S\}$. Dalje, za proizvoljne elemente a/x

i b/y iz AS^{-1} postoje $r,s,z \in S$ i $c \in A$ takvi da je $xr = ys = u$ i $xc = bz$, i tada su sa

$$(2) \qquad \frac{a}{x} + \frac{b}{y} = \frac{ar+bs}{u}, \qquad \frac{a}{x} \cdot \frac{b}{y} = \frac{ac}{yz}$$

(dobro) definisane dve binarne operacije + i · na skupu AS^{-1} u odnosu na koje je skup AS^{-1} prsten (sa jedinicom). Sam prsten AS^{-1} je izomorfan univerzalnom S-invertibilnom prstenu A_S, i uz to za odgovarajući S-invertibilni morfizam $h:A \to AS^{-1}$ važi (**) $h(a) = 0$ akko za neko $x \in S$ važi $ax = 0$. Zato ćemo, u slučaju kada je S desni denominator u prstenu A, prstene A_S i AS^{-1} poistovećivati. Inače, samu konstrukciju prstena AS^{-1} zovemo *lokalizacijom* prstena A na skupu S. (*MALCEV* [1])

Ako je S desni denominator prstena A, tada S-invertibilni morfizam $h:A \to A_S$ ne mora biti injekcija. Prema (**) to će biti slučaj akko S ne sadrži desnih delitelja nule prstena A. Kako je za svaki podskup S od $R(A)$ uslov *D2* automatski ispunjen, imamo:

Neprazan podskup S skupa $R(A)$ svih regularnih elemenata prstena A je desni denominator u A akko važi $aS \cap xA \neq \Theta$ $(a \in A,\ x \in S)$, i tada je kanonički morfizam $h:A \to A_S$ injekcija.

Ako je $S \subset R(A)$ denominator u prstenu A, tada prsten A_S zovemo *prstenom S-razlomaka* nad prstenom A, a u slučaju $S = R(A)$ govorimo samo o *prstenu desnih razlomaka* nad prstenom A. Pri tome je sam prsten A izomorfan potprstenu $\tilde{A} = \{a/1:\ a \in A\}$ prstena AS^{-1}. (*ORE* [2], *COHN* [ ])

Ako je S desni denominator prstena A, tada prsten A_S ne mora biti proširenje prstena A. Kako za svako $a \in A$ i $x \in S$ važi $a/x = (a/1)(1/x)$, $(x/1)^{-1} = 1/x$, umesto $a/1$, $1/x$, a/x pisaćemo redom i a, x^{-1}, ax^{-1}. □

TEOREMA 1-1

Neka je S desni denominator u prstenu A. Ako je G desni euklidski podskup prstena A, $\lambda = \partial(GA^*)$ i $L = GS^{-1}$, tada za svako $\alpha < \lambda$ važi:

$$(3) \qquad (GA_\alpha)S^{-1} \subset (GS^{-1})(AS^{-1})_\alpha ,$$

i $L = \{\frac{a}{x}:\ a \in G,\ x \in S\}$ je desni euklidski skup u prstenu $AS^{-1} = A_S$.

DOKAZ. Jasno je da *(3)* važi za $\alpha=0$. Neka je $a_0 = a/x = ax^{-1}$ proizvoljan element iz $(GA_1)S^{-1}$, sa $a \in GA_1$ i $x \in S$. Kako je $a \in G \cap U_2(A)$, postoji $b \in A$ za koje je $ab=1$. Stavimo $b_0 = xb = (x/1)(b/1)$ (u prstenu AS^{-1}). Tada u prstenu AS^{-1} važi $a_0 b_0 = (ax^{-1})(xb) = ab/1 = 1$, pa je a_0 leva jednota prstena AS^{-1}. Otuda a_0 pripada desnom L-euklidskom razredu stepena 1 u prstenu AS^{-1}, pa *(3)* važi i za $\alpha=1$. Neka je $\eta \geq 1$ $(\eta < \lambda)$ fiksiran ordinal i pretpostavimo da *(3)* važi za svako $\alpha < \eta$. Kako je

$$(4) \qquad \cup_{\alpha<\eta} (GA_\alpha)S^{-1} = (\cup_{\alpha<\eta} GA_\alpha)S^{-1} = (GA^*_\eta)S^{-1},$$

kao i $\cup_{\alpha<\eta} L(AS^{-1})_\alpha = L(AS^{-1})^*_\eta$, biće (*) $(GA^*_\eta)S^{-1} \subset L(AS^{-1})^*_\eta$. Neka su $b_0 = b/y$ $(b \in GA_\eta,\ y \in S)$ i $a_0 = a/x$ $(a \in A,\ x \in S)$ proizvoljni elementi iz $(GA_\eta)S^{-1}$ i AS^{-1} respektivno. Kako je $b \in GA_\eta$, postoji $r \in GA^*_\eta$ za koje je $a+bA = r+bA$. To znači da u prstenu A za neko $q \in A$ važi $a-r = bq$, pa u prstenu AS^{-1} imamo

$$(5) \qquad ax^{-1} - rx^{-1} = (by^{-1})q_0,$$

pri čemu je stavljeno $(yq)/x = q_0$. Kako je $q_0 \in AS^{-1}$, stavljajući $r_0 = r/x$ iz *(5)* sledi (**) $a_0 - r_0 \in b_0(AS^{-1})$. S druge strane je $r \in GA^*_\eta$, pa prema (*) imamo $r_0 = rx^{-1} \in L(AS^{-1})^*_\eta$, što zajedno sa (**) upravo znači da je kanoničko preslikavanje $LB^*_\eta \to B/b_0 B$ (sa $B = AS^{-1}$) surjekcija. Otuda je $b_0 \in LB_\eta$, a time i $(GA_\eta)S^{-1} \subset L(AS^{-1})_\eta$, pa *(3)* važi i za $\alpha=\eta$. Uz to je $G = \cup_{\alpha>0} GA_\alpha$, pa na osnovu upravo dokazanog dela tvrdjenja imamo da je

$$(6) \qquad L = GS^{-1} = (\cup_\alpha GA_\alpha)S^{-1} = \cup_{\alpha>0} (GA_\alpha)S^{-1},$$

to jest $L \subset L(AS^{-1})^*$, i prema tome $L = L(AS^{-1})^*$, što prema *II, Teorema 1-3* upravo znači da je $L = GS^{-1}$ desni euklidski podskup prstena AS^{-1}. □

KOROLAR 1-1

> *Neka je S desni denominator prstena A. Ako je prsten A euklidski zdesna, onda je takav i prsten AS^{-1}. Ako je prsten A Λ-euklidski zdesna i $S \subset R(A)$, onda je to slučaj i sa prstenom AS^{-1}.*

DOKAZ. Prvi deo tvrdjenja sledi neposredno iz prethodne *Teoreme 1-1* za

$G = A^0$. Za dokaz drugog dela tvrdjenja stavimo $L = R_\ell(A)$. Kako je prsten A L-euklidski zdesna, prema *Teoremi 1-1* skup LS^{-1} je euklidski zdesna u prstenu AS^{-1}. Otuda će tvrdjenje biti dokazano ako dokažemo da važi (*) $LS^{-1} = R_\ell(AS^{-1})$. Neka je $ax^{-1} \in LS^{-1}$ sa $a \in L$ i $x \in S$, i pretpostavimo da za neko by^{-1} iz AS^{-1} važi $(a/x)(b/y) = 0$. Neka su $c \in A$ i $z \in S$ takvi da je (**) $xc = bz$. Tada je $0 = (a/x)(b/y) = (ac)/u$, i dakle $acs = 0$ za neko $s \in S$. Kako je $a, s \in S$ i $S \subset R(A)$, iz $acs = 0$ sledi $c = 0$, što sa (**) i $z \in S$ daje $b = 0$, a time i $b/y = 0$ u prstenu AS^{-1}. Otuda je LS^{-1} podskup od $R_\ell(AS^{-1})$.

Neka je sada a/x proizvoljan element iz $R_\ell(AS^{-1})$, i pretpostavimo da za neko $b \in A$ važi $ab = 0$. Tada je $(a/x)(xb/1) = 0$, pa u prstenu AS^{-1} mora biti $xb/1 = 0$, a time i $xbs = 0$ za neko $s \in S$, pa slično prethodnom zaključujemo da mora biti $b = 0$. Dakle je $a \in L$, tj. $ax^{-1} \in AS^{-1}$, a time i $R_\ell(AS^{-1}) \subset LS^{-1}$. Otuda i tvrdjenje. □

Prvi deo tvrdjenja iz *Korolara 1-1* u slučaju *komutativnog* prstena A dokazan je (nezavisno) i u *SAMUEL* [1]. Inače, svaki desni euklidski domen zadovoljava desni *Ore*-ov uslov. Iz *Korolara 1-1* za $S = R(A)$ sledi da je A_S telo kome je A potprsten. Otuda se svaki desni (odnosno levi) euklidski domen može utopiti u telo.

TEOREMA 1-2

Ako je A komutativan euklidski prsten, $G = R(A)$ i A_G odgovarajući prsten razlomaka nad A, tada je svaki "medjuprsten" M ($A \subset M \subset A_G$) euklidski i oblika $M = A_S$ za neki multiplikativan podskup S od A.

DOKAZ. Kako je prsten A komutativan, jasno je da je G denominator u A, pa je prsten A_G euklidski. Dokažimo da je $M = A_S$ za neki multiplikativan podskup (a time i denominator) S prstena A. Stavimo

$$S = \{x \in A:\ x^{-1} \in M\} \tag{7}$$

(x^{-1} je inverz od x u prstenu A_G). Neposredno se proverava da je S denominator u A. Uz to prsten M sadrži svaki od elemenata ax^{-1} sa $a \in A$ i $x \in S$, pa je $A_S \subset M$. Obratno, neka je b proizvoljan element prstena M. Iz $M \subset A_G$ sledi da za neko $a \in A$ i $x \in G$ važi $b = a/x$. Pri tome su u prstenu

A svi ideali glavni pa je (*) $aA + xA = cA$. Otuda je $a = cp$, $x = cy$, kao i (**) $cpu + cyv = c$ za neko $p,y,u,v \in A$. Kako je $x = cy = yc$ i $x \in G$, biće i $c \in G$, pa iz (**) sledi $pu + yv = 1$. Iz istih razloga je $y \in G$, pa poslednja jednakost (u prstenu A_G) daje $y^{-1} = y^{-1}pu + v$. S druge strane imamo

$$b = a/x = (cp)/(cy) = p/y = y^{-1}p, \tag{8}$$

što sa prethodnim daje $y^{-1} = bu + v$. Uz to je $u,v \in A$, $A \subset M$ i $b \in M$, pa mora biti $y^{-1} \in M$, a time i $y \in S$. Dakle je $b = p/y$ sa $p \in A$ i $y \in S$, pa je $b \in A_S$. Otuda je $M \subset A_S$, i prema tome $M = A_S$. Sada "euklidnost" prstena A_S sledi direktno iz *Korolara 1-1*. □

PRIMER 1-1. *Neka je A komutativan euklidski domen, K prsten razlomaka nad A i P neprazan podskup skupa $\Pi = \Pi(A)$ svih prostih elemenata prstena A. Tada je*

$$A_{(P)} = \{\tfrac{a}{b} \in K:\ p \in P \Rightarrow p \nmid b\} \tag{9}$$

euklidski potprsten prstena K. Štaviše, svaki međuprsten M između A i K je oblika $A_{(P)}$ za neki podskup P od Π. Posebno, ako je $P = \{p\}$, tada je prsten $A_{(p)}$ lokalni i (p^n) $(n \in N)$ su jedini njegovi pravi ideali.

Zaista, ako je $S = A - (\cup_{p \in P} pA)$ skup svih elemenata a iz A koji nisu deljivi ni sa jednim od elemenata iz P, neposredno se proverava da je S multiplikativan podskup od A za koji važi $A_S = A_{(P)}$. Otuda i prvi deo tvrdjenja. S druge strane, ako je S proizvoljan denominator u A i P skup svih prostih elemenata $p \in \Pi$ koji ne dele nijedan element skupa S, tada je $A_{(P)} = A_S$ (naime, ako je G zasićenje skupa S biće $A_S = A_G$). Kako je uz to, prema Teoremi 1-2, svaki međuprsten M, $A \subset M \subset K$, oblika $M = A_S$ za neki multiplikativni podskup S prstena A, imamo i drugi deo tvrdjenja.

Najzad, ako je $P = \{p\}$, tada je element a/b inverzibilan u prstenu $B = A_{(p)}$ ako i samo ako $p \nmid a$. Otuda je $L = B - U(B)$ upravo skup svih a/b iz B za koje je $p \mid a$, i dakle $L = (p)$. To upravo znači da je prsten $A_{(p)}$ lokalni i da je (p) njegov maksimalni ideal. Dalje, kako je svaki ideal H prstena $A_{(p)} = A_S$ oblika $H = I_S$ za neki ideal I prstena A, to za neko $a \in A$ važi $H = (aA)_S$. Domen A je sa jednoznačnom "faktorizacijom", pa za

neko $n \in N_0$ *i* $c \in A$ *važi* $a = p^n c$ *sa* $p|c$. *Tada je* H *upravo skup svih* $b \in B$ *koji su deljivi sa* p^n, *i dakle* $H = (p^n)$. *Otuda i tvrdjenje.* □

TEOREMA 1-3

Ako je G *multiplikativan desni euklidski podskup i* D *odgovarajući* G*-euklidski defekt* G*-*GA *prstena* A, *tada je i* $S = \{1\} \cup D$ *multiplikativan podskup prstena* A.

Ako je s *desni denominator u prstenu* A *(što će, na primer, sigurno biti ako je* s *u centru* $Z(A)$ *prstena* A*), tada je skup* G_S *euklidski zdesna u prstenu* A_S.

DOKAZ. Neka je $a,b \in D$, a time i $a,b \in G$. Kako je $G \subset A^0$ multiplikativan podskup prstena A, biće $ab \in G$ i $ab \neq 0$. Dalje je $G = D \cup GA^*$, pa je $ab \in D$ ili $ab \in GA^*$. Pretpostavimo da je $ab \in GA^*$. To znači da za neki ordinal α važi $ab \in GA^*$, to jest da je kanoničko preslikavanje $GA^* \to A/abA$ surjekcija. Jasno je da je tada i kanoničko preslikavanje $GA^* \to A/aA$ surjekcija, pa je $a \in GA^*$, a time i $a \in GA^*$, što je u suprotnosti sa učinjenom pretpostavkom $a \in D$, to jest $a \in G\text{-}GA^*$. Dakle je $ab \in D$, pa je D, a samim tim i S, multiplikativan podskup prstena A.

Ako je S desni denominator u prstenu A, tada na osnovu *Teoreme 1-1* važi (*) $(GA^*)S^{-1} \subset H(AS^{-1})^*$, gde je $H = GS^{-1} = G_S$. Dalje, iz $D \subset S$ sledi da je svaki element a/x $a \in D$, $x \in S$ iz D_S inverzibilan u prstenu A_S. Uz to je $a \in D \subset G$, pa je i $a/x \in G_S$, tj. $a/x \in H$, i dakle $a/x \in H(A_S)^*$. Otuda je (**) $D_S \subset H(A_S)^*$. Sada na osnovu (*) i (**) jedno za drugim imamo:

$$H = G_S = (GA^* \cup D)_S = (GA^*)_S \cup (D_S) \tag{10}$$
$$\subset H(A_S)^* \cup (D_S)$$
$$= H(A_S)^*,$$

što sa $H(A_S)^* \subset H$ daje $H = H(A_S)^*$, pa je $H = G_S$ desni euklidski podskup prstena A_S (*II, Th. 1-3*). Otuda i tvrdjenje u celini. □

KOROLAR 1-2

Ako za euklidski defekt D *komutativnog prstena* A *važi* $D \subset R(A)$, *i ako je* $S = D \cup \{1\}$, *tada je prsten* A_S *euklidski.*

DOKAZ. Kako je $A^{\bullet} \cup D = A^{0}$ i $D \subset R(A)$, biće $ab \in A^{\bullet}$ ili $ab \in D$ za svako a,b iz D. Radeći slično kao pri dokazu *Teoreme 1-3*, zaključujemo da ne može biti $ab \in A^{\bullet}$, pa je $ab \in D$. (Primetimo da to ne sledi direktno iz *Th. 1-3* jer skup A^{0} ne mora biti zatvoren u odnosu na množenje.) Preostali deo dokaza je istovetan sa odgovarajućim delom dokaza *Teoreme 1-3* za $G = A^{0}$, jer je (zbog komutativnosti prstena A) skup S denominator u A. □

Ako je D desni Γ-euklidski defekt prstena A i $S = D \cup \{1\}$, tada je S multiplikativan podskup prstena A. Uz to, ako je S desni denominator u A (što će sigurno biti ako je prsten A komutativan), tada na osnovu *Teoreme 1-3* i *Korolara 1-1* neposredno zaključujemo da je odgovarajući prsten razlomaka A_S Γ-euklidski zdesna. □

PRIMER 1-2. *Neka je B proizvoljan komutativan domen, K polje razlomaka nad B i $A = B[X]$. Ako B nije polje, tada je euklidsko jezgro prstena A upravo podskup $U(B)$ prstena B (II, Primer 1-1). Unija S skupova $\{1\}$ i $B^{0}-U(B)$ je denominator prstena A koji je sadržan u euklidskom defektu od A. Lokalizacija A_S prstena A na skupu S je upravo prsten $K[X]$. Kako je K polje, biće prsten A_S euklidski. Uz to euklidski defekt prstena A nije zasićenje skupa S (jer, na primer, $x \in A$ nije proizvod elemenata iz skupa S). Otuda, ako je D euklidski defekt prstena A i $G = D \cup \{1\}$, tada su A_S i A_G različiti euklidski prsteni za koje je $S \subset G$.* □

Ako je prsten B komutativan onda je takav i prsten $A = B[[X]]$ svih formalnih redova po X sa koeficijentima iz B. Otuda postoji prsten razlomaka nad prstenom $B[[X]]$. Označimo ga sa $B((X))$. Jasno je da je $B((X))$ raširenje prstena $B(X)$. Uz to, ako je K prsten razlomaka nad prstenom B, biće $B((X)) \subset K((X))$. Primer prstena $B=Z$ pokazuje da tu ne mora biti $B((X)) = K((X))$. Ako je $B=K$ polje, tada je svaki element iz $K[[X]]$ pridružen nekoj potenciji od X. Otuda je prsten $K[[X]]$ euklidski, i $K((X))$ je upravo lokalizacija prstena $K[[X]]$ na podskupu $S = \{1, X, X^{2}, ..\}$, i dakle $K((X)) = K[[X]][1/X]$. Ako je B *komutativan* euklidski domen, tada prsten $B[[X]]$ ne mora biti euklidski, ali je to slučaj sa prstenom $B[[X]][1/X]$ (*P. SAMUEL* [1]). Dokazaćemo da slično tvrdjenje važi i za prsten oblika $A = B[[X,f,\delta]]$ (to jest prsten svih *formalnih desnih* (f,δ)-*redova* po X sa koeficijentima u *desnom euklidskom* prstenu B).

Elementi prstena $A = B[[X,f,\delta]]$ su formalni redovi $a = \Sigma_{n\geq 0} X^n a_n$, sa koeficijentima iz prstena B. Pri tome je $f:B\to B$ endomorfizam, a δ *desno iterirano f-diferenciranje* prstena B. Drugim rečima, δ je odredjen niz preslikavanja $\delta_n:B\to B$ $(n\in N)$ za koja važi $\delta_n(a+b) = \delta_n(a)+\delta_n(b)$ $(n\in N)$, $\delta_n(1) = 0$ i

$$(11) \qquad \delta_n(ab) = \Sigma_r \delta_r(a)\Delta_r^n(b) \qquad (\delta_0 = f),$$

gde je Δ_r^n "koeficijent" uz T^{n+1} u "polinomu" $P = \left(\Sigma T^{k+1}\delta_k\right)^{r+1}$. Tako, na primer, ako je f surjekcija, $\delta_1 = \delta f$ i $\delta_n = 0$ za $n>1$, tada *(11)* daje $\delta(ab) = \delta(a)f(b)+a\delta(b)$, što upravo znači da je δ desno f-diferenciranje prstena B. Ako je $\delta_n = \delta^n f$ $(n\in N)$ za neko desno f-diferenciranje $\delta:B\to B$ prstena B, tada se *(11)* svodi na dobro poznatu *Leibniz-ovu formulu* za *n-ti f-izvod* $\delta_n(ab)$ proizvoda ab. Zbir dva formalna reda iz A definiše se na uobičajeni način, a proizvod pomoću dodatnog *komutacionog* pravila

$$(12) \qquad aX = Xf(a) + X^2\delta_1(a) + X^3\delta_2(a) + \cdots, \qquad (a\in B).$$

Za $\delta = 0$ *(12)* se svodi na $aX = Xf(a)$, i tada umesto $A = B[[X,f,\delta]]$ pišemo samo $A = B[[X,f]]$. Važan je slučaj kada je $\delta_n = \delta^n f$ $(n\in N)$, pri čemu je δ nilpotentno desno f-diferenciranje prstena B (*T. SMITS [1]*). Ako je bar jedan od koeficijenata a_i formalnog reda a različit od 0, tada ćemo sa $\omega(a)$ označavati najmanji indeks n za koji je $a_n \neq 0$. U tom slučaju sam koeficijent a_n zovemo *početnim koeficijentom* formalnog reda a. □

TEOREMA 1-4

Neka je $f:B\to B$ automorfizam i δ desno iterirano f-diferenciranje prstena B, i označimo sa $A = B[[X,f,\delta]]$ odgovarajući prsten desnih formalnih (f,δ)-redova po X sa koeficijentima iz prstena B.

(α) Skup $S = \{1,X,X^2,..\}$ je levi i desni denominator u prstenu A.

(β) Ako je $\phi:B\to W$ desna euklidska valuacija prstena B za koju je par $(f,1_W)$ automorfizam euklidskog para (B,ϕ), tada je i prsten $A_S = B[[X,f,\delta]][1/X]$ euklidski zdesna.

DOKAZ. (α) Pre svega, na osnovu *(12)* indukcijom po n zaključujemo da za svako $a\in B$ i $n\in N$ važi (*) $aX^n = X^n f^n(a) + X^{n+1}p$, pri čemu je $p = p(a,n)$

jednoznačno odredjen element prstena A. Neka su $a=\Sigma X^n a_n$ i $b=\Sigma X^n b_n$ proizvoljni elementi iz A. Ako je $ab=\Sigma X^n c_n$, tada za svako $n\in N_0$ važi

$$c_n = f^n(a_0)b_n + (\cdot\cdot) + a_n b_0 , \tag{13}$$

pri čemu je $(\cdot\cdot)$ suma od konačno mnogo sabiraka oblika $h(a_i)b_j$, gde je $i,j<n$, a h kompozicija konačno mnogo δ_i-ova (sa $\delta_0=f$). Tako je, npr., $c_0=a_0b_0$, $c_1=f(a_0)b_1+a_1b_0$, $c_2=f^2(a_0)b_2+\delta_0(a_1)b_1+\delta_1(a_0)b_1+a_2b_0$. Posebno je $\omega(ab)\geqslant\omega(a)+\omega(b)$, pri čemu u slučaju kada je B oblast celih važi jednakost.

Dokažimo sada da je S desni denominator u prstenu A. Jasno je da je svaki element $X^n\in S$ regularan sleva. Pretpostavimo da za neko $a\in A$ važi $aX^n=0$. Tada (13) za $b=X^n$ daje $0=f^n(a_0)$, pa kako je f injekcija mora biti $a_0=0$. Otuda je $a=X\tilde{a}$ sa $\tilde{a}=\Sigma X^n a_{n+1}$ $(n\geqslant 0)$, pa iz $aX^n=0$ i leve regularnosti od X sledi da je i $\tilde{a}X^n=0$. Radeći slično prethodnom, dobijamo da je $a_1=0$. Indukcijom po n zaključujemo da za svako $n\in N$ važi $a_n=0$, to jest $a=0$, pa je X^n regularno i zdesna u prstenu A. Dokažimo i da za svako $a\in A$ i $x\in S$ važi $aS\cap xA\neq\Theta$. Neka je $x=X^n$ i $aX^n=\Sigma X^r c_r$. Tada iz (13) (za $b=X^n$) sledi $c_r=0$ za $r<n$, i dakle $\omega(aX^n)\geqslant n$. Otuda je $aX^n=X^n c$ za neko $c\in A$, pa je S desni denominator u A.

Najzad, ako je $c=\Sigma X^n c_n$ proizvoljan element iz A, na osnovu (16) zaključujemo da je s-ti koeficijent u cX^n oblika $f^{n+s}(c_s)+(\cdot\cdot)$, pri čemu u $(\cdot\cdot)$ figurišu c_i-ovi sa $i<s$. Kako je uz to f automorfizam prstena B, za svako $a\in A$ postoji (tačno jedno) $c\in A$ takvo da je $X^n a=cX^n$ (prvo se odredi c_0, zatim c_1, itd.). Otuda je $Sa\cap Ax\neq\Theta$ za svako $a\in A$ i $x\in S$, pa je S i levi denominator u prstenu A. (Prethodno tvrdjenje ne mora da važi ako f nije automorfizam prstena A.)

(β) Za dato $u\in B$ stavimo $q=\Sigma X^n\delta_{n+1}f^{-1}(u)$. Prema upravo dokazanom delu tvrdjenja, postoji tačno jedno $p\in A$ takvo da je $Xq=pX$. Dokažimo da za tako odredjeno p važi

$$uX^{-1} = X^{-1}f^{-1}(u) - p. \tag{14}$$

Zaista, kako je X inverzibilno u prstenu $A_S=A[1/X]$, množeći jednakost (14) zdesna sa X dobijamo njoj ekvivalentnu jednakost $u=X^{-1}vX-pX$ sa $v=f^{-1}(u)$. Kako je $vX=Xf(v)+X^2\delta_1(v)+\cdot\cdot=Xu+Xq$, iz $u=X^{-1}vX-pX$

sledi $u = u + Xq - pX$, to jest $Xq = pX$, za čime se i išlo. Sada na osnovu (*) i (14) zaključujemo da za svako $u \in B$ i svaki ceo broj $m \in Z$ postoji tačno jedan element $p = p(u,m)$ prstena A takav da je

$$(15) \qquad \omega x^m = x^m f^m(u) + x^{m+1} p.$$

To posebno znači da se svaki element $z = a/x$ $(a \in A,\ x \in S)$ prstena $A[1/X]$ (to jest prstena A_S) može (na tačno jedan način) pretstaviti u obliku *Loran-ovog* formalnog reda $z = \Sigma_{s \geqslant m} X^s c_s$ (sa $c_m \neq 0$ za $z \neq 0$), pri čemu je $m = \omega(z)$ izvestan ceo broj i $c_s \in B$ $(s \geqslant m)$. Ako sa $\Omega(z)$ označimo početni koeficijent od $z \in A_S$ (uz dodatni dogovor da je $\Omega 0 = 0$), tada je $\psi = \phi\ \Omega$ desna euklidska valuacija prstena A_S.

