2. SZÁMTESTEK ÉS AZOK BŐVÍTÉSEI

2.A.Definíció. A komplex számok $R \subseteq \mathbb{C}$ részhalmazáról azt mondjuk, hogy **számgyűrű** (vagy azt, hogy **részgyűrűje $\mathbb{C}$-nek**), ha $1 \in R$ és R zárt az összeadásra, kivonásra és a szorzásra nézve: $r_1, r_2 \in R$ esetén $r_1 + r_2 \in R$, $r_1 - r_2 \in R$ és $r_1 r_2 \in R$.
A komplex számok $K \subseteq \mathbb{C}$ részhalmazáról azt mondjuk, hogy **számtest** (vagy azt, hogy **résztest $\mathbb{C}$-ben**), ha K számgyűrű és nem zéró K-beli szám reciproka is K-beli: $0 \neq u \in K$ esetén $u^{-1} = \frac{1}{u} \in K$. Tehát $1 \in K$ és az $u_1, u_2 \in K$ valamint az $0 \neq u \in K$ számokra

$$u_1 + u_2 \in K \ , \ u_1 - u_2 \in K \ , \ u_1 u_2 \in K \text{ és } u^{-1} = \frac{1}{u} \in K.$$

Ha a $K \subseteq \mathbb{C}$ és $L \subseteq \mathbb{C}$ számtestekre a $K \subseteq L$ tartalmazás teljesül, akkor a $K \subseteq L$ **testbővítésről** beszélünk.♡

Tetszőleges $R \subseteq \mathbb{C}$ számgyűrűre abból, hogy $1 \in R$ és abból, hogy R zárt az összeadásra és a kivonásra azt kapjuk, hogy R tartalmazza az egész számokat: $\mathbb{Z} \subseteq R$. Ha $K \subseteq \mathbb{C}$ számtest, akkor K zárt az osztásra nézve is (0-val nem osztunk!), hiszen $u_1, u_2 \in K$ és $u_2 \neq 0$ esetén az u_1-nek és a szintén K-beli $u_2^{-1} = \frac{1}{u_2}$-nek a szorzata is K-beli: $\frac{u_1}{u_2} = u_1 u_2^{-1} \in K$. Mivel $\mathbb{Z} \subseteq K$, ezért az osztásra való zártság miatt $\mathbb{Q} \subseteq K$ is teljesül.

2.1.Állítás. *Ha a $K_\lambda \subseteq C$ számtestek a $\Lambda \neq \varnothing$ halmaz elemeivel vannak indexelve, akkor ezeknek a $\bigcap_{\lambda \in \Lambda} K_\lambda$ halmazelméleti metszete is számtest.*
Másképpen fogalmazva: ha $\mathcal{K} \neq \varnothing$ egy tetszőleges olyan halmaz, amelynek elemei számtestek, akkor a $\mathcal{K}$-beli számtestek $\bigcap_{K \in \mathcal{K}} K$ halmazelméleti metszete is számtest.

Bizonyítás. Az első megfogalmazásban a

$$\bigcap_{\lambda \in \Lambda} K_\lambda = \{u \mid u \in K_\lambda \text{ minden } \lambda \in \Lambda \text{ indexre}\}$$

és a második megfogalmazásban a

$$\bigcap_{K \in \mathcal{K}} K = \{u \mid u \in K \text{ minden } K \in \mathcal{K} \text{ elemre}\}$$

halmazról könnyen belátható, hogy teljesíti a 2.A.Definícióban a számtestre megkövetelt tulajdonságokat.

□□□

2.B.Definíció. Egy $K \subseteq \mathbb{C}$ számtest és egy tetszőleges $\varnothing \neq \Gamma \subseteq \mathbb{C}$ részhalmaz esetén **K-nak Γ-val való bővítésén** a K és Γ mindegyikét részhalmazként tartalmazó $L \subseteq \mathbb{C}$ számtestek metszetét értjük (a $\mathbb{C}$ egyike azoknak a számtesteknek, amelyek tartalmazzák K-t is és Γ-t is):

$$K(\Gamma) = \bigcap_{\substack{K \cup \Gamma \subseteq L \subseteq \mathbb{C} \\ L \text{ számtest}}} L,$$

amely a 2.1.Állítás szerint maga is számtest. Nyilvánvaló, hogy $K(\Gamma)$ a „legszűkebb" olyan számtest, amely a K számtestet is és a Γ halmazt is tartalmazza. Amennyiben $\Gamma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ véges, akkor $K(\{\alpha_1, \alpha_2, ..., \alpha_n\})$ helyett az egyszerűbb $K(\alpha_1, \alpha_2, ..., \alpha_n)$ jelölést alkalmazzuk.

