1. Bevezető

1.1 Relációk, műveletek

1.1.1 Definíció: legyen H tetszőleges halmaz. **H** feletti n-változós reláció ($n\in\mathbb{N}$) alatt H^n – kétváltozós esetben $H\times H$ – egy $\Re$ részhalmazát értjük. Az $a_1,a_2,\dots,a_n\in H$ elemek (ebben a sorrendben) akkor állnak relációban, ha $(a_1,a_2,\dots,a_n)\in\Re$. Kétváltozós esetben azt, hogy a és b relációban állnak, gyakran $a\Re b$ jelöli. Ha a reláció jele $\le$, akkor ebből $a\le b$ lesz.

Egy reláció tekinthető $\Re: H^n\to\{\text{igaz},\text{hamis}\}$ leképezésnek is; ekkor $\Re(a_1,a_2,\dots,a_n)$ jelöli, hogy az illető elemek relációban állnak.

1.1.2 Definíció: a H feletti $\Re$ kétváltozós reláció reflexív, ha $\forall a\in H: a\Re a$, azaz minden elem relációval áll önmagával. Antireflexív, ha $\nexists a\in H: a\Re a$. Pl. a valósok feletti szokásos $\le$ művelet reflexív, hiszen $\forall a\in\mathbb{R}: a\le a$, míg $<$ antireflexív, hiszen $\nexists a\in\mathbb{R}: a<a$.

1.1.3 Definíció: az $\Re$ kétváltozós reláció tranzitív, ha $(a\Re b \text{ és } b\Re c) \Rightarrow a\Re c$. Pl. a fent említett két reláció tranzitív. Nem (feltétlenül) tranzitív reláció pl. egy gráf pontjai közt a szomszédsági reláció.

1.1.4 Definíció: a H feletti $\Re$ reláció szimmetrikus, ha abból, hogy az $a_1,a_2,\dots,a_n\in H$ elemek relációban állnak, következik, hogy ezen elemek bármely sorrendbe állítva relációban állnak. Kétváltozós esetben ez azt jelenti, hogy $a\Re b\Rightarrow b\Re a$.

Kettőnél több változó esetén egy reláció lehet „kicsit" szimmetrikus, azaz megeshet, hogy a változók bizonyos átrendezése (permutációja, ld. később) nem befolyásolja. (Pl. a sík egy egyenesén az a háromváltozós $\Re$ reláció, melyre $(A,B,C)\in\Re$ pontosan akkor teljesül, ha A és C közrefogja B-t, nyilván érzéketlen a szélső első két elem cseréjére.) $\Re$-t akkor nevezzük ciklikusan szimmetrikusnak, ha $(a_1,a_2,\dots,a_n)\in\Re \Rightarrow (a_n,a_1,\dots,a_{n-1})\in\Re$.

Legyen mostantól $\Re$ kétváltozós, H feletti reláció.

1.1.5 Definíció: a H feletti $\Re$ kétváltozós reláció antiszimmetrikus, ha $(a\Re b \text{ és } b\Re a) \Rightarrow a=b$. Ha $\Re$ antireflexív, akkor ez úgy is írható, hogy $\nexists a,b\in H: (a\Re b \text{ és } b\Re a)$.

Definíció: az $\Re$ reláció megfordítása alatt azt az $\overline{\Re}$ relációt értjük, melyre $a\overline{\Re}b\Leftrightarrow b\Re a$.

1.1.6 Definíció: $\Re$ ekvivalencia-reláció, ha **(1)** reflexív, **(2)** szimmetrikus és **(3)** tranzitív.

1.1.7 Tétel: $\Re$ pontosan akkor ekvivalencia-reláció, ha létezik H-nak olyan $H=\coprod_{\alpha\in\mathbf{I}}H_\alpha$ partíciója (diszjunkt halmazokra bontása), hogy $a\Re b$ pontosan akkor áll fenn, ha a és b egyazon H_α halmazba tartoznak.

Bizonyítás: legyen minden $a\in H$ esetén $H_a=\{b\in H \mid a\Re b\}$. $\Re$ reflexivitása miatt $\forall a\in H: a\in H_a$, azaz $H\subseteq\bigcup_{a\in H}H_a$. Másrészt az unió minden tagja H részhalmaza, így $H=\bigcup_{a\in H}H_a$ is teljesül. Vegyük észre, hogy ezen előállításban bármely két tag vagy diszjunkt, vagy azonos. Valóban, tekintsünk egy H_a és H_c tagot. Ha diszjunktak, akkor igazunk van, tegyük hát fel, hogy nem azok, azaz $\exists b\in H_a\cap H_c$. A megfelelő halmazok definíciója szerint ekkor fennáll $a\Re b$ és $c\Re b$. A szimmetriát, majd a tranzitivitást kihasználva $a\Re c$. Ezek után tetszőleges $b'\in H_c$ elemre $a\Re c, c\Re b'$ szerint $a\Re b'$, azaz $b'\in H_a$. Így $H_c\subseteq H_a$ és hasonlóan $H_a\subseteq H_c$, így a két halmaz valóban azonos.

Állítsuk most elő a $\{H_a \mid a\in H\}$ halmazt $\{H_\alpha \mid \alpha\in\mathbf{I}\}$ alakban úgy, hogy a különböző indexű elemek valóban különbözőek legyenek (tehát minden elemet pontosan egyszer soroljunk fel). Ekkor $\bigcup_{\alpha\in\mathbf{I}}H_\alpha$ minden tagja különböző, azaz előbbi észrevételünk szerint a tagok páronként diszjunktak. Másrészt $\bigcup_{\alpha\in\mathbf{I}}H_\alpha=\bigcup_{a\in H}H_a=H$, hiszen a második unió minden tagja szerepel a bal oldalon és viszont. Így hát $H=\coprod_{\alpha\in\mathbf{I}}H_\alpha$.

$a\Re b$ valóban akkor és csakis akkor áll fenn, ha a és b egyazon H_α halmazba tartoznak, mert $a\Re b \Leftrightarrow H_a=H_b$.

1.1.8 Definíció: a fenti partícióban szereplő részhalmazokat ekvivalencia-osztályoknak hívjuk.

Megjegyzés: legyen $\Re$ tetszőleges reláció. Definiáljuk az $\Re^\circ$ és $\Re^*$ relációkat a következő módon: $(a,b)\in\Re^\circ\Leftrightarrow(a\Re b \text{ vagy } a=b)$ illetve $(a,b)\in\Re^*\Leftrightarrow(a\Re b \text{ és } a\ne b)$. Ekkor $\Re^\circ$ reflexív, $\Re^*$ pedig antireflexív lesz. Ez a

három reláció nyilván pontosan ugyanakkor szimmetrikus vagy antiszimmetrikus. Ha $\mathfrak{R}^*$ tranzitív, akkor $\mathfrak{R}$ is az, ha $\mathfrak{R}$ tranzitív, akkor $\mathfrak{R}^\circ$ is az, továbbá ha $\mathfrak{R}$ (és ezzel $\mathfrak{R}^\circ$,$\mathfrak{R}^*$ is) antiszimmetrikus, akkor a tranzitivitás a másik irányban is öröklődik.

Nyilván $\mathfrak{R}^{\circ *}=\mathfrak{R}^*$ és $\mathfrak{R}^{*\circ}=\mathfrak{R}^\circ$, továbbá ha $\mathfrak{R}$ reflexív ill. antireflexív volt, akkor $\mathfrak{R}=\mathfrak{R}^\circ$ ill. $\mathfrak{R}=\mathfrak{R}^*$.