Zaista, neka su $a = \Sigma_{s \geqslant m} X^s a_s$ i $b = \Sigma_{s \geqslant n} X^s b_s$ $(b_n \neq 0)$ proizvoljni elementi prstena A_S. Kako je f automorfizam, biće i $u = f^{m-n}(b_n) \neq 0$, pa kako je (B,ϕ) desni euklidski par, postoje $\tilde{q}_0, r \in B$ takvi da je

$$(16) \qquad a_m = u\tilde{q}_0 + r, \qquad \phi(r) < \phi(u).$$

S druge strane, kako je $(f, 1_W)$ automorfizam euklidskog para (B,ϕ), biće $\phi\ f = \phi$, a time i $\phi = \phi\ f^s$ $(s \in Z)$. Otuda je $\phi(u) = (\phi\ f^{m-n})(u) = \phi(b_n)$, i dakle $\phi(r) < \phi(b_n)$, a samim tim i $\phi(r) < \psi(b)$. Stavimo $q_0 = X^{m-n}\tilde{q}_0$. Tada na osnovu (15) i (16) imamo

$$(17) \qquad bq_0 = X^n b_n X^{m-n}\tilde{q}_0 + X^{m+1} c = X^m f^{m-n}(b_n)\tilde{q}_0 + X^{m+1} d,$$

i prema tome

$$(18) \qquad r_0 = a - bq_0 = X^m r + X^{m+1} p,$$

pri čemu su c,d,p izvesni elementi prstena A_S. U slučaju da je $r \neq 0$, iz (18) sledi $a = bq_0 + r_0$ sa $\psi(r_0) = \phi(r) < \psi(b)$, i stvar je gotova. Ako je $r = 0$, tada prethodni postupak ponovimo zamenjujući a sa r_0, itd. Tako dolazimo do dva niza (q_n) i (r_n) elemenata prstena A_S takvih da za $n \in N$ važi r_{n-1} $bq_n + r_n$, to jest (*) $a = b(q_0 +\ \ + q_n) + r_n$, i pri čemu je $\psi(r_n) < \psi(b)$ ili $\omega(q_{n+1}) > \omega(q_n)$, $\omega(r_{n+1}) > \omega(r_n)$. Ako za bar jedno $n \in N$ važi $\psi(r_n) < \psi(b)$, iz (*) sledi $a = bq + r_n$ sa $\psi(r_n) < \psi(b)$, i proces je

završen. U suprotnom za svaki prirodan broj n važi $\omega(r_n) \geqslant n+\omega(r_0)$, kao i $\omega(q_{n+1}) > \omega(q_n)$. To posebno znači da je familija (q_n) $(n\in N)$ zbirljiva u prstenu A_S, pa je $q = \Sigma_{s>0} q_s$ potpuno odredjen element toga prstena. Puštajući u $\omega r_n \geqslant n + \omega r_0$ i (*) da $n \to \infty$ dobijamo $a = bq + 0$. Kako je uz to $\psi(0) < \psi(b)$, imamo i samo tvrdjenje. □

KOROLAR 1-3

Uz pretpostavke i simboliku Teoreme 1-4 pod (B), neka je B domen, K telo razlomaka nad B, h automorfizam tela K čija se restrikcija na prstenu A podudara sa f, i $\delta=0$. Tada za svako $a,b \in B[[X,f]]$ sa $\omega(b)=0$ postoji $c \in K[[X,f]]$ za koje je $a=bc$.

Prsten $A_S = B[[X,f][1/X]$ ima desnu euklidsku valuaciju ψ takvu da za svako $a,b\in A_S$, $b\neq 0$, postoje $q,r\in A_S$ za koje važi (*) $a=bq+r$ sa $\psi r<\psi b$, pri čemu je najvise konačno mnogo koeficijenata od q različito od nule.

DOKAZ. Neka su $a=\Sigma X^n a_n$ i $b=\Sigma X^n b_n$ $(b_0\neq 0)$ proizvoljni elementi iz A i $c=\Sigma X^n c_n$ formalni red iz $K[[X,h]]$. Tada je jednakost $a=bc$ u prstenu $K[[X,h]]$ ekvivalentna sa konjunkcijom sledećih jednakosti (jer je $\delta=0$):

$$a_n = h^n(b_0)c_n + \Sigma_{s<n} h^s(b_{n-s})c_s \qquad (n\in N_0) \tag{19}$$

Kako je $b_0\neq 0$ i h injekcija, biće i $h^n(b_0)\neq 0$ za svako $n\in N$. Na osnovu toga neposredno zaključujemo da "linearni sistem" po c_n-ovima, dat sa (19), ima bar jedno rešenje nad telom K (prvo se odredi c_0, zatim c_1, i tako dalje). Ako svi c_i-ovi nisu u B, neka je n najmanji "indeks" za koji je $c_n\in K-B$ (i dakle $c_i\in B$ za $i<n$). Kako su svi a_s-ovi i b_s-ovi u prstenu B, iz (19) sledi da za uočeno n mora biti $\alpha = h^n(b_0)c_n \in B$. Pri tome je (B,ϕ) desni euklidski par i $\beta = h^n(b_0)\neq 0$, pa postoje κ i γ iz B takvi da je $\alpha=\beta\kappa+\gamma$ sa $\phi(\gamma)<\phi(\beta)$, i prema tome

$$c_n = \kappa + \beta^{-1}\gamma, \qquad \phi(\gamma)<\phi(b_0), \tag{20}$$

jer je $\beta = h^n(b_0) = f^n(b_0)$ i $\phi\circ f = \phi$. Uz to je $\gamma\neq 0$, jer bi u suprotnom prema (20) bilo $c_n\in B$, što smo isključili. Stavimo $q = \Sigma_{s<n} X^s c_s + X^n\kappa$ i $a-bq=r$. Tada je r formalni red iz A čiji je "početni koeficijent"

upravo γ, pa je $a=bq+r$ sa $\psi(r)=\phi(\gamma)<\phi(b_0)=\psi(b)$ (u slučaju kada su a i b formalni redovi iz A).

Neka su sada $\tilde{a}$ i $\tilde{b}$ proizvoljni elementi prstena A_S. Ako je $\tilde{a},\tilde{b}\neq 0$ i $\omega(\tilde{a})=m$, $\omega(\tilde{b})=n$, tada postoje formalni redovi a i $b=\Sigma X^s b_s$ $(b_0\neq 0)$ iz A takvi da je $\tilde{a}=X^m a$, $\tilde{b}=X^n b$. Stavimo $c=\Sigma X^s f^{m-n}(b_s)$. Pri tome je f injekcija, pa iz $b_0\neq 0$ sledi da je i $c_0=f^{m-n}(b_0)\neq 0$, što zajedno sa $\phi\circ f=\phi$ daje $\phi(b_0)=\phi(c_0)$, a time i $\psi(b)=\psi(c)$. Prema upravo dokazanom delu tvrdjenja postoji polinom $q_0\in A$ i formalni red $r_0\in A$ takvi da je $a=cq_0+r_0$ sa $\psi r_0<\psi c$. Množeći poslednju jednakost sleva sa X^m dobijamo $\tilde{a}=X^m cq_0+r$, pri čemu je stavljeno $r=X^m r_0$. Uz to je $\psi r=\psi r_0<\psi c=\psi b$. S druge strane, za svako $u\in B$ i $s\in Z$ je $uX^s=X^s f^s(u)$, a samim tim i $X^s u=f^{-s}(u)X^s$, (jer je f automorfizam prstena B), pa za $s=m-n$ imamo

$$X^s c=\Sigma_{i\geq 0} X^i X^s f^s(b_i)=\Sigma_{i\geq 0} X^i f^{-s}(b_i)X^s \tag{21}$$
$$=\Sigma_{i\geq 0} X^i b_i X^s,$$

to jest $X^s c=bX^s$. Otuda je $X^m cq_0=X^n(X^{m-n}c)q_0=X^n bq$ sa $X^{m-n}q_0=q$, što zajedno sa prethodnim daje $\tilde{a}=\tilde{b}q+r$. Uz to je $\psi(r)<\psi(b)=\psi(\tilde{b})$, i q ima najviše konačno mnogo koeficijenata različitih od nule (jer je to slučaj sa polinomom q_0). Otuda i tvrdjenje. □

TEOREMA 1-5

Ako je (A,ϕ) desni euklidski par i S multiplikativan podskup od A koji je sadržan u centru $Z(A)$ prstena A, tada za proizvoljne elemente a_i $(1\leq i\leq n)$ iz S bez zajedničkih levih faktora, i za svako a iz A, postoje $c_i, c\in A$ takvi da važi

$$\frac{a}{a_1\cdots a_n}=c+\frac{c_1}{a_1}+\cdots+\frac{c_n}{a_n} \tag{22}$$

sa $\phi(c_i)<\phi(a_i)$ $(1\leq i\leq n)$. Ako je uz to A komutativan domen i $S=A^0$, tada je rastav (22) jednoznačan ako i samo ako valuacija ϕ zadovoljava uslova (M) $\phi(a+b)\leq \max\{\phi a, \phi b\}$.

DOKAZ. Neka je $n=1$ i $a=a_1c+c_1$ sa $\phi c_1<\phi a_1$. Iz $S\ Z(A)$ sledi da je S denominator u prstenu A. Kako je $a_1\in S$ biće $a_1c=ca_1$, pa u prstenu A_S

važi $a/a_1 = c + c_1/a_1$, a time i *(22)* za $n=1$. Neka je $n>1$ zadat prirodan broj i pretpostavimo da tvrdjenje važi za svaki prirodan broj manji od n. Kako je u prstenu A svaki desni ideal glavni, postoji $c \in A$ takvo da je $a_1A+\cdots+a_nA = cA$, i dakle

$$(23) \qquad a_1\tilde{b}_1 +\cdots+ a_n\tilde{b}_n = c, \qquad a_s = cc_s \quad (1 \leqslant s \leqslant n),$$

za neke $\tilde{b}_s$-ove i c_s-ove iz A. Uz to a_s-ovi nemaju (pravih) zajedničkih levih delitelja, pa mora biti $c \in U(A)$. Ne umanjujući opštost možemo uzeti da je $c=1$. Kako a_s-ovi pripadaju centru prstena A, množeći prvu od jednakosti *(23)* sleva sa a, i stavljajući $a\tilde{b}_s = b_s$, dobijamo $a = \Sigma\, b_s a_s$. Stavimo $p = a_1\cdots a_n$ i označimo sa p_s proizvod koji se dobije kada se u proizvodu p izostavi faktor a_s. Kako je $a_s \in Z(A)$, biće $p = p_s a_s$ $(1 \leqslant s \leqslant n)$ i prema tome $b_s a_s/p = b_s/p_s$, što sa (*) $a/p = b_1a_1/p_1+\cdots+ b_na_n/p$ daje

$$(24) \qquad a/p = b_1/p_1 +\cdots+ b_n/p_n .$$

Uz to je svaki od p_s-ova proizvod od po $n-1$ različitih elemenata skupa $\{a_1,\ldots,a_n\}$, pa na osnovu induktivne pretpostavke svaki od "razlomaka" b_s/p_s u prstenu A_s ima rastav oblika *(22)*, što zajedno sa *(24)* znači da za neke d_s-ove iz A važi (**) $a/p = d_1/a_1 +\cdots+ d_n/a_n$. Najzad, kako je za $n=1$ tvrdjenje već dokazano, postoje q_s-ovi i c_s-ovi iz A za koje je $d_s/a_s = q_s + c_s/a_s$ sa $\phi c_s < \phi a_s$ $(1 \leqslant s \leqslant n)$, pa stavljajući $q_1+\cdots+q_n = c$ iz (**) dobljamo rastav *(22)* sa $\phi c_s < \phi a_s$ $(1 \leqslant s \leqslant n)$.

Neka je sada A komutativan domen i $S = A^0$. Prema *I, Teorema 2-5*, ϕ zadovoljava uslov (M) ako i samo ako za svako $a \in A$ i $b \in A^0$ postoje jednoznačno odredjeni elementi $q, r \in A$ takvi da je $a = bq+r$ sa $\phi r < \phi b$. Na osnovu toga, iz jednoznačnosti rastava *(22)* neposredno sledi da valuacija ϕ zadovoljava uslov (M) (dovoljno je uzeti $n=1$ i $b=a_1$). Obratno, ako ϕ zadovoljava uslov (M), indukcijom po n neposredno zaključujemo da $0 = 0/p$ ima jednoznačan rastav oblika *(22)* (naime, množeći *(22)* sa a_n na desnoj strani dobljamo sumu od $n-1$ razlomaka, itd.). Jasno je da su tada svi rastavi oblika *(22)* (sa $\phi c_s < \phi a_s$) jednoznačni.

Ako valuacija ϕ zadovoljava uslov (M), tada za svako $a \in A$ i $b \in S$ postoje a_s-ovi iz A takvi da je $a = \Sigma_s\, b^{n-s} a_s$ $(0 \leqslant s \leqslant n)$ sa $\phi a_s < \phi b$ za $s > 0$, a time i $a/b^r = c + c_1/b +\cdots+ c_r/b^r$, $\phi c_s < \phi b$ $(1 \leqslant s \leqslant r)$. □

Neka je L ideal prstena A. Za element $a \in A$ kažemo da je *L-regularan sleva (zdesna)* ako za svako $b \in A$ važi $ab \in L \Rightarrow b \in L$ ($ba \in L \Rightarrow b \in L$). Element a je *L-regularan* (ili *regularan* u odnosu na dati ideal L) ako je L-regularan i sleva i zdesna. Jasno je da se (leva, desna) regularnost u odnosu na nula-ideal u prstenu A podudara sa uobičajenom (levom desnom) regularnošću u tom prstenu. Sa $R_d(A,L)$, $R_l(A,L)$ i $R(A,L)$ označavaćemo redom skupove svih elemenata prstena A koji su (zdesna, sleva) regularni u odnosu na ideal L.

Za prsten A kažemo da je *prost* ako za svaka dva njegova ideala L i G važi $LG = 0 \Rightarrow (L=0 \vee G=0)$, što je ekvivalentno sa tim da za svako $a,b \in A$ važi $aAb = 0 \Rightarrow (a=0 \vee b=0)$. Prsten A je *poluprost* ako za svaki njegov ideal L važi $L^2 = 0 \Rightarrow L = 0$. Za ideal P prstena A kažemo da je *prost* (*poluprost*) ako je takav prsten A/P, to jest ako za svako $a,b \in A$ važi implikacija $aAb \subset P \Rightarrow (a \in P \vee b \in P)$ (odnosno: $aAa \subset P \Rightarrow a \in P$).

Pod *invarijantnim* elementom prstena A podrazumevamo svaki njegov element a za koji je $aA = Aa$ (*COHN* [*10*]). Skup svih takvih elemenata u prstenu A označavaćemo sa $I(A)$. Glavne ideale prstena A generisane nekim invarijantnim elementom zvaćemo njegovim *invarijantnim idealima*. Regularan element $a \in A$ je invarijantan akko su aA, Aa obostrani ideali prstena A. Ako za elemente $a,b \in A$ važi $aA = bA$, tada a i b ne moraju da budu pridruženi zdesna u prstenu A. Dalje, ako je $L = aA = Ab$ obostrani glavni ideal prstena A, tada ne mora biti $L = cA = Ac$ ni za jedno c iz A.

TEOREMA 1-6

Neka je P prost ideal desnog euklidskog prstena A. Ako je prsten A neterovski sleva, tada je skup $S = R(A,P)$ svih P-regularnih elemenata prstena A multiplikativan podskup od A, i za svako $a \in A$ i $x \in S$ važi $aS \cap xA \neq \Theta$. Ako je uz to $S \subset R_d(A)$, S je desni denominator u prstenu A, i prsten A_S je euklidski zdesna.

DOKAZ. Neka je $x,y \in S$. Tada iz $xya \in P$ sledi $ya \in P$, a time i $a \in P$. Slično iz $axy \in P$ sledi $a \in P$, pa je $xy \in S$, što sa $1 \in S$ upravo znači da je S multiplikativan podskup prstena A. Dokažimo da za svako $a \in A$ i $x \in S$ važi $aS \cap xA \neq \Theta$. Zaista, kako je ideal P prost, A/P je prost desni euklidski i levi neterovski prsten. Otuda je $R(A/P)$ desni denominator u prstenu

A/P (*GOLDIE* [2], *Th. 4-1*). Kako je $\tilde{x} = x+P$ regularno u prstenu A/P akko je $x \in S$, postoje $y \in S$ i $b \in A$ takvi da je $\tilde{a}\tilde{y} = \tilde{x}\tilde{b}$, i dakle (*) $ay - xb = r$ za neko $r \in P$.

S druge strane, svaki desni ideal prstena A je glavni, pa postoji $c \in A$ za koje je $aA + xA = cA$, i dakle $au - xv = c$, $a = ca_0$, $x = cx_0$ za neko $u, v, x_0, a_0 \in A$. Otuda (*) možemo zapisati u obliku (**) $c(a_0 y - x_0 b) = r$. Dalje, kako je prsten A neterovski sleva, biće to i prsten A/P, pa se u prstenu A/P levi i desni delitelji 0 podudaraju (*GOLDIE* [1], *Lema 3-9*). Otuda je $R_d(A/P) = R(A/P)$, a time i $R_d(A,P) = R(A,P) = S$.

Kako je P obostran ideal prstena A, $zc \in P$ povlači $zcx_0 \in P$, to jest $zx \in P$, pa $x \in S$ daje $z \in P$. To upravo znači da je $c \in R_d(A,P)$, a time i $c \in S$. Uz to je $r \in P$, pa iz (**) sledi $a_0 y - x_0 b = r_0$ sa $r_0 \in P$ i $r = cr_0$. Množeći jednakost $au - xv = c$ zdesna sa r_0, i stavljajući $ur_0 = p$ i $vr_0 = q$ dobijamo $ap - xq = r$, što sa (*) daje $a(y-p) = x(b-q)$. Dalje, $r_0 \in P$ povlači $p, q \in P$, pa stavljajući $y_0 = y - p$ i $b_0 = b - q$, biće $y_0 = y$, tj. $y_0 \in S$, što sa $ay_0 = xb_0$ daje $aS \cap xA \neq \Theta$. Otuda i prvi deo tvrdjenja.

Za dokaz drugog dela tvrdjenja dovoljno je dokazati da je svako x iz S regularno sleva u prstenu A, a time i $S \subset R(A)$. Pretpostavimo da za neko $x \in S$ i $a \in A$ važi $xa = 0$, i stavimo $L_n = \{c \in A: \ x^n c = 0\}$. Pri tome je (L_n) $(n \in N)$ rastući niz desnih ideala desnog euklidskog prstena A, pa u nizu (L_n) mora biti jednakih članova. Neka je $L_n = L_{n+1}$. Kako je $x^n \in S$, prema dokazanom delu tvrdjenja postoje $y \in S$ i $b \in A$ takvi da je $ay = x^n b$. Uz to je $xa = 0$, pa množeći prethodnu jednakost sleva sa x dobijamo da je $0 = x^{n+1} b$. To znači da je $b \in L_{n+1}$, a time i $b \in L_n$. Otuda je $x^n b = 0$, što sa $ay = x^n b$ daje $ay = 0$, pa kako je $y \in S$ i $S \subset R_d(A)$, mora biti $a = 0$. Prema tome, za svako $a \in A$ i $x \in S$ važi $xa = 0 \Rightarrow a = 0$, što zajedno sa $S \subset R_d(A)$ znači da je i $S \subset R(A)$. Otuda i tvrdjenje u celini. □

PRIMER 1-3. *Neka je A desni euklidski prsten o kome je bilo reči u II, Primer 1-2. Ako je $e = M_{01}$, tada je $E = eA$ obostran ideal prstena A. Uz to je $ee = 0$, pa ideal E ne sadrži nijedan regularan element prstena A. Prsten A je neterovski sleva. Zaista, ako je I proizvoljan levi ideal prstena A i $G = \{M_{ab}: \ a, b \in L[X]\}$, tada se neposredno zaključuje da skup $H = I \cap G$ generiše levi ideal I (jer je $AI = I$). Označimo sa $u = M_{ab}$ bilo koji od elemenata skupa H, pri čemu je b polinom po X^2 minimalnog stepena, i sa $v = M_{pq}$ bilo koji od elemenata iz H, pri čemu je $q \notin L[X^2]$*

polinom sa minimalnim "neparnim" stepenom. Kako je L[X] i levi i desni euklidski prsten, posle kraćeg računa dobijamo da je svaki element M_{xy} iz H oblika

$$M_{xy} = M_{\alpha\beta}M_{ab} + M_{rs}M_{pq} \tag{25}$$

za neke "skalare" α,ß,r,s∈K. Otuda je H ⊂ Au+Av, pa kako je u,v∈I i H generatrisa (levog) ideala I, imamo I = Au + Av. Dakle, svaki levi ideal I prstena A ima dvočlanu generatrisu, pa je prsten A neterovski sleva, i dakle zadovoljava uslove Teoreme 1-6.

S druge strane, neposredno se proverava da za svako u,v iz A važi uAv⊂E => (u∈E ∨ v∈E), pa je ideal E prost. Pri tome je R(A) = A-E, a samim tim i R(A,E) ⊂ R(A). Otuda je, prema Teoremi 1-6, skup S=R(A,E) je desni denominator prstena A i prsten A_S je euklidski zdesna. □

KOROLAR 1-4

Neka je A prost desni euklidski (ili glavnoidealski) prsten. Tada za svaki prost invarijantan ideal P prstena A važi R(A,P)⊂R(A). Ako je uz to prsten A neterovski sleva, tada je skup R(A,P) desni denominator u A.

DOKAZ. Jasno je da drugi deo tvrdjenja sledi iz prvog dela i prethodne *Teoreme 1-6*. Zato dokažimo samo da je svako *a* iz *S = R(A,P)* regularno u prstenu *A*. Pretpostavimo da za neko *x∈A* važi *xa = 0*, a time i *xa∈P*. Kako je a *P*-regularno, mora biti *x∈P*. Dalje, ideal *P* je invarijantan pa za neko *c∈A* važi *P = cA = Ac*. Uz to je *c* regularan element prstena *A* (*GOLDIE* [3], *Lemma 1-1*). Indukcijom po *n∈N* zaključujemo da za svaki prirodan broj *n* važi $x \in c^n P$. Neka je *L* ideal prstena *A* generisan sa *x*. Tada za neko *b* iz *R(A)* važi *L = bA*. Pri tome iz $x \in c^n A$ i *cA = Ac* sledi $L \subset c^n A = Ac^n$. Otuda za svako *n∈N* postoji $b_n \in A$ takvo da je (*) $b = b_n c^n$.

Ako je $L_n = \{u \in A: uc^n \in L\}$, tada je (L_n) $(n \in N)$ rastući niz desnih ideala prstena *A*, pa medju njima mora biti jednakih. Neka je $L_n = L_{n+1}$. Tada iz $b_{n+1}c^{n+1} = b \in L$ sledi $b_{n+1} \in L_{n+1}$, a time i $b_{n+1} \in L_n$. Otuda je $b_{n+1}c^n \in L$, i dakle $b_{n+1}c^n = bv$ za neko $v \in A$. Množeći prethodnu relaciju zdesna sa *c*, na osnovu prethodnog dobijamo $b = bvc$. Uz to je $b \in R(A)$ pa za $n>0$ važi $1 = vc$, a time i $P = A$. Prema tome, za $P \neq 0$ mora biti $L = 0$,

to jest $x=0$, pa je $a \in R_{\hat{c}}(A)$. Slično zaključujemo da je $a \in S$ regularno i sleva u prstenu A, što zajedno sa prethodnim daje $S \subset R(A)$, a time i samo tvrdjenje. □

2. PROIZVOD I DIREKTNA SUMA EUKLIDSKIH PRSTENA

Ako je I neprazan skup indeksa i (A_i) $(i \in I)$ proizvoljna familija prstena (sa jedinicama), tada ćemo sa ΠA_i $(i \in I)$ označavati njen (dekartovski) proizvod, a sa ΘA_i $(i \in I)$ njenu direktnu sumu. U slučaju kada je $A_i = A$ za svako $i \in I$, umesto ΠA_i i ΘA_i pisaćemo redom A^I i $A^{(I)}$. Za $I = \{1,..,n\} = [1,n]$ koristićemo uobičajene oznake za proizvod i sumu od konačno mnogo prstena (odnosno modula).

Prema *II, Korolar 1-2*, proizvod dva desna euklidska (Λ-euklidska) prstena je desni euklidski (Λ-euklidski) prsten. Jasno je da to važi i za proizvod od konačno mnogo takvih prstena. S druge strane, proizvod (konačno mnogo) prstena je samo jedan primer *projektivnog limesa* odredjene projektivne familije u kategoriji *ANN*, pa se samo po sebi nameće pitanje da li prethodni rezultat važi i u tom slučaju. Na neke teškoće u vezi sa tim problemom ukazuje naredna *Teorema 2-1*.

U prvom poglavlju (*I, Definicija 1-4*) je uveden pojam *kategorije* desnih euklidskih parova, koju ćemo označavati sa *EUC*. Ako je $F = (f,h)$ morfizam u kategoriji *EUC*, neposredno se dokazuje da je f monomorfizam u kategoriji *ANN* (jer je h injekcija).

TEOREMA 2-1

(α) Proizvod A proizvoljne familije (A_i) $(i \in I)$ euklidskih prstena ne mora biti euklidski prsten. Pri tome može biti i $I = N$.

(β) Ako je I dobro uredjen skup, tada je proizvod A Λ-euklidskih prstena A_i $(i \in I)$ takodje Λ-euklidski prsten.

DOKAZ. (α) Neka je $I = N$ i $A_i = R$ za svako $i \in N$. Tada je A upravo prsten R^N svih realnih nizova (sa koordinatnim operacijama). Za proizvoljno k

iz N označimo sa e_k niz iz A dat sa: $e_k(k)=1$, $e_k(s)=0$ $(s\neq k)$. Ako bi prsten A bio euklidski, tada bi svaki njegov ideal bio glavni, i dakle oblika aA za neko $a=(a_i)$ iz A. To bi posebno važilo za ideal L generisan skupom $\{e_1,e_2,..\}$. Ako je $L=aA$, tada za neki niz $b=(b_i)$ $(i\in I)$ iz A važi $e_k=ab=(a_i)(b_i)\in L$, a time i $1=a_kb_k$. Kako tu k može biti bilo koji prirodan broj, zaključujemo da je svaki član niza a različit od 0. Medjutim, to nije moguće jer je a A-linearna kombinacija e_k-ova, pa je najviše konačno mnogo članova niza a različito od nule. Dakle, u komutativnom prstenu $A=R^N$ svi ideali nisu glavni pa time ne može biti ni euklidski.