Ha $T_1 \subseteq \mathbb{C}$ és $T_2 \subseteq \mathbb{C}$ számtestek, akkor jelölje $T_1 \vee T_2$ a $T_1 \cup T_2$ halmazelméleti uniót tartalmazó számtestek metszetét, ekkor:

$$T_1 \vee T_2 = \bigcap_{\substack{T_1 \cup T_2 \subseteq L \subseteq \mathbb{C} \\ L \text{ számtest}}} L = T_1(T_2) = T_2(T_1)$$

A $T_1 \vee T_2$ számtestet nevezzük a T_1 és T_2 **számtestek szuprémumának** (vagy **kompozitumának**).♡

Egy $K \subseteq \mathbb{C}$ számtestre és a $\Gamma_1, \Gamma_2 \subseteq \mathbb{C}$ részhalmazokra

$$(K(\Gamma_1))(\Gamma_2) = (K(\Gamma_2))(\Gamma_1) = K(\Gamma_1 \cup \Gamma_2) = K(\Gamma_1) \vee K(\Gamma_2),$$

$K(\Gamma_1 \cap \Gamma_2) \subseteq K(\Gamma_1) \cap K(\Gamma_2)$, de általában $K(\Gamma_1 \cap \Gamma_2) \neq K(\Gamma_1) \cap K(\Gamma_2)$.

2.2.Állítás. *A $T_1 \subseteq \mathbb{C}$ és $T_2 \subseteq \mathbb{C}$ számtestek $T_1 \vee T_2$ szuprémumának bármely eleme az*

$$\frac{a_1b_1 + a_2b_2 + ... + a_nb_n}{c_1d_1 + c_2d_2 + ... + c_md_m}$$

alakban írható, ahol $c_1d_1 + c_2d_2 + ... + c_md_m \neq 0$ és $a_i, c_j \in T_1$ valamint $b_i, d_j \in T_2$ az $1 \leq i \leq n$ és $1 \leq j \leq m$ egészekre.

Bizonyítás. A bizonyítás során végig megköveteljük, hogy a felírt törtek nevezője nem zéró. Mivel az $a_k, c_l \in T_1$ és $b_k, d_l \in T_2$ ($1 \leq k \leq n$, $1 \leq l \leq m$) számok mindegyike $T_1 \cup T_2$-ben található és $T_1 \vee T_2$ olyan számtest, amelyre $T_1 \cup T_2 \subseteq T_1 \vee T_2$, ezért

$$\frac{a_1b_1 + a_2b_2 + ... + a_nb_n}{c_1d_1 + c_2d_2 + ... + c_md_m} \in T_1 \vee T_2.$$

Már csak annyit kell igazolni, hogy a

$$T = \left\{ \frac{a_1b_1 + a_2b_2 + ... + a_nb_n}{c_1d_1 + c_2d_2 + ... + c_md_m} \mid a_k, c_l \in T_1 \text{ és } b_k, d_l \in T_2 \text{ a } 1 \leq k \leq n \text{ , } 1 \leq l \leq m \text{ egészekre} \right\}$$

halmaz zárt az összeadásra, kivonásra, szorzásra és a reciprok képzésére nézve (ekkor ugyanis T egy olyan számtest, amelyre $T_1 \cup T_2 \subseteq T$ miatt $T_1 \vee T_2 \subseteq T$ is teljesülni fog). Most csak annyit igazolunk, hogy két T-beli szám összege T-ben van (T-nek a többi műveletre való zártsága és $T_1 \cup T_2 \subseteq T$ szintén egyszerűen látható):

$$\frac{a_1b_1 + a_2b_2 + ... + a_nb_n}{c_1d_1 + c_2d_2 + ... + c_md_m} + \frac{a'_1b'_1 + a'_2b'_2 + ... + a'_pb'_p}{c'_1d'_1 + c'_2d'_2 + ... + c'_qd'_q} =$$

$$= \frac{(a_1b_1 + a_2b_2 + ... + a_nb_n)(c'_1d'_1 + c'_2d'_2 + ... + c'_qd'_q) + (a'_1b'_1 + a'_2b'_2 + ... + a'_pb'_p)(c_1d_1 + c_2d_2 + ... + c_md_m)}{(c_1d_1 + c_2d_2 + ... + c_md_m)(c'_1d'_1 + c'_2d'_2 + ... + c'_qd'_q)} =$$

$$= \frac{\sum\limits_{\substack{1 \leq k \leq n \\ 1 \leq s \leq q}} (a_kb_k)(c'_sd'_s) + \sum\limits_{\substack{1 \leq r \leq p \\ 1 \leq l \leq m}} (a'_rb'_r)(c_ld_l)}{\sum\limits_{\substack{1 \leq l \leq m \\ 1 \leq s \leq q}} (c_ld_l)(c'_sd'_s)} = \frac{\sum\limits_{\substack{1 \leq k \leq n \\ 1 \leq s \leq q}} (a_kc'_s)(b_kd'_s) + \sum\limits_{\substack{1 \leq r \leq p \\ 1 \leq l \leq m}} (a'_rc_l)(b'_rd_l)}{\sum\limits_{\substack{1 \leq l \leq m \\ 1 \leq s \leq q}} (c_lc'_s)(d_ld'_s)},$$

ahol az $a_k, a'_r, c_l, c'_s \in T_1$ és a $b_k, b'_r, d_l, d'_s \in T_2$ számokra $a_k c'_s, a'_r c_l, c_l c'_s \in T_1$ és $b_k d'_s, b'_r d_l, d_l d'_s \in T_2$ teljesül tetszőleges $1 \leq k \leq n$, $1 \leq l \leq m$, $1 \leq r \leq p$, $1 \leq s \leq q$ egészekre. Tehát

$$\frac{\sum\limits_{\substack{1\leq k\leq n\\1\leq s\leq q}} (a_k c'_s)(b_k d'_s) + \sum\limits_{\substack{1\leq r\leq p\\1\leq l\leq m}} (a'_r c_l)(b'_r d_l)}{\sum\limits_{\substack{1\leq l\leq m\\1\leq s\leq q}} (c_l c'_s)(d_l d'_s)} \in T.$$