1.1.9 Definíció: $\mathfrak{R}$ (‘$\leq$‘ típusú) részbenrendezés, ha **(1)** reflexív, **(2)** antiszimmetrikus és **(3)** tranzitív. Néha részbenrendezés alatt ‘$<$‘ típusú ~-t értünk, ekkor azt követeljük meg, hogy **(1′)** reflexív, **(2′)** antiszimmetrikus és **(3′)** tranzitív legyen. Előbbi megjegyzésünk szerint ez a két fogalom gyakorlatilag azonos, hiszen ha $\mathfrak{R}$ az egyik feltételhármast teljesíti, akkor a megjegyzés jelöléseivel $\mathfrak{R}^*$ ill. $\mathfrak{R}^\circ$ a másikat.

Általában $\leq$ és $<$ (esetleg $\preceq$ és $\prec$) jelöli egy részbenrendezés reflexív és antireflexív változatát, megfordításukat rendre $\geq$ és $>$ ($\succeq$ és $\succ$).

1.1.10 Definíció: $\leq$ (vagy $<$) rendezés, ha részbenrendezés, továbbá bármely két elem összehasonlítható. Ez azt jelenti, hogy $a\leq b$, $b\leq a$ valamelyike bármely $a,b\in H$ esetén teljesül. Ekkor persze pontosan egy áll fenn $a<b$, $b<a$, $a=a$ közül.

1.1.11 Definíció: $(H,\leq)$ részbenrendezett halmaz, ha $\leq$ részbenrendezés H felett. Rendezett halmaz avagy lánc, ha $\leq$ rendezés.

Megjegyzés: ha egy reláció (részben)rendezés H felett, akkor nyilván minden részhalmazára megszorítva is az.

Példák:
- rendezés $\leq$ és $<$ a valós számokon;
- részbenrendezés $\subseteq$ és $\subset$ bármilyen halmazrendszeren;
- részbenrendezés az oszthatóság a természetes számok felett.

1.1.12 Definíció: legyen $(H,\leq)$ részbenrendezett halmaz, $A\subseteq H, m\in A$. m legnagyobb eleme A-nak, ha $\forall a\in A: a\leq m$ és maximális eleme, ha $\nexists a\in A: m<a$. Legkisebb eleme, ha $\forall a\in A: a\geq m$ és minimális eleme, ha $\nexists a\in A: m>a$. Láncban a legnagyobb és a maximális elem fogalma megegyezik, akárcsak a legkisebb és a minimális elemé.

1.1.13 Definíció: egy $H^n\to H$ leképezést – tehát egy olyan leképezést, ami H rendezett n-eseihez H egy elemét rendeli – a H halmaz feletti n-változós ($n\in\mathbb{N}$) műveletnek nevezünk.

Néha $H_1\times H_2\times\ldots\times H_n\to H_i$ leképezéseket is szoktunk műveletnek nevezni, pl. egy K test feletti V vektortér esetén a skalárral szorzást (ld. később), ami egy $K\times V\to V$ leképezés.

1.1.14 Definíció: a H halmaz feletti μ kétváltozós művelet asszociatív, ha átzárójelezhető, azaz $\forall a,b,c\in H: \mu(\mu(a,b),c)=\mu(a,\mu(b,c))$. Ha a műveletet a szorzás jelével jelöljük, akkor ezt így írhatjuk: $\forall a,b,c\in H: (a\cdot b)\cdot c=a\cdot(b\cdot c)$.

Ha a szorzás (összeadás) asszociatív, akkor van értelme az $a\cdot b\cdot c$ ($a+b+c$) jelölésnek, hiszen bárhogyan zárójelezve ugyanazt az eredményt adja. Hasonlóan értelmezhető $\prod_{i=1}^n a_i=a_1\cdot a_2\cdot\ldots\cdot a_n$ ($\sum_{i=1}^n a_i=a_1+a_2+\ldots+a_n$).

1.1.15 Definíció: a H halmaz feletti μ kétváltozós művelet kommutatív, ha $\forall a,b\in H: \mu(a,b)=\mu(b,a)$. A szorzás jelölésével $\forall a,b\in H: a\cdot b=b\cdot a$.

Ha a szorzás (összeadás) asszociatív és kommutatív, akkor van értelme a $\prod_{i\in\mathbf{I}} a_i$ ($\sum_{i\in\mathbf{I}} a_i$) jelölésnek, ahol **I** véges indexhalmaz, hiszen az eredmény minden sorrendnél és zárójelezésnél ugyanaz.

1.1.16 Definíció: legyenek σ és π kétváltozós műveletek H felett. Ekkor π balról disztributív σ-ra nézve, ha $\forall a,b,c\in H: \pi(\sigma(a,b),c)=\sigma(\pi(a,c),\pi(b,c))$. Jobbról disztributív, ha $\forall a,b,c\in H: \pi(a,\sigma(b,c))=\sigma(\pi(a,b),\pi(a,c))$. Például $a\cdot(b+c)=a\cdot b+b\cdot c$ illetve $(a+b)\cdot c=a\cdot c+b\cdot c$ jelenti, hogy a szorzás disztributív az összeadásra.

A disztributivitásnak akkor is van értelme, ha $\pi: H_1\times H_2\to H_3$ és σ több H_i halmaz feletti kétváltozós műveletként is értelmes. (Pl. a geometriában vektorok skaláris szorzása ($\cdot: \mathbb{R}^n\times\mathbb{R}^n\to\mathbb{R}$) ebben az értelemben disztributív az összeadásra.)

1.2 A Zorn-lemma

Zorn-lemma: legyen $\preceq$ olyan részbenrendezés **P**-n, hogy ha valamely $\mathbf{H}\subseteq\mathbf{P}$-re $(\mathbf{H},\preceq|_{\mathbf{H}})$ rendezés, akkor $\exists m\in\mathbf{P}\,\forall h\in\mathbf{H}\colon h\preceq m$. Ez esetben $\exists m^*\in\mathbf{P}\,\forall x\in\mathbf{P}\colon m^*\not\prec x$. (Azaz ha minden **P**-beli láncnak van felső korlátja, akkor **P**-nek van maximális eleme.)

Ennek speciális esete a következő: legyen **H** tetszőleges halmaz és az $\mathcal{X}\subseteq\mathcal{P}(\mathbf{H})$ halmazrendszer olyan, hogy bármely $\mathcal{L}\subseteq\mathcal{X}$ láncra (bármely két $\mathcal{L}$-beli elem egyike tartalmazza a másikat) $\bigcup\mathcal{L}=\bigcup_{\mathbf{A}\in\mathcal{L}}\mathbf{A}\in\mathcal{X}$, akkor $\exists\mathbf{M}_{\mathcal{X}}\in\mathcal{X}\,\forall\mathbf{A}\in\mathcal{X}\colon\mathbf{M}_{\mathcal{X}}\subset\mathbf{A}$.

Mindkét változat ekvivalens a kiválasztási axiómával; ennek bizonyítása a halmazelmélet témakörébe tartozik. Mi egyszerűen használni fogjuk.

1.3 A legalapvetőbb algebrai struktúrák

1.3.1 Definíció: félcsoport egy olyan $(G,\cdot)$ rendszer, ahol a szorzás egy asszociatív kétváltozós művelet a G halmaz felett. Ha a szorzás kommutatív, akkor G kommutatív félcsoport.

1.3.2 Definíció: legyen $(G,\cdot)$ félcsoport. $e\in G$ baloldali egységelem, ha $\forall x\in G\colon ex=x$ és jobboldali egységelem, ha $\forall x\in G\colon xe=x$. Ha e bal- és jobboldali egységelem is, akkor egységelemnek nevezzük és 1-el jelöljük. (Ha a művelet az összeadás, akkor 0-val.) Ha G egységelemes félcsoport, ha van benne egységelem.