(β) Neka je $\phi_i:A_i\to W_i$ $(i\in I)$ desna euklidska valuacija prstena A_i i označimo sa $W=\prod W_i$ proizvod familije (W_i) $(i\in I)$ u kategoriji Ens. Kako je skup indeksa I dobro uredjen, skup W je dobro uredjen u odnosu na leksiografsko uredjenje. Dokazaćemo da je sa

$$\phi a=(\phi_i a_i),\qquad a=(a_i)\in A, \tag{1}$$

definisana jedna desna Λ-euklidska valuacija $\phi:A\to W$ prstena A. Neka su $a=(a_i)$ i $b=(b_i)$ redom proizvoljni elementi iz A i $R(A)$. Kako je $R(A)$ upravo proizvod $\prod R(A_i)$ $(i\in I)$, biće $b_i\in R(A_i)$ za svako $i\in I$. Prsten A_i je Λ-euklidski zdesna, pa postoje $q_i\in A_i$ i $r_i\in R_0(A_i)$ takvi da je

$$a_i=b_iq_i+r_i,\qquad \phi_ir_i<\phi_ib_i. \tag{2}$$

Ako je u (2) $r_i=0$ za svako $i\in I$, stavimo $r=(r_i)=0$. Ako je bar jedan od r_i-ova različit od 0, stavimo $r=(\bar r_i)$ i $q=(\bar q_i)$, gde je $\bar r_i=r_i$ i $\bar q_i=q_i$ za $r_i\neq 0$, odnosno $\bar r_i=b_i$ i $\bar q_i=q_i-1$ za $r_i=0$. Tada za svako $i\in I$ važi $a_i=b_i\bar q_i+\bar r_i$, a time i (*) $a=b\bar q+\bar r$. Pri tome za svako i iz I važi $\phi_i\bar r_i<\phi_ib_i$, sa $\phi_k\bar r_k<\phi_kb_k$ za bar jedno $k\in I$. Kako je uredjenje u skupu W leksiografsko, biće $(\phi_i\bar r_i)<(\phi_ib_i)$, što prema (1) znači da je (**) $\phi r<\phi b$. Uz to je $r\in R_0(A)$, što sa (*) i (**) upravo znači da je ϕ jedna desna Λ-euklidska valuacija prstena A. □

Neka je (B_I) $(i\in N)$ familija desnih euklidskih prstena, $A=\prod B_I$, i za svaki prirodan broj n stavimo $A_n=B_1\times\cdots\times B_n$. Ako je f_n "kanonički" monomorfizam prstena A_n u prsten A, tada (desna) euklidnost prstena A_n

povlači euklidnost potprstena $P_n = f_n(A_n)$ prstena A. To posebno znači da je (P_n) $(n\in N)$ jedan lanac (desnih) euklidskih potprstena prstena A. Radeći slično kao pri dokazu *Teoreme 2-1* pod (α) zaključujemo da unija P "uzlazne" familije euklidskih prstena P_n $(n\in N)$ ne mora biti euklidski prsten. Iz *Teoreme 2-1* takodje sledi da postoji komutativan Λ-euklidski prsten koji nije euklidski.

TEOREMA 2-2

Neka je I dobro uredjen skup i (P_i,F_{ij}) projektivna I-familija u kategoriji EUC, *pri čemu je $P_i=(A_i,\phi_i)$ i $F_{ij}=(f_{ij},h_{ij})$ $(i\leqslant j)$.*

Ako je (A,f_i) projektivni limes projektivne I-familije (A_i,f_{ij}) u kategoriji ANN, *i ako za svako $i\in I$ desna euklidska valuacija ϕ_i zadovoljava uslov (M) $\phi_i(a+b)\leqslant \max(\phi_i a, \phi_i b)$ $(a,b\in A_i)$, tada i prsten A ima desnu euklidsku valuaciju koja zadovoljava uslov (M).*

DOKAZ. Za $a\in A$ postoji tačno jedno $a_i\in A_i$ takvo da je $f_i a = a_i$, pa ćemo pisati $a=(a_i)$ $(i\in I)$ (uz napomenu da ćemo za proizvoljno preslikavanje f umesto $f(x)$ pisati i fx). Pri tome za $i\leqslant j$ važi (*) $f_i = f_{ij}\circ f_j$, pa za $a=(a_i)\in A$ imamo $a_i = f_{ij}a_j$ $(i,j\in I,\ i\leqslant j)$. Ako je $a_i=0$ za bar jedno $i\in I$, tada je i $a=0$. Naime, za $j<i$ je $a_j = f_{ji}a_i = f_{ji}0 = 0$, dok za $i\leqslant j$ imamo $0=a_i=f_{ij}a_j$, a time i $a_j=0$ (jer je f_{ij} monomorfizam).

Neka su $a=(a_i)$ i $b=(b_i)$ redom proizvoljni elementi iz A, odnosno A^0. Tada je $b_i\neq 0$ za svako $i\in I$. Kako je ϕ_i (desna) euklidska valuacija prstena A_i, postoje q_i,r_i iz A_i takvi da je

$$a_i = b_i q_i + r_i, \qquad \phi_i r_i < \phi_i b_i \qquad (i\in I). \tag{3}$$

Dokažimo da $q=(q_i)$ i $r=(r_i)$ pripadaju prstenu A, to jest da za $i\leqslant j$ važi $q_i = f_{ij}q_j$ i $r_i = f_{ij}r_j$. Kako $a,b\in A$, iz $a_j = b_j q_j + r_j$ sledi (za $i\leqslant j$)

$$f_{ij}a_j = (f_{ij}b_j)(f_{ij}q_j) + (f_{ij}r_j), \tag{4}$$

to jest (**) $a_i = b_i\tilde{q}_i + \tilde{r}_i$, gde je $\tilde{q}_i = f_{ij}q_j$, $\tilde{r}_i = f_{ij}r_j$. Uporedjujući relacije (3) i (**) dobijamo (¤) $\tilde{r}_i - r_i = b_i(q_i-\tilde{q}_i)$, $r_i,\tilde{r}_i\in A_i$ $(i\in I)$.

Stavimo $\alpha = \max\{\phi_i r_i, \phi_i r_i\}$ i $\beta = \phi_i b_i$. Kako valuacija ϕ_i zadovoljava

uslov (M), biće i $\phi_i(r_i-r_i) \leqslant \alpha$. Ako bi bilo $q_i \neq \bar{q}_i$, tj. $q_i-\bar{q}_i \neq 0$, tada bi iz (π) sledilo

$$\alpha \geqslant \phi_i(\bar{r}_i-r_i) = \phi_i\big(b_i(q_i-\bar{q}_i)\big) \geqslant \phi_i b_i. \tag{5}$$

S druge strane, (f_{ij},h_{ij}) je morfizam (desnog euklidskog) para (A_j,ϕ_j) u par (A_i,ϕ_i), pa je $h_{ij}\circ\phi_j = \phi_i\circ f_{ij}$. Uz to funkcija h_{ij} strogo raste, pa $\phi_j r_j < \phi_j b_j$ povlači $h_{ij}\phi_j r_j < h_{ij}\phi_j b_j$, to jest $\phi_i f_{ij} r_j < \phi_i f_{ij} b_j$, i prema tome $\phi_i \bar{r}_i < \phi_i b_i$. Otuda je i $\alpha < \phi_i b_i$, što je u suprotnosti sa relacijom (5). Dakle, mora biti $\bar{q}_i = q_i$, a samim tim i $\bar{r}_i = r_i$. To znači da za svako $i,j \in I$ $(i<j)$ važi $r_i = f_{ij} r_j$, $q_i = f_{ij} q_j$, pa je $r,q \in A$, za čime se i išlo.

Ako je $W_i = \phi_i(A_i)$, označimo sa W proizvod ΠW_i $(i \in I)$ u kategoriji Ens. Kako je skup I dobro uredjen, biće i skup W dobro uredjen u odnosu na leksografsko uredjenje. Neka je $\phi: A \to W$ preslikavanje definisano sa $\phi a = (\phi_i a_i)$ $(i \in I)$, gde je $a = (a_i)$ $(i \in I)$ proizvoljan element prstena A. Prema (3) za svako $a \in A$ i $b \in A^0$ postoje $q,r \in A$ za koje je $a = bq+r$. Uz to je $\phi r = (\phi_i r_i) < (\phi_i b_i) = \phi b$, što sa prethodnim upravo znači da je ϕ jedna desna euklidska valuacija prstena A.

Dokažimo sada da i valuacija ϕ zadovoljava uslov (M). Neka su a i b proizvoljni elementi prstena A i pretpostavimo da je $\phi a \leqslant \phi b$. Tada je $\phi_i a_i \leqslant \phi_i b_i$ za svako $i \in I$. Naime, ako je 0 minimalni član skupa I, tada iz $\phi a = (\phi_i a_i) < (\phi_i b_i) = \phi b$ sledi $\phi_0 a_0 \leqslant \phi_0 b_0$. Pretpostavimo da za neko $s \in I$ važi $\phi_s a_s > \phi_s b_s$. Tada je i $h_{os}\phi_s a_s > h_{os}\phi_s b_s$, što sa $h_{os}\phi_s = \phi_o f_{os}$ i $f_{os}a_s = a_o$, $f_{os}b_s = b_o$ daje $\phi_0 a_0 > \phi_0 b_0$, a to je suprotno prethodnom zaključku. S druge strane, svaka od valuacija ϕ_i zadovoljava uslov (M) pa za svako $i \in I$ važi $\phi_i(a_i-b_i) \leqslant \phi_i b_i$, a samim tim i $\phi(a-b) \leqslant \phi b$, što sa $\phi a \leqslant \phi b$ upravo znači da i valuacija ϕ zadovoljava uslov (M). Otuda i tvrdjenje u celini. □

KOROLAR 2-1

Neka je I dobro uredjen skup i (A_i) $(i \in I)$ opadajući lanac potprstena nekog prstena B. Ako svaki od prstena A_i ima desnu euklidsku valuaciju ϕ_i koja zadovoljava uslov (M), i ako za svako $i<j$ važi $\phi_i|A_j = \phi_j$, tada i prsten $A = \cap A_i$ $(i \in I)$ ima euklidsku valuaciju koja zadovoljava uslov (M).

DOKAZ. Stavimo $W_i = \phi_i(A_i)$, $i \in I$. Tada za svako $i<j$ važi $W_i \supset W_j$. Ako su $f_{ij}: A_j \to A_i$ i $h_{ij}: W_j \to W_i$ kanoničke injekcije, neposredno se proverava da su za $P_i = (A_i, \phi_i)$ i $F_{ij} = (f_{ij}, h_{ij})$ ispunjeni uslovi Teoreme 2-2, pa je $\hat{A} = \varprojlim A_i$ desni euklidski prsten koji ima bar jednu desnu euklidsku valuaciju ϕ koja zadovoljava uslov *(M)*. S druge strane, jasno je da je $A = \cap_{i \in I} A_i$ projektivni limes projektivne familije (A_i, f_{ij}) u kategoriji *ANN*, pa su prsteni A i $\hat{A}$ izomorfni. □

TEOREMA 2-3

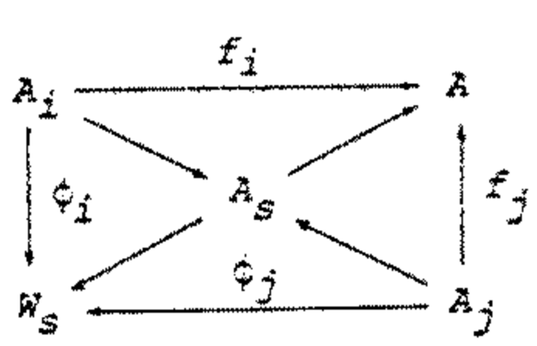
> *Neka je $(I, \leqslant)$ desni filtar i $F = (P_i, F_{ji})$ $(i,j \in I,\ i \leqslant j)$ induktivna familija u kategoriji EUC, gde je $P_i = (A_i, \phi_i)$ i $F_{ji} = (f_{ji}, h_{ji})$.*
>
> *Ako za svako $i \leqslant j$ važi $h_{ji} \circ \phi_i = \phi_i$, tada u kategoriji EUC postoji induktivni limes (P, F_i) familije F. Ako je pri tome $F_i = (f_i, h_i)$ i $P = (A, \phi)$, tada je (A, f_i) induktivni limes familije (A_i, f_{ji}) $(i \in I)$ u kategoriji ANN.*

DOKAZ. Jasno je da je (A_i, f_{ji}) induktivna familija u *ANN*. Kako je $(I, \leqslant)$ desni filtar, familija (A_i, f_{ji}) ima induktivni limes (A, f_i) u kategoriji *ANN*. Dokažimo prvo da je prsten A euklidski zdesna. Pre svega, za svako $a \in A$ postoji bar jedno $i \in I$ i $a_i \in A_i$ takvi da je $a = f_i a_i$. Pri tom za svako $i,j \in I$ važi

$$f_i a_i = f_j a_j \quad \Rightarrow \quad \phi_i a_i = \phi_j a_j. \tag{6}$$

Zaista, kako je f_{ji} injekcija za svako i j, biće to slučaj i sa svakim od morfizama f_i (jer je $Ker(f_i) = \cup_{j \geqslant i} Ker(f_{ji})$). Dalje, kako je $(I, \leqslant)$ desni filtar, za svako $i,j \in I$ postoji bar jedno $s \in I$ za koje je $i,j \leqslant s$, a time i $f_i = f_s \circ f_{si}$, $f_j = f_s \circ f_{sj}$. Uz to dijagram

(7)



komutira, pa $f_i a_i = f_j a_j$ daje $f_s f_{si} a_i = f_s f_{sj} a_j$, to jest $f_{si} a_i = f_{sj} a_j$ (jer je f_s injekcija). Otuda je $\phi_s f_{si} a_i = \phi_s f_{sj} a_j$, tj. $\phi_i a_i = \phi_j a_j$, a

samim tim i *(6)*. Prema tome, ako za $a \in A$ važi $a = f_i a_i$ i $a = f_j a_j$, tada je $\phi_i a_i = \phi_j a_j$, pa je sa

$$\phi a = \phi_i a_i , \qquad a = f_i a_i \in A , \tag{8}$$

(dobro) definisano jedno preslikavanje $\phi: A \to \tilde{W}$ prstena A u dobro uredjen skup $\tilde{W} = \cup_{i \in I} W_i$ (čije je uredjenje indukovano uredjenjima skupova W_i). Dokažimo da je ϕ desna euklidska valuacija prstena A. Za proizvoljno a iz A i b A postoje $i,j \in I$ i $a_i \in A_i$, $b_j \in A_j$ za koje je $a = f_i a_i$, odnosno $b = f_j b_j$. Pri tome je $i,j \leqslant s$ za bar jedno $s \in I$, pa je

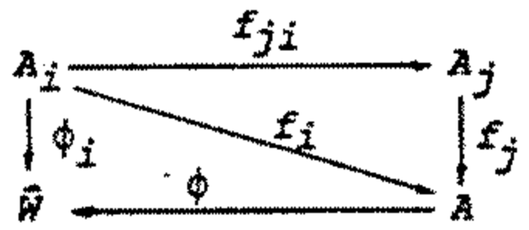
$$a = f_i a_i = f_s f_{si} a_i = f_s a_s , \tag{9}$$

i slično $b = f_s b_s$, gde su $a_s = f_{si} a_i$ i $b_s = f_{sj} b_j$ članovi prstena A_s. Uz to je f_{sj} injekcija pa je i $b_s \neq 0$. Kako je (A_s, ϕ_s) desni euklidski par, postoje $q_s, r_s \in A_s$ takvi da je $a_s = b_s q_s + r_s$ sa $\phi_s r_s < \phi_s b_s$. Otuda, ako stavimo $q = f_s q_s$ i $r = f_s r_s$, biće

$$a = f_s a_s = f_s(b_s q_s + r_s) = \cdots = bq + r , \tag{10}$$

sa $\phi r = \phi_s r_s$ i $b = \phi_s b_s$, i dakle $\phi r < \phi b$, pa je $\phi: A \to W$ desna euklidska valuacija prstena A, a time i (A,ϕ) odredjen objekt u kategoriji *EUC*. Dalje, prema *(8)* je $\phi_i a_i = \phi a = \phi f_i a_i$ $(a_i \in A_i)$, pa dijagram

(11)



komutira za svako $i \leqslant j$ $(i,j \in I)$. Ako je $W = \phi(A)$, tada iz *(11)* sledi da je $F_i = (f_i, 1_W)$ morfizam objekta (A_i, ϕ_i) u objekt (A,ϕ) u *EUC*, kao i da za svako $i,j \in I$, $i \leqslant j$, važi $F_i = F_j \circ F_{ji}$.

Najzad, neka je (B,ψ) objekt i $G_i = (g_i, u_i)$ $(i \in I)$ morfizam objekta (A_i,ϕ_i) u (B,ψ). Ako za svako $i \leqslant j$ važi $G_i = G_j \circ F_{ji}$, dokažimo da tada postoji tačno jedan morfizam $G = (g,u)$ od (A,ϕ) u (B,ψ) sa svojstvom da za svako $i \in I$ važi $G_i = G \circ F_i$. Zaista, za $i \leqslant j$ iz $G_i = G_j \circ F_{ji}$ sledi da je $g_i = g_j \circ f_{ji}$, kao i $u_i = u_j \circ 1_W = u_j$. Neka je s fiksiran element iz I Kako za svako $i \in I$ postoji $k \in I$ za koje je $i,s \leqslant k$, biće $u_s = u_i = u_k$, a time i

$u_i = u_s$ za svako $i \in I$. Stavimo $u_s = u$. S druge strane, (A, f_i) je induktivni limes familije (A_i, f_{ji}) $(i,j \in I,\ i \leqslant j)$ u kategoriji *ANN*, pa kako (u toj kategoriji) za morfizme $g_i : A_i \to B$ važi $g_i = g_j \circ f_{ji}$ $(i,j \in I,\ i \leqslant j)$, postoji tačno jedan morfizam $g : A \to B$ takav da je $g_i = g \circ f_i$ za svako $i \in I$. Dokažimo da je $G = (g,u)$ morfizam para (A,ϕ) u par (B,ψ) koji zadovoljava uslove tvrdjenja.

Naime, kako je $G_i = (g_i,u)$ morfizam para (A_i,ϕ_i) u par (B,ψ), biće $u\phi_i = \psi g_i$ za svako $i \in I$, što sa $g_i = g f_i$ daje $u\phi_i = (\psi g) f_i$ $(i \in I)$. S druge strane je $\phi_i = \phi f_i$, pa za svako $i \in I$, $a_i \in A_i$ važi $u\phi f_i a_i = \psi g f_i a_i$, a time i $(u\phi)a = (\psi g)a$ $(a \in A)$. Otuda je $u\phi = \psi g$, pa je G odredjen morfizam para (A,ϕ) u par (B,ψ). Pri tome se neposredno proverava da za svako $i \in I$ važi $G_i = G \circ F_i$. Najzad, ako i morfizam $\tilde{G} = (\tilde{g},\tilde{u})$ para (A,ϕ) u (B,ψ) ima ista svojstva, tada $G_i = \tilde{G} \circ F_i$ daje $\tilde{u} = u$ i $g_i = \tilde{g} \circ f_i$ $(i \in I)$. Kako u kategoriji *ANN* važi $(A, f_i) = \varinjlim (A_i, f_{ji})$, iz $g_i = g \circ f_i$, $g_i = \tilde{g} \circ f_i$ $(i \in I)$ sledi $\tilde{g} = g$, a time i $\tilde{G} = G$. Otuda i tvrdjenje u celini. □

KOROLAR 2-2

> *Neka je I uredjen skup i (P_i) $(i \in I)$ familija desnih euklidskih parova $P_i = (A_i,\phi_i)$. Ako je (A_i) $(i \in I)$ rastući lanac potprstena nekog prstena B i $\phi_i = \phi_j | A_i$ $(i,j \in I,\ i \leqslant j)$, tada je i $A = \cup_{i \in I} A_i$ desni euklidski potprsten prstena B.*

DOKAZ. Ako je $W_i = \phi_i(A_i)$, neka su $f_{ji} : A_i \to A_j$ i $h_{ji} : W_i \to W_j$ kanoničke injekcije (sa $i \leqslant j$), i stavimo $F_{ji} = (f_{ji}, h_{ji})$. Tada je (P_i, F_{ji}) jedna I-induktivna familija u kategoriji *EUC* koja zadovoljava uslove *Teoreme 2-3*. Kako je uz to A objekt induktivnog limesa familije (A_i, f_{ji}) u *ANN*, tvrdjenje sledi iz *Teoreme 2-3*. Inače, prema "komentaru" uz *Teoremu 2-1* prethodno tvrdjenje ne mora da važi za proizvoljan rastući lanac desnih euklidskih potprstena nekog prstena. □

TEOREMA 2-4

> *Ako su A,B,C euklidski prsteni, tada tenzorski proizvod prstena A i B nad prstenom C ne mora biti euklidski prsten. Otuda sledi da Teorema 2-3 ne mora da važi ako $(I,\leqslant)$ nije desni filtar.*

DOKAZ. Neka je $I = \{i,j,k\}$ i stavimo $A_i = A$, $A_j = B$, $A_k = C$. Ako su prsteni A,B,C komutativni i $\leqslant$ uredjajna relacija na skupu I data sa $i > k$, $j > k$,

tada je objekt T induktivnog limesa odgovarajuće I-induktivne familije $\{A,B,C\}$ u kategoriji Ann upravo tenzorski proizvod $A \times_C B$ prstena A i B nad prstenom C, to jest

$$\varinjlim\{A,B,C\} = A \times_C B. \tag{12}$$

Medjutim, ako su A,B,C komutativni euklidski prsteni, to ne mora biti i prsten $A \times_C B$. Zaista, ako je, na primer, $C=K$ polje, $A=K[X]$, $B=K[Y]$, biće $A \times_C B = K[X,Y]$. Uz to je svaki od prstena A,B i C euklidski, dok to nije slučaj sa prstenom $K[X,Y] = K[X][Y]$. Otuda i samo tvrdjenje. □

Ako je $I=\{1,2\}$ sa $1<2$, $A_1=Z[X]$, $A_2=Q[X]$ i f_{11},f_{21},f_{22} odgovarajuće kanoničke injekcije, tada je induktivni limes $Q[X]$ induktivne familije $\{A_1,A_2\}$ u kategoriji Ann euklidski prsten, ali to nije slučaj sa prstenom A_1. Otuda u *Teoremi 2-3* ne mora da važi obrnuto tvrdjenje. U vezi sa tim važi:

TEOREMA 2-5

Neka je (A_i) $(i\in I)$ proizvoljna familija prstena. Ako je proizvod A (odnosno direktna suma B) prstena A_i $(i\in I)$ desni euklidski prsten, onda je to slučaj i sa svakim od prstena A_i $(i\in I)$.

DOKAZ. Neka je $B=\Theta_{i\in I}A_i$ desni euklidski prsten. Ne umanjujući opštost možemo pretpostaviti da je B potprsten prstena $A=\Pi_{i\in I}A_i$, uz dogovor da $a=(a_i)$ iz A pripada prstenu B akko je najviše konačno mnogo a_i-ova različito od nule. Neka je $f_i:A\to B$ $(i\in I)$ kanonički monomorfizam, i za fiksirano $s\in I$ i $a_s,b_s\in A_s$ stavimo $a=f_sa_s$ i $b=f_sb_s$. Uz to je $b_s\neq 0$ akko je $b=f_sb_s\neq 0$. Otuda, ako je $b_s\neq 0$ i ϕ desna euklidska valuacija prstena B, postoje $q,r\in B$ takvi da je

$$a = bq + r, \qquad \phi r < \phi b. \tag{13}$$

Dokazaćemo da je $\phi_s=\phi\circ f_s$ desna euklidska valuacija prstena A_s. Prvo, iz $a,b\in A_s$ sledi da je $a_i=0$ i $b_i=0$ za svako $i\neq s$. Dalje, stavimo $q=(q_i)$ i $r=(r_i)$ $(i\in I)$. Tada iz *(13)* sledi da je $r_i=0$ za svako $i\neq s$, i dakle $r=f_sr_s$ sa $r_s\in A_s$. Sada iz *(13)* sledi $a_s = b_sq_s + r_s$, gde je $q_s,r_s\in A_s$

i $\varphi_S r_S = \varphi f_S r_S = \varphi r < \varphi b = \varphi f_S b_S = \varphi_S b_S$, pa je φ_S $(= \varphi \circ f_S)$ jedna desna euklidska valuacija prstena A_S. Slično se dokazuje da desna euklidnost prstena $A = \Pi_{i \in I} A_i$ povlači desnu euklidnost svakog od "faktora" A_i. □

Pod *rastavom* prstena A na proizvod prstena $A_1, \ldots, A_n$ podrazumevamo svaki izomorfizam $f: A \to \Pi A_i$ prstena A na proizvod prstena A_i $(0<i\leqslant n)$. U tom slučaju postoje ideali L_i prstena A takvi da je $A = L_1 \dotplus \cdots \dotplus L_n$, i tada kažemo da je prsten A direktna suma ideala L_i $(1\leqslant i\leqslant n)$. Uobičajeno je da se umesto $A \simeq A_1 \times \cdots \times A_n$ piše i $A = A_1 \times \cdots \times A_n$. Prema *Teoremi 2-5* i *II, Korolar 1-2*, prsten $A = A_1 \times \cdots \times A_n$ je euklidski zdesna ako i samo ako je to slučaj sa svakim od "faktora" A_i $(1\leqslant i\leqslant n)$. □

TEOREMA 2-6

Ako za prave desne ideale U i V prstena A u kategoriji Mod_A važi $A = U + V$, tada je prsten A euklidski zdesna ako i samo ako svaki od ideala U i V ima neprazan presek sa desnim euklidskim jezgrom A^* prstena A.

DOKAZ. Iz $A = U + V$ sledi $A \simeq B \times C$ sa $B = A/U$, $C = A/V$. Otuda je prsten A (kao desni A-modul) euklidski zdesna ako i samo ako je svaki od desnih A-modula B i C euklidski. S druge strane, ako desni ideali U i V imaju neprazne preseke sa A^*, prema *II, Teorema 1-7* biće desni A-moduli A/U i A/V euklidski, pa je takav i njihov proizvod $A = B \times C$. □

TEOREMA 2-7

Neka je A desni euklidski prsten za koji važi $R_d(A) = R(A) = S$. Ako prsten A ima prsten desnih S-razlomaka K, i ako je $K = K_1 \dotplus \cdots \dotplus K_n$, tada postoje desni euklidski prsteni A_i $(1 \leqslant i \leqslant n)$ sa svojstvom da je K_i prsten desnih razlomaka nad A_i i $A \simeq A_1 \times \cdots \times A_n$.

DOKAZ. Iz $K = K_1 \dotplus \cdots \dotplus K_n$ sledi da postoji n idempotentnih i ortogonalnih elemenata $e_i \in K_i$ koji pripadaju centru $Z(K)$ prstena K. S obzirom da e_i komutira sa svakim elementom iz K, biće $e_i A$ potprsten prstena K. Ako je $e_i = a_i/c_i$ i $c = c_1 \cdots c_n$, tada iz istih razloga važi $ce_i \in A$. Uz to je c regularan element prstena A. Otuda je $ce_i A$ $(0<i\leqslant n)$ desni ideal prstena

A, pa kako je u prstenu A svaki desni ideal glavni, postoji $a \in A$ takvo da važi

$$ce_1A + \cdots + ce_nA = aA. \tag{14}$$

S druge strane je $e_1 + \cdots + e_n = 1$, pa iz (14) sledi egzistencija bar jednog $b \in A$ za koje je $c = ab$. Kako je $c \in R(A)$, biće $a \in R_d(A)$, a time i $a \in R(A)$ (prema uslovu tvrdjenja). Na osnovu toga, zamenjujući u (14) c sa ab, dobijamo $be_1A + \cdots + be_nA = A$. Stavimo $A_i = be_iA$ $(1 \leqslant i \leqslant n)$. Uz to za svako $i \neq s$ važi $A_i \cap A_s \subset K_i \cap K_s = \{0\}$, pa je $A = A_1 \times \cdots \times A_n$. Kako je prsten A euklidski zdesna, biće to slučaj i sa svakim od prstena A_i $(1 \leqslant i \leqslant n)$.