□□□

2.C.Definíció. Ha $K \subseteq \mathbb{C}$ számtest és $u_1, u_2, ..., u_n \in \mathbb{C}$ komplex számok, akkor

1. ezeknek a $\lambda_1, \lambda_2, ..., \lambda_n \in K$ együtthatókkal képzett K**-lineáris kombinációján** a $\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n$ kifejezést (komplex számot) értjük;

2. a K-lineáris kombinációk által alkotott halmazra az

$$[u_1, u_2, ..., u_n]_K = \{\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n \mid \lambda_1, \lambda_2, ..., \lambda_n \in K\}$$

jelölést használjuk és ezt az $u_1, u_2, ..., u_n$ elemek K**-lineáris burkának** (**generátumának**) nevezzük (amely nem függ az u_k, $1 \leq k \leq n$ elemeknek a sorrendjétől);

3. azt mondjuk, hogy $u_1, u_2, ..., u_n$ **lineárisan függetlenek a** K **(számtest) felett**, ha a $\lambda_1, \lambda_2, ..., \lambda_n \in K$ együtthatókkal képzett K-lineáris kombinációra

$$\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n = 0$$

csak a triviális $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$ esetben teljesül (a lineáris függetlenségnél sem számít az u_k, $1 \leq k \leq n$ elemek sorrendje); amennyiben $u_1, u_2, ..., u_n$ nem lineárisan függetlenek a K számtest felett, akkor azt mondjuk, hogy **lineárisan összefüggenek** K**-felett**.♡

2.3.Állítás. *Legyenek $K \subseteq L \subseteq \mathbb{C}$ számtestek és $u_1, u_2, ..., u_n \in \mathbb{C}$ komplex számok.*

1. $u_1, u_2, ..., u_n \in [u_1, u_2, ..., u_n]_K \subseteq K(u_1, u_2, ..., u_n)$ *és* $[u_1, u_2, ..., u_n]_K$ *zárt az összeadásra, kivonásra és K-beli elemmel való szorzásra: $\lambda \in K$ és $v, w \in [u_1, u_2, ..., u_n]_K$ esetén*

$$v \pm w \in [u_1, u_2, ..., u_n]_K \text{ és } \lambda v \in [u_1, u_2, ..., u_n]_K \ .$$

2. *Ha $v_1, v_2, ..., v_m \in [u_1, u_2, ..., u_n]_K$, akkor $[v_1, v_2, ..., v_m]_K \subseteq [u_1, u_2, ..., u_n]_K$.*

3. *Ha $u_1, u_2, ..., u_n$ lineárisan függetlenek a K felett, akkor tetszőleges*

$1 \leq k_1 < k_2 < ... < k_r \leq n$ *indexekre az $u_{k_1}, u_{k_2}, ..., u_{k_r}$ részsorozat elemei is lineárisan függetlenek a K felett.*

4. *Ha $u_1, u_2, ..., u_n$ lineárisan függetlenek a K felett, akkor tetszőleges $1 \leq k \leq n$ indexre*

$$u_k \notin [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K \ .$$

5. *Ha $u_1, u_2, ..., u_n$ lineárisan függetlenek a K felett, akkor $1 \leq k < l \leq n$ esetén $u_k \neq u_l$.*

6. *Ha* $u_1, u_2, ..., u_n$ *lineárisan függetlenek a* K *felett és egy* $v \in \mathbb{C}$ *komplex számra a* $v, u_1, u_2, ..., u_n$ *elemek már lineárisan összefüggenek* K *felett, akkor*

$$v \in [u_1, u_2, ..., u_n]_K \ .$$

7. *Ha* $u_1, u_2, ..., u_n$ *lineárisan függetlenek a* K *felett, akkor a* $\lambda_1, \lambda_2, ..., \lambda_n, \mu_1, \mu_2, ..., \mu_n \in K$ *együtthatókkal a*

$$\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n = \mu_1 u_1 + \mu_2 u_2 + ... + \mu_n u_n$$

egyenlőség csak a $\lambda_1 = \mu_1$, $\lambda_2 = \mu_2$,...,$\lambda_n = \mu_n$ *esetben teljesül, ami azt jelenti, hogy ilyenkor* $[u_1, u_2, ..., u_n]_K$ *bármely elemét egyértelműen lehet az* $u_1, u_2, ..., u_n$ *számok* K*-lineáris kombinációjaként felírni.*

8. $[u_1, u_2, ..., u_n]_K \subseteq [u_1, u_2, ..., u_n]_L$.