Megjegyzés: legyen a $(G,\cdot)$ félcsoportban e baloldali, e' jobboldali egységelem. Ekkor $e=e\cdot e'=e'$, tehát $e=e'$ kétoldali egységelem.

1.3.3 Definíció: legyen $(G,\cdot)$ egységelemes félcsoport. $x'\in G$ baloldali inverze $x\in G$-nek, ha $x'\cdot x=1$ és jobboldali inverze, ha $x\cdot x'=1$. Ha x' jobb- és baloldali inverze is x-nek, akkor x^{-1}-el jelöljük (ha a művelet az összadás, akkor $(-x)$) és x (kétoldali) inverzének nevezzük.

Megjegyzés: legyen a $(G,\cdot)$ egységelemes félcsoportban x' baloldali, x'' jobboldali inverze x-nek. Ekkor $x'=x'\cdot(x\cdot x'')=(x'\cdot x)\cdot x''=x''$ miatt x' (kétoldali) inverze x-nek.

1.3.4 Definíció: $(G,\cdot)$ csoport, ha olyan egységelemes félcsoport, ahol minden elemnek van inverze. Ha a művelet kommutatív, akkor a csoportot kommutatív vagy Abel-csoport hívjuk.

1.3.5 Definíció: legyen $(G,\cdot)$ félcsoport vagy csoport. Az $a,b\in G$ elemek felcserélhetőek, ha $a\cdot b=b\cdot a$. A mindennel felcserélhető elemek halmazát G centrumának hívjuk és $Z(G)$-vel jelöljük. Könnyen ellenőrizhető, hogy ha G félcsoport, egységelemes félcsoport ill. csoport, akkor $Z(G)$ elemei az örökölt műveletekre kommutatív félcsoportot, egységelemes kommutatív félcsoportot ill. csoportot alkotnak.

1.3.6 Definíció: $(H,+,\cdot)$ félgyűrű, ha $(H,+)$ kommutatív félcsoport, $(H,\cdot)$ félcsoport és a szorzás disztributív az összeadásra.

1.3.7 Definíció: gyűrű egy olyan $(R,+,\cdot)$ rendszer, ahol $(R,+)$ kommutatív csoport, $(R,\cdot)$ félcsoport, és a szorzás disztributív az összeadásra. Ha $(R,\cdot)$ egységelemes és/vagy kommutatív félcsoport, akkor $(R,+,\cdot)$ egységelemes és/vagy kommutatív gyűrű. Az összeadás egységeleme a nullelem, a szorzás egységeleme – ha van – az egységelem.

Megjegyzés: $\forall x\in R\colon x\cdot 0=x\cdot(0+x)-x\cdot x=x\cdot x-x\cdot x=0$, azaz a nullát bármivel szorozva nullát kapunk.

1.3.8 Jelölés: legyen $(G,\cdot)$ félcsoport, $x\in G, n\in\mathbb{Z}$. Ekkor x^n (x n-edik hatványa) alatt $n>0$ esetén G azon elemét értjük, amelyet úgy kapunk, hogy az x elem n példányát összeszorozzuk; $n=0$ esetén az egységelemet (ha van), $n<0$ esetén pedig x inverzének (ha van) $|n|$-edik hatványát (ez egyben $x^{|n|}$ inverze). Könnyen belátható, hogy $x^{n+m}=x^n\cdot x^m$ és $x^{nm}=(x^n)^m$. (Tehát x hatványai felcserélhetőek.)

Ha a művelet az összeadás, akkor ezt inkább $n\cdot x$ vagy nx jelöli, ekkor $(n+m)x=nx+mx$ és $(nm)x=n(mx)$.

1.3.9 Definíció: nullosztónak hívjuk egy gyűrű azon elemeit, melyeket a gyűrű valamely nem 0 elemével szorozva 0-t kaphatunk. Egy gyűrű nullosztómentes, ha csak a 0 nullosztó, azaz ha $x,y\neq 0\Rightarrow x\cdot y\neq 0$.

1.3.10 Definíció: ferdetestnek nevezünk egy olyan – legalább kételemű – egységelemes $(R,+,\cdot)$ gyűrűt, amelyben a nullelem kivételével minden elemnek van inverze a szorzásra nézve. Minden ferde test nullosztómentes, azaz $a\neq 0, ab=0 \Rightarrow b=0$. Ugyanis $a\neq 0, ab=0 \Rightarrow \exists a^{-1} \Rightarrow b=1\cdot b=(a^{-1}a)\cdot b=a^{-1}(ab)=a^{-1}\cdot 0$.

1.3.11 Definíció: $(K,+,\cdot)$ (kommutatív) test, ha olyan ferde test, ahol a szorzás kommutatív, azaz:

(K1) $+: K\times K\to K$
(K2) $\forall x,y,z\in K: x+(y+z)=(x+y)+z$
(K3) $\forall x,y\in K: x+y=y+x$
(K4) $\exists 0\in K: \forall x\in K: x+0=0+x=x$
(K5) $\forall x\in K: \exists(-x)\in K: x+(-x)=(-x)+x=0$
(K6) $\cdot: K\times K\to K$
(K7) $\forall x,y,z\in K: x\cdot(y\cdot z)=(x\cdot y)\cdot z$
(K8) $\forall x,y\in K: x\cdot y=y\cdot x$
(K9) $\exists 1\in K: \forall x\in K: x\cdot 1=1\cdot x=x$
(K10) $\forall x\in K\setminus\{0\}: \exists x^{-1}\in K: x\cdot x^{-1}=x^{-1}\cdot x=1$
(K11) $\forall x,y,z\in K: x(y+z)=xy+xz, (x+y)z=xz+yz$

1.3.12 Definíció: vegyük egy K testben az $n\cdot x$ alakú számokat, ahol $x\in K\setminus\{0\}$ rögzített, n pedig végigfut az egész számokon. Ezek vagy mind különbözőek, vagy nem. Ha valamely $m<n$ egészekre $mx=nx$, akkor $(n-m)x=0$, tehát van olyan legkisebb $p\in\mathbb{Z}^+$, amelyre $p\cdot x=0$. (Különben nincs, mert $0\cdot x=0$, tehát más n-re $nx\neq 0$.) Legyen az utóbbi esetben K karakterisztikája p, különben 0. Jelölése $char(K)$.

Állítás: $char(K)$ jóldefiniált. Ugyanis ha $x,x'\in K\setminus\{0\}$, akkor $\exists a\in K\setminus\{0\}: x'=xa$ és $p\cdot x=0 \Leftrightarrow (p\cdot x)a=0 \Leftrightarrow p(xa)=0 \Leftrightarrow p\cdot x'=0$.

1.3.13 Állítás: ha K karakterisztikája $p\neq 0$, akkor p prím.

Bizonyítás: $\nexists p$ nem prím. Ekkor $p=ab$, ahol $a,b\in\mathbb{Z}^+$ és $a,b<0$. Így $(1\cdot a)\cdot(1\cdot b)=1\cdot ab=1\cdot p=0$ a disztributivitásból. K nullosztómentessége miatt $(1\cdot a)=0$ vagy $(1\cdot b)=0$, de p választása miatt mindkettő $\lightning$.

Példák: a szokásos műveletekkel a valós ($\mathbb{R}$) és a racionális számok ($\mathbb{Q}$), a *mod p* (p prím) maradékosztályok ($\mathbb{F}_p$) testet alkotnak. Az egész számok ($\mathbb{Z}$) egységelemes, kommutatív, nullosztómentes gyűrűt, a *mod m* maradékosztályok egységelemes kommutatív gyűrűt (Z_m vagy $\mathbb{Z}/(m)$), a természetes számok ($\mathbb{N}$) pedig kommutatív félgyűrűt. Csoportot alkotnak például egy kör egybevágósági transzformációi a kompozícióra.