Jasno je da je $R(A_i) = A_i \cap R(A)$. Stavimo $S_i = A_i \cap S$. Kako je $S = R(A)$ desni denominator u prstenu A, za svako $a \in A_i$ i $x \in S_i$ postoje $\Sigma y_i = y \in S$ i $\Sigma b_i = b \in A$ $(y_i \in S_i,\ b_i \in A_i)$ takvi da je $ay = xb$, a time i $ay_i = xb_i$ sa $y_i \in S_i$, pa je S_i desni denominator u prstenu A_i. To znači da svaki od prstena A_i ima desni prsten razlomaka nad A_i. Označimo ga sa L_i. Kako je $A_i \subset K_i$, neposredno se zaključuje da mora biti $L_i = K_i$. □

Svaki *komutativan* glavnoidealski prsten A je izomorfan direktnom proizvodu $P \times Q$ dva prstena P i Q, pri čemu je $P = A_1 \times \cdots \times A_m$ direktan proizvod konačno mnogo glavnoidealskih domena A_i, a $Q = B_1 \times \cdots \times B_n$ direktan proizvod konačno mnogo tzv. *specijalnih* prstena B_j. Pri tome za komutativan prsten B kažemo da je *specijalan* ako ima bar jedan nilpotentan element $b \in B$, sa stepenom nilpotentnosti k, sa svojstvom da svako $a \in B$ ima tačno jedan rastav oblika

$$a = ub^r, \qquad 0 \leqslant r < k, \qquad u \in U(B), \tag{15}$$

(*SAMUEL* [4], *IV*, *245*, ili *BOURBAKI* [2], *6-7*, *Ex.*, §*1*, *6*). Jasno je da je svaki specijalan prsten euklidski, pa se na osnovu prethodnih tvrdjenja neposredno zaključuje da važi:

TEOREMA 2-8

Svaki komutativan euklidski prsten A je ili euklidski domen, ili specijalan prsten, ili proizvod konačno mnogo takvih prstena. □

Problem rastava *nekomutativnog* euklidskog prstena je znatno teži i složenijl. Prema *GOLDIE* [3] svaki desni glavnoidealski prsten A, koji je neterovski sleva, izomorfan je direktnom proizvodu $\bar{A}$ konačno mnogo desnih glavnoidealskih prstena, od kojih je svaki *prost* ili *primaran*. Pri tome za prsten kažemo da je *primaran* ako ima najviše jedan prost ideal. Kako je direktan prolzvod konačno mnogo prostih (primarnih) desnih glavnoidealskih prstena jedan *poluprost* (odnosno *Artinov*) desni glavnoidealski prsten, $S=R(A)$ je desni denominator u datom prstenu A, i odgovarajući prsten desnih razlomaka A_S je artinovski zdesna. Otuda:

TEOREMA 2-9

Svaki desni euklidski prsten A, koji je neterovski sleva, izomorfan je direktnom proizvodu $P\times Q$ dva desna euklidska prstena, od kojih je prvi poluprost, a drugi artinovski zdesna. Pri tome je P (odnosno Q) direktan proizvod konačno mnogo prostih (primarnih) desnih euklidskih prstena. Uz to je $S=R(A)$ desni denominator u A i prsten A_S je euklidski i artinovski zdesna. □

PRIMER 2-1. *Neka je L proizvoljno polje, K polje razlomaka nad prstenom $L[X]$ i $f:K\to K$ endomorfizam polja K dat sa $f(a)=a$ $(a\in L)$ i $f(X)=X^2$. Prsten $A=K[Y,f]$ svih desnih f-polinoma po Y sa koeficijentima u polju K je euklidski zdesna. Uz to je f monomorfizam pa je A oblast celih, a time i prost prsten.*

Medjutim, prsten A nije neterovski i sleva. Naime, kako morfizam f nije surjektivan, postoji $c\in K$ takvo da je $c\in f(K)$. Stavimo $a=Y+c$, $x=Y^2$ i $S=A^0$. Tada je $Sa\cap Ax=\Theta$. To posebno znači da skup $S=A^0$ svih regularnih elemenata prstena A nije levi denominator u A. Kako to važi u svakom levom neterovskom domenu, prsten A nije neterovski sleva. To znači da Teoremom 2-9 nisu "obuhvaćeni" svi prsteni koji su euklidski zdesna. Inače, ako je poluprost desni glavnoidealski prsten neterovski sleva, može se dokazati da je taj prsten i glavnoidealski sleva. □

Ako prsten $A=B\times C$ ima bar jednu desnu euklidsku valuaciju ϕ koja zadovoljava uslov *(M)*, onda to svojstvo ima i svaki od prstena $B\times\{0\}$ i $\{0\}\times C$, a time i sami prsteni B i C.

O PRSTENIMA HERMITSKOG TIPA

Mnogi problemi u (linearnoj) algebri su u uskoj vezi sa problemom *svodjenja* (*redukcije*) matrica (nad izvesnim prstenom) na matrice nekog posebnog oblika (dijagonalne, kvazidijagonalne, trougaone, i sl.). Pri tome se odgovarajući "proces" svodjenja date matrice M nad prstenom A obično sastoji u uzastopnom množenju (sleva, zdesna) te matrice nekim posebnim matricama (na primer inverzibilnim, elementarnim, regularnim) nad prstenom A. Jedan od klasičnih rezultata u vezi sa tim problemom je da se svaka matrica M iz $M_{mn}(Z)$ uzastopnim množenjem (sleva i zdesna) elementarnim matricama može svesti na neku dijagonalnu matricu formata $m \times n$ nad prstenom Z.

KAPLANSKI [1] definiše *desni (levi) hermitski prsten* A kao prsten sa svojstvom da za svaku matricu $M = [a, b]$ iz $M_{12}(A)$ postoji bar jedna inverzibilna matrica P iz $M_2(A)$ takva da je matrica MP (odnosno PM^T) donje-trougaona (odnosno gornje-trougaona), to jest da za neko c iz A važi $MP = [c\ 0]$ (odnosno $PM^T = [c\ 0]^T$). Svaki desni hermitski prsten je desni *Bezuov* prsten, tj. prsten u kome je suma ma koja dva glavna desna ideala takodje glavni desni ideal. U slučaju desnog euklidskog prstena važi i obrnuto tvrdjenje. Medjutim, još uvek je otvoren problem da li obrnuto tvrdjenje važi i u slučaju proizvoljnog desnog Bezuovog domena.

U ovom poglavlju biće reči o jednoj klasi prstena sličnog "tipa", koja obuhvata (leve, desne) hermitske prstene kao poseban slučaj. Otuda i naziv "prsteni hermitskog tipa". Sa $M_{mn}(A)$ ili A_{mn} označavaćemo skup svih matrica formata $m \times n$ nad prstenom A. Za $m=n$ umesto $M_{mn}(A)$ pisaćemo samo $M_n(A)$, odnosno A_n. Naravno, tada oznake $U(A_n)$, $R(A_n)$, $R_d(A_n)$, i tako dalje, imaju uobičajena značenja. Jediničnu matricu prstena $M_n(A)$ označavaćemo sa E.

Za element $a \in A$ kažemo da je *desni (levi) delitelj* elementa $b \in A$ u prstenu A ako važi $b \in Aa$ (odnosno $b \in aA$). Ako je $b \in Aa \cap aA$, tada kažemo da je a *obostrani delitelj* od b. Element a je *totalni* (ili *potpuni*) *delitelj* od b ako važi $AbA \subset Aa \cap aA$. U tom slučaju kažemo i da a *deli* b i pišemo $a|b$. Inače, relacija $|$ u prstenu A ne mora biti refleksivna.

Pod *elementarnom transformacijom* na vrstama (kolonama) matrice M nad prstenom A podrazumevamo svaku transformaciju njenih vrsta (kolona) jednog od sledeća tri tipa:

(P) *Zamena mesta dvema vrstama (kolonama) matrice* M;

(H) *Množenje neke vrste (kolone) matrice* M *sleva (odnosno zdesna) nekom jednotom prstena* A;

(L) *Dodavanje nekoj od vrsta (kolona) matrice* M *neke od preostalih vrsta (kolona) pomnožene sleva (zdesna) nekim elementom prstena* A.

Pod *elementarnom matricom* reda n nad prstenom A podrazumevamo svaku od matrica prstena A_n koja se može dobiti iz jedinične matrice E primenom neke od elementarnih transformacija na njenim vrstama (kolonama). Jasno je da je svaka elementarna matrica invertibilna. Sa $\mathcal{E}(A_n)$ označavaćemo podgrupu grupe $U(A_n)$ što je generišu elementarne matrice iz A_n.

Ako matrica $\tilde{M}$ nastaje iz matrice $M \in A_{mn}$ primenom neke elementarne transformacije θ na vrstama (kolonama), i ako je P elementarna matrica koja nastaje iz matrice $E \in A_m$ (odnosno $E \in A_n$) primenom iste elementarne transformacije θ, tada je $\tilde{M} = PM$ (odnosno $\tilde{M} = MP$), i obrnuto. To posebno znači da se *kvazi-dijagonalna* suma $P \dotplus Q$ dve elementarne matrice $P \in A_m$ i $Q \in A_n$ može pretstaviti kao proizvod elementarnih matrica reda $m+n$. □

DEFINICIJA 1-1

Neka je A *prsten (sa ili bez jedinice) i* H_n $(n \in N)$ *multiplikativan podgrupoid prstena* A_n *koji ne sadrži nulu. Tada za niz* (H_n) $(n \in N)$ *kažemo da je* HERMITSKI *ako zadovoljava uslov*

$$(1) \qquad P \in H_1 \wedge Q \in H_n \Rightarrow P \dotplus Q, Q \dotplus P \in H_{n+1} \qquad (n \in N).$$

(Za svako $a \in A$ matricu $P = [a]$ formata 1×1 poistovećivaćemo sa samim a.)

LEMA 1-1

Ako je (H_n) $(n\in N)$ *hermitski niz nad prstenom* A, *tada za svako* m,n *i* $[a],[b]\in H_1$, $P\in H_m$, $Q\in H_n$ *vazi*

$$(2)\qquad aP\in H_m,\quad Qb\in H_n,\quad aP\dot{+}Qb\in H_{m+n},\quad Pa\dot{+}bQ\in H_{m+n}.$$

Ako prsten A *ima jedinicu i ako je* $[1]\in H_1$, *tada je i* $P\dot{+}Q\in H_{m+n}$.

DOKAZ. Kako je niz (H_n) hermitski i $[a],[b]\in H_1$, iz $[1]$ neposredno sledi da matrice $S=diag(a,..,a)$ iz A_m i $T=diag(b,..,b)$ iz A_n pripadaju redom skupovima H_m i H_n. Stavimo $U=S\dot{+}Q$ i $V=P\dot{+}T$, to jest

$$(3)\qquad U=\left[\begin{array}{c|c} S & O \\ \hline O & Q \end{array}\right],\qquad V=\left[\begin{array}{c|c} P & O \\ \hline O & T \end{array}\right].$$

Svaki od skupova H_s $(s\in N)$ je multiplikativan grupoid, pa iz $S,P\in H_m$ i $T,Q\in H_n$ sledi $SP,PS\in H_m$ i $QT,TQ\in H_n$. S druge strane je $SP=aP$, $PS=Pa$, $QT=Qb$, $TQ=bQ$, što sa prethodnim daje $aP\in H_m$ i $Qb\in H_n$.

Kako je $UV=SP\dot{+}QT$ i $VU=PS\dot{+}TQ$, prema prethodnom važi $UV=aP\dot{+}Qb$ i $VU=Pa\dot{+}bQ$. Dalje, iz (1) neposredno sledi $U,V\in H_{m+n}$, a samim tim i $UV,VU\in H_{m+n}$, što sa prethodnim daje preostali deo tvrdjenja. Ako H_1 ne sadrži matricu $[1]$, tada iz $P\in H_m$ i $Q\in H_n$ u opštem slučaju ne mora da sledi $P\dot{+}Q\in H_{m+n}$. □

LEMA 1-2

(α) *Ako je* A *prsten sa jedinicom i* $H_n=U_l(A_n)$ *tada je* (H_n) $(n\in N)$ *jedan hermitski niz nad prstenom* A. *Tvrdjenje ostaje na snazi i u slucaju da je* $H_n=U_d(A_n)$, *odnosno* $H_n=U(A_n)$.

(β) *Ako je* A *prsten (sa ili bez jedinice) i* $H_n=R_l(A_n)$, *tada je niz* (H_n) $(n\in N)$ *hermitski nad prstenom* A. *Analogno tvrdjenje važi i u slučaju da je* $H_n=R(A_n)$, *odnosno* $H_n=R_d(A_n)$.

(γ) *Ako je* $H_n=\mathcal{E}(A_n)$ *podgrupa grupe* $U(A_n)$ *generisana elementarnim matricama iz* A_n, *tada je* (H_n) $(n\in N)$ *hermitski niz nad prstenom* A.

(δ) *Ako je* (H_n) $(n\in N)$ *bilo koji od hermitskih nizova o kojima je reč pod* (α)-(γ), *tada za* $P\in A_m$, $Q\in A_n$ *vazi* $P\dot{+}Q\in A_{m+n}$ $\Rightarrow$ $P\in H_m$, $Q\in H_n$.

DOKAZ. (α) Kako prsten A ima jedinicu, svaki od skupova H_n sadrži bar jediničnu matricu (odgovarajućeg reda), i dakle nije prazan. Pri tome je jasno da nijedan od skupova H_n ne sadrži nulu prstena A_n. Dalje, ako je $P,Q \in H_n$, biće $PX = E$ i $QY = E$ za neko $X,Y \in A_n$, pa $(PQ)(YX) = E$ daje $PQ \in H_n$. Otuda je H_n neprazan multiplikativan podskup od A_n^0. Dokažimo da niz (H_n) $(n \in N)$ zadovoljava uslov *(1)*. Naime, za svako $P \in H_m$ i $Q \in H_n$ postoje matrice $X \in A_m$ i $Y \in A_n$ takve da je $PX = E_m$ i $QY = E_n$, a time i

$$(4) \qquad (P \dot{+} Q)(X \dot{+} Y) = PX \dot{+} QY = E_m \dot{+} E_n = E_{m+n},$$

što sa $P \dot{+} Q, X \dot{+} Y \in A_{m+n}$ daje $P \dot{+} Q \in H_{m+n}$. Otuda i samo tvrdjenje pod (α).

(β) Neka je [a] proizvoljan element skupa H_1. Tada je $a \in R_\ell(A)$, i dakle $ax = 0$ akko je $x = 0$. Stavimo $S = diag(a,..,a)$, $S \in A_n$. Tada za svaku matricu $X \in A_n$ važi $SX = 0$ akko je $X = 0$. Otuda je $S \in H_n$, pa je svaki od skupova H_n $(n \in N)$ neprazan. Uz to je jasno da je H_n multiplikativan podskup od A_n^0 za svako $n \in N$. Dokažimo još da niz (H_n) $(n \in N)$ zadovoljava uslov *(1)*. Pre svega, primetimo da za $P \in H_m$ i proizvoljnu matricu X iz A_{mn} važi $PX = O$ akko je $X = O$. Neka je $P \in H_m$, $Q \in H_n$ i

$$(5) \qquad V = \left[\begin{array}{c|c} X & Y \\ \hline Z & T \end{array}\right]$$

proizvoljna matrica iz A_{m+n}, pri čemu je $X \in A_m$ i $T \in A_n$. Neposredno se proverava da tada važi

$$(6) \qquad (P \dot{+} Q)V = \left[\begin{array}{c|c} PX & PY \\ \hline QZ & QT \end{array}\right],$$

pa $(P \dot{+} Q)V = O$ povlači $PX = O$, $PY = O$, $QZ = O$, $QT = O$, što sa $P \in H_m$ i $Q \in H_n$ daje $X = O$, $Y = O$, $Z = O$, $T = O$, to jest $V = O$, i dakle $P \dot{+} Q \in H_{m+n}$. Posebno, ako je neka od matrica P i Q reda *1* dobijamo implikaciju *(1)*.

(γ) Kako je po samoj definiciji H_n multiplikativan podskup od A_n^0, treba još dokazati da za $a \in U(A)$ i $P \in H_n$ važi $a \dot{+} P \in H_{n+1}$. Zaista, neka su P_i $(1 \leqslant i \leqslant s)$ elementarne matrice iz A_n za koje važi $P = P_1 \cdot\cdot P_s$. Ako je E jedinična matrica iz A_n i $S_0 = a \dot{+} E$, $S_i = 1 \dot{+} P_i$ $(1 \leqslant i \leqslant s)$, tada se neposredno proverava da je $a \dot{+} P = \prod S_i$, što sa $S_i \in \mathcal{E}(A_{n+1})$ daje tvrdjenje.

(δ) Neka je prvo (H_n) $(n\in N)$ hermitski niz o kome je reč pod (α) i pretpostavimo da za neke matrice $P\in A_m$ i $Q\in A_n$ važi $P+Q\in H_{m+n}$. Ako je V matrica oblika (5) za koju važi $(P+Q)V=E=E_m+E_n$, tada na osnovu (6) dobijamo $PX=E_m$ i $QT=E_n$, a time i $P\in H_m$, $Q\in H_n$.

Neka je sada (H_n) $(n\in N)$ hermitski niz o kome je reč pod (β). Tada $P+Q\in H_{m+n}$ povlači da za svaku matricu $V\in A_{m+n}$ važi $(P+Q)V=O$ akko je $V=O$. Posebno, ako za matrice $X\in A_m$ i $Y\in A_n$ važi $PX=O$ i $QY=O$, tada $(P+Q)(X+Y)=PX+QY=0+0=O$ daje $X+Y=O$, to jest $X=O$ i $Y=O$, a samim tim i $P\in H_m$ i $Q\in A_n$. Otuda i tvrdjenje u celini. □

DEFINICIJA 1-2

Za matricu $M\in A_{mn}$ kažemo da je DIJAGONALIZABILNA *u odnosu na dati hermitski niz (H_n) $(n\in N)$ nad prstenom A ako postoje matrice $P\in H_m$ i $Q\in H_n$ takve da je matrica*

$$\tilde{M}=PMQ \tag{7}$$

dijagonalna. Ako je uz to $\tilde{M}=diag(a_1,a_2,..)$ sa $a_r\mid a_{r+1}$ $(r=1,2,..)$ tada govorimo o ELEMENTARNOJ *dijagonalizabilnosti date matrice M.*

Za prsten A kažemo da je *prsten sa elementarnim deliteljima* u odnosu na hermitski niz (H_n) $(n\in N)$ ako je svaka matrica nad njim elementarno dijagonalizabilna.u odnosu na niz (H_n). Posebno, ako je $H_n=U(A_n)$, tada kažemo samo da je A prsten sa *elementarnim deliteljima* (KAPLANSKY [1]).

DEFINICIJA 1-3

Pod DESNIM (LEVIM) *PRSTENOM HERMITSKOG TIPA podrazumevamo svaki prsten A nad kojim je svaka matrica formata 1×2 (odnosno 2×1) dijagonalizabilna u odnosu na neki fiksirani hermitski niz (H_n) nad tim prstenom.*

Ako je prsten A hermitskog tipa i sleva i zdesna u odnosu na isti hermitski niz, tada kažemo samo da je prsten A hermitskog tipa u odnosu na taj niz. Pod (levim, desnim) *HERMITSKIM PRSTENOM* podrazumevamo svaki

prsten A koji je (sleva, zdesna) hermitskog tipa u odnosu na hermitski niz $H_n = U(A_n)$ (*KAPLANSKY* [1]).

Ako je u *Definiciji 1-3* niz (H_n) neki od hermitskih nizova $R(A_n)$, $R_d(A_n)$, $R_l(A_n)$ o kojima je reč u *Lemi 1-2* pod (β), tada kažemo da je A redom (*desni, levi*) *Γ-HERMITSKI*, *Δ-HERMITSKI*, *Λ-HERMITSKI* prsten. □

LEMA 1-3

(α) Domen A je desni Λ-hermitski prsten ako i samo ako zadovoljava desni Ore-ov uslov. Desni neterovski domen je Λ-hermitski zdesna.

(β) Ako u desnom Λ-hermitskom prstenu A važi $R_l(A) \subset R_d(A)$, tada tada u prstenu A važi desni Ore-ov uslov.

(γ) Svaki (levi, desni) hermitski prsten A je Γ-hermitski, ali ne i obratno.

DOKAZ. (α) Neka domen A ima desno Ore-ovo svojstvo. Tada za svako $a \in A$ i $b \in A^0$ postoje $c \in A^0$ i $\tilde{d} \in A$ takvi da je $ac = b\tilde{d}$, to jest $ac + b\tilde{c} = 0$ (sa $d = -\tilde{d}$). Otuda za svaku matricu $P = \begin{bmatrix} p & c \\ q & d \end{bmatrix}$ $(p,q \in A)$ važi

$$(\beta) \qquad [a \;\; b]\begin{bmatrix} p & c \\ q & d \end{bmatrix} = [\alpha \;\; 0],$$

sa $\alpha = ap + bq$. Ako je $p=0$ i $q=c$ neposredno se proverava da je matrica P regularna sleva, pa je prsten A Λ-hermitski zdesna. Obratno, ako je A desni Λ-hermitski domen, tada za svako $a \in A$ i $b \in A^0$ postoji leva regularna matrica P za koju važi *(β)*, a time i (*) $ac + bd = 0$. Pri tome je $c \neq 0$, jer bi u suprotnom zbog $b \in R(A)$ moralo biti i $d = 0$, pa matrica P ne bi bila regularna sleva. Otuda i tvrdjenje.

(β) Neka je $a \in A$ i $b \in R(A)$. Kako je prsten A Λ-hermitski zdesna, za bar jednu levu regularnu matricu $P \in A_2$ važi *(β)*. Otuda postoje c,d iz A takvi da je (**) $ac + bd = 0$. Pri tome element c mora biti regularan. Naime, kako je $R_l(A) \subset R_d(A)$, u suprotnom bi za bar jedno $x \in A^0$ bilo $cx = 0$. Tada množeći (**) zdesna sa x dobijamo $bdx = 0$, što zajedno sa $b \in R(A)$ daje $dx = 0$. No, to bi značilo da je $P \cdot [0 \; x]^T = 0$ sa $x \neq 0$, što je nemoguće zbog leve regularnosti matrice $P \in A_2$. Naime, matrica $P \in A_n$ je regularna sleva akko za svaku kolona-matricu $X \in A_{n1}$ važi $PX = 0 \Rightarrow X = 0$.

Otuda je $c \in R_l(A)$, a time i $c \in R(A)$, što sa prethodnim znači da prsten A ima desno Ore-ovo svojstvo.

(γ) Jasno je da je svaki (levi, desni) hermitski prsten A u isto vreme i Γ-hermitski (sleva, zdesna). S druge strane, prema *KAPLANSKY* [1] svaki desni hermitski domen je i desni *Bezuov* prsten. To posebno znači da, na primer, prsten $Z[X]$ nije hermitski. Medjutim, prsten $A = Z[X]$ je neterovski, a time i Γ-hermitski domen. □

TEOREMA 1-1

Ako je A desni prsten hermitskog tipa u odnosu na (hermitski) niz (H_n) $(n \in N)$, tada za svaku matricu $M \in M_{mn}(A)$ postoji matrica $P \in H_n$ takva da je matrica $T = MP$ donje trougaona.

DOKAZ. Dokažimo prvo da tvrdjenje važi za $m=1$, to jest za svaku matricu M formata $1 \times n$ $(n \in N)$. Za $n=1$ to je jasno, a za $n=2$ tvrdjenje sledi direktno iz definicije desnog prstena hermitskog tipa. Neka je $n>2$ zadat prirodan broj i pretpostavimo da tvrdjenje važi za sve prirodne brojeve manje od n. Ako je $M = [a_1 .. a_n]$, stavimo $B = [a_2 .. a_n]$, tj. $M = [a_1\ B]$. Matrica B je formata $1 \times (n-1)$ pa prema induktivnoj pretpostavci postoji matrica $Q \in H_{n-1}$ takva da je matrica $S = BQ$ donje trougaona, tj. oblika $S = [b\ 0 .. 0]$ za neko $b \in A$. Za proizvoljno $[\alpha] \in H_1$ stavimo $U = [\alpha] \dot{+} Q$. Tada je $U \in H_n$ i važi

$$MU = [a_1\ B] \cdot ([\alpha] \dot{+} Q) = [a\ b\ 0 .. 0], \tag{9}$$

pri čemu je $a = a_1\alpha$. Ako je $S \in H_2$ matrica za koju važi $[a\ b]S = [c\ 0]$ i $D = diag(\alpha, .., \alpha)$ matrica iz H_{n-2}, stavimo $V = S \dot{+} D$. Tada je $V \in H_n$, pa kako je i $U \in H_n$, biće $P = UV \in H_n$. Uz to je $M(UV) = (MU)V = [c\ 0 .. 0]$, pa imamo i samo tvrdjenje.

Pretpostavimo sada da tvrdjenje važi za svaku matricu B koja ima manje od m vrsta ($m>1$ fiksiran prirodan broj), i neka je M proizvoljna matrica iz A_{mn}. Sa F označimo prvu vrstu, a sa G podmatricu od M koja nastaje iz matrice M uklanjanjem njene prve vrste F. Kako je tvrdjenje već dokazano za vrsta-matrice, postoji matrica $X \in H_n$ i $c \in A$ takvi da je $FX = [c\ 0..0]$. Tada je $MX = \left[\begin{array}{c|c} c & O \\ \hline K & S \end{array}\right]$, pri čemu je S izvesna matrica koja ima $m-1$ vrstu.

Kako matrica S ima manje od m vrsta, postoji matrica $Y \in H_{n-1}$ za koju je matrica $V = SY$ donje trougaona. Ako je $[b] \in H_1$, stavimo $U = [b] + Y$. Tada je $U \in H_n$, što sa $X \in H_n$ daje $P = XU \in H_n$. Pri tome je

$$MP = \begin{bmatrix} F \\ G \end{bmatrix} \cdot X \cdot \left[\begin{array}{c|c} b & O \\ \hline O & Y \end{array}\right] = \left[\begin{array}{c|c} c & O \\ \hline K & S \end{array}\right] \left[\begin{array}{c|c} b & O \\ \hline O & Y \end{array}\right] = \left[\begin{array}{c|c} a & O \\ \hline L & V \end{array}\right], \tag{10}$$

sa $a = cb$ i $L = Kb$. Kako je uz to matrica V donje trougaona, prema (10) to je slučaj i sa matricom MP. Otuda i tvrdjenje u celini. □

KOROLAR 1-1

Za svaku matricu $M \in A_{mn}$ nad desnim (odnosno levim) Γ-hermitskim prstenom A postoji regularna matrica $P \in A_n$ (odnosno $Q \in A_m$) takva da je matrica MP (odnosno QM) donje trougaona (gornje trougaona).

Analogno tvrdjenje važi i za svaki desni (odnosno levi) hermitski prsten (KAPLANSKY [1]).

Ako je svaka matrica formata 2×2 nad hermitskim prstenom A dijagonalizabilna, onda je to slučaj i sa svakom matricom M nad ... i A je prsten sa elementarnim deliteljima (*KAPLANSKY* [1]). Kasnije ćemo dokazati da sličan rezultat važi i za Γ-hermitske prstene. □

TEOREMA 1-2

Ako je A desni Λ-hermitski prsten, onda je to slučaj i sa svakim od prstena $M_n(A)$ ($n \in N$). Analogno tvrdjenje važi i za Δ-hermitske, odnosno Γ-hermitske prstene.