9. *Ha* $u_1, u_2, ..., u_n$ *lineárisan függetlenek az* L *felett, akkor lineárisan függetlenek a* K *felett.*

10. *Amennyiben* $[u_1, u_2, ..., u_n]_K = L$ *és* $v_1, v_2, ..., v_m \in \mathbb{C}$ *tetszőlegesek, akkor*

$$[v_1, v_2, ..., v_m]_L = [u_k v_l \mid 1 \leq k \leq n, 1 \leq l \leq m]_K \ .$$

11. *Amennyiben* $u_1, u_2, ..., u_n \in L$ *lineárisan függetlenek a* K *felett és* $v_1, v_2, ..., v_m \in \mathbb{C}$ *lineárisan függetlenek az* L *felett, akkor az* $u_k v_l$, $1 \leq k \leq n$, $1 \leq l \leq m$ *szorzatok lineárisan függetlenek* K *felett.*

Bizonyítás.

1. $0, 1, \lambda_1, \lambda_2, ..., \lambda_n \in K$ és $u_1, u_2, ..., u_n \in K(u_1, u_2, ..., u_n)$ miatt

$$u_k = 0u_1 + 0u_2 + ... + 0u_{k-1} + 1u_k + 0u_{k+1} + ...0u_n \in [u_1, u_2, ..., u_n]_K \ ,$$

$$\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n \in K(u_1, u_2, ..., u_n),$$

továbbá $v = \lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n$ és $w = \mu_1 u_1 + \mu_2 u_2 + ... + \mu_n u_n$ (itt $\mu_1, \mu_2, ..., \mu_n \in K$) esetén

$$v \pm w = (\lambda_1 \pm \mu_1)u_1 + (\lambda_2 \pm \mu_2)u_2 + ... + (\lambda_n \pm \mu_n)u_n \in [u_1, u_2, ..., u_n]_K \ ,$$

$$\lambda v = (\lambda\lambda_1)u_1 + (\lambda\lambda_2)u_2 + ... + (\lambda\lambda_n)u_n \in [u_1, u_2, ..., u_n]_K \ .$$

2. Mivel $v_1, v_2, ..., v_m \in [u_1, u_2, ..., u_n]_K$ és az 1. részben már igazoltuk, hogy $[u_1, u_2, ..., u_n]_K$ zárt az összeadásra, kivonásra és K-beli elemmel való szorzásra, ezért $[v_1, v_2, ..., v_m]_K$-nek tetszőleges $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_m v_m$ (itt $\alpha_1, \alpha_2, ..., \alpha_m \in K$) eleme is $[u_1, u_2, ..., u_n]_K$-beli.

3. Ha a $\lambda_1, \lambda_2, ..., \lambda_r \in K$ számokkal $\lambda_1 u_{k_1} + \lambda_2 u_{k_2} + ... + \lambda_r u_{k_r} = 0$, akkor

$\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0$ is teljesül, ahol $\alpha_{k_1} = \lambda_1$, $\alpha_{k_2} = \lambda_2$, ...,$\alpha_{k_r} = \lambda_r$ és $l \notin \{k_1, k_2, ..., k_r\}$ esetén az $1 \leq l \leq n$ indexre $\alpha_l = 0$. Így az $u_1, u_2, ..., u_n$ lineáris függetlensége K felett az $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$ következménnyel jár, ahonnan

$\lambda_1 = \lambda_2 = ... = \lambda_r = 0$ adódik.

4. Ha $u_k \in [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K$ teljesülne, akkor léteznének olyan $\lambda_1, ..., \lambda_{k-1}, \lambda_{k+1}, ..., \lambda_n \in K$ elemek, amelyekre

$$u_k = \lambda_1 u_1 + ...\lambda_{k-1} u_{k-1} + \lambda_{k+1} u_{k+1} + ... + \lambda_n u_n.$$

Innen a

$$\lambda_1 u_1 + ... + \lambda_{k-1} u_{k-1} + (-1) u_k + \lambda_{k+1} u_{k+1} + ... + \lambda_n u_n = 0$$

egyenlőséghez jutunk, ami a $-1 \in K$ tartalmazásra való tekintettel ellentmond az $u_1, u_2, ..., u_n$ elemek K feletti lineáris függetlenségének.

5. Mivel az 1. részben az $u_l \in [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K$ és a 4. részben az $u_k \notin [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K$ viszonylatokat igazoltuk, ezért $u_k \neq u_l$.