1.4 Komplex számok

Legyen i olyan, hogy $i^2=-1$. Legyen a komplex számok halmaza $\mathbb{C}=\{a+b\cdot i \mid a,b\in\mathbb{R}\}$. A műveleteket legyenek „ugyanolyanok", mint a felett (azaz pl. $(a+b\cdot i)(c+d\cdot i)=ac+ad\cdot i+bc\cdot i+bd\cdot i^2$). Mivel ez nem valami precíz definíció, tekintsük inkább a következő konstrukciót:

1.4.1 Definíció: legyen $\mathbb{C}$ azon rendezett (a,b) párok halmaza, ahol $a,b\in\mathbb{R}$. Legyen $\mathbb{C}$ elemei fölött $(a,b)+(c,d)=(a+c,b+d)$, $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$.

Könnyen látható, hogy ekkor az $(a,0)$ alakú párok éppúgy viselkednek, mint a valós számok, azaz a valós számokkal izomorf (bár ezt még nem definiáltuk) struktúrát alkotnak az így megadott műveletekkel. Megtehetjük tehát, hogy $(a,0)\in\mathbb{C}$ elemet az $a\in\mathbb{R}$ számmal azonosítjuk.

1.4.2 Definíció: jelölje i a $(0,1)\in\mathbb{C}$ elemet.

Ekkor $(a,b)\in\mathbb{C}$ előáll $(a,b)=(a,0)+(0,b)=(a,0)+(0,1)\cdot(b,0)=a+b\cdot i$ alakban, azaz $\mathbb{C}=\{a+b\cdot i \mid a,b\in\mathbb{R}\}$. Vegyük észre továbbá, hogy $i^2=(0,1)^2=(0\cdot 0-1\cdot 1, 0\cdot 1+1\cdot 0)=-1$.

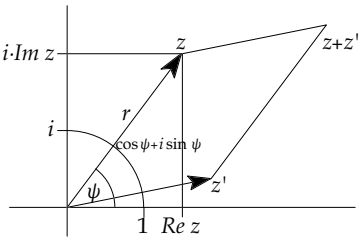
1.4.3 Állítás: $(\mathbb{C},+,\cdot)$ test.

Bizonyítás: **(K1)**, **(K6)** feltételek a műveletek definíciója szerint teljesülnek. **(K2)**, **(K3)**, **(K7)**, **(K8)**, **(K11)** könnyen kiszámolható a valós számok műveleti tulajdonságaiból. Legyen $z=a+b\cdot i\in\mathbb{C}$ tetszőleges. **(K4)**, **(K5)**, **(K9)** teljesül $0_{\mathbb{C}}=0+0\cdot i\in\mathbb{C}$, $-z=(-a)+(-b)\cdot i\in\mathbb{R}$ és $1_{\mathbb{C}}=1+0\cdot i\in\mathbb{C}$ választással. Ha $z\neq 0$, akkor $a^2+b^2=r^2\neq 0$, így $\exists z^{-1}=\frac{a}{r^2}-\frac{b}{r^2}\cdot i\in\mathbb{C}$ és ez kielégíti **(K10)**-et. Ezzel az állítást beláttuk.

1.4.4 Definíció: $z=a+bi\in\mathbb{C}$ valós része $\mathbf{Re}\,z=a$, képzetes része $\mathbf{Im}\,z=b$, konjugáltja $\bar{z}=a-bi$. Ekkor $\mathbf{Re}(z_1\pm z_2)=\mathbf{Re}\,z_1\pm\mathbf{Re}\,z_2$, $\mathbf{Im}(z_1\pm z_2)=\mathbf{Im}\,z_1\pm\mathbf{Im}\,z_2$, $\overline{(z_1\pm z_2)}=\bar{z}_1\pm\bar{z}_2$, $\overline{(z_1\cdot z_2)}=\bar{z}_1\cdot\bar{z}_2$ és $\overline{(z^{-1})}=(\bar{z})^{-1}$.

A valós számokat kiválóan tudtuk ábrázolni a számegyenesen. A valós számokat egy kétdimenziós derékszögű koordináta-rendszerben (síkon) ábrázolhatjuk úgy, hogy az $a+bi$ komplex számnak az (a,b) pontot feletetjük meg (így kapjuk a (Gauss-féle) komplex számsíkot). Ez egy kölcsönösen egyértelmű megfeleltetés lesz. Nézzük meg, minek felelnek meg a műveletek a síkon.

Az összeadás a vektoriális összeadásnak felel meg, a konjugálás az x tengelyre való tükrözésnek, az additív inverz (ellentett) hozzárendelése az origóra való tükrözésnek.



1.4.5 Definíció: $z=a+bi\in\mathbb{C}$ abszolútértéke $|a+bi|=\sqrt{a^2+b^2}=\sqrt{z\bar{z}}$. Ez a síkon éppen a z-t reprezentáló vektor hossza (r) lesz.

Az 1 abszolútértékű számok az origó közepű egységkörön lesznek. Vegyük ezek közül azt (z_1), amelyik az x tengellyel φ szöget zár be. Ez $z_1=\cos\varphi+i\cdot\sin\varphi$ alakba írható. Hasonlóan tetszőleges z komplex szám felírható $z=r\cdot(\cos\psi+i\cdot\sin\psi)$ alakban, ahol $r\geq 0, 0\leq\psi<2\pi$.

1.4.6 Definíció: a fenti felírást z trigonometrikus alakjának nevezzük. A ψ szög z argumentuma, jelölése **Arg** z.

Megjegyzés: **Arg** z és $|z|$ egyértelműek (ha $z\neq 0$) és egyértelműen meghatározzák z-t, azaz két komplex szám pontosan akkor egyezik meg, ha argumentumuk és abszolútértékük megegyezik (vagy mindkettő 0).

A trigonometrikus alak segítségével meg tudjuk mondani, minek felel meg a Gauss -féle számsíkon a szorzás:

$$z_1z_2=r_1(\cos\varphi_1+i\cdot\sin\varphi_1)\cdot r_2(\cos\varphi_2+i\cdot\sin\varphi_2)=r_1r_2(\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2+i\cdot(\sin\varphi_1\cos\varphi_2+\cos\varphi_1\sin\varphi_2))=$$
$$=r_1r_2\cdot(\cos(\varphi_1+\varphi_2)+i\cdot\sin(\varphi_1+\varphi_2))$$

Két komplex számot tehát úgy kell összeszorozni, hogy az abszolútértéküket összeszorozzuk, az argumentumukat összeadjuk (és esetleg levonunk belőle 2π-t, hogy $[0,2\pi)$-be essen). Rögzített z_0 komplex számra tehát a $z\mapsto z\cdot z_0$ transzformáció egy origó közepű, $|z_0|$ arányú, **Arg** z_0 szögű forgatva nyújtás.

Látható, hogy $z=r(\cos\varphi+i\cdot\sin\varphi)\neq 0$ inverze $z^{-1}=\frac{1}{r}\cdot(\cos(-\varphi)+i\cdot\sin(-\varphi))$, tehát a (multiplikatív) inverz hozzárendelése a síkon az egységsugarú körre való inverzió és a konjugálás (tetszőleges sorrendben vett) kompozíciója.

1.4.7 Megjegyzés: szorzás fenti képletéből $z^n=(r(\cos\varphi+i\cdot\sin\varphi))^n=r^n(\cos(n\varphi-2k\pi)+i\cdot\sin(n\varphi-2k\pi))$.