DOKAZ. Treba dokazati da za proizvoljne matrice F, G iz Γ_n postoji leva regularna matrica $\vec{P} \in M_2(A_n)$ takva da je

$$[F, G] \cdot \vec{P} = [H, O], \tag{11}$$

pri čemu je H izvesni element prstena A_n. Kako je prsten A Λ-hermitski zdesna, postoji leva regularna matrica $P = \begin{bmatrix} X & Y \\ Z & W \end{bmatrix}$ iz $M_{2n}(A)$ takva da je matrica T data sa:

$$T = \left[\begin{array}{c|c} F & G \\ \hline O & O \end{array}\right] \left[\begin{array}{c|c} X & Y \\ \hline Z & W \end{array}\right] = \left[\begin{array}{c|c} H & O \\ \hline U & V \end{array}\right] \tag{12}$$

donje trougaona. Pri tome su $X,Y,..,V$ kvadratne matrice reda n, i dakle odredjeni elementi prstena A_n. Označimo sa P matricu iz prstena $M(A_n)$ koja "odgovara" matrici P, to jest shvatajući X,Y,Z,W kao članove prstena A_n. Tada iz *(12)* sledi *(11)* za neku matricu $P \in M_2(A_n)$. Još treba dokazati da je tako odredjena matrica P regularna sleva u $M_2(A_n)$.

Naime, za $B \in A_{2n}$ u prstenu A_{2n} važi $PB = O$ ako i samo ako je $\tilde{P}\tilde{B} = \tilde{O}$ u prstenu $M_2(A_n)$. S druge strane, kako je matrica P regularna sleva u prstenu A_{2n}, iz $\tilde{P}\tilde{B} = \tilde{O}$ sledi $PB = O$, to jest $B = O$, a time i $\tilde{B} = O$. Otuda i tvrdjenje. □

LEMA 1-4

Ako u desnom Λ-hermitskom prstenu A važi $R_l(A) = R(A)$, tada je u prstenu A_n trougaona matrica T regularna sleva ako i samo ako je to slučaj sa svakim elementom njene dijagonalu u prstenu A.

DOKAZ. Pre svega, iz $R_l(A) = R(A)$ sledi da je svaki desni delitelj nule u prstenu A istovremeno i levi delitelj nule. Dokažimo prvo da tvrdjenje važi za svaku donje trougaonu matricu

$$T = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ \vdots & & \\ a_{n1} & a_{n2} & \cdots\ a_{nn} \end{bmatrix} \tag{13}$$

iz prstena A_n. Neka je $X = [x_1,..,x_n]^T$ proizvoljna matrica formata $n \times 1$ nad prstenom A. Tada je $TX = O$ ako i samo ako važi

$$\begin{aligned} a_{11}x_1 &= 0, \\ a_{21}x_1 + a_{22}x_2 &= 0, \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= 0. \end{aligned} \tag{14}$$

Pretpostavimo da je svaki od elemenata a_{ii} $(1 \leqslant i \leqslant n)$ regularan sleva u prstenu A. Tada $a_{11}x_1 = 0$ daje $x_1 = 0$. Sada za $x_1 = 0$ iz *(14)* sledi $a_{22}x_2 = 0$,

i dakle $x_2=0$. Slično zaključujemo da je $x_3=0$, itd. Otuda je $X=0$, pa je matrica T regularna sleva. Primetimo da upravo dokazani deo tvrdjenja važi i bez pretpostavke $R_\ell(A)=R(A)$.

Dokažimo sada da je uslov i dovoljan. Jasno je da tvrdjenje važi za $n=1$. Neka je $n>1$ fiksiran prirodan broj i pretpostavimo da tvrdjenje važi za svaki prirodan broj $<n$. Ako je matrica $T\in A_n$ data sa (13) regularna sleva u prstenu A_n, tada je a_{nn} regularno sleva u prstenu A. Naime, u suprotnom bi za bar jedno $x\in A^0$ bilo $a_{nn}x=0$, pa bi za matricu $X=[0\ldots 0\ x]^T$ važilo $TX=O$ sa $X\neq O$, što je suprotno pretpostavci da je matrica T regularna sleva.

Označimo sa S komatricu polja (n,n) matrice T. Matrica S je donje trougaona i reda $n-1$. Dokažimo da je i ona regularna sleva. Zaista, u suprotnom bi za bar jednu kolona matricu $Y=[y_1\ldots y_{n-1}]^T$, $Y\neq O$, bilo $SY=O$. Stavimo

$$a=\Sigma a_{ni}y_i \quad (1\leqslant i<n), \qquad b=a_{nn}. \tag{15}$$

Prsten A je Λ-hermitski zdesna pa postoji $c\in A$ i leva regularna matrica $P=\begin{bmatrix} u & x \\ v & y \end{bmatrix}$ takvi da je $[a,\ b]\cdot P=[c,\ 0]$, a time i (*) $ax+by=0$. Ako bi za neko $z\neq 0$ bilo $xz=0$, tada bi iz (*) sledilo $byz=0$, a samim tim i $yz=0$ (jer je b regularno sleva). Neka je $U=[0\ z]^T$. Kako je $PU=O$ i matrica P regularna sleva, mora biti $U=O$. Otuda je $z=0$, tj. $x\in R_\ell(A)$, a time i $x\in R(A)$.

Stavimo $x_i=y_ix$ $(1\leqslant i<n)$, $x_n=y$, $V=[x_1,\ldots,x_{n-1}]$, $X=[x_1,\ldots,x_n]$. Tada je $V=Yx$ i $X=[V\ x_n]$. Dalje je $SV=SYx=Ox=O$, pa na osnovu (*) i (15) zaključujemo da je i (**) $TX=O$. S druge strane, kako je $Y\neq O$, a x regularno i zdesna, biće $V=Yx\neq O$, i dakle $X\neq O$. Medjutim, to je nemoguće jer je prema pretpostavci matrica T regularna sleva, dok prema prethodnom važi $TX=O$.

Prema tome, matrica S mora biti regularna sleva. Uz to je matrica S reda $n-1$, pa na osnovu induktivne pretpostavke svaki od "elemenata" a_{ii} $(1\leqslant i<n)$ njene glavne dijagonale je regularan sleva u prstenu A. Kako je uz to i $a_{nn}\in R(A)$, biće i svaki od elemenata glavne dijagonale matrice T regularan sleva.

U slučaju gornje trougaone matrice T dokaz je analogan prethodnom,

samo što se prvo zaključi da je element a_{11} regularan (sleva) u prstenu A, dok je S komatrica polja $(1,1)$ matrice T. □

TEOREMA 1-3

Ako je A desni Λ-hermitski prsten, tada za svaki prirodan broj n važi implikacija

$$(16) \qquad R_l(A) = R(A) \quad \Rightarrow \quad R_l(A_n) = R(A_n).$$

Ako uz to prsten A ima jedinicu, tada u svakom od prstena A_n $(n \in N)$ važi $PQ = E \Rightarrow QP = E$.

DOKAZ. Neka je M bilo koja leva regularna matrica iz A_n. Prema *Teoremi 1-1* postoji leva regularna matrica $P \in A_n$ za koju je matrica $T = MP$ donje trougaona. Pri tome je i matrica T regularna sleva, pa kako u prstenu A važi $R_l(A) = R(A)$, svaki element glavne dijagonale matrice

$$(16) \qquad T = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ \vdots & & \\ a_{n1} & a_{n2} & \cdots a_{nn} \end{bmatrix}$$

je regularan sleva, a time i zdesna (*Lema 1-4*). Neka je $X = [x_{ij}]$ bilo koja matrica iz A_n za koju važi $XM = O$. Tada je $XT = XMP = O$, i prema tome

$$(17) \qquad [XT]_{in} = X_{i*} \circ T_{*n} = x_{in} a_{nn} = 0$$

za svako $1 \leqslant i \leqslant n$. Kako je $a_{nn} \in R(A)$, mora biti $x_{in} = 0$ $(1 \leqslant i \leqslant n)$ pa je prva kolona matrice X nula-kolona. Na osnovu toga, slično zaključujemo da je i $(n-1)$-va kolona matrice X jednaka nuli, itd. Prema tome, mora biti $X = O$, pa je matrica M regularna i zdesna.

Dokažimo sada i drugi deo tvrdjenja. Neka za matrice $P, Q \in A_n$ važi $PQ = E$. Tada je matrica Q regularna sleva, a time i zdesna (prema upravo dokazanom delu tvrdjenja). Ako je $QP = S$, biće $QPQ = SQ$, to jest $QE = SQ$, i dalje $(S-E)Q = O$, što sa $Q \in R(A_n)$ daje $E = S = QP$. Otuda i tvrdjenje. □

PRIMEDBA 1-1. *Za prsten A (sa jedinicom) kažemo da je SLABO n-KONAČAN*

ako za svako $U,V\in A_n$ važi $UV=E \Leftrightarrow VU=E$. Prsten A je SLABO KONAČAN ako je slabo n-konačan za svaki prirodan broj n. Ako je prsten A slabo n-konačan i $m<n$, tada je prsten A i slabo m-konačan.

TEOREMA 1-4

Neka je A slabo 1-konačan prsten i $H_n=U_l(A_n)$ $(n\in N)$. Ako je prsten A hermitski zdesna (sleva) u odnosu na niz (H_n), tada je on i slabo konačan, a time i hermitski zdesna (sleva).

DOKAZ. Treba dokazati da za svako $n\in N$ i $U,V\in A_n$ važi $UV=E \Leftrightarrow VU=E$. Za $n=1$ to sledi iz pretpostavke da je prsten A slabo 1-konačan. Neka je $n>1$ fiksiran prirodan broj i pretpostavimo da je za svako $m<n$ prsten A slabo m-konačan. Dokažimo da je tada prsten A i slabo n-konačan, tj. da za svako $U,V\in A_n$ važi (*) $UV=E \Rightarrow VU=E$. Neka je prvo

$$U=\left[\begin{array}{c|c} a & O \\ \hline X & Y \end{array}\right], \qquad V=\left[\begin{array}{c|c} b & F \\ \hline G & H \end{array}\right], \tag{18}$$

pri čemu su Y i H kvadratne podmatrice reda $n-1$. Tada iz $UV=E$ sledi (**) $ab=1$, $aF=O$, $Xb+YG=O$, $XF+YH=E_{n-1}$. Kako je prsten A slabo 1-konačan, iz $ab=1$ sledi $ba=1$, pa je $F=ba\cdot F=b(aF)=O$, što zajedno sa (**) daje $YH=E$ (sa $E_{n-1}=E$). Kako je prsten A slabo $(n-1)$-konačan, biće i $HY=E$, i prema tome $VU=\left[\begin{array}{c|c} 1 & O \\ \hline Ga+HX & E \end{array}\right]$. S druge strane, na osnovu relacija (**) imamo $Xb+YG=O$, to jest $HXb+HYG=O$, pa kako je $HY=E$, biće $G=-HXb$. Otuda je $Ga+HX=HX-HXba=HX-HX=O$, što sa prethodnim zaključkom daje $VU=E$.

Neka su sada U i V proizvoljne matrice iz A_n za koje važi $UV=E$. Kako je prsten A hermitski zdesna u odnosu na niz (H_n), prema *Teoremi 1-1* postoji leva jednota P prstena A_n takva da je matrica $T=UP$ donje trougaona. Neka je Q bilo koja matrica iz A_n za koju je $PQ=E$. Tada iz $UV=E$ sledi $(UP)(QV)=E$, i matrice UP i QV su oblika (18), pa na osnovu dokazanog dela tvrdjenja važi $QV\cdot UP=E$. Množeći tu jednakost sleva sa P, a zdesna sa Q, dobijamo $(PQ)(VU)(PQ)=PQ$, a time i $VU=E$. □

PRIMEDBA 1-2. (α) *Pod (unutrašnjim) RANGOM matrice M $(M\neq O)$ formata $m\times n$*

nad prstenom A podrazumevamo najmanji prirodan broj r sa svojstvom da postoje matrice $P \in M_{mr}(A)$ *i* $Q \in M_{rn}(A)$ *za koje je* $M = PQ$. *Označavaćemo ga sa* $\rho(M)$. *Rang matrice nad desnim glavnoidealskim domenom jednak je rangu slobodnog modula što ga generišu njene kolone (vrste). To važi i za matrice nad desnim Bezuovim domenom.*

(β) *Za prsten A kažemo da ima INVARIJANTNO BAZISNO svojstvo, ili da je prsten sa INVARIJANTNIM BAZISNIM BROJEM (kratko IBB), ako svaki slobodan A-modul ima jednoznačan rang. Netrivijalan prsten A nema IBB akko za bar jedan par (m,n) različitih prirodnih brojeva važi* $A^m \simeq A^n$. *Svaki slabo konačan prsten A ima invarijantno bazisno svojstvo. Prsten sa IBB ne mora biti slabo konačan (COHN [ ]).*

(γ) *Za elemente* u_i $(1 \leqslant i \leqslant n)$ *desnog A-modula M kažemo da su linearno ZAVISNI ako postoji vrsta-matrica* $a = [a_1 \,..\, a_n]$ *nad prstenom A takva da je (*)* $u_1 a_1 + \cdots + u_n a_n = 0$ *i* $a \neq 0$. *Ako je uz to* $a\alpha \neq 0$ *za svaki "skalar"* $\alpha \in A^0$, *tada kažemo da su elementi* u_i $(1 \leqslant i \leqslant n)$ *Γ-LINEARNO ZAVISNI. U suprotnom za te elemente kažemo da su linearno NEZAVISNI, odnosno Γ-LINEARNO NEZAVISNI.* □

TEOREMA 1-5

Svaki desni Λ-hermitski (ili hermitski) prsten ima invarijantno bazisno svojstvo.

DOKAZ. Prsten A ima invarijantno bazisno svojstvo akko ne postoji par različitih prirodnih brojeva m i n za koje su moduli A^m i A^n izomorfni. U "matričnoj""terminologiji to znači da prsten A ima *IBB* ako i samo ako ne postoje matrice $U \in A_{mn}$ i $V \in A_{nm}$ takve da je

$$UV = E_m, \qquad VU = E_n. \tag{19}$$

Pretpostavimo da za neke matrice U i V nad prstenom A važi (19), gde je $m \neq n$. Neka je, na primer, $m < n$. Prsten A je Λ-hermitski zdesna, pa postoji leva regularna matrica $P \in A_n$ za koju je UP jedna donje trougaona matrica. Pri tome je broj m vrsta matrice UP manji od broja n "njenih" kolona, pa poslednja kolona matrice UP mora biti jednaka O. Otuda je i poslednja kolona matrice VUP nula-kolona. Medjutim, to nije moguće jer

iz druge od jednakosti *(19)* sledi $VUP = E$. Kako je matrica $P \in A_n$ regularna sleva, ona nema nula-kolona. Prema tome, ne može biti $m < n$. Zbog simetrije ne može biti ni $n < m$, pa (19) može da važi jedino ako je $m = n$. Otuda i tvrdjenje. □

TEOREMA 1-6

Ako je rang $r = \rho(M)$ matrice M nad desnim Λ-hermitskim prstenom A manji od broja njenih kolona, tada su njene kolone Γ-linearno zavisne zdesna.

DOKAZ. Neka je $M \in A_{mn}$ i $r < n$. Tada postoje matrice U i V formata $m \times r$ i $r \times n$ takve da je (*) $M = UV$. Uz to je prsten A Λ-hermitski zdesna pa je matrica VP donje trougaona za bar jednu levu regularnu matricu P iz A_n. Pri tome je matrica VP formata $r \times n$ sa $r < n$, što sa prethodnim znači da njena poslednja kolona, a time i poslednja kolona matrice $MP = UVP$ mora biti nula-kolona.

S druge strane, leva regularnost matrice P povlači da za $a \in R_\lambda(A)$ i $X = [0,..,0,a]^T$ mora biti $PX \neq O$, dok je $MPX = O$ (jer je poslednja kolona matrice MP nula-kolona). Stavimo $Y = PX = [a_1 .. a_n]$. Tada je $MY = O$, a time i $M_{*1}a_1 + \cdots + M_{*n}a_n = O$. Pri tome je $Yb \neq O$ za svako $b \neq 0$, jer bi u suprotnom bilo $Yb = O$, to jest $P(Xb) = O$, pa leva regularnost matrice P daje $Xb = O$, a time i $ab = O$. Medjutim, to nije moguće jer je element a regularan sleva i $b \neq 0$. Otuda i tvrdjenje. □

KOROLAR 1-2

Rang $\rho(M)$ leve regularne matrice M nad desnim Λ-hermitskim prstenom A jednak je broju njenih kolona. Ako je prsten A desni (levi) hermitski domen, tada važi i obrnuto tvrdjenje. Obrnuto tvrdjenje ne mora da važi u slučaju Λ-hermitskog prstena.

DOKAZ. Prvi deo tvrdjenja sledi neposredno iz *Teoreme 1-6*, a drugi iz činjenice da je svaki desni hermitski domen *Bezuov* (za koji je poznato da ima svojstvo o kome je reč). Zato dokažimo samo da važi i poslednji deo tvrdjenja. Neka je $A = K[X,Y,Z,T;\ XT=YZ]$ komutativan domen, gde je K polje i X,Y,Z,T *neodredjene* za koje važi $XT = YZ$. Na osnovu *Leme 1-3*

zaključujemo da je A desni Λ-hermitski domen. Ako je $M=\begin{bmatrix} X & Y \\ Z & T \end{bmatrix}$ matrica iz $M_2(A)$, biće $det(M)=XT-YZ=O$, pa matrica M nije regularna sleva u prstenu A_2. S druge strane, bez teškoća se proverava da nad prstenom A ne nože biti $M=\begin{bmatrix} a \\ b \end{bmatrix}\begin{bmatrix} p & q \end{bmatrix}$, pa je $\rho(M)>1$, a time i $\rho(M)=2$. □

TEOREMA 1-7

Neka je A desni Λ-hermitski prsten. Ako je, za bar jedno $a\in R_\ell(A)$ i bar jednu vrstu V matrice $M\in A_n$, aV leva linearna kombinacija preostalih vrsta matrice M, tada su kolone matrice M Γ-linearno zavisne zdesna.

Posebno, ako je A desni Λ-hermitski domen, tada iz leve linearne zavisnosti vrsta matrice M iz A_n sledi desna linearna zavisnost njenih kolona.

DOKAZ. Neka je $V=M_{i\to}$. Kako je aV leva linearna kombinacija preostalih vrsta matrice M, postoji vrsta matrica $Y=[b_1 \dots b_n]$, sa $b_i=a$, za koju je (*) $YM=O$. Označimo sa U podmatricu matrice M koja ne sadrži jedino njenu i-tu vrstu. Kako matrica U ima manje od n kolona, biće $\rho M<n$, pa su kolone matrice U Γ-linearno zavisne zdesna (*Teorema 1-6*). Otuda za bar jednu vrsta matricu X važi (**) $UX=O$ sa $Xb\neq O$ za svako b iz A^0. S druge strane, iz (*) sledi $YMX=O$, pa na osnovu (**) zaključujemo da da je $aM_{i\to}X=O$, što sa $a\in R_\ell(A)$ daje $M_{i\to}X=O$. To zajedno sa (**) znači da je $MX=O$, pa kako za svako $b\in A^0$ važi $Xb\neq O$, biće kolone matrice M Γ-linearno zavisne zdesna. □

LEMA 1-5

Ako je u desnom Λ-hermitskom prstenu A svaki levi regularni element inverzibilan, onda to svojstvo ima i svaki od prstena $M_n(A)$.

DOKAZ. Neka je M proizvoljna leva regularna matrica iz A_n. Tada postoji leva regularna matrica $P\in A_n$ takva da je matrica $MP=T$ donje trougaona. Pri tome je i matrica T regularna sleva. Dalje je $R_\ell(A)=R(A)$, pa na osnovu *Leme 1-4* zaključujemo da svi element glavne dijagonale matrice T moraju biti inverzibilni u prstenu A. Otuda za svaku kolona matricu Y formata n matrična jednačina $TX=Y$ ima (tačno jedno) rešenje $X=SY$ (naime, "odgovarajući" linearni sistem je trougaoni sa inverzibilnim

dijagonalnim" koeficijentima . Pri tome matrica S ne zavisi od Y, pa kako $TSY = Y$, to jest $(TS-E)Y = O$ važi za svaku matricu $Y \in M_{n1}(A)$, mora biti $TS = E$.

Iz $TS = E$ i $MP = I$ sledi $M(PS) = E$, pa je matrica M inverzibilna, a matrica $U = PS$ regularna sleva u prstenu A_n. Kako je $R_l(A) = R(A)$, prema *Teoremi 1-3* matrica U je regularna i zdesna. Ako je $UM = X$, biće $UMU = XU$ to jest $U = XU$, pa desna regularnost matrice U daje $X = E$. Dakle je $UM = E$, pa je matrica M inverzibilna i zdesna. Otuda i tvrdjenje. □

TEOREMA 1-8

Ako je A desni Λ-hermitski prsten i $S \subset R(A)$ desni denominator u A, tada je i prsten A_S Λ-hermitski zdesna.

DOKAZ. Neka su a/x i b/y $(a,b \in A;\ x,y \in S)$ proizvoljni elementi prstena A_S. Kako je prsten A Λ-hermitski zdesna, postoji leva regularna matrica $P_0 = \begin{bmatrix} p & r \\ q & s \end{bmatrix}$ iz A_2 takva da je $[a,\ b]P_0 = [h,\ 0]$ sa $h \in A$, a samim tim i

$$(20) \qquad \begin{bmatrix} a/x & b/y \end{bmatrix} \begin{bmatrix} xp & xr \\ yq & ys \end{bmatrix} = \begin{bmatrix} h & 0 \end{bmatrix}.$$

Označimo sa P drugu od matrica na levoj strani u *(20)*.i dokažimo da je ona regularna sleva u prstenu $M_2(A_S)$. Pretpostavimo da za neku kolona matricu $X = \begin{bmatrix} c/u, & d/v \end{bmatrix}^T$ $(c,d \in A;\ u,v \in S)$ važi $PX = O$. Kako su x i y regularni elementi prstena A, iz $PX = O$ sledi

$$(21) \qquad pc/u + xd/v = 0, \qquad qc/u + sd/v = 0.$$

S druge strane, iz $uA \cap vS \neq \Theta$ sledi da za neko $e \in A$ i $z \in S$ važi $ue = vz$. Pri tome iz $v,z \in S$ sledi $w = vz \in S$, a time i $w \in R(A)$. Ako jednakosti u *(21)* pomnožimo zdesna sa w, dobijamo njima ekvivalentne jednakosti (jer je w regularno u prstenu A), pa kako je $u^{-1}w = e$ i $v^{-1}w = z$ (u A_S) biće

$$(22) \qquad pce + rdz = 0, \qquad qce + sdz = 0.$$

Ako je $Y = [ce\ dz]^T$, iz *(22)* sledi $P_0Y = O$, pa kako je Y matrica nad A i P_0 leva regularna matrica iz A_2, mora biti $Y = O$, a time i $ce = 0$, $dz = 0$.

Uz to je $z \in S$, pa $dz = 0$ daje $d = 0$. Sada iz *(21)* sledi $pc=0$ i $qc=0$, to jest $P_0 X_0 = O$ sa $X_0 = [x\ 0]^T$, pa leva regularnost matrice P_0 u prstenu A_2 daje $x = 0$, a time i $X = O$. To upravo znači da je matrica P regularna sleva u prstenu $M_2(A_S)$, pa imamo i samo tvrdjenje. □

KOROLAR 1-3

Ako u desnom Λ-hermitskom prstenu A važi $R_\ell(A) = R(A) = S$, tada je S desni denominator u A, prsten A_S je hermitski zdesna i u svakom od prstena $M_n(A_S)$ regularni i inverzibilni elementi se podudaraju.

Posebno, ako je A komutativan neterovski domen, tada za svako $n \in N$ prsten $M_n(A)$ ima desni prsten razlomaka.

DOKAZ. S obzirom na *Teoremu 1-8* treba još jedino dokazati da za svako $a \in A$ i $x \in S$ važi $aS \cap xA \neq \Theta$. Zaista, prsten A je Λ-hermitski zdesna, pa postoje $c \in A$ i leva regularna matrica $P = \begin{bmatrix} p & r \\ q & s \end{bmatrix}$ iz $M_2(A)$ za koje važi $[a\ x]P = [c\ 0]$, a time i (*) $ar+xs = 0$. Pretpostavimo da za neko $u \in A$ važi $ru = 0$. Tada iz (*) sledi $xsu = 0$, i dakle $su = 0$ (jer je $x \in S$). Otuda je $PX = O$ sa $X = [0\ u]^T$, pa leva regularnost matrice P daje $X = O$, a time i $u = 0$. Dakle je $r \in S$, što sa (*) daje $aS \cap xA \neq \Theta$. Dalje, kako u prstenu A_S važi $R_\ell(A_S) = R(A_S)$, drugi deo tvrdjenja sledi iz *Leme 1-5*.

Ako je A komutativan neterovski domen, prema *Teoremi 1-2* svaki od prstena A_n je Λ-hermitski zdesna, i matrica $M \in A_n$ je regularna akko je $det(M) \neq 0$. Otuda za $B = A_n$ važi $R_\ell(B) = R(B)$, pa se poslednji deo tvrdjenja svodi na prethodni slučaj. □

TEOREMA 1-9

Ako u Λ-hermitskom prstenu A važi $R_\ell(A) = R_d(A) = S$, i ako za svaku matricu M iz $M_2(A)$ postoje leve regularne matrice P i Q za koje je matrica PMQ dijagonalna, onda to važi i za svaku matricu M nad prstenom A.

DOKAZ. Prsten A je Λ-hermitski i sleva i zdesna, pa je, prema *Korolaru 1-3*, prsten A_S hermitski. Dokažimo da za svaku matricu M iz $M_2(A_S)$ postoje inverzibilne matrice U i V iz $M_2(A_S)$ takve da je matrica $D = UMV$

dijagonalna. Pre svega, kako je A_S prsten (desnih) razlomaka nad A, za proizvoljne elemente a_i $(1 \leqslant i \leqslant n)$ iz prstena A_S postoji regularan element $a \in S$ takav da je $a_i a \in S$ za svako $1 \leqslant i \leqslant n$. To posebno znači da za proizvoljnu matricu M nad prstenom A_S postoji regularan element $a \in S$ za koji je Ma matrica nad prstenom A.

Neka je M proizvoljna matrica iz $M_2(A_S)$ i $a \in S$ takvo da je matrica Ma u prstenu $M_2(A)$. Tada prema pretpostavci postoje leve regularne matrice P i Q iz $M_2(A)$ za koje je matrica (*) $P(Ma)Q = D$ dijagonalna. Iz $a \in S$ sledi da je i matrica aQ regularna sleva u prstenu $M_2(A_S)$. Otuda su matrice $U = P$ i $V = aQ$ u prstenu $M_2(A_S)$ i inverzibilne (*Korolar 1-3*). Uz to je $UMV = D$, za čime smo i išli.