6. Ha $v, u_1, u_2, ..., u_n$ lineárisan összefüggenek K felett, akkor találunk olyan $\mu, \lambda_1, \lambda, ..., \lambda_n \in K$ együtthatókat, amelyekre

$$\mu v + \lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n = 0$$

és $\{\mu, \lambda_1, \lambda, ..., \lambda_n\} \neq \{0\}$. Itt $\mu = 0$ esetén $\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n = 0$ és $\{\lambda_1, \lambda, ..., \lambda_n\} \neq \{0\}$ teljesülne, ellentmondva $u_1, u_2, ..., u_n$ lineáris függetlenségének K felett. Tehát $\mu \neq 0$ és így a fenti egyenlőségből

$$v = \left(-\frac{\lambda_1}{\mu}\right) u_1 + \left(-\frac{\lambda_2}{\mu}\right) u_2 + ... + \left(-\frac{\lambda_n}{\mu}\right) u_n \in [u_1, u_2, ..., u_n]_K$$

adódik.

7. Ha a $\lambda_1, \lambda_2, ..., \lambda_n, \mu_1, \mu_2, ..., \mu_n \in K$ együtthatókkal

$$\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n = \mu_1 u_1 + \mu_2 u_2 + ... + \mu_n u_n,$$

akkor az innen kapható

$$(\lambda_1 - \mu_1) u_1 + (\lambda_2 - \mu_2) u_2 + ... + (\lambda_n - \mu_n) u_n = 0$$

egyenlőség és $u_1, u_2, ..., u_n$ lineáris függetlensége K felett a

$$\lambda_1 - \mu_1 = \lambda_2 - \mu_2 = ... = \lambda_n - \mu_n = 0$$

következménnyel jár.

8. $K \subseteq L$ miatt nyilvánvaló.

9. $K \subseteq L$ miatt nyilvánvaló.

10. Az 1. rész alapján a $\lambda_{kl} \in K \subseteq L$, $u_k \in L$ és $v_l \in [v_1, v_2, ..., v_m]_L$ elemekre $\lambda_{kl} u_k \in L$ miatt $(\lambda_{kl} u_k) v_l \in [v_1, v_2, ..., v_m]_L$ teljesül minden $1 \leq k \leq n$, $1 \leq l \leq m$ indexre. Így az 1. részben igazoltak szerint

$$\sum_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} \lambda_{kl} u_k v_l \in [v_1, v_2, ..., v_m]_L \ ,$$

azaz

$$[u_k v_l \mid 1 \leq k \leq n, 1 \leq l \leq m]_K \subseteq [v_1, v_2, ..., v_m]_L.$$

$[u_1, u_2, ..., u_n]_K = L$ miatt tetszőleges $\alpha_l \in L$ elemhez találunk olyan $\lambda_1, \lambda_2, ..., \lambda_n \in K$ együtthatókat, amelyekre $\alpha_l = \lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n$. Tehát

$$\alpha_l v_l = \lambda_1 u_1 v_l + \lambda_2 u_2 v_l + ... + \lambda_n u_n v_l \in [u_k v_l \mid 1 \leq k \leq n, 1 \leq l \leq m]_K \ ,$$

ahonnan az 1. részre való tekintettel

$$\sum_{1 \leq l \leq m} \alpha_l v_l \in [u_k v_l \mid 1 \leq k \leq n, 1 \leq l \leq m]_K \ ,$$

azaz

$$[v_1, v_2, ..., v_m]_L \subseteq [u_k v_l \mid 1 \leq k \leq n, 1 \leq l \leq m]_K$$

adódik.

11. A $\lambda_{kl} \in K$, $1 \leq k \leq n, 1 \leq l \leq m$ együtthatókkal teljesüljön

$$\sum_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} \lambda_{kl}(u_k v_l) = 0,$$

ekkor a $\beta_l = \sum_{1 \leq k \leq n} \lambda_{kl} u_k \in L$, $1 \leq l \leq m$ számokra

$$\sum_{1 \leq l \leq m} \beta_l v_l = \sum_{1 \leq l \leq m} \left(\sum_{1 \leq k \leq n} \lambda_{kl} u_k \right) v_l = \sum_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} \lambda_{kl} u_k v_l = 0$$

adódik. Kihasználva $v_1, v_2, ..., v_m$ lineáris függetlenségét az L felett, kapjuk a

$$\beta_1 = \beta_2 = ... = \beta_m = 0$$

egyenlőségeket. Mivel $u_1, u_2, ..., u_n \in L$ lineárisan függetlenek a K felett, ezért egy $1 \leq l \leq m$ egészre a

$$\sum_{1 \leq k \leq n} \lambda_{kl} u_k = \beta_l = 0$$

egyenlőségből kapjuk, hogy

$$\lambda_{1l} = \lambda_{2l} = ... = \lambda_{nl} = 0.$$

Tehát $\lambda_{kl} = 0$ minden $1 \leq k \leq n$ és $1 \leq l \leq m$ indexre.