1.4.8 Definíció: $z_0=r_0(\cos\varphi_0+i\cdot\sin\varphi_0)\in\mathbb{C}$ n-edik gyökei azok a $z=r\cdot(\cos\varphi+i\cdot\sin\varphi)$ komplex számok, melyekre $z^n=z$.

Keressük meg ezeket. $z_0=0$ esetén $z=0$, mert a komplex számok testet alkotnak és egy test nullosztómentes. Ha $z_0\neq 0$, akkor

$$z^n=z_0\Leftrightarrow r^n(\cos(n\varphi-2k\pi)+i\sin(n\varphi-2k\pi))=r_0(\cos\varphi_0+i\cdot\sin\varphi_0)\Leftrightarrow\left\{\begin{matrix}r^n=r_0\\ n\varphi-2k\pi=\varphi_0\end{matrix}\right\}\Leftrightarrow\left\{\begin{matrix}r=\sqrt[n]{r_0}\\ \varphi\in\{\frac{\varphi_0}{n}+\frac{2k\pi}{n}\,|\,0\leq k\leq n-1\}\end{matrix}\right\}$$

ahol $\sqrt[n]{r_0}$ az r pozitív valós szám pozitív valós n-edik gyöke. Ez egyértelmű, φ-nek pedig pontosan n lehetséges értéke van, tehát $z\in\mathbb{C}\setminus\{0\}$-nak pontosan n n-edik gyöke van. Ezek abszolútértéke azonos, argumentumaik pedig $\frac{2\pi}{n}$-enként követik egymást, azaz egy origó közepű szabályos n-szöget alkotnak a komplex számsíkon.

1.4.9 Definíció: n-edik egységgyöknek nevezzük az 1 n-edik gyökeit a komplex testben. Ezek $\{\sqrt[n]{1}\}=\{\cos\frac{2k\pi}{n}+i\cdot\sin\frac{2k\pi}{n}\,|\,0\leq k\leq n-1\}$. (A jövőben az $\varepsilon_n=\cos\frac{2\pi}{n}+i\cdot\sin\frac{2\pi}{n}$ jelölést fogom használni.)

1.4.10 Definíció: az n-edik egységgyök primitív n-edik egységgyök, ha ω egész kitevős hatványaiként az összes n-edik egységgyök előáll.

1.4.11 Állítás: az ω n-edik egységgyök pontosan akkor primitív n-edik egységgyök, ha $1\leq k<n\Rightarrow\omega^k\neq 1$.

1.4.12 Bizonyítás: $\Leftarrow$: ha ω n-edik egységgyök, akkor nyilván minden hatványa is. Ha tehát az első n hatványa különböző, akkor pont az összes n-edik egységgyök. Ha $1\leq k<n$ esetén $\omega^k\neq 1$, akkor az első n hatvány közül semelyik kettő hányadosa nem lehet 1, mert vagy a hányados, vagy a reciproka ω^k alakú; tehát valóban különbözőek.

$\Rightarrow$: ha ω n-edik egységgyök, akkor hatványai n szerint ciklikusak, tehát csak úgy fedhetik le az összes n-edik egységgyököt, ha az első n hatvány páronként különböző. Az n-edik hatvány 1, azaz ω^k nem lehet egy, ha $1\le k<n$.

1.4.13 Állítás: $\omega=\varepsilon_n^k$ pontosan akkor primitív n-edik egységgyök, ha k és n relatív prímek.

Bizonyítás: ha k és n relatív prímek, akkor bármely $1\le l<n$-re $kl=qn+r$, ahol $0\le r<n$ a maradékos osztás alapján és $r\neq 0$, mert kl nem lehet n többszöröse. $\omega^l=\varepsilon_n^{kl}=\varepsilon_n^{qn+r}=(\varepsilon_n^n)^q\varepsilon_n^r=\varepsilon_n^r$. Viszont $\varepsilon_n^r\neq 1$, mert ε_n primitív n-edik egységgyök, így $\omega^l\neq 1$, ω is primitív n-edik egységgyök. Ha k és n nem relatív prímek, akkor a legkisebb közös többszörösük kn-nél kisebb, azaz k-t egy $1\le l<n$ számmal megszorozva megkaphatjuk. Ekkor $kl=qn$ lesz, és a fenti módon $\omega^l=1$, ω valóban nem primitív n-edik egységgyök.

1.4.14 Állítás: minden n-edik egységgyök m-edik primitív egységgyök valamely m-re.

Bizonyítás: teljes indukció n-re. n=1-re igaz. Ezután ha egy n-edik egységgyök nem primitív, akkor valamely $k<n$-re k-adik hatványa 1, azaz k-adik egységgyök, és az indukciós feltevés szerint m-edik primitív egységgyök. Könnyű belátni, hogy m a legkisebb l egész, amelyre az l-edik hatvány 1.

1.5 Kvaterniók

Legyen $i^2=j^2=k^2=-1$, $ij=k$, $jk=i$, $ki=j$. Úgy próbáljuk megadni a műveleteket, hogy a $\mathbb{H}=\{a+bi+cj+dk\,|\,a,b,c,d\in\mathbb{R}\}$ halmaz minél „jobb” struktúra legyen.

1.5.1 Definíció: a fenti $\mathbb{H}$ halmaz elemeit kvaternióknak hívjuk (és mindjárt definiáljuk közöttük a műveleteket).

Az összeadás legyen tagonkénti összeadás, ekkor összeadásra ugyanúgy kommutatív csoport lesz, mint a valós számok.

Azt is szeretnénk, ha pl. $(b_1i)\cdot(b_2i)=b_1b_2\cdot i^2=-b_1b_2$, $(cj)\cdot(dk)=cd\cdot jk=cd\cdot i$ lenne, azaz egy szorzat egy tényezőjét egy valós számmal szorozva a szorzat értéke is ezzel a valós számmal szorzódjon. A valós számok tehát legyenek mindennel felcserélhetőek. Ebből már következik, hogy az 1 valós szám lesz a szorzás egységeleme.

A szorzás disztributivitásához az összeadásra nézve ragaszkodunk. Ez azt jelenti, hogy

$$(a+bi+cj+dk)(A+Bi+Cj+Dk)=aA-bB-cC-dD+(aB+Ab)i+(aC+Ac)j+(aD+Ad)k+bC\cdot ij+cD\cdot jk+dB\cdot ki+cB\cdot ji+dC\cdot kj+aD\cdot ik$$

lesz. Hogy ezt $(a'+b'i+c'j+d'k)$ alakra tudjuk hozni, már csak a ji,ik,kj szorzatokat kell megadnunk. Vegyük észre, hogy $ji=-j\cdot(-1)\cdot i=-j\cdot k^2\cdot i=-jk\cdot ki=-ij=-k$. Hasonlóan $kj=-jk=-i$, $ik=-ki=-j$. A szorzás tehát nem lesz kommutatív. Viszont lesz a szorzásra inverz, mégpedig az alábbi: legyen $\alpha=a+bi+cj+dk$ konjugáltja $\bar{\alpha}=a-bi-cj-dk$. Könnyen látható, hogy $\alpha\bar{\alpha}=a^2+b^2+c^2+d^2=r^2$, ami egy nemnegatív valós szám és csak akkor 0, ha $\alpha=0$ (r-t hívjuk α abszolútértékének). Ha tehát $\alpha\neq 0$, akkor $\alpha\cdot\frac{\bar{\alpha}}{r^2}=1$.

1.5.2 Állítás: $\mathbb{H}$ ferde test (ezt láttuk be az imént).