Kako je prsten A_S hermitski (*Teorema 1-8*), i kako je svaka matrica iz $M_2(A_S)$ dijagonalizabilna, prema *KAPLANSKY*[1] biće takva i svaka matrica nad prstenom A_S. To posebno znači da za proizvoljnu matricu M nad prstenom A postoje inverzibilne matrice U i V nad prstenom A_S takve da je matrica

$$UMV = D_0 \tag{23}$$

dijagonalna (nad prstenom A_S). Neka je $b \in S$ regularan element prstena A za koji je Vb matrica nad A. Kako je prsten A i Δ-hermitski sleva, a uz to $R_d(A) = R(A)$, biće S i levi denominator u A, pa postoji $a \in S$ za koje je i aU matrica sa elementima iz prstena A. Najzad, neka je c regularan element iz A takav da je $D = aD_0bc$ jedna matrica nad A. Stavimo $P = aU$, $Q = Vbc$ i $D = aD_0bc$. Tada su P, Q, D matrice nad prstenom A, i prema (23) važi $PMQ = D$. Uz to su matrice P i Q regularne (sleva), dok je matrica D dijagonalna. Otuda i tvrdjenje. □

KOROLAR 1-4

Za svaku matricu M formata $m \times n$ nad obostranim neterovskim domenom A postoje leve regularn matrice $P \in A_m$ i $Q \in A_n$ takve da je matrica $PMQ = D$ dijagonalna Pri tome se u opštem slučaju matrice P i Q ne mogu zameniti inverzibilnim matricama U i V nad prstenom A. □

PRIMEDBA 1-3. *Za desne (leve) ideale I i J prstena A (sa ili bez jedinice) kažemo da su SLIČNI, i pišemo $I \sim J$, ako su desni (levi) A-moduli*

izomorfni. Ako su a,b regularni elementi prstena A, tada je aA∿bA ako i samo ako je Aa∿Ab. Za elemente a,b∈A kažemo da su SLIČNI zdesna, i pišemo a∿b, ako su takvi desni ideali aA i bA. Jasno je da je ∿ jedna relacija ekvivalencije na skupu A, kao i da klasa ekvivalencije ã koja sadrži a takodje sadrži i svaki od elemenata b∈A za koje je aA = bA. Ako je u prstenu A svaki desni glavni ideal istovremeno i levi ideal u A, tada za svako a,b∈A važi a∿b ⇔ aA = bA (COHN [ ]). Ako su uz to svi desni delitelji prstena A u njegovom radikalu, tada je a∿b ako i samo ako su a i b pridruženi zdesna u prstenu A. □

Prema *Definiciji 1-2* matrice M formata $m\times n$ nad prstenom A je elementarno dijagonalizabilna u odnosu na hermitski niz (H_n) ako postoje matrice $P\in H_m$ i $Q\in H_n$ takve da je

$$PMQ = diag[a_1, a_2, ..], \qquad a_i \| a_{i+1} . \tag{24}$$

U tom slučaju a_i-ove zovemo *ELEMENTARNIM DELITELJIMA* matrice M. U vezi sa tim nameće se pitanje "jednoznačnosti" a_i-ova. Tako, na primer, ako je $H_n \subset U(A_n)$, i ako uz *(24)* za neke matrice $S\in H_m$ i $T\in H_n$ važi i

$$SMT = diag[b_1, b_2, ..], \qquad b_i \| b_{i+1} , \tag{25}$$

tada je $a_i = 0 \Leftrightarrow b_i = 0$, ali ne mora biti $a_i = b_i$, Štaviše, ne mora biti ni $a_iA = b_iA$ (što posebno znači da elementi a_i i b_i u opštem slučaju ne moraju biti uzajamno pridruženi). U vezi sa tim važi:

TEOREMA 1-10

Neka je (H_n) $(n\in N)$ hermitski niz nad prstenom A, pri čemu je H_n podgrupa grupe $U(A_n)$ $(n\in N)$.

(α) Ako su sve matrice formata 1×2, 2×1, 2×2 nad prstenom A elementarno dijagonalizabilne u odnosu na niz (H_n), onda je to slučaj i sa svakom matricom nad prstenom A.

(β) Ako su svi delitelji nule obostrano glavnoidealskog prstena A u njegovom radikalu, tada je A prsten sa elementarnim deliteljima u odnosu na hermitski niz (H_n).

(γ) *Ako prsten* A *zadovoljava uslove pod* (ε) *sa* $H_n = U(A_n)$, *tada su elementarni delitelji matrice* $M \in A_{mn}$ *odredjeni jednoznačno do na sličnost (Primedba 1-3). Ako su uz to svi ideali prstena* A *obostrani, tada su elementarni delitelji matrice* M *iz* $M_{mn}(A)$ *odredeni jednoznačno do na pridruženost.*

(δ) *Ako je* A *prsten sa elementarnim deliteljima (u odnosu na dati niz* H_n*) u kome su svi ideali obostrani, i ako za matricu* M *iz* A_{mn} *vazi (24) i (25) sa* $P,S \in A_m$ *i* $Q,T \in A_n$, *tada je* (*) $a_i A = b_i A$, *kao i* (**) $(a_1 \cdot\cdot a_i)A = (b_1 \cdot\cdot b_i)A$ $(i=1,2,..)$.

DOKAZ. (α) Dokaz je analogan dokazu *Th. 5-1*, *KAPLANSKY* [*1*]. (β) Pod datim pretpostavkama A je domen ili valuacioni prsten (*KAPLANSKY* [*1*]), pa tvrdjenje sledi iz (α) (*TEICHMULLER* [*1*] u slučaju kada je $H_n = U(A_n)$ i A domen).

(γ) *NAKAYAMA* [*1*] u slučaju kada je A domen, i *KAPLANSKY* [*1*] u slučaju kada je A valuacioni prsten.

(δ) Prvi deo tvrdjenja, to jest (*), sledi iz *Th.9-3*, *KAPLANSKI* [*1*]. Dokažimo da važi i (**). Naime, iz $a_1 A = b_1 A$ sledi $a_1 = b_1 x$ za neko x iz A. Kako je $a_2 A$ i levi ideal prstena A, biće $x a_2 A \subset a_2 A$, što zajedno sa $a_2 A = b_2 A$ daje $x a_2 A \subset b_2 A$. Množeći poslednju inkluziju (sleva) sa b_1 dobijamo $a_1 a_2 A \subset b_1 b_2 A$. Slično zaključujemo da je i $b_1 b_2 A \subset a_1 a_2 A$, pa je $a_1 a_2 A = b_1 b_2 A$. Radeći slično, indukcijom po i zaključujemo da tvrdjenje važi za svako i. □

DEFINICIJA 1-4

Ako je A *prsten sa elementarnim deliteljima, u odnosu na niz* (H_n), *i ako su za svaku matricu* M *nad* A *i njene elementarne delitelje* a_i $(1 \leqslant i \leqslant r)$ *desni ideali* $(a_1 \cdot\cdot a_s)A$ $(1 \leqslant s \leqslant r)$ *odredjeni jednoznačno, tada kažemo da je* A *prsten sa* DETERMINANTNIM *idealima* □

Ako su a_s $(1 \leqslant s \leqslant r)$ elementarni delitelji matrice M nad komutativnim prstenom A sa determinantnim idealima, tada je $(a_1 \cdot\cdot a_s)A$ upravo ideal prstena A generisan determinantama kvadratnih podmatrica reda s matrice M (otuda i naziv). Prema *Teoremi 1-10* pod (δ) postoje i nekomutativni prsteni sa determinantnim idealima. □

V

O MATRICAMA NAD EUKLIDSKIM PRSTENIMA

Ako je u prstenu A svaki desni ideal glavni, onda to svojstvo ima i svaki od prstena $A_n = M_n(A)$ $(n \in N)$. Zato se prirodno nameće pitanje da li desna "euklidnost" (Λ-euklidnost) prstena A povlači desnu euklidnost (Λ-euklidnost) svakog od prstena $M_n(A)$. U vezi sa tim, *I. SANOV* [1] je dokazao da ako *komutativan* domen A ima *konačnu* euklidsku valuaciju ϕ koja zadovoljava uslov (N) $\phi(ab) = (\phi a)(\phi b)$, tada je $\psi = \phi \circ det$ jedna Γ-euklidska valuacija prstena A_n, to jest za svaku matricu M iz $M_n(A)$ i svaku *regularnu* matricu $B \in R(A_n)$ postoje matrice $Q \in A_n$ i $R \in R_0(A_n)$ takve da je $M = BQ + R$, $\psi(R) < \psi(B)$. Pri tome za $n > 1$ valuacija ψ nije *euklidska* (jer, na primer, i za $M \neq O$ može biti $\psi M = 0$). Dokazaćemo da to važi i pod znatno slabijim pretpostavkama za prsten A, kao i da je tada prsten $M_n(A)$ euklidski zdesna. Uzgred primetimo da (u opštem slučaju) *determinanta* nad *nekomutativnim* prstenom nije ni definisana. Simbolika i terminologija iz prethodnih poglavlja važiće i u ovom poglavlju, što se posebno odnosi na simboliku u vezi sa prstenom $M_n(A)$.

TEOREMA 1-1

Ako prsten A ima bar jednu konačnu desnu euklidsku valuaciju, tada je prsten A hermitski zdesna u odnosu na hermitski niz $\mathfrak{E}(A_n)$. Pri tome za svaku matricu $M \in A_{mn}$ postoji matrica $P \in \mathfrak{E}(A_n)$ takva da je matrica MP donje trougaona.

DOKAZ. Neka je ϕ minimalna desna euklidska valuacija prstena A. Dalje, neka je $M = [a\ b]$ proizvoljna matrica iz $M_{12}(A)$ i stavimo $a_0 = a$, $a_1 = b$. Ako je $a_0 \neq 0$, tada postoje $q_1, a_2 \in A$ takvi da važi (*) $a_0 = a_1 q_1 + a_2$ sa

$\phi a_2 < \phi a_1$. Dodajući prvoj koloni matrice M njenu drugu kolonu pomnoženu zdesna sa $-q_1$, i zamenjujući mesta kolonara u tako dobijenoj matrici, dobijamo matricu $M_1 = [a_1\ a_2]$. Ako je $a_2 = 0$, stvar je gotova. U slučaju da je $a_2 \neq 0$, opisani postupak primenjujemo na matricu M_1, itd. Na taj način dolazimo do "niza" matrica $M_n = [a_n\ a_{n+1}]$ $(n = 0,1,..)$ takvih da za $a_n \neq 0$ važi $\phi a_n < \phi a_{n-1}$. No, kako je valuacija ϕ konačna, za bar jedno n mora biti $\phi a_n = 0$, to jest $a_n = 0$, i dakle $M_n = [c\ 0]$ sa $c = a_{n-1}$. Prema tome, primenom konačno mnogo elementarnih transformacija na kolonama matrice M možemo je svesti na neku donje trougaonu matricu T. To znači da postoji matrice $P \in \mathcal{E}(A_2)$ za koju je $MP = T$, pa je prsten A hermitski zdesna u odnosu na niz $\mathcal{E}(A_n)$. Otuda i tvrdjenje. □

LEMA 1-1

Ako prsten A ima bar jednu konačnu desnu euklidsku valuaciju ϕ, i ako vazi bilo koji od uslova:

(α) $U_l(A) = U(A)$,

(β) $\phi(a) = \phi(1)$ za svako $a \in U_d(A)$,

(γ) *Svi desni delitelji nule prstena A su u njegovom radikalu J,*

tada je svaka inverzibilna matrica nad prstenom A proizvod konačno mnogo elementarnih matrica nad tim prstenom, i dakle $U(A_n) = \mathcal{E}(A_n)$.

DOKAZ. Neka je M proizvoljna matrica iz $U(A_n)$. Prema *Teoremi 1-1* postoji matrica $P \in \mathcal{E}(A_n)$ takva da je matrica $MP = T$ donje trougaona, to jest

$$(1) \qquad T = MP = \left[\begin{array}{c|c} a & O \\ \hline B & C \end{array}\right], \qquad T_0 = \left[\begin{array}{c|c} a & O \\ \hline O & \hat{M} \end{array}\right],$$

pri čemu je $a \in A$ i $B = [b_2 .. b_n]^T$ izvesna matrica formata $(n-1)\times 1$. Kako su matrice M i P inverzibilne, biće to slučaj i sa matricom MP. Ako je uz to $[T^{-1}]_{11} = b$, tada iz $TT^{-1} = E$ sledi (*) $ab = 1$. Dokažimo da je i $ba = 1$. Naime, ako prsten A zadovoljava uslov (α), to sledi neposredno iz (*). Ako prsten A zadovoljava uslov (β), biće $\phi b = \phi 1$. Uz to postoje $q, r \in A$ takvi da je $1 = bq + r$ sa $\phi r < \phi b$, i dakle $1 = bq$ (jer $\phi r < \phi 1 \Rightarrow r = 0$). Otuda, množeći (*) zdesna sa q dobijamo $a = q$, to jest $1 = ba$, a samim tim i $a \in U(A)$. Najzad, ako su svi desni delitelji nule prstena A u njegovom radikalu J, množeći (*) zdesna sa a dobijamo $a(1-ba) = 0$, tj. $1-ba \in J$,

i prema tome $a \in U(A)$.

Jasno je da tvrdjenje važi za $n=1$. Neka je $n>1$ fiksiran prirodan broj i pretpostavimo da tvrdjenje važi za sve prirodne brojeve $<n$. Kako je $a \in U(A)$, dodajući i-toj vrsti $(2 \leqslant i \leqslant n)$ matrice $T=MP$ njenu prvu vrstu pomnoženu sleva sa $-b_i a^{-1}$, dobijamo matricu T_0 oblika (1). Uz to za neku matricu $Q \in \mathcal{E}(A_n)$ važi $T_0 = QT$, pa je i matrica $T_0 = a + \tilde{M}$, a time i matrica M inverzibilna. Otuda je $\tilde{M} \in U(A_{n-1})$, pa na osnovu induktivne pretpostavke postoje elementarne matrice P_i za koje je $\tilde{M} = P_1 \cdot\cdot P_k$. Ako je E jedinična matrica reda $n-1$, tada su $Q_0 = a+E$ i $Q_i = 1 \dot{+} P_i$ $(1 \leqslant i \leqslant k)$ elementarne matrice iz A_n. Pri tome je $T_0 = a \dot{+} \tilde{M} = Q_0 Q_1 \cdot\cdot Q_k$, a time i:

$$M = Q^{-1} T_0 P^{-1} = Q^{-1} Q_0 \cdot\cdot Q_k P^{-1}. \tag{2}$$

Otuda i tvrdjenje, jer su P, Q, Q_i $(0 \leqslant i \leqslant k)$ elementi grupe $\mathcal{E}(A_n)$, pa iz (2) sledi da je i $M \in \mathcal{E}(A_n)$. (U slučaju komutativnog prstena prethodno tvrdjenje važi i za proizvoljnu euklidsku valuaciju $\phi: A \to W$.) □

TEOREMA 1-2

Ako je minimalna euklidska valuacija prstena A konačna, tada je A prsten sa elementarnim deliteljima u odnosu na hermitski niz $\mathcal{E}(A_n)$.

Ako su svi delitelji nule euklidskog prstena A u njegovom radikalu, tada je A prsten sa elementarnim deliteljima (i u slučaju kada prsten A nema konačnih euklidskih valuacija).

DOKAZ. Radeći slično kao pri dokazu *Teoreme 1-1*, posle kraćeg "računa" zaključujemo da su sve matrice formata 1×2, 2×1, 2×2 nad A dijagonalizabilne u odnosu na niz $\mathcal{E}(A_n)$, pa prema *IV, Teorema 1-10* to važi i za svaku matricu nad prstenom A. Drugi deo tvrdjenja sledi iz *IV, Teorema 1-10*, jer je prsten A glavnoidealski. □

Ako je A euklidski prsten sa determinantnim idealima (str.) i $\phi: A \to W$ prirodna desna euklidska valuacija, tada su za svaku matricu M iz $M_{mn}(A)$ i njene elementarne delitelje a_i $(1 \leqslant i \leqslant r)$ ideali $(a_1 \cdot\cdot a_i)A$, a time i elementi $\phi(a_1 \cdot\cdot a_i)$ $(1 \leqslant i \leqslant r)$ skupa W odredjeni jednoznačno za datu matricu M.

DEFINICIJA 1-1

Za desni euklidski par (A,ϕ) kažemo da ima DETERMINANTNO SVOJSTVO *(kratko* δ*-SVOJSTVO) ako je A prsten sa elementarnim deliteljima takav da za svaku matricu M nad A i njene elementarne delitelje $a_1,..,a_r$, odnosno $b_1,..,b_r$ važi*

$$(3)\qquad \phi(a_1\cdot\cdot a_s) = \phi(b_1\cdot\cdot b_s) \qquad (1 \leqslant s \leqslant r),$$

to jest da su $\phi(a_1\cdot\cdot a_s)$ $(1 \leqslant s \leqslant r)$ određeni jednoznačno matricom M. Tada kažemo i da prsten A ima δ-SVOJSTVO u odnosu na euklidsku valuaciju ϕ.

PRIMER 1-1. *Jasno je da svaki euklidski prsten sa determinantnim idealima ima δ-svojstvo u odnosu na svaku prirodnu euklidsku valuaciju ϕ prstena A. Obrnuto tvrdjenje ne mora da važi. Zaista, neka je A euklidski domen koji ima bar jednu euklidsku valuaciju $\phi: A \to W$ koja zadovoljava uslov (M) $\phi(a+b) \leqslant \max(\partial a, \partial b)$. Tada za neki automorfizam $f: K \to K$ i f-diferenciranje δ tela $K = U_0(A)$ važi $A = K[X,f,\delta]$. Uz to je $\phi = h\circ\partial$ kompozicija stepene valuacije i jedne strogo rastuće funkcije $h: N_0 \to W$.*

Ako je $a = X^n a_n + \cdots + a_0$ $(a_n \neq 0)$ proizvoljan element iz A, tada se svaki element $x \in A$ može na tačno jedan način pretstaviti u obliku $aq+r$ sa $\partial r < \partial a = n$. Drugim rečima, za svako $x \in A$ postoji tačno jedno r takvo da je $x + aA = r + aA$ sa $\partial r < n$, to jest

$$(4)\qquad x + aA = r_0 + Tr_1 + \cdots + T^s r_s \qquad (s = n-1),$$

pri čemu je $r = \sum X^i r_i$ $(0 \leqslant i < n)$ i $T^i = X^i + aA$. Otuda je dimenzija desnog K-modula A/aA jednaka $n = \partial a$. Prema tome, ako su a i b slični elementi prstena A, biće desni A-moduli, a time i desni K-moduli A/aA i A/bA izomorfni, pa je $\dim_K(A/aA) = \dim_K(A/bA)$, to jest $\partial a = \partial b$, što zajedno sa $\phi = h\circ\partial$ daje $\phi a = \phi b$. Otuda u prstenu A važi: $a \backsim b \Rightarrow \phi a = \phi b$.

Ako su a_i-ovi i b_i-ovi $(1 \leqslant i \leqslant m)$ elementarni delitelji matrice M nad prstenom A, tada je $a_i \backsim b_i$, i dakle $\phi a_i = \phi b_i$ $(1 \leqslant i \leqslant m)$. Uz to je $\partial(ab) = \partial a + \partial b$, pa $\phi = h\circ\partial$ povlači $\phi(a_1\cdot\cdot a_s) = \phi(b_1\cdot\cdot b_s)$ $(1 \leqslant s \leqslant m)$, što upravo znači da prsten A ima δ-svojstvo u odnosu na valuaciju ϕ. Jasno je da se tu ϕ može zameniti sa ∂.

Medjutim, prsten A ne mora biti prsten sa determinantnim idealima, to jest, ne mora biti $(a_1 \cdot\cdot a_s)A = (b_1 \cdot\cdot b_s)A$ $(1 \leqslant s \leqslant m)$. *Naime, kako je A domen, iz* $a_1A = b_1A$ *bi sledilo da su* a_1 *i* b_1 *uzajamno pridruženi, što znači da bi tada važila implikacija* $a \backsim b \Rightarrow a \simeq b$. *Neka je* $\delta = 0$ *i f automorfizam tela K koji nije identično preslikavanje. Tada je* $A = K[X,f]$ *euklidski domen sa δ-svojstvom u odnosu na valuaciju ∂, ali u prstenu A slični elementi ne moraju biti pridruženi. Tako, na primer, ako za* $c \in K$ *važi* $f(c) \neq c$, *tada su polinomi* $a = X+1$ *i* $b = X+c^{-1}f(c)$ *slični, ali ne i pridruženi u prstenu A. Pri tome su 1,a i 1,b elementarni delitelji matrice* $M = diag[1, a]$. □

DEFINICIJA 1-2

Za desnu (levu) Σ-euklidsku valuaciju ϕ $A \to W$ *kažemo da zadovoljava* USLOV KANCELACIJE *ako za svako* $a,b \in \Sigma$ *i* $u,v \in A$ *takve da uav i ubv pripadaju skupu Σ, važi*

$$(K) \qquad \phi(uav) > \phi(ubv) \Rightarrow \phi(a) > \phi(b).$$

Jasno je da svaka (desna) euklidska valuacija ϕ koja zadovoljava neki od uslova (N) i (L) (str.) zadovoljava i uslov (K). Ako desna euklidska valuacija $\phi: A \to N_0$ domena A zadovoljava uslov (M), tada ϕ zadovoljave i uslov (K). Naime, u tom slučaju ϕ je kompozicija jedne stepene valuacije ∂ i jedne "strogo rastuće" funkcije h. Svaka (desna) euklidska valuacije ϕ koja zadovoljava uslov (K) je prirodna (i sleva i zdesna). Naime, ako je $\phi(ab) < \phi(a)$, tada prema uslovu (K) mora biti $\phi b < \phi 1$, i dakle $b = 0$. □

TEOREMA 1-3

Ako komutativan domen A ima bar jednu euklidsku valuaciju $\phi: A \to W$ *koja zadovoljava uslov (K), tada je za svaki prirodan broj n prsten* $M_n(A)$ *euklidski (i sleva i zdesna).*

DOKAZ. Stavimo $\tilde{W} = W \cup W^2 \cup \cdot\cdot \cup W^n$ i označima sa $\leqslant$ binarnu relaciju na skupu $\tilde{W}$ definisanu sa: (1) $0 \leqslant \alpha$ za svako $\alpha \in \tilde{W}$; (2) ako je $\alpha \in W^r$, $\beta \in W^s$ i $\alpha \neq 0$, tada važi $r > s \Rightarrow \alpha < \beta$; (3) restrikcija od $\leqslant$ na W^s je leksiografsko uredjenje skupa W^s. Tada je $(\tilde{W}, \leqslant)$ dobro uredjen skup i $0 = min\, \tilde{W}$.

Neka je $M \neq O$ proizvoljna matrica iz A_n, a_s $(1 \leqslant s \leqslant r)$ njeni elementarni delitelji, i za $1 \leqslant s \leqslant r$ stavimo $\hat{a}_s = a_1 \cdots a_s$. Iz *IV, Teorema 1-10* pod (ć) sledi da su ideali $a_s A$ odredjeni jednoznačno matricom M (jer je prsten A komutativan). S druge strane, valuacija ϕ je prirodna pa iz $aA = bA$ sledi $\phi a = \phi b$. Otuda su i elementi $\phi \hat{a}_s$ $(1 \leqslant s \leqslant r)$ skupa W odredjeni jednoznačno matricom M, pa je sa $\psi O = 0$ i

$$\psi(M) = (\phi \hat{a}_1, \ldots, \phi \hat{a}_r) \qquad (M \in A_n) \tag{5}$$

(dobro) definisano jedno preslikavanje ψ skupa A_n u dobro uredjen skup $\hat{W}$. Dokazaćemo da je tako definisano preslikavanje $\psi: A_n \to \hat{W}$ desna (leva) euklidska valuacija prstena A_n.

Pre svega, ako su P i Q inverzibilne matrice iz $M_n(A)$ za koje, uz prethodnu simboliku, važi $PMQ = diag[a_1, \ldots, a_r, \ldots]$, tada za proizvoljne inverzibilne matrice U, V iz A_n važi $S(UMV)T = PMQ$, pri čemu je $S = PU^{-1}$ i $T = V^{-1}Q$, a time i $\psi(UMV) = \psi(M)$ za proizvoljne jednote $U, V \in M_n(A)$.

Za $n=1$ je $\psi = \phi$, pa se tada tvrdjenje svodi na samu pretpostavku o valuaciji ϕ. Neka je $n > 1$ fiksiran prirodan broj i pretpostavimo da je $\psi = \psi(m)$ euklidska valuacija prstena A_m za svaki prirodan broj $m < n$. Za proizvoljnu matricu $B \neq O$ iz A_n i njene elementarne delitelje $b_1, \ldots, b_r$ postoje matrice $S, T \in U(A_n)$ takve da je

$$SBT = diag[b_1, b_2, \ldots]. \tag{6}$$

Stavimo $\tilde{B} = SBT$ i neka je M proizvoljna matrica iz A_n. Kako je prsten A hermitski, postoji inverzibilna matrica $P \in A_n$ za koju je matrica $\tilde{M} = SMP$ donje trougaona. Ako postoje matrice $\tilde{Q}, \tilde{R} \in A_n$ takve da je

$$\tilde{M} = \tilde{B}\tilde{Q} + \tilde{R}, \qquad \psi\tilde{R} < \psi\tilde{B}, \tag{7}$$

tada, množeći jednakost *(7)* sleva sa S^{-1} i zdesna sa P^{-1}, i stavljajući $Q = T\tilde{Q}P^{-1}$ i $R = S^{-1}\tilde{R}P^{-1}$, dobijamo

$$M = BQ + R, \qquad \psi R < \psi B, \tag{8}$$

jer je $S^{-1}\tilde{M}P^{-1} = M$, $S^{-1}\tilde{B}T^{-1} = B$, $\psi(\tilde{B}) = \psi(B)$, $\psi(S^{-1}\tilde{R}P^{-1}) = \psi(\tilde{R})$. Otuda je dovoljno dokazati da postoje matrice Q i R za koje važi (7). Drugim

rečima, dovoljno je dokazati da (8) važi za donje trougaone matrice M i matrice B oblika $B=diag[b_1,b_2,..]$ sa $a_s \| a_{s+1}$ $(1 \leqslant s \leqslant r)$, pa ćemo se u daljnjem izlaganju ograničiti na "takve" matrice M i B.

Označimo sa M_0 i B_0 redom komatrice polja (n,n) matrica M i B. Iz $B \neq O$ sledi $b_1 \neq 0$, a time i $B_0 \neq O$. Matrice M_0 i B_0 su reda $n-1$. U toje matrica M_0 donje trougaona i $B_0 = diag[b_1,b_2,..]$, gde su b_s-ovi elementarni delitelji matrice B_0. Otuda prema induktivnoj pretpostavci postoje matrice Q_0 i R_0 iz A_{n-1} takve da je $M_0 = B_0Q_0 + R_0$ sa $\psi R_0 < \psi B_0$, a time i

$$(9) \qquad \begin{bmatrix} M_0 & O \\ L & a \end{bmatrix} = \begin{bmatrix} B_0 & O \\ O & b \end{bmatrix} \begin{bmatrix} Q_0 & G \\ F & q \end{bmatrix} + \begin{bmatrix} R_0 & K \\ H & c \end{bmatrix},$$

to jest $M = BQ+R$, pri čemu je $[L\ a]$ poslednja vrsta matrice M, $b = [B]_{nn}$, $a = bq+c$ sa $\phi c < \phi b$ za $b \neq 0$, $c=a$ za $b=0$, F izvesna vrsta matrica, G izvesna kolona matrica, $H = L-bF$, $K = -B_0G$, i

$$(10) \qquad Q = \begin{bmatrix} Q_0 & G \\ F & q \end{bmatrix}, \qquad R = \begin{bmatrix} R_0 & K \\ H & c \end{bmatrix}.$$

Tvrdjenje će biti dokazano ako dokažemo da se matrice $[q], F, G, Q$ mogu izabrati tako da uz prethodnu simboliku važi (*) $\psi R < \psi B$. (Radi kraćeg izražavanja, ako su a_s-ovi elementarni delitelji neke matrice M, tada ćemo sa $\tilde{a}_s$ označavati proizvod $a_1 \cdot\cdot a_s$.)