□□□

2.4.Lemma. *Ha $K \subseteq \mathbb{C}$ számtest, $v_1, v_2, ..., v_m \in \mathbb{C}$ tetszőlegesek és az $u_1, u_2, ..., u_n \in [v_1, v_2, ..., v_m]_K$ elemek lineárisan függetlenek K felett, akkor bármelyik $1 \leq k \leq n$ indexhez létezik olyan $1 \leq l \leq m$ index, hogy a $v_l, u_1, ..., u_{k-1}, u_{k+1}, ..., u_n$ elemek is lineárisan függetlenek K felett (azaz bármelyik u_k kicserélhető valamelyik v_l-re úgy, hogy a lineáris függetlenség a K felett megmaradjon).*

Bizonyítás. A 2.3.Állítás 3.része szerint $u_1, ..., u_{k-1}, u_{k+1}, ..., u_n$ is lineárisan függetlenek K felett, ezért ha $v_l, u_1, ..., u_{k-1}, u_{k+1}, ..., u_n$ lineárisan összefüggenek K felett, akkor a 2.3.Állítás

6.része alapján $v_l \in [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K$. Ha ez minden $1 \leq l \leq m$ indexre teljesül, akkor a 2.3.Állítás 2.részét használva kapjuk, hogy

$$[v_1, v_2, ..., v_m]_K \subseteq [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K.$$

Így $u_k \in [v_1, v_2, ..., v_m]_K$ miatt $u_k \in [u_1, ..., u_{k-1}, u_{k+1}, ..., u_n]_K$, ami a 2.3.Állítás 4.részére való tekintettel ellentmondásban van $u_1, u_2, ..., u_n$ lineáris függetlenségével K felett.
Tehát valamelyik $1 \leq l \leq m$ egészre teljesül, hogy $v_l, u_1, ..., u_{k-1}, u_{k+1}, ..., u_n$ lineárisan függetlenek K felett.

□□□

2.5.Tétel. *Ha $K \subseteq \mathbb{C}$ számtest, $v_1, v_2, ..., v_m \in \mathbb{C}$ tetszőlegesek és az $u_1, u_2, ..., u_n \in [v_1, v_2, ..., v_m]_K$ elemek lineárisan függetlenek K felett, akkor $n \leq m$.*

Bizonyítás. A 2.4.Lemma szerint van olyan $1 \leq l_1 \leq m$ index, hogy $v_{l_1}, u_2, ..., u_n$ lineárisan függetlenek K felett. Mivel $v_{l_1}, u_2, ..., u_n \in [v_1, v_2, ..., v_m]_K$, ezért ismételten a 2.4.Lemmát alkalmazva kapjuk a létezését olyan $1 \leq l_2 \leq m$ indexnek, hogy $v_{l_1}, v_{l_2}, u_3, ..., u_n$ lineárisan függetlenek K felett. Így folytatva a 2.4.Lemma k-adik alkalmazása után a
$v_{l_1}, v_{l_2}, ..., v_{l_k}, u_{k+1}, ..., u_n$ (K felett) lineárisan független elemeket kapjuk. Most

$$v_{l_1}, v_{l_2}, ..., v_{l_k}, u_{k+1}, ..., u_n \in [v_1, v_2, ..., v_m]_K \ ,$$

ezért a 2.4.Lemma újra használható. Az eljárásunk végén az $u_1, u_2, ..., u_n$ elemeket egyenként kicserélve a $v_{l_1}, v_{l_2}, ..., v_{l_n}$ (K felett) lineárisan független elemekhez jutunk. A 2.3.Állítás 5.része szerint $v_{l_1}, v_{l_2}, ..., v_{l_n}$ különböznek egymástól, ami csak úgy történhet meg, ha az

$$l_1, l_2, ..., l_n \in \{1, 2, ..., m\}$$

indexek is különbözőek. Nyilvánvaló, hogy az $\{1, 2, ..., m\}$ halmaznak csak akkor lehet n különböző eleme, ha $n \leq m$.

□□□

2.D.Definíció. Legyenek $K \subseteq L \subseteq \mathbb{C}$ számtestek, ekkor az $u_1, u_2, ..., u_n \in \mathbb{C}$ komplex számok az **L-nek bázisát alkotják a K-felett** (vagy **K-ra nézve**), ha

$$[u_1, u_2, ..., u_n]_K = L$$

és $u_1, u_2, ..., u_n$ lineárisan függetlenek a K felett (nyilvánvaló, hogy a bázis elemeire $u_1, u_2, ..., u_n \in L$). A 2.3.Állítás 7.része szerint ilyenkor bármely $a \in L$ elem egyértelműen írható

$$a = \lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n$$

alakban, ahol a fenti K-lineáris kombinációban szereplő $\lambda_1, \lambda_2, ..., \lambda_n \in K$ együtthatókat nevezzük az a **elemnek az** $u_1, u_2, ..., u_n$ **bázisra vonatkozó koordinátáinak**.
A $K \subseteq L \subseteq \mathbb{C}$ **testbővítésről** azt mondjuk, hogy **véges**, ha létezik L-nek bázisa a K felett. Ha L-nek létezik bázisa K felett, akkor egy ilyen bázisnak az elemszámát nevezzük az L **számtest** K **feletti dimenziójának**. Amennyiben $u_1, u_2, ..., u_n$ és $v_1, v_2, ..., v_m$ is bázisa L-nek K felett, akkor előbb az $u_1, u_2, ..., u_n \in L = [v_1, v_2, ..., v_m]_K$ elemek K feletti lineáris függetlenségére, majd a $v_1, v_2, ..., v_m \in L = [u_1, u_2, ..., u_n]_K$ elemek K feletti lineáris függetlenségére való tekintettel a 2.5.Tétel előbb az $n \leq m$, majd a fordított $m \leq n$ egyenlőtlenséget szolgáltatja. Tehát bármely két bázisnak az elemszáma megegyező, $n = m$, ami azt jelenti, hogy véges testbővítésre a dimenzió fenti értelmezése elfogadható. A dimenzió jelölése az alábbiak szerint szokásos:

$$[L : K] = \dim_K L = n. \heartsuit$$

2.6.Állítás. *A $K \subseteq L \subseteq \mathbb{C}$ számtestekre és az $m \geq 1$ egész számra a következő állítások ekvivalensek.*