Megjegyzés: a tisztán képzetes kvaterniókhoz a háromdimenziós tér vektorait megfeleltetve két elem szorzatának valós része a skalárszorzat ellentettje, képzetes része a vektoriális szorzat lesz.

1.6 Polinomok

1.6.1 Definíció: legyen R (lehetőleg egységelemes) gyűrű. Nevezzük az x változó R feletti polinomjának a $p(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ alakú formális kifejezéseket, ahol az a_i számok – melyeket együtthatóknak nevezünk – R elemei. Egy változó R feletti polinomjainak halmaza az R feletti polinomgyűrű, jelölése $R[x]$. Két polinomot akkor tekintünk azonosnak, ha formálisan azonosak, azaz összes együtthatójuk azonos. (A ki nem írt együtthatókat nullának tekintjük.)

1.6.2 Definíció: egy $p(x)\in R[x]$ polinom behelyettesítési értéke R egy r elemére – jelölése $p(r)$ – az az R-beli elem, melyet akkor kapunk, ha $p(x)$-ben r–t írunk az x szimbólumok helyére, és a számolásokat elvégezzük. p polinom gyökei R azon elemei, melyek behelyettesítési értéke R nulleleme.

Az összeadás két polinom között legyen a tagonkénti összeadás, azaz $p(x)=\sum_{k=0}^{n}a_kx^k$ és $q(x)=\sum_{k=0}^{m}b_kx^k$ összege $(p+q)(x)=\sum_{k=0}^{\mathbf{max}(n,m)}(a_k+b_k)x^k$ (a hiányzó együtthatók helyére írjunk nullákat). Nullelem az azonosan 0 polinom (amelynek minden együtthatója 0).

1.6.3 Definíció: p polinom foka az a legnagyobb k egész, amelyre a k-adfokú tag együtthatója nem 0. Ezt az együtthatót főegyütthatónak nevezzük. A 0 polinom foka $-\infty$ (esetleg nincs is foka). Jelölése $deg(p)$ vagy $gr(p)$. A nulladfokú polinomokat és az azonosan 0 polinomot együtt konstans polinomoknak hívjuk.

1.6.4 Állítás: **(1)** nyilván $deg(p+q)=\mathbf{max}(deg(p),deg(q))$ ha $deg(p)\neq deg(q)$. Azonos fokú polinomok összegének foka az első olyan k egész, amelyre a k-adik tag együtthatója a két polinomban nem egymás additív inverze (ellentettje) – ez legfeljebb az eredeti polinomok foka, azaz **(2)** $deg(p+q)\leq\mathbf{max}(deg(p),deg(q))$ mindig teljesül.

Az összeadás kommutativitása és a disztributivitás miatt az összegbe behelyettesítve R egy r elemét ugyanazt kapjuk, mintha a két öszeadandóba helyettesítettünk volna be és az eredményeket adtuk volna össze:

$$p_1(r)+p_2(r)=\sum a_kr^k+\sum b_kr^k=\sum(a_kr^k+b_kr^k)=\sum(a_k+b_k)r^k=(p_1+p_2)(r).$$

A szorzás legyen a következő: $p,q\in R[x]$esetén $p\cdot q$ t-edfokú együtthatója legyen azon együtthatópárok szorzatainak összege, ahol a hozzájuk tartozó x-es tagok kitevőinek összege t. Formálisan: $(\sum_{i=0}^{n}a_ix^i)\cdot(\sum_{k=0}^{m}b_kx^k)=\sum_{t=0}^{n+m}(\sum_{i+k=t}a_ib_k)\cdot x^t$. Ha R egységelemes, akkor a konstans 1 polinom egységeleme $R[x]$-nek.

Ha a gyűrű nullosztómentes és a tényezők egyike sem a 0 polinom volt, akkor a kapott polinom foka a két tényező fokának összege, főegyütthatója a főegyütthatók szorzata lesz. (Nagyobb fokú nem nulla együttható nyilván nem lehet, ez a tag pedig valóban a két főegyüttható szorzata lesz. Ez nem lesz 0, ha a gyűrű nullosztómentes.) Ekkor tehát $R[x]$ is nullosztómentes. Ha R-ben $a,b\neq0$ és $ab=0$, akkor $R[x]$-ben a konstans a és a konstans b nem (azonosan) 0 polinomok szorzata a(z azonosan) 0 polinom, tehát $R[x]$ sem nullosztómentes.

Ha R kommutatív gyűrű, akkor az R feletti műveleti szabályokból kiszámolható, hogy a szorzás is felcserélhető a behelyettesítéssel. (Az is elég, hogy az együtthatók – vagy a behelyettesítendő érték – $(R,\cdot)$ centrumában legyenek.)

1.6.5 Állítás: $(R[x],+,\cdot)$ gyűrű és ha R egységelemes, kommutatív ill. nullosztómentes, akkor $R[x]$ is az. (Ezt részben beláttuk, a többi egyszerűen levezethető az R feletti műveleti szabályokból.)

Ha R nullosztómentes, akkor a legalább elsőfokú polinomokat bármilyen nem 0 polinommal megszorozva legalább elsőfokú polinomot kapunk, nem a konstans 1 polinomot, azaz szorzásra nem lesz inverze. Így osztani általában nem lehet, ill. ferdetest felett oszthatunk a nulladfokú polinomokkal. (Az azonosan 0 és a nulladfokú polinomok R elemeinek felelnek meg.)

Foglalkozzunk most egy K test feletti polinomgyűrűvel.

1.6.6 Definíció: K test algebrailag zárt, ha minden legalább elsőfokú K feletti polinomnak van gyöke K-ban.

Ezt valóban csak testre érdemes definiálni, mert ha az R gyűrű nem kommutatív, akkor nem szeretünk behelyettesíteni, ha pedig nem ferde test, akkor $(ax-b)$-nek nem minden a,b párosra van gyöke.

1.6.7 Tétel: $\mathbb{C}$ algebrailag zárt. (Ezt majd egyszer bebizonyítjuk.)

1.6.8 Állítás: minden $K[x]$-beli $g\neq0,f$ polinomokra $\exists q,r\in K[x]: f=q\cdot g+r$ ($deg\,r<deg\,g$ vagy $r=0$), azaz $K[x]$-ben van maradékos osztás.

1.6.9 Bizonyítás: $deg(f)<deg(g)$ esetén $q=0,r=f$ megfelelő. Ha $deg(f)\geq deg(g)$, akkor legyen f főegyütthatója a, g főegyütthatója pedig $b\neq0$. Így $q_1=\frac{a}{b}\cdot x^{deg(f)-deg(g)}\in K[x]$. Az $r_1=(f-q_1\cdot g)$ polinom $deg(f)$ fokú együtthatója $a-\frac{a}{b}\cdot b=0$ lesz, azaz r_1 legalább eggyel alacsonyabb fokú lesz f-nél. Ha még mindig legalább olyan fokú, mint g, akkor r_1-hez is találhatunk olyan q_2 polinomot, melyre $r_2=(r_1-q_2\cdot g)$ alacsonyabb fokú. Ezt folytassuk addig, amíg végül $deg(r_k)<deg(g)$ lesz. Ekkor $f-q_1g-q_2g-\ldots-q_kg=r_k$. q-t a q_i-k összegének választva $r=r_k$ lesz, aminek valóban alacsonyabb a foka g fokánál. Ráadásul pontosan egy ilyen q lehet, mert ha lenne két különböző, akkor azok különbsége legalább nulladfokú lenne. $r-r'=(f-q\cdot g)-(f-q'\cdot g)=(q'-q)\cdot g$ foka kevesebb, mint $deg(g)$, mert r és r' foka alacsonyabb g fokánál. Másrészt ez g és egy legalább nulladfokú polinom szorzata, tehát legalább $deg(g)$ fokú, ami ellentmondás. Csak egy hányadospolinom lehet jó, így a maradék is egyértelmű.