Pretpostavimo prvo da je $R_0 \neq O$ i neka su a_s $(1 \leqslant s \leqslant k)$ elementarni delitelji matrice R_0. Tada iz $\psi R_0 < \psi B_0$ sledi $k > r_0$, gde je r_0 $(r_0 \leqslant r)$ broj elementarnih delitelja matrice B_0. Pri tome je ili $k>r_0$, ili je $k=r_0$ i $\phi\tilde{a}_s \leqslant \phi\tilde{b}_s$ $(1 \leqslant s \leqslant r_0)$ sa $\phi\tilde{a}_s < \phi\tilde{b}_s$ za bar jedno $s \leqslant r_0$. Neka su U_0 i V_0 inverzibilne matrice za koje je $U_0R_0V_0 = diag[a_1,a_2,..]$, i označimo sa U i V redom inverzne matrice matrica U_0+1 i V_0+1. Ako je $F=O$ i $G=O$, a time i $K=O$ i $H=L$, tada se neposredno proverava da važi $R = USV$, gde je

$$(11) \qquad S = \left[\begin{array}{ccc|c} a_1 & 0 & \cdot\cdot & 0 \\ 0 & a_2 & & 0 \\ \vdots & & & \\ \hline u_1 & u_2 & \cdot\cdot & c \end{array}\right],$$

sa $LV_0 = [u_1,u_2,..]$. Stavimo $S_0 = U_0R_0V_0$. Ako su c_s $(1 \leqslant s \leqslant m)$ elementarni

delitelji matrice S, tada je $\tilde{c}_s$ upravo najveći zajednički delitelj svih minora reda s matrice S (jer je domen A komutativan). To posebno znači da je $m \geqslant k$, kao i da $\tilde{c}_s | \tilde{a}_s$ za $1 \leqslant s \leqslant k$. Otuda je $\phi\tilde{c}_s \leqslant \phi\tilde{a}_s$ $(1 \leqslant s \leqslant k)$, pa kako je i $m > k$, biće $\psi R = \psi S \leqslant \psi R_0 < \psi B_0$. Ako je $b=0$, tada je $\psi B = \psi B_0$, i prema tome $\psi R < \psi B$.

Ako je $b \neq 0$, tada c možemo izabrati tako da je $\phi c \leqslant \phi b$ i $c \neq 0$. Na-ime, ako je $c=0$, neposredno se proverava da *(9)* važi i u slučaju da se q i c redom zamene sa $q_0 = q-1$ i b, pa tada Q i R možemo izabrati tako da *(9)* važi sa $c = b$. Kako je $\tilde{a}_k c \neq 0$, matrica S ima bar jednu regularnu podmatricu reda $k+1$, pa je $m \geqslant k+1$. S druge strane, iz $b \neq 0$ sledi da je $r = n$. Otuda je $k = n-1$, što sa prethodnim daje $m = n$. Sada iz $\psi R_0 < \psi B_0$ i $k = n-1$ sledi da za bar jedno $s \leqslant n-1$ važi $\phi a_s < \phi b_s$, a time i $\phi\tilde{c}_s < \phi\tilde{b}_s$, dok je $\phi\tilde{c}_s \leqslant \phi\tilde{a}_s \leqslant \phi\tilde{b}_s$ za svako $s \leqslant n-1$. Uz to je $c = b$, pa iz $\phi\tilde{a}_k \leqslant \phi\tilde{b}_k$ sledi $\phi(\tilde{a}_k c) \leqslant \phi(\tilde{b}_k c)$ sa $k = n-1$ (jer ϕ zadovoljava uslov kancelacije), i dakle $\phi(\tilde{a}_{n-1} c) \leqslant \phi(\tilde{b}_n)$. Kako je $det(S)$ jedini minor reda n matrice S biće $\tilde{c}_n$ i $detS$ uzajamno pridruženi elementi u prstenu A, što zajedno sa prethodnim daje $\phi\tilde{c}_n \leqslant \phi\tilde{b}_n$, a time i $\psi R < \psi B$.

Neka je sada $R_0 = O$. Tada se neposredno proverava da (9) važi i ako se Q_0 i R_0 zamene redom sa $Q_0 - E$ i B_0. Označimo ponovo sa Q i R matrice koje nastaju iz "prethodnih" matrica Q i R kada se u njima podmatrice Q_0 i R_0 zamene sa $Q_0 - E$ i B_0. Tada za $F = O$ imamo

$$(12) \qquad R = \left[\begin{array}{ccc|c} b_1 & 0 & \cdots & -B_0 G \\ 0 & b_2 & & \\ \vdots & & & \\ \hline u_1 & u_2 & \cdots & c \end{array}\right],$$

pri čemu je $L = [u_1, u_2, \ldots]$. Neka su d_s $(1 \leqslant s \leqslant p)$ elementarni delitelji matrice R. Jasno je da je tada $p > r_0$ i $\tilde{d}_s | \tilde{b}_s$ $(1 \leqslant s \leqslant r_0)$, pa za svako $s \leqslant r_0$ važi (**) $\phi\tilde{d}_s \leqslant \phi\tilde{b}_s$, a time i $\psi R \leqslant \psi B_0$.

Neka je prvo $b = 0$, i dakle $\psi B = \psi B_0$. Ako je pri tome $c \neq 0$, stavimo $G = O$. Tada matrica R ima bar jedan minor reda $r_0 + 1$ koji je različit od nule. Otuda je $p > r_0$, i prema tome $\psi R < \psi B_0 = \psi B$. Pretpostavimo sada da je $c = 0$. Ako je uz to i $L = O$, tada za $G = O$ dobijamo $R = B$, pa $M = BQ + R$ daje $M = B(Q+E) = BQ$, i stvar je gotova. Zato pretpostavimo da je $L \neq O$, i neka je, na primer, $u_i \neq 0$. Ako tada za matricu G uzmemo kolona matricu čija je i-ta koordinata 1 a preostale 0, biće $-B_0 G = [0, \ldots, -b_i, \ldots, 0]$,

pa dodajući poslednjoj koloni matrice R njenu i-tu kolonu R_{+i} dobljamo matricu oblika *(12)* za $G=O$ i $c=u_i$, i za koju važi $\psi T = \psi R$. Kako je $u_i \neq 0$, na osnovu već apsolviranog slučaja $(G=O$ i $c \neq 0)$ imamo da je $\psi T < \psi B$, a time i $\psi R < \psi B$.

Pretpostavimo sada da je $b \neq 0$. Tada je $r=n$ i $r_0=n-1$, a samim tim i $k \geqslant n-1$. Ako je $u_i = bq_i + r_i$ sa $\phi r_i < \phi b$, tada za matricu $F = [q_1, q_2, ..]$ važi $H = L - bF = [r_1, r_2, ..]$ sa $\phi r_i < \phi b$ $(1 \leqslant i < n)$. Drugim rečima, možemo pretpostaviti da u *(12)* važi $\phi u_i < \phi b$ $(1 \leqslant i < n)$. Neka je prvo $c \neq 0$. Tada za $G=O$ iz $\tilde{b}_{n-1} c \neq 0$ sledi $k > n-1$, i dakle $k = n$. Kako uz to valuacija ϕ zadovoljava uslov (K), $\phi c < \phi b$ daje $\phi(\tilde{b}_{n-1} c) < \phi(\tilde{b}_{n-1} b)$. S druge strane je $\tilde{d}_n = \tilde{b}_{n-1} c$ i $\tilde{b}_n = \tilde{b}_{n-1} b$, pa je $\phi \tilde{d}_n < \phi \tilde{b}_n$, što sa $(**)$ upravo znači da je $\psi R < \psi B$.

Najzad, neka je $c = 0$. Ako je i $u_i = 0$ $(1 \leqslant i \leqslant n)$, tada za c možemo uzeti samo b (zamenjujući u *(9)* q sa $q-1$), pa za $G = O$ dobljamo $R = B$, i prema tome $M = BQ + R = B(Q+E) = B\tilde{Q}$. Ako je $u_i \neq 0$ za bar jedno i, neka je G kolona matrica čija je i-ta koordinata 1 a preostale 0, a T matrica koja nastaje iz matrice R dodajući njenoj poslednjoj koloni njenu i-tu kolonu. Tada je $\psi T = \psi R$ i $\tilde{d}_n = \tilde{b}_{n-1} u_i$, pa kako je $\phi u_i < \phi b$, slično kao u prethodno "podslučaju" (za $c \neq 0$) zaključujemo da je $\phi \tilde{d}_n < \phi \tilde{b}_n$, i dakle $\psi R = \psi T < \psi B$.

Prema tome, u (9) se F, G, Q_0 i q mogu izabrati tako da je $M = BQ + R$ sa $\psi R < \psi B$, pa je prsten $M_n(A)$ euklidski zdesna. No, kako je $\psi M = \psi M^T$ za za svaku matricu $M \in A_n$, iz $M^T = B^T Q^T + R^T$, $\psi R^T < \psi B^T$ sledi $M = QB + R$ sa $\psi R < \psi B$. Kako to važi za proizvoljne matrice M i B $(B \neq O)$ iz A_n, prsten A_n je euklidski i sleva. Otuda i tvrdjenje u celini. □

KOROLAR 1-1

Za svako telo K i prirodan broj n prsten $A = M_n(K)$ je euklidski, i preslikavanje $\psi_0 : A \to N_0$ definisano sa $\psi_0(O) = 0$ i

$$\psi_0(M) = n - \rho(M) + 1 \qquad (M \in A^0), \tag{13}$$

je jedna njegova euklidska valuacija. Pri tome $\rho(M)$ označava rang matrice M (koji je jednak broju njenih elementarnih delitelja).

DOKAZ. Neka je $\phi : K \to N_0$ euklidska valuacija data sa $\phi 0 = 0$, $\phi a = 1$ $(a \neq 0)$, i $\psi : A \to \tilde{N}_0$ preslikavanje o kome je reč u dokazu prethodne *Teoreme 1-3* za

$W=N_0$ i $A=K$. Slično kao pri dokazu *Teoreme 1-3* zaključujemo da je ψ i leva i desna euklidska valuacija prstena $A=M_n(K)$ (i u slučaju da telo K nije komutativno). S druge strane, ako su a_s-ovi $(1\leqslant s\leqslant r)$ elementarni delitelji matrice $M\neq O$, biće $\phi(\tilde{a}_s)=1$ $(1\leqslant s\leqslant r)$, pa je $\psi(M)=(1,..,1)$ (r jedinica). Uz to je $r=\rho M$, pa se neposredno zaključuje da za $S,T\in A$ važi: $\psi S<\psi T \Leftrightarrow \psi_0 S<\psi_0 T$, odakle sledi i preostali deo tvrdjenja. □

TEOREMA 1-4

Ako komutativan prsten A sa elementarnim deliteljima ima bar jednu Γ-euklidsku valuaciju $\phi: A\to W$ koja zadovoljava uslov kancelacije, tada je i svaki od prstena $M_n(A)$ Γ-euklidski.

DOKAZ. Neka je $\psi:A_n\to W$ preslikavanje o kome je reč u *Teoremi 1-3*. Kako je prsten A komutativan, na osnovu *Kramerove teoreme* zaključujemo da je matrica B regularna u prstenu A_n ako i samo ako je to slučaj sa njenom determinantom $det(B)$ u prstenu A. Otuda, ako su b_s $(1\leqslant s\leqslant r)$ elementarni delitelji matrice B, tada mora biti $r=n$ i $b_s\in R(A)$ $(1\leqslant s\leqslant n)$. Vodeći računa o tome, dokaz dalje teče "paralelno" dokazu *Teoreme 1-3* za slučaj $b\neq 0$. Jedino treba napomenuti da, uz simboliku *Teoreme 1-3*, u_i-ove i c možemo birati tako da je $u_i, c\in R_0(A)$, jer je po pretpostavci prsten A Γ-euklidski. □

Ako je $\delta:A_n\to W$ preslikavanje definisano sa: $\delta(M)=\phi(\det M)$, tada se, uz prethodnu simboliku, neposredno zaključuje da za svako S i T iz $R_0(A_n)$ važi: $\psi S<\psi T \Leftrightarrow \delta S<\delta T$. Otuda sledi da je, zajedno sa ψ, i δ jedna Γ-euklidska (ali ne i euklidska) valuacija prstena A_n. U *SANOV* [1] je (na jedan drugi način) dokazano da je (uz našu terminologiju) ϕ *det* jedna Γ-euklidska valuacija prstena A_n u slučaju kada je A komutativan domen čija euklidska valuacija ϕ (sa kodomenom N_0) zadovoljava uslov norme (*N*) $\phi(ab)=(\phi a)(\phi b)$.

Inače, ako je m prirodan broj i B bilo koji od prstena Z, $Z[\sqrt{m}]$ i $K[X]$, pri čemu je K proizvoljno polje i $m\in Z$ ceo broj za koji je prsten $Z[\sqrt{m}]$ euklidski u odnosu na normu, tada prsten $A=B\times..\times B$ (r faktora) zadovoljava uslove *Teoreme 1-4*. Pri tome za $r>1$ prsten A nije domen. S obzirom na *Korolar 1-1*, tvrdjenje iz *Teoreme 1-4* važi i za prstene

oblika B^r, gde je B proizvoljno telo. Bolje od toga, *Teorema 1-4* važi za svaki euklidski (pa dakle i nekomutativan) prsten čiji su regularni elementi inverzibilni. Takav je, na primer, svaki od prstena $A = M_n(K)$, gde je K proizvoljno telo. Dokaz je sličan dokazu *Teorema 1-3* i *1-4*. □

TEOREMA 1-5

Ako prost domen A ima bar jednu euklidsku valuaciju $\phi: A \to W$ koja zadovoljava uslov kancelacije, tada je svaki od prstena $B = M_n(A)$ i euklidski i Γ-euklidski.

DOKAZ. Dokaz teče "paralelno" dokazima *Teorema 1-3* i *1-4*, pri čemu je potrebno posebno obrazložiti one detalje tih dokaza u kojima je korišćen pojam determinante (jer prsten A ne mora biti komutativan). Neka je zato simbolika iz *Teoreme 1-3*. Kako je prsten A prost, on nema pravih (obostranih) ideala. Ako u prstenu A važi $a|b$, tada a deli i sleva i zdesna svaki element ideala $I = (b)$ prstena A, tj. $I \subset aA \cap Aa$. Kako A nema pravih ideala, mora biti $I = O$ ili $I = A$. Otuda sledi da u prstenu A važi $a|b$ ako i samo ako je $a = 0$ ili $a \in U(A)$. To posebno znači da za elementarne delitelje a_s $(1 \leqslant s \leqslant r)$ proizvoljne matrice $M \neq O$ iz A_n mora biti $a_s \in U(A)$ za svako $s < r$. U tom slučaju možemo uzeti $a_s = 1$ $(s < r)$.

Neka je prvo $R_0 \neq O$. Ako je S matrica data sa *(11)*, tada je prema prethodnim zaključcima $a_s = 1$ $(1 \leqslant s < k)$ i $a_k = x \neq 0$. Ako u matrici S poslednjoj vrsti dodamo dodamo njenu i-tu vrstu pomnoženu sa $-u_i$ $(i < k)$, dobijamo matricu $\tilde{S} = E + X$, pri čemu je E jedinična matrica reda $k-1$, a X donje trougaona matrica sa glavnom dijagonalom $[x, 0, .., c]$. Neka su U i V inverzibilne matrice za koje je $UXV = diag[1, .., 1, h, 0, .]$ $(= X_0)$, i neka u X_0 "figuriše" t jedinica (izuzimajući h). Tada je $(E+U)\tilde{S}(E+V) = E + X_0$, pa su $1, .., 1, h$ ($k+t-1$ jedinica) elementarni delitelji matrice $\tilde{S}$ a time i matrice S. Dokažimo da za $c \neq 0$ mora biti $t \geqslant 1$. U suprotnom bi bilo $X_0 = \begin{bmatrix} h & O \\ O & O \end{bmatrix}$, pa bi iz $X = U^{-1} X_0 V^{-1}$ sledilo

$$x = a_{11} h b_{11}, \qquad 0 = a_{11} h b_{1n}, \qquad c = a_{n1} h b_{1n}, \tag{13}$$

pri čemu je $U^{-1} = [a_{ij}]$ i $V^{-1} = [b_{ij}]$. No, kako su x, c, h regularni elementi prstena A, iz druge od jednakosti *(13)* sledi $a_{11} = 0$ ili $b_{1n} = 0$, što se kosi sa preostale dve od jednakosti *(13)*. Dakle je $t \geqslant 1$. Jasno je da

u tom slučaju važi $\psi S = \psi\tilde{S} < \psi R_0$.

Ako je $t = 0$ (a time i $c = 0$), biće $h \| x$, i dakle $AxA \subset hA \cap Ah$. Otuda je $\phi h < \phi x$, a time i $\psi S = \psi\tilde{S} < \psi R_0$. Uz to je $\psi R_0 < \psi B_0$, pa za $b = 0$ važi $\psi R = \psi S < \psi B_0 = \psi B$. Ako je $b \neq 0$, biće $b_s = 1$ $(1 \leqslant s < n)$, pa tada $\psi R_0 < \psi B_0$ povlači $R_0 = 0$. Naime, u suprotnom bi bilo $k = n-1$ i $\phi\tilde{a}_s \leqslant \phi\tilde{b}_s = \phi 1$ za bar jedno $s \leqslant n-1$, a time i $a_s = 0$ za bar jedno $s \leqslant n-1$, što nije moguće.

Neka je sada $R_0 = 0$. Uz simboliku iz odgovarajućeg dela dokaza *Teoreme 1-3*, za $s < p$ važi $d_s = 1$. Neka je prvo $b = 0$. Ako je uz to $u_i = c = 0$ za $i < n$, biće (za $G = 0$) $R = B$, i dakle $M = BQ + B = BQ$. Ako je $c \neq 0$ ili $u_i \neq 0$ za bar jedno $i < n$, tada je matrica T oblika *(11)* sa $c \neq 0$, pa mora biti $p > r$, a time i $\psi R = \psi T < \psi B_0 = \psi B$.

Najzad, neka je $b \neq 0$, i dakle $b_s = 1$ $(1 \leqslant s < n)$. Ako u matrici R (za $G = 0$) poslednjoj vrsti dodamo njenu i-tu vrst pomnoženu sa $-u_i$ $(1 \leqslant i < n)$ dobljamo dijagonalnu matricu $D = diag[1,..,1,c]$, pa za $c \neq 0$ iz $\phi c < \phi b$ sledi $\psi R = \psi D < \psi B$. Slučaj $c = 0$ apsolvira se analogno kao "odgovarajući" slučaj u dokazu *Teoreme 1-3*. Time je dokazano da je prsten A_n euklidski zdesna, a time i sleva.

Dokaz drugog dela tvrdjenja je analogan dokazu *Teoreme 1-4* (samo što se umesto na *Teoremu 1-3* treba pozvati na upravo dokazani deo tvrdjenja). Jedino, zbog eventualne nekomutativnosi datog prstena A, treba posebno dokazati da je matrica $B \in A_n$ sa elementarnim deliteljima b_s $(1 \leqslant s \leqslant r)$ regularna akko je $r = n$ i $b_s \in R(A)$ za svako $s \leqslant n$. Zaista, ako su U i V inverzibilne matrice za koje je $B = UB_0V$ sa $B_0 = diag[b_1,..,b_n]$, biće $BX = 0$ akko je $UB_0VX = 0$, to jest (*) $B_0Y = 0$ sa $Y = VX$. Kako je uz to matrica V inverzibilna, biće $X = 0$ akko je $Y = 0$, pa je data matrica B regularna akko je to slučaj sa matricom B_0. S druge strane, jasno je da je matrica B_0 regularna akko su takvi njeni dijagonalni elementi u prstenu A. Otuda i tvrdjenje u celini. □

Prethodno tvrdjenje važi i u slučaju kada prsten A nije domen ako valuacija ϕ zadovoljava uslov kancelacije na skupu $R(A)$. Jasno je da svako telo A zadovoljava uslove *Teoreme 1-5*. Pri tome uslove drugog dela te teoreme zadovoljava i svaki od prstena $A = M_n(K)$ za proizvoljno telo K (na osnovu *Korolara 1-1*). Naredni *Primer 1-2* pokazuje da postoje euklidski domeni koji nisu tela, a zadovoljavaju uslove *Teoreme 1-5*. □

PRIMER 1-2. *Neka $K=Q(T)$ polje razlomaka nad prstenom $Q[T]$, $f=1_K$ i δ uobičajeno diferenciranje u polju K. Tada je $A=K[X,\delta]$ i levi i desni euklidski domen u odnosu na stepenu valuaciju ∂. Jasno je da valuacija ∂ zadovoljava uslov (K). Dokažimo i da je prsten A prost, a samim tim i da zadovoljava uslove Teoreme 1-5. Pa neka je $I\neq 0$ proizvoljan ideal prstena A i označimo sa*

$$a = X^n b + X^{n-1}c + \cdots + a_0 \qquad (b\neq 0), \tag{14}$$

bilo koji polinom minimalnog stepena koji pripada idealu I. Kako su u prstenu A svi levi i desni ideali glavni, biće $I=aA=Aa$. To posebno znači da za neko $x\in A$ važi (*) $Ta=ax$. Kako je $\partial(Ta)=\partial T+\partial a=n$, iz (*) sledi $x=0$, i dakle $x\in K$. S druge strane, za $u\in K$ je $uX=X+\delta u$, pa indukcijom po m zaključujemo da za $m\in N$ važi

$$uX^m = \Sigma X^{m-s}\binom{m}{s}\delta^s(u) \qquad (0\leqslant s\leqslant m). \tag{15}$$

Kako je $\delta T=1$ i $\delta^s(T)=0$ za $s>1$, za $u=T$ (15) daje $TX^m=X^mT+X^{m-1}m$, pa zamenjujući a iz (14) u (*), izmedju ostalog dobijamo da mora biti

$$Tb = bx, \qquad nb+Tc = cx. \tag{16}$$

Kako je $b\neq 0$, iz $Tb=bx$ sledi $T=x$, pa druga jednakost u (16) daje $nb=0$, a time i $n=0$. Prema (14) to znači da je $a=b\in K$ jednota prstena A, pa je $I=aA=A$. Otuda i tvrdjenje. (Prethodno tvrdjenje ostaje na snazi i ako se polje Q zameni proizvoljnim telom karakteristike 0, a δ bilo kojom spoljnom derivacijom tela K, to jest bilo kojom derivacijom koja nije oblika $u\to au-ua$ $(u\in K)$ za neko fiksirano $a\in K$.) □

Pod *VALUACIONIM* prstenom podrazumevamo svaki prsten A sa svojstvom da za svako $a,b\in A$ važi $a\|b$ v $b\|a$. U svakom valuacionom prstenu levi i desni ideali se podudaraju, i skup $J=A-U(A)$ svih neinverzibilnih elemenata prstena A je jedini njegov maksimalan ideal. Pri tome je J i radikal prstena A, što posebno znači da su svi delitelji 0 valuacionog prstena u njegovom radikalu. Lako se dokaže (*KAPLANSKI* [1]) da je svaki valuacioni prsten A prsten sa elementarnim deliteljima (čak i u odnosu

na hermitski niz $\{A_n\}$, kao i da su elementarni delitelji proizvoljne matrice M nad A odredjeni jednoznačno do na pridruženost. Jedan od bitnih detalja u dokazima *Teorema 1-3* i *1-4* je da za svaku matricu S iz $M_n(A)$ oblika

$$S = \left[\begin{array}{ccc|c} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & 0 \\ \vdots & & & \\ \hline u_1 & u_2 & \cdots & c \end{array}\right], \qquad a_s \| a_{s+1}, \quad (a_s = 0 \text{ za } s>k), \tag{17}$$

i njene elementarne delitelje c_s $(1 \leqslant s \leqslant m)$ važi $m \geqslant k$ i $\phi\tilde{a}_s \geqslant \phi\tilde{c}_s$ $(1 \leqslant s \leqslant k)$. Dokažimo da to važi i za proizvoljan valuacioni prsten A. U tom slučaju je čak $c_s \| a_s$, a time i $\tilde{c}_s \| \tilde{a}_s$ $(1 \leqslant s \leqslant k)$. Zaista, kako je prsten A valuacioni, bar jedan od elemenata matrice S deli sve njene elemente. Označimo sa c_1 bilo koji od njih. Neka je $c_1 = [S]_{ij}$. Jasno je da tada elementarnim transformacijama matricu S možemo transformisati u matricu oblika $T = \begin{bmatrix} c_1 & 0 \\ 0 & S_0 \end{bmatrix}$, pri čemu je S_0 kvadratna matrica reda $n-1$ oblika (17), čija je dijagonala $[a_1,..,a_{j-1},a_{j+1},..,a_{n-1},c_0]$. Uz to c_1 deli sve elemente matrice S_0. Na osnovu toga, tvrdjenje sledi neposredno indukcijom po n, jer su elementarni delitelji matrice T, a time i matrice S, upravo c_1 i elementarni delitelji c_s $(2 \leqslant s \leqslant n)$ matrice S_0.

Sada dokaz *Teoreme 1-3* možemo modifikovati tako da dobijemo dokaz sličnog tvrdjenja za valuacione prstene. Uz to svaka prirodna euklidska valuacija ϕ valuacionog prstena A zadovoljava uslov kancelacije. Zaista, pretpostavimo da za neko $a,b,u,v \in A$, $ubv \neq 0$, važi $\phi(uav) > \phi(ubv)$ sa $\phi a \leqslant \phi b$. Kako je valuacija ϕ prirodna i $a \| b$ v $b \| a$, biće $a \| b$. Otuda je $b = ac$ za neko $c \in A$, a time i (*) $ubv = uavx$, pri čemu je $cv = vx$ (jer se u prstenu A levi i desni ideali podudaraju). S druge strane, iz (*) sledi $\phi(ubv) = \phi(uav \cdot x) \geqslant \phi(uav)$, što je u suprotnosti sa učinjenom pretpostavkom. Otuda i naredna

TEOREMA 1-6

Ako je valuacioni prsten A euklidski (Γ-euklidski), onda je takav i svaki od prstena $M_n(A)$. □

PRIMER 1-3. *Neka je K proizvoljno telo, $f: K \to K$ automorfizam tela K, i*

$A = K[[X,f]]$ prsten desnih formalnih f-redova po X sa koeficijentima u telu K. Svako $a \in A^0$ se može na tačno jedan način pretstaviti u obliku $a = X^m u$, pri čemu je $m = m(a) \geqslant 0$ ceo broj i u jednota prstena A, to jest $u = \Sigma X^s a_s$ $(0 \leqslant s,\ a_0 \neq 0)$. Tada je sa $\phi(a) = m(a)$ $(a \in A^0)$ definisana jedna euklidska valuacija prstena A. Ako su $a = X^m u$ i $b = X^n v$, pri čemu su u i v jednote prstena A, proizvoljni elementi iz A, tada je $a \| b$ ili $b \| a$. Otuda je A i valuacioni prsten (koji za $f \neq 1_K$ nije komutativan), i prema tome zadovoljava uslove Teoreme 1-6. □

Ako su svi delitelji nule euklidskog prstena A u njegovom radikalu $J(A)$, tada je domen ili valuacioni prsten (o čemu je već bilo reči). Ako je uz to prsten A komutativan i sa bar jednom euklidskom valuacijom koja zadovoljava uslov *(K)* na skupu $R(A)$, tada je svaki od prstena A_n i euklidski i Γ-euklidski (*Teoreme 1-3* i *1-6*). Naredna teorema pokazuje da važi i znatno opštije tvrdjenje.