1. *Található m darab L-beli elem úgy, hogy azok K-lineáris burka az egész L.*

2. *Akárhogyan választva $m+1$ darab L-beli elemet, azok lineárisan összefüggőek lesznek K felett.*

3. *Az L-nek létezik bázisa K-ra nézve és $[L:K] \leq m$.*

Bizonyítás. 1. $\Longrightarrow$ 2. Ha $[v_1, v_2, ..., v_m]_K = L$, akkor a 2.5.Tétel szerint az $u_1, u_2, ..., u_m, u_{m+1}$ L-beli elemek K feletti lineáris függetlensége az $m+1 \leq m$ ellentmondáshoz vezetne.
2. $\Longrightarrow$ 3. Legyen $u_1, u_2, ..., u_n \in L$ a legnagyobb elemszámú K felett lineárisan független L-beli sorozatok egyike, ekkor $n \leq m$. Most $[u_1, u_2, ..., u_n]_K = L$, hiszen egy tetszőleges $v \in L$ elemet választva $v, u_1, u_2, ..., u_n$ már lineárisan összefüggenek K felett (az $u_1, u_2, ..., u_n$ választása miatt) és így a 2.3.Állítás 6.része a $v \in [u_1, u_2, ..., u_n]_K$ tartalmazást szolgáltatja. Tehát $u_1, u_2, ..., u_n$ bázisa L-nek K felett és $[L:K] = n \leq m$.
3. $\Longrightarrow$ 1. Ha $u_1, u_2, ..., u_n$ bázisa L-nek K felett és $n = [L:K] \leq m$, akkor

$$[u_1, u_2, ..., u_n, u_{n+1}, ..., u_m]_K = [u_1, u_2, ..., u_n]_K = L,$$

ahol $u_{n+1} = u_{n+2} = ... = u_m = 0$.

□□□

2.7.Tétel. *A $K \subseteq L \subseteq M \subseteq \mathbb{C}$ számtestekre a következő állítások teljesülnek.*

1. *Ha M-nek létezik bázisa L-re nézve és L-nek létezik bázisa K-ra nézve, akkor M-nek létezik bázisa K-ra nézve és*

$$[M:K] = [M:L][L:K].$$

2. *Ha M-nek létezik bázisa K-ra nézve, akkor M-nek létezik bázisa L-re nézve és L-nek létezik bázisa K-ra nézve.*

Bizonyítás.

1. Ha $v_1, v_2, ..., v_m$ bázisa M-nek L-re nézve és $u_1, u_2, ..., u_n$ bázisa L-nek K-ra nézve, akkor a 2.3.Állítás 10. és 11.része alapján az $u_k v_l$, $1 \leq k \leq n$, $1 \leq l \leq m$ szorzatok az M-nek bázisát alkotják K-ra nézve: $[M:K] = mn = [M:L][L:K]$.

2. Legyen $w_1, w_2, ..., w_d$ bázisa M-nek K-ra nézve.

   Ekkor $L \subseteq M$ és a 2.3.Állítás 8.része miatt

$$M = [w_1, w_2, ..., w_d]_K \subseteq [w_1, w_2, ..., w_d]_L \subseteq M.$$

   Tehát $[w_1, w_2, ..., w_d]_L = M$, ami az $L \subseteq M$ bővítésre a 2.6.Állítás 1.részének és ezzel együtt a 3.résznek a teljesülését is jelenti, következésképpen M-nek létezik bázisa L-re nézve.

   A 2.6.Állítás 3.része teljesül a $K \subseteq M$ bővítésre, ezért (lásd a 2.részt) $d+1$ darab L-beli elemet akárhogyan választva (az L-től bővebb M-ből is választhatjuk ezeket), azok lineárisan összefüggőek lesznek K felett. Tehát a 2.6.Állítás 2.része teljesül a $K \subseteq L$ bővítésre is, ami azt jelenti, hogy a 3.rész is teljesül, azaz L-nek létezik bázisa K-ra nézve.

□□□

2.8.Állítás. *A $K \subseteq L \subseteq M \subseteq \mathbb{C}$ számtestekre a következő állítások teljesülnek.*

1. *Ha $[L : K] = 1$, akkor $L = K$.*
2. *Ha $[M : K] = [L : K]$, akkor $M = L$.*

Bizonyítás.