1.6.10 Definíció: ha f-et elosztva g-vel a maradék 0, azaz $f=q\cdot g$, akkor g osztja f-et, jelölése $g\mid f$. Van tehát oszthatóság, maradékos osztás, ebből euklideszi algoritmus, legnagyobb közös osztó, legkisebb közös többszörös.

1.6.11 Állítás: p-nek pontosan akkor gyöke α, ha $(x-\alpha)\mid p$.

Bizonyítás II.: $f(x)=f(x)-f(\alpha)=\sum_{k=0}^{n}a_k(x^k-\alpha^k)=\sum_{k=0}^{n}\left(a_k(x-\alpha)\cdot\sum_{i=0}^{k-1}x^i\alpha^{k-i-1}\right)=(x-\alpha)\cdot\sum\sum(\dots)$.

Bizonyítás I.: osszuk el maradékosan: $p(x)=q(x)\cdot(x-\alpha)+r(x)$, ahol r vagy nulladfokú, vagy nulla, tehát konstans. Behelyettesítve α-t: $0=f(\alpha)=q(x)\cdot(\alpha-\alpha)+r=r$, azaz $r=0$ kell legyen.

Ha α gyöke egy p polinomnak, akkor $(x-\alpha)$-t p gyöktényezőjének hívjuk. Az előzőek alapján ekkor $f(x)=f_1(x)\cdot(x-\alpha)$. Legyen β egy α-tól különböző gyöke: $0=f(\beta)=f_1(\beta)\cdot(\beta-\alpha)$. Mivel a test nullosztómentes és $(\beta-\alpha)\neq 0$, $f_1(\beta)=0$ kell legyen. Eszerint egy polinomból egy gyöktényezőjét kiemelve a többi gyök megmarad (gyöke lesz a hányadosnak) és a többi gyöktényező is sorra kiemelhető. Tehát

1.6.12 Tétel: egy test feletti n-edfokú polinomnak legfeljebb n gyöke, mert ha m gyöke van, akkor az m gyöktényező szorzata – egy m-edfokú polinom – osztja, tehát legalább m-edfokú.

Ez gyűrűben már nem feltétlenül igaz, mert például a Z_8 kommutatív gyűrűben az x^2-1 polinomnak gyöke az $1,2,3,7$ maradékosztályok mindegyike. Sőt, a $\mathbb{H}$ ferde testben az x^2+1 polinomnak végtelen sok gyöke van.

Legyen p egy K test feletti n-edfokú polinom, amelynek n gyöke van. Emeljük ki sorra a gyöktényezőit. Ekkor $p(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$. Ezt hívjuk p gyöktényezős alakjának. Mivel két polinom pontosan akkor azonos, ha formálisan azonos, a szorzatot kifejtve p együtthatóit kell kapjuk. Eszerint

1.6.13 Tétel: a fenti feltételek mellett $a_{n-k}=(-1)^k a_n\cdot\sum_{1\le i(1)<i(2)<\ldots<i(k)\le n}\left(\prod_{j=1}^{k}\alpha_{i(j)}\right)$. (Például $a_{n-1}=(-a_n)\cdot\left(\sum_{i=0}^{n}\alpha_i\right)$, $a_{n-1}=a_n\cdot\left(\sum_{1\le i<j\le n}\alpha_i\alpha_j\right)$, $a_0=(-1)^n a_n\cdot\prod_{i=1}^{n}\alpha_i$. Ez a gyökök és együtthatók közti összefüggés. Szokták Viète-formulák néven is emlegetni.

Ha $K=\mathbb{C}$ és $p(x)=x^n-1$, akkor $\{\alpha_i\mid 1\le i\le n\}=\{\varepsilon_n^i\mid 1\le i\le n\}$. Ekkor a gyökök és együtthatók közti összefüggés szerint az n-edik egységgyökök szorzata $(-1)^{n-1}$, k tagú szorzataik összege $1<k\le n$ esetén 0.

1.7 Többszörös gyök, polinom deriváltja

1.7.1 Definíció: $p\in K[x]$-nek $\alpha\in K$ legalább k-szoros gyöke, ha $(x-a)^k$ osztja p-t. (Pontosan) k-szoros gyöke, ha legalább k-szoros gyöke, de nem legalább $k+1$-szeres gyöke.

1.7.2 Definíció: $p=\sum_{k=0}^{n}a_k x^k\in K[x]$ polinom deriváltja $p'=\sum_{k=1}^{n}(k\cdot a_k)x^{k-1}$. Második derivált a derivált deriváltja, stb.

Összeg deriváltja nyilván a deriváltak összege.

1.7.3 Állítás: $\forall p,q\in K[x]$: $(pq)'=p'q+qp$.

Bizonyítás: legyen $p=\sum_{k=0}^{n}a_k x^k$, $q=\sum_{k=0}^{m}b_k x^k$. Ekkor pq-ban x^k együtthatója $\sum_{(\dots)}a_t b_{k-t}$. x^{i-1} együtthatója $(pq)'$-ben $k\cdot\sum_{(\dots)}a_t b_{k-t}$. Ugyanez $p'q$-ban $\sum_{(\dots)}t\cdot a_t b_{k-t}$, $q'p$-ben $\sum_{(\dots)}a_t\cdot(k-t)b_{k-t}$. Ezeket összeadva épp a bizonyítandó állítást kapjuk.

1.7.4 Állítás: α többszörös (legalább kétszeres) gyöke p-nek $\Leftrightarrow$ gyöke p-nek és a deriváltjának is.

Bizonyítás: $\Rightarrow$: $p'(x)=((x-\alpha)^2\cdot q(x))'=(x-\alpha)^2\cdot q'(x)+2(x-\alpha)q(x)=(x-\alpha)\cdot(\dots)$

$\Leftarrow$: ha $(x-\alpha)$ osztja p-t, de csak egyszeres gyök, akkor $p(x)=(x-\alpha)q(x)$, ahol q-nak már nem gyöke α. Ekkor $p'(x)=(x-\alpha)q'(x)+q(x)$, tehát $(x-\alpha)$ nem osztja p'-t.

1.7.5 Tétel: ha K algebrailag zárt és $p\in K[x]$ n-edfokú, akkor p-nek pontosan n gyöke van (multiplicitással számolva, azaz ha egy k-szoros gyököt k gyöknek tekintünk).

Bizonyítás: emeljünk ki addig gyöktényezőket, amíg tudunk. Így p-t (a főegyütthatótól eltekintve) gyöktényezők szorzatára bontjuk, mert ha maradna legalább másodfokú tényező, annak még lenne gyöke K választása miatt, így ki lehetne emelni még egy gyöktényezőt. A szorzatpolinom fokszámára vonatkozó állítás szerint p pontosan n gyöktényező (és egy főegyüttható) szorzata, amiből a tétel állítása következik.