TEOREMA 1-7

Ako komutativan prsten A ima bar jednu euklidsku valuaciju ϕ koja zadovoljava uslov kancelacije, tada je za svako $n \in N$ prsten $M_n(A)$ i euklidski i Γ-euklidski.

DOKAZ. Pre svega, za proizvoljne prstene *G* i *H* i svaki prirodan broj *n* prsteni $M_n(G \times H)$ i $M_n(G) \times M_n(H)$ su izomorfni. Kako prsten A zadovoljava uslove iz *III*, *Teorema 2-8*, biće

$$A = (G_1 \times \cdots \times G_r) \times (H_1 \times \cdots \times H_s), \tag{18}$$

pri čemu je svaki od G_i-ova euklidski domen, dok je svaki od prstena H_j specijalan, a time i valuacioni euklidski prsten. Uz to restrikcija ϕ_i od ϕ na G_i takodje zadovoljava uslov *(K)*, pa je prema *Teoremama 1-3* i *1-6* svaki od prstena $M_n(G_i)$ i $M_n(H_j)$ i euklidski i Γ-euklidski. Kako iz (*18*) sledi

$$M_n(A) \simeq M_n(G_1) \times \cdots \times M_n(H_s), \tag{19}$$

prema *III*, *Teorema 2-8*, biće i prsten A_n i euklidski i Γ-euklidski. □

Primer 1-2 pokazuje da postoje i nekomutativni domeni za koje važi tvrdjenje iz *Teorema 1-3*. Dokazaćemo da je prsten $M_n(A)$ I-euklidski za svaki domen A koji ima bar jednu konačnu euklidsku valuaciju koja zadovoljava uslov *(N)* ili uslov *(K)*. Pri tome je za $n=1,2$ prsten $M_n(A)$ i euklidski. Ostaje otvoren problem "euklidnosti" prstena $M_n(A)$ za svaki prirodan broj n (u slučaju proizvoljnog euklidskog domena A).

Pri dokazu najavljenog tvrdjenja koristićemo pojam *DETERMINANTE* kvadratne matrice nad proizvoljnim telom u smislu *DIEUDONNE*[1]. Naime, ako je K telo, tada je $R(K_n)=U(K_n)$ podgrupa multiplikativne polugrupe $K_n=M_n(K)$. Označimo sa C i C_n redom *komutante* grupa K^0 i $U(K_n)$, to jest podgrupe grupa K^0 i $U(K_n)$ što ih generišu njihovi *komutatori*. Tada su C i C_n najmanje invarijantne podgrupe od K^0 i $U(K_n)$ za koje su količničke grupe K^0/C i $U(K_n)/C_n$ komutativne. Grupa $U(K_n)/C_n$ je izomorfna grupi K^0/C za svaki prirodan broj n (*DIEUDONNE*[1]). Sa K/C označavaćemo skup svih "koseta" $\tilde{a}=aC$ $(a\in K)$, uz dogovor da za svako $a\in K$ važi $aC\cdot 0C=0C$. Ako je K polje, tada je $K/C\cong K$.

U *DIEUDONNE*[1] *determinanta* nad telom K je definisana kao jedno preslikavanje $det: M(K)\to K/C$ skupa $M(K)$ svih kvadratnih matrica nad K u skup K/C (koja se u slučaju polja podudara sa uobičajenim pojmom determinante). Osnovna svojstva preslikavanja det (koja to preslikavanje i karakterišu) data su sa:

(α) Ako je $[a,0,..,0]$ prva kolona i S komatrica polja $(1,1)$ matrice M iz K_n, tada je $detM=\tilde{a}\cdot detS$. Pri tome je $det[a]=aC$.

(β) Ako se nekoj vrsti (koloni) matrice M doda neka druga vrste (kolona) te matrice pomnožena sleva (zdesna) bilo kojim elementom a iz K, za dobijenu matricu S važi $detS=detM$.

(γ) Ako je S matrica koja nastaje iz matrice M množeći neku njenu vrstu (kolonu) sleva (zdesna) elementom $a\in K$, tada je $detS=\tilde{a}\cdot detM$.

(δ) Ako se u matrici M dvema vrstama (kolonama) zamene mesta, za dobijenu matricu S važi $detS=-\tilde{1}\cdot detM$, gde je $-\tilde{1}=-1C$.

(τ) Za svaku matricu M iz $M_n(K)$ važi $det(M)=det(M^T)$.

(θ) Za svake dve matrice P,Q iz A_n važi $det(PQ)=det(P)\cdot det(Q)$.

Posebno je važno svojstvo (θ). Inače, svojstva (α)-(δ) omogućuje da se i eksplicitno odredi $det(M)$ za proizvoljnu matricu M iz $M(K)$. Ako je a proizvod dijagonalnih elemenata trougaone matrice T, tada je $detT = \tilde{a}$.

TEOREMA 1-8

Ako domen A ima bar jednu euklidsku valuaciju $\phi: A \to N_0$ koja zadovoljava uslov (N) $\phi(ab) = (\phi a)(\phi b)$, tada je svaki od prstena $M_n(A)$ Γ-euklidski. Tu se uslov (N) može zameniti i uslovom (M).

DOKAZ. Domen A ima prsten razlomaka K i preslikavanje $a \to a/1$ $(a \in A)$ je monomorfizam prstena A u telo K. Uz to je A_n potprsten prstena K_n. Neka su $u = a/x$ i $v = b/y$ proizvoljni elementi iz K. Tada je $u = v$ akko je $ac = bd$ i $xc = yd$ za neko $c, d \in A$. Valuacija ϕ zadovoljava uslov norme pa iz $u = v$ sledi $(\phi a)(\phi c) = (\phi b)(\phi d)$, $(\phi x)(\phi c) = (\phi y)(\phi d)$, i prema tome $(\phi a)/(\phi x) = (\phi b)/(\phi y)$. Otuda je sa

$$\tilde{\phi}(a/x) = (\phi a)/(\phi x) \qquad (a \in A,\ x \in A^0) \tag{20}$$

dobro definisano jedno preslikavanje $\tilde{\phi}: K \to Q$ tela K u skup Q racionalnih brojeva. Domen A zadovoljava desni *Oreov* uslov, pa za neko c, d iz A^0 važi $xc = bd$, i dakle $uv = (ac)/(bd)$, kao i $(\phi x)(\phi c) = (\phi b)(\phi d)$, što zajedno sa *(20)* daje (jer je množenje u Q komutativno)

$$\tilde{\phi}(uv) = (\tilde{\phi}u)(\tilde{\phi}v) \qquad (u, v \in K). \tag{21}$$

To znači da i preslikavanje $\tilde{\phi}$ zadovoljava uslov norme. Jasno je da za svako $a \in K^0$ važi $\tilde{\phi}a^{-1} = 1/(\tilde{\phi}a)$, a time i $\tilde{\phi}(c) = 1$ za svaki komutator c grupe K^0. Kako je svaki element a komutanta C grupe K^0 proizvod konačno mnogo njenih komutatora, na osnovu prethodnog i *(21)* biće $\tilde{\phi}(a) = 1$ za svako $a \in C$. Otuda, ako je $aC = bC$, biće $b^{-1}a \in C$, i dakle $\tilde{\phi}a = \tilde{\phi}b$. Prema tome, za svako $a, b \in K$ važi

$$aC = bC \quad \Leftrightarrow \quad \tilde{\phi}a = \tilde{\phi}b. \tag{22}$$

Ako je, uz prethodnu simboliku, $detM = aC$ determinanta matrice M nad telom K (u smislu *DIEUDONNE* [1]), tada na osnovu (22) zaključujemo da je sa (*) $\tilde{\psi}(M) = \tilde{\phi}(a)$ $(M \in K_n,\ detM = aC)$ dobro definisano jedno presli-

kavanje $\tilde{\psi}: K_n \to Q$ prstena K_n u skup Q racionalnih brojeva. Dokazaćemo da je restrikcija ψ od $\tilde{\psi}$ na skupu A_n, tj. preslikavanje ψ skupa A_n dato sa

$$\psi(M) = \phi(a) \qquad (M \in A_n,\ \det M = aC) \tag{23}$$

jedna Γ-euklidska valuacija prstena A_n, sa kodomenom N_0. Dokažimo prvo da ψM pripada skupu N_0 za svaku matricu M iz A_n. Neka su a_s $(1 \leqslant s \leqslant r)$ elementarni delitelji matrice M i stavimo $\tilde{M} = diag\,[a_1, a_2, ..]$. Na osnovu *Teoreme 1-2* matrica $\tilde{M}$ se može dobiti iz matrice M primenom elementarnih transformacija "tipa" (β)-(δ). Kako su M i $\tilde{M}$ matrice i nad telom K, biće $\det(M) = e^k \cdot \det(\tilde{M})$, pri čemu je $e = -1C$ koset podgrupe C koji sadrži -1, a k izvestan prirodan broj. Za $r < n$ je $\det(\tilde{M}) = 0$, a time i $\det M = 0$. Ako je $r = n$ i $a = a_1 \cdot\cdot a_n$, tada je $a \in A$ i $\det M = aC$. Otuda je

$$\psi(M) = \tilde{\phi}(e^k a) = \tilde{\phi}(e^k)\tilde{\phi}(a) = \phi(a), \tag{24}$$

jer valuacija $\tilde{\phi}$ zadovoljava uslov norme, i, naravno, $\tilde{\phi}(e) = 1$. No, kako je $a \in A$, zajedno sa ϕa biće i ψM nenegativan ceo broj. Dalje, za proizvoljne matrice $P, Q \in A_n$ stavimo $\det P = aC$ i $\det Q = bC$. U tom slučaju je $\det(PQ) = \det P \cdot \det Q = aC \cdot bC = abC$, i dakle

$$\psi(PQ) = \tilde{\phi}(ab) = (\tilde{\phi}a)(\tilde{\phi}b) = \psi(P)\psi(Q), \tag{25}$$

pa i valuacija ψ zadovoljava uslov norme. Posebno, ako je $PQ = E$, biće $(\psi P)(\psi Q) = 1$, što sa $\psi P, \psi Q \in N_0$ daje $\psi P = \psi Q = 1$. Drugim rečima, za svaku inverzibilnu matricu $P \in A_n$ važi $\psi P = 1$.

Neka su b_s $(1 \leqslant s \leqslant k)$ elementarni delitelji matrice $B \in A_n$. Matrica B je regularna akko je $k = n$ i $b_s \in R(A)$ za svako $s \leqslant n$. S druge strane, svaki regularan element prstena A ima inverz u telu K. Otuda regularna matrica $\tilde{B} = diag[b_1, .., b_n]$ iz A_n ima inverz $\hat{D} = diag[1/b_1, .., 1/b_n]$ u prstenu K_n. Ako su S i T inverzibilne matrice iz A_n za koje je $SBT = \tilde{B}$, tada za matricu $D = T\hat{D}S$ važi $BD = DB = E$. Prema tome, matrica $B \in A_n$ je regularna u prstenu $M_n(A)$ akko je inverzibilna u prstenu $M_n(K)$.

Dokažimo sada da za svaku matricu $M \in A_n$ i svaku regularnu matricu $B \in R(A_n)$ postoje matrice $Q \in A_n$ i $R \in R_0(A_n)$ za koje je $M = BQ + R$, $\psi R < \psi B$. Zaista, kako je prsten A hermitski zdesna, postoje inverzibilne matrice

U i V iz A_n za koje su matrice MU i BV donje trougaone. Iz regularnosti matrice BV u prstenu A_n sledi njena invertibilnost u prstenu K_n. Uz to je i matrica $(BV)^{-1} = V^{-1}B^{-1}$ donje trougaona u prstenu K_n. Kako je proizvod donje trougaonih matrica takodje donje trougaona matrica, biće i matrica (*) $F = V^{-1}B^{-1}.MU$ donje trougaona, to jest

$$F = \begin{bmatrix} a_{11} & 0 & \cdot\cdot & 0 \\ a_{21} & a_{22} & & 0 \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdot\cdot & a_{nn} \end{bmatrix} \tag{26}$$

za neke a_{ij}-ove iz K. Ako je $F \in A_n$, tada iz (*) za $Q = VFU^{-1} \in A_n$ sledi $M = BQ$, i stvar je gotova. Zato pretpostavimo da F nije u A_n, to jest da bar jedan od a_{ij}-ova ne pripada prstenu A. Stavimo (**) $a_{ij} = u_{ij}/b_{ij}$ sa $u_{ij}, b_{ij} \in A$. Kako je valuacija ϕ euklidska i sleva i zdesna, postoje c_{ij}-ovi i r_{ij}-ovi iz A takvi da je: $u_{ij} = c_{ij}b_{ij} + r_{ij}$, $\phi r_{ij} < \phi b_{ij}$, pa iz (**) sledi

$$u_{ij} = c_{ij} + v_{ij}, \qquad v_{ij} = r_{ij}/b_{ij}, \tag{27}$$

pri čemu je $\tilde{\phi} v_{ij} = (\phi r_{ij})/(\phi b_{ij}) < 1$. Neka je m najmanji i k najveći indeks za koje je $v_{mk} \neq 0$. Jasno je da mora biti $m > k$. Neka je $G = [g_{ij}]$ matrica iz A_n koja je za $m = k$ data sa

$$g_{ij} = \begin{cases} c_{ii} - 1 & \text{za } i=j,\ v_{ii}=0, \\ c_{ij} & \text{u svim preostalim slučajevima,} \end{cases} \tag{28}$$

a za $m > k$ sa: $g_{kk} = c_{kk}$, $g_{km} = 1$, i sa (28) u svim preostalim slučajevima. Dokažimo da tada za matricu $H = F - G$ važi $\tilde{\psi}(H) < 1$. Označimo sa $\tilde{H}$ matricu koja se u slučaju $m=k$ podudara sa matricom H, a u slučaju $m > k$ nastaje iz matrice H dodajući njenoj k-toj vrsti njenu m-tu vrstu. Tada se neposredno proverava je matrica $\tilde{H}$ donje trougaona (jer za $m > k$ važi $[H]_{kk} = 0$, $[H]_{km} = -1$, $[H]_{mm} = 1$). Uz to, ako je $[h_1, \ldots, h_n]$ njena dijagonala, tada je $h_k = v_{mk}$, dok za $i \neq k$ važi $h_i \in \{1, v_{ii}\}$. To posebno znači da je $\phi(h_k) < 1$, $\phi(h_i) \leq 1$ $(i \neq k)$. Stavimo $h = h_1 \cdot\cdot h_n$. Kako $\tilde{\phi}$ zadovoljava uslov norme, na osnovu prethodnog imamo: $\tilde{\phi}(h) = (\tilde{\phi}h_1) \cdot\cdot (\tilde{\phi}h_n) < 1$. No, s druge strane jasno je da važi $det(H) = det(\tilde{H}) = hC$, pa na osnovu (24) dobijamo $\tilde{\psi}(H) = \tilde{\phi}(h) < 1$.

Množeći jednakost (*) sleva matricom BV, a zdesna matricom U^{-1}, i zamenjujući F sa $G+H$, dobijamo $M = BQ+R$, gde je $Q = VGU^{-1}$, $R = BVHU^{-1}$. Kako su V, G, U^{-1} matrice iz prstena A_n, biće to slučaj i sa matricom Q. Sada su M, B, Q matrice iz A_n, pa je to slučaj i sa matricom $R = M-BQ$. Uz to je $\bar{\psi}V = \bar{\psi}U = 1$, pa na osnovu prethodnog zaključka imamo da je

$$(29) \qquad \psi(R) = \psi(BVHU^{-1}) = (\psi B)(\psi V)(\psi H)(\psi U)^{-1} < \psi(B)$$

(jer i ψ zadovoljava uslov norme). Otuda je i $\psi R < \psi B$. Najzad, kako je matrica H regularna, biće takva i matrica R (kao "prolzvod" regularnih matrica), pa je $M = BQ+R$, $\psi R < \psi B$, sa $Q \in A_n$ i $R \in R_0(A_n)$. Otuda i samo tvrdjenje u slučaju kada ϕ zadovoljava uslov (N). Drugi deo tvrdjenja se svodi na prethodni slučaj, jer svaki domen koji ima euklidsku valuaciju koja zadovoljava uslov (M), ima i bar jednu euklidsku valuaciju koja zadovoljava uslov norme. □

TEOREMA 1-9

Ako domen A ima bar jednu euklidsku valuaciju ϕ koja zadovoljava uslova (M) $\phi(a+b) \leqslant \max(\phi a, \phi b)$, tada je prsten $M_2(A)$ euklidski.

DOKAZ. Svaki takav domen je oblika $K[X, f, \delta]$, pri čemu je K izvesno telo, a f i δ redom automorfizam i desno f-diferenciranje tela K (jer je valuacija ϕ euklidska i sleva i zdesna). Neka je ∂ odgovarajuća stepena valuacija. Tada, prema *V, Primer 1-1*, za slične elemente a, b u prstenu A važi $\partial a = \partial b$. Na osnovu toga možemo govoriti o valuaciji $\psi: M_0(A) \to W$ o kojoj je reč u *Teoremi 1-3* (za $\phi = \partial$ i $n=2$) i u slučaju kada prsten A nije komutativan. Neka je zato simbolika iz *Teoreme 1-3* za $\phi = \partial$ i $n=2$. Dokazaćemo da je ψ euklidska valuacija prstena $M_2(A)$.

Ako je B regularna matrica iz A_2, tada prema *Teoremi 1-8* za svaku matricu $M \in A_2$ postoje matrice $Q \in A_2$ i $R \in R_0(A_2)$ za koje je $M = BQ+R$ sa $\psi R < \psi B$. Pretpostavimo zato da matrica B nije regularna. U tom slučaju matrica $B \neq O$ ima tačno jedan elementarni delitelj, na primer b. Slično kao pri dokazu *Teoreme 1-3* zaključujemo da je dovoljno dokazati da za svaku donje trougaonu matricu $M = \begin{bmatrix} a & 0 \\ u & c \end{bmatrix}$ i svaku matricu $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$ $(b \neq 0)$ postoje matrice $Q, R \in A_2$ za koje je $M = BQ+R$, $\psi R < \psi B$. U tu svrhu

stavimo $Q = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$, i dakle $R = \begin{bmatrix} a-bp & -bq \\ u & c \end{bmatrix}$. Slučaj $b=c=0$ se lako apsolvira. Ako je $c \neq 0$ izaberimo p tako da bude $a-bp \neq 0$ (što je moguće zbog $b \neq 0$). Tada je za $q=0$ matrica R regularna, pa ima dva elementarna delitelja. Kako matrica B ima jedan elementarni delitelj, biće $\psi R < \psi B$. Najzad, ako je $c=0$ i $u \neq 0$, tada je za $q=1$ matrica R regularna, pa je opet $\psi R < \psi B$. Otuda i tvrdjenje. □

TEOREMA 1-10

Ako domen A nije telo, tada za $n>1$ prsten $A_n = M_n(A)$ nema nijednu konačnu euklidsku valuaciju.

DOKAZ. Dovoljno je dokazati da tvrdjenje važi za $n=1$. Ako prsten $M_2(A)$ ima bar jednu euklidsku valuaciju, neka je ψ minimalna medju njima, sa $\psi(A_2) = W$. Dokazaćemo da valuacija ψ nije konačna.

Neka je $a \neq 0$ bilo koji element domena A koji nije inverzibilan i stavimo $M = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$ i $F = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Kako matrica M nije inverzibilna u prstenu A_2, prema *I, Lema 1-1* niz (ψM^n) $(n \in N)$ strogo raste. To posebno znači da za svako $k \in W$, $k < \omega$, postoji regularna matrica $G = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}$ za koju je $\psi G > k$ (na primer, $G = M^n$ za dovoljno veliko n). Pretpostavimo da da je $\psi F = m < \omega$. Ako je $B \neq O$ singularna matrica iz $M_2(A)$, tada za neke inverzibilne matrice U,V važi $UBV = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = F \cdot bE$ sa $b \in R(A)$. Kako je valuacija ψ prirodna i matrica bE regularna, iz $B = U^{-1}F(bE)V^{-1}$ sledi $\psi B > \psi F$. Kako to važi za svaku singularnu matricu $B \neq O$, zaključujemo da euklidski razred stepena $< m$ prstena A_2 ne sadrži nijednu singularnu matricu. To znači da postoje matrice $Q \in A_2$ i R iz $R_0(A_2)$ takve da važi $G = FQ+R$, $\psi R < \psi F$, a time i $R = \begin{bmatrix} 1-p & -q \\ 0 & c \end{bmatrix}$ za neko $p,q \in A$. Kako je $c \neq 0$ biće $R \neq O$, pa je matrica R regularna. Otuda je i $1-p \neq 0$. Označimo sa S matricu koja nastaje iz G zamenjujući c sa 1. Tada je $R = GS$, i dakle $\psi R > \psi G$, a time i $m > k$. Kako tu k može biti proizvoljan prirodan broj, mora biti $\psi F = m > \omega$, pa valuacija ψ nije konačna. Jasno je da to onda ne može biti ni neka druga euklidska valuacija prstena A_2. Napomenimo još da slično tvrdjenje ne važi i za Γ-euklidske valuacije prstena A_2.

LITERATURA

AMITSUR, A. S.

[1] On unique factorization in rings. *Riveon Lematema. 2 (1948) 28-29*

[2] Remarks on principal ideal rings. *Osaka Math. J. 15 (1963) 59-69*

BOURBAKI N.

[1] "Algebre I, chap. 1-3", *Hermann, Paris, 1970.*

[2] "Algebre". *Ch 4-5 Ch 6-7 Hermann Paris 1973*

BUCUR, I., DELEANU, A.

[1] Introduction to the Theory of Categories and Functors. *New York/London/Sydney, 1968.*

COHN, P. M.

[1] On a generalization of the Euclidean algorithm. *Proc. Comb. Phil. Soc. 57 (1961) 18-30*

[2] Rings with a weak algorithm. *Trans. Amer. Math. Soc. 109 (1963).*

[3] Rings with a transfinite weak algorithm. *Bull. London Math. Soc. 1 (1969) 55-59.*

[4] Some remarks on the invariant basis property. *Topology 5 (1966), 215-228.*

[5] A remark on matrix rings over free ideal rings. *Proc. Camb. Phil. Soc. 62 (1966) 1-4.*

[6] Noncomutative unique factorization domains. *Trans. Amer. Mathem. Soc. 109 (1963) 313-332.*

[7] Rings of fractions. *Amer. Math. Monthly 78 (1971) 596-615.*

[8] "Universal Algebra", *New York, 1965.*

[9] "Free Rings and Their Relations", *New York, Academic Press, 1971.*

[10] "Algebra I, II", *London, 1977.*

[11] "Skew Field Constructions", *Cambridge University Press LNS, 1977.*

[12] Equations dans les corps gauches. *Bull. Soc. Math. Belg. 201-223.*

CURTIS, C. W.

[1] A note on non-commutative polynomial rings. *Proc. Amer. Math. Soc. 3 (1952) 965-969.*

DIEUDONNE J.

[1] Les determinants sur un corps non commutatif. *Bull. Soc. Mathem. France 71 (1943) 27-45.*

[2] "La geometrie des groupes classiques", *Springer-Verlag 1971.*

ELIZAROV, V. P.

[1] Rings of fractions. *Algebra i Logika, 8, No.4 (1969) 381-424.*

GABRIEL, P.

[1] Des catégories abeliennes. *Bull. Soc. Math. Fr. 90 (1962) 323-448.*

GOLDIE, A. W.

[1] The structure of prime rings under ascending chain conditions . *Proc. London Math. Soc. (3), 8 (1958) 589-608.*

[2] Semi-prime rings with maximum condition. *Proc. London Math. Soc. (3) 10 (1960) 201-220.*

[3] Non-commutative Principal Ideal Rings. *Archiv. Mathem. 13 (1962) 213-221.*

[4] Localization in non-commutative Noetherian rings. *J. Alg. 5 (1969)*

JACOBSON, N.

[1] A note on non-commutative polynomials. *Ann. Math. 35 (1934) 209-210*

[2] Some remarks on one-sided inverses. *Proc Amer. Math. Soc. (1950) 1, 352-355.*

[3] "Theory of Rings", *Providence, 1943.*

[4] "Structure of Rings", *Providence, 1964.*

JATEGAONKAR, A. V.

[1] A counter-example in homological algebra and ring theory. *J. Alg. 12 (1969) 418-440.*

[2] Left principal ideal domains. *J. Algebra, 8 (1968) 148-155.*

KALAJDŽIĆ, G.

[1] A representation of a class of euclidean rings. *Mat. Balkanika, 4 (1974) 313-316.*

[2] On Euclideans classes and kernel of module. *(U pripremi za štampu).*

[3] Matrices sur anneaux euclidiens. *Matematica Balkanika, 10, 1981.*
[4] On Euclideans valuations with some particular properties. *(Ibid).*

KAPLANSKY, I.

[1] Elementary divisors and modules. *Trans. Am. Math. Soc. 66 (1949), 464-491.*
[2] "Commutative rings", *Boston, 1970.*
[3] "Rings of operators", *New York, 1968.*
[4] "Linear Algebra and Geometry", *New York, 1974.*

KUREPA, DJ.

[1] On triangular matrices. *Glas. Mat. Fiz. II, 20 (1965), 1-22.*
[2] Une généralisation des matrices. *C. R. Acad. Sci. Paris 239 (1954) 19-20.*
[3] On a definition and notation of matrices. On a kind of switch matrices. *Vesnik Društva Mat. Fiz. N.R.Srbije 4 (1952), 1-7.*
[4] "Viša algebra I, I", *Beograd, 1979.*
[5] "Teorija skupova", *Zagreb 1951.*

LAFON, J-P.

[1] L'algebre commutative, *Hermann, Paris, 1974.*

MOTZKIN, T. S.

[1] The euclidean algorithm. *Bull. Amer. Math. Soc. 55 (1949) 1142-46.*

MALCEV, A. I.

[1] On the immersion of an algebraic ring into a field. *Math. Ann. 113 686-691 (1936).*

NAKAYAMA, T.

[1] A note on the elementary divisor theory in noncommutative domains. *Bull. Amer. Math. Soc. 44 (1938), 719-723.*

ORE, O.

[1] Theory of non-commutative polynomials. *Ann. Math. 34 (1933) 480-508.*
[2] Linear equations in non-commutative fields. *Ann. Math. 32 (1931) 463-477.*

SAMUEL, P.

[1] About euclidean rings. *J. of Algebra 19 (1971), 262-301.*

[2] Unique factorization. *Amer. Math. Monthly, 75 (1968), 945-952.*

[3] Théorie algébrique des nombres. *Hermann, Paris, 1967.*

[4] Commutative Algebra I, II (sa O. ZARISKI), *Princeton, 1958.*

SANOV, I. N.

[1] Euclidean algorithm and one-sided prime factorization for matrix rings. *Sibirsk. Mat. Ž. 8 (1967), 846-852.*

SMITS, T. H. M.

[1] Nilpotent *S*-derivations. *Indag. Math. 30 (1968), 72-86.*

[2] Skew polynomial rings. *Indag. Math. 30 (1968), 209-224*

TEICHMULLER, O.

[1] Der Elementarteilersatz fur nichtkommutative Ringe. *S-B. Preuss. Akad. Wiss. (1937), 169-177.*