1. Ha u_1 egyelemű bázisa L-nek K-ra nézve, akkor $1 \in L$ és $[u_1]_K = L$ miatt van olyan $\lambda_1 \in K$ együttható, amelyre $\lambda_1 u_1 = 1$. Így $\lambda_1 \neq 0$ és tetszőleges $\lambda \in K$ elemre

$$\lambda u_1 = \left(\frac{\lambda}{\lambda_1}\right)(\lambda_1 u_1) = \frac{\lambda}{\lambda_1} \in K,$$

   ami azt jelenti, hogy $L = [u_1]_K \subseteq K$. Tehát $L = K$.

2. Ha $[M : K] = [L : K]$, akkor a 2.7.Tétel szerinti $[M : K] = [M : L][L : K]$ egyenlőségből $[M : L] = 1$ és innen a már igazolt 1.rész szerint $M = L$ adódik.

□□□

2.9.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges testbővítés és a $K \subseteq R \subseteq L$ köztes halmaz zárt az összeadásra, kivonásra és a szorzásra nézve (azaz R egy köztes számgyűrű), akkor R zárt a reciprok képzésére nézve is, tehát ilyenkor R egy köztes számtest.*

Bizonyítás. Mivel az $n = [L : K]$ dimenzió létezik, ezért tetszőleges $n + 1$ darab L-beli elem lineárisan összefüggő a K felett (lásd a 2.6.Állítást), speciálisan egy $0 \neq b \in R$ elemnek az $1, b, b^2, ..., b^n$ hatványairól is elmondható ugyanez. Következésképpen léteznek olyan $\lambda_0, \lambda_1, \lambda_2, ..., \lambda_n \in K$ számok, amelyek nem mindegyike zéró és amelyekre

$$\lambda_0 + \lambda_1 b + \lambda_2 b^2 + ... + \lambda_n b^n = 0.$$

Ha λ_k a legkisebb indexű nem zéró együttható, akkor a

$$\lambda_k b^k + \lambda_{k+1} b^{k+1} + ... + \lambda_n b^n = 0$$

egyenlőségből egyszerű átalakításokkal (először $\lambda_k b^{k+1}$-el osztunk) kapjuk, hogy

$$\frac{1}{b} = -\frac{1}{\lambda_k}(\lambda_{k+1} + \lambda_{k+2} b + ... + \lambda_n b^{n-(k+1)}).$$

Mivel $-\frac{1}{\lambda_k} \in K \subseteq R$ miatt $-\frac{1}{\lambda_k}, \lambda_{k+1}, \lambda_{k+2}, ..., \lambda_n \in R$, továbbá R zárt az összeadásra és a szorzásra, ezért a $b \in R$ tartalmazást is felhasználva jutunk a kívánt

$$\frac{1}{b} = -\frac{1}{\lambda_k}(\lambda_{k+1} + \lambda_{k+2} b + ... + \lambda_n b^{n-(k+1)}) \in R$$

tartalmazáshoz.

□□□

2.10.Állítás. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges testbővítés, akkor a $K \subseteq T_1 \subseteq L$ és $K \subseteq T_2 \subseteq L$ köztes számtestek $T_1 \vee T_2$ szuprémumának bármely eleme az*

$$a_1b_1 + a_2b_2 + ... + a_nb_n$$

alakban írható, ahol $n \geq 1$ egész és $a_1, a_2, ..., a_n \in T_1$ valamint $b_1, b_2, ..., b_n \in T_2$.

Bizonyítás. Az

$$R = \{a_1b_1 + a_2b_2 + ... + a_nb_n \mid n \geq 1 \text{ egész } a_1, a_2, ..., a_n \in T_1 \text{ és } b_1, b_2, ..., b_n \in T_2\}$$

halmazra a $K \subseteq T_1 \cup T_2 \subseteq R \subseteq T_1 \vee T_2 \subseteq L$ tartalmazások nyilvánvalóan teljesülnek, továbbá R egy számgyűrű. Nyilvánvaló, hogy két R-beli szám összege és különbsége is R-ben van, a szorzásra való zártságot az alábbiak mutatják:

$$(a_1b_1 + a_2b_2 + ... + a_nb_n)(a'_1b'_1 + a'_2b'_2 + ... + a'_mb'_m) = \sum_{\substack{1\leq k\leq n\\1\leq l\leq m}} (a_kb_k)(a'_lb'_l) = \sum_{\substack{1\leq k\leq n\\1\leq l\leq m}} (a_ka'_l)(b_kb'_l),$$

ahol az $a_k, a'_l \in T_1$ és a $b_k, b'_l \in T_2$ számokra $a_ka'_l \in T_1$ és $b_kb'_l \in T_2$ teljesül minden $1 \leq k \leq n$ és $1 \leq l \leq m$ egészre. Tehát

$$\sum_{\substack{1\leq k\leq n\\1\leq l\leq m}} (a_ka'_l)(b_kb'_l) \in R.$$

A 2.9.Tétel szerint R egy számtest, amelyre $T_1 \cup T_2 \subseteq R$ miatt $T_1 \vee T_2 \subseteq R$ is teljesül.

□□□