1.8 Permutációk

1.8.1 Definíció: permutációnak egy (véges) halmaz önmagára („-ra": minden elem előáll, mint kép) való egy-egyértelmű leképezését nevezzük. (Mi csak a véges alaphalmazok esetével foglalkozunk.) Azt a permutációt, ami $(x_1,x_2,x_3,\dots,x_n)$-hez $(x_{i(1)},x_{i(2)},x_{i(3)},\dots,x_{i(n)})$-t rendeli, $\binom{x_1\ x_2\ x_3\ \dots\ x_n}{x_{i(1)}\ x_{i(2)}\ x_{i(3)}\ \dots\ x_{i(n)}}$-el jelöljük. Ha az $\alpha:\mathbf{H}_1\to\mathbf{H}_1, \beta:\mathbf{H}_2\to\mathbf{H}_2$ permutációkra létezik olyan $f:\mathbf{H}_1\to\mathbf{H}_2$ kölcsönösen egyértelmű megfeleltetés, amelyre $\forall x\in\mathbf{H}_1: f(\alpha(x))=\beta(f(x))$, azaz α ugyanúgy viselkedik $\mathbf{H}_1$-ben, mint β $\mathbf{H}_2$-ben, akkor a két permutációt azonosnak tekintjük. Elég tehát az $(1,2,3,\dots,n)$ halmaz permutációit vizsgálni.

1.8.2 Definíció: az S_n n-edfokú szimmetrikus csoport az n elemű permutációk csoportja a függvénykompozícióra. Be kell persze látnunk, hogy valóban csoportot alkotnak.

Legyen $\mathbf{H}=\{1,\dots,n\}$. A $\mathbf{H}$ feletti $\alpha: i\mapsto i\alpha$, $\beta: i\mapsto i\beta$ permutációkra a kompozíciójuk $\alpha\beta: i\mapsto (i\alpha)\beta$ is nyilván permutáció, hiszen bijekciók kompozíciója is bijekció. Az asszociativitás is teljesül, mert leképezések között a kompozíció mindig asszociatív művelet.

Egységelem az identikus permutáció (minden elem képe önmaga). Egy α permutáció inverze a fenti jelölésekkel $\alpha^{-1}=\binom{(1)\alpha\ (2)\alpha\ \dots\ (n)\alpha}{1\ \ 2\ \dots\ \ n}$. Így S_n valóban csoport. Ha $n\geq 3$, akkor $\binom{1\,2\,3\,4\,5\,\dots}{2\,1\,3\,4\,5\,\dots}$, $\binom{1\,2\,3\,4\,5\,\dots}{2\,3\,1\,4\,5\,\dots}$ nem cserélhetőek fel, tehát a művelet nem kommutatív; ha $n\in\{1,2\}$, akkor igen.

Tekintsünk most egy α permutációt. Vegyünk az alaphalmazban egy a_1 elemet, aztán annak a képét (a_2), majd annak a képét (a_3) és ezt folytassuk mindaddig, amíg nem jutunk olyan elemhez, ami már szerepelt. Ez nem lehet egy közbülső elem, mert minden elem pontosan egy elemnek a képe, és az egynél nagyobb indexű elemek a megelőző indexű elemek képei, nem egy későbbinek. Tehát olyan elemeket kapunk, melyekre $a_1\alpha=a_2, a_2\alpha=a_3,\dots,a_{k-1}\alpha=a_k, a_k\alpha=a_1$. Ezt ciklusnak hívjuk és $(a_1a_2a_3\dots a_k)$-val jelöljük.

Nyilván minden α permutáció előáll diszjunkt ciklusok szorzataként; sőt, az előállítás lényegében egyértelmű. (A sorrendtől (diszjunkt permutációk felcserélhetőek), az egyelemű ciklusoktól és egyazon ciklus különböző felírásaitól eltekintve egyértelmű.) Ezt a felírást hívjuk α ciklikus alakjának.

A kételemű ciklusokat transzpozíciónak nevezzük.

1.8.3 Állítás: minden permutáció felírható transzpozíciók szorzataként.

Bizonyítás: elég ciklusokra belátni, márpedig $(123\dots k)=(12)(13)(14)\dots(1k)$.

1.8.4 Állítás: ha α előáll l_1 és l_2 számú transzpozíció szorzataként is, akkor l_1 és l_2 paritása azonos.

Bizonyítás: legyen $f=\prod_{1\leq i<k\leq n}(x_k-x_i)$ n változós polinom és minden α permutációra $f_\alpha=\prod_{1\leq i<k\leq n}(x_{k\alpha}-x_{i\alpha})$. Ez bármely permutációra f vagy $-f$ lesz. Nevezzük α-t páros permutációnak, ha $f_\alpha=f$, és páratlannak, ha $f_\alpha=-f$. Legyen $s_\alpha=\frac{f_\alpha}{f}$. (Ez páros permutációra 1, páratlanra -1.) s_β nem változik attól, hogy f-ben néhány változót megcserélünk, azaz például f_α-t csinálunk f-ből. Eszerint $f_{\alpha\beta}=s_\beta\cdot f_\alpha \Rightarrow s_{\alpha\beta}=s_\alpha\cdot s_\beta$, ami azt jelenti, hogy két páratlan vagy két páros permutáció szorzata páros, egy páros és egy páratlan vagy egy páratlan és egy páros szorzata pedig páratlan. Nézzük meg, hogy egy tetszőleges $\alpha=(rs)$: $r<s$ transzpozíció páros vagy páratlan. Az olyan (x_j-x_i) tényezők, ahol i,k egyike sem r vagy s, nem változnak. Ugyanígy nem változnak azok, ahol k az r, s számok valamelyike és $i<r,s$. (Ekkor f-ben (x_r-x_i) és (x_s-x_i), f_α-ban $(x_{r\alpha}-x_i)=(x_s-x_i)$ és $(x_{s\alpha}-x_i)=(x_r-x_i)$ szerepel.) Ugyanez a helyzet, ha $i\in\{r,s\}$ és $k>r,s$. Ha i,k egyike r és s között van, a másik pedig r vagy s, akkor az (x_k-x_i) tényező előjele könnyen ellenőrizhetően megfordul. Ilyenből esetből $2\cdot(s-r-1)$ van, összesítve tehát páros sok előjelváltást okoznak, ami nem számít. Az (x_s-x_r) tényező helyére $(x_{s\alpha}-x_{r\alpha})=-(x_s-x_r)$ kerül, azaz $f_\alpha=-f$ lesz $\Rightarrow$ minden transzpozíció páratlan. Így a páros permutációk csak páros, a páratlanok csak páratlan sok transzpozíció szorzataként állíthatóak elő. Ezzel az állítást beláttuk.

1.8.5 Definíció: egy α n elemű permutáció inverziószáma azon párok száma egy n elemű halmazban, melyek megfordulnak, ha α-t alkalmazzuk. Ennek paritása is megadja, hogy egy permutáció páros vagy páratlan. (Pont azok a párok fordulnak meg, amelyekre (x_k-x_i) más előjellel szerepel f-ben, mint f_α-ban.) Jelölése $sgn(\alpha)$.

1.8.6 Definíció: az n elemű páros permutációk csoportját A_n-el jelöljük és n-edfokú alternáló csoportnak nevezzük. Ez valóban csoport, hiszen az identikus permutáció páros, páros permutációk szorzata, így inverze is páros, az asszociativitást pedig örökli S_n-ből.

Vegyünk egy n elemű páratlan permutációt. Végigszorozva minden n elemű páratlan permutációval páronként különböző n elemű páros permutációkat kapunk. Megszorozva minden páros n elemű permutációval páronként különböző n elemű páratlan permutációkat kapunk. Eszerint legalább és legfeljebb ugyanannyi páros permutáció van, mint páratlan, tehát ugyanannyi.

1.9 Mátrixok

1.9.1 Definíció: legyen R gyűrű. Legyen ekkor $R^{n\times k}$ az R feletti n soros és k oszlopos mátrixok halmaza, azaz az olyan $a_{i,j}$ elemekből álló táblázatok halmaza, ahol $1\le i<n, 1\le j<k, a_{i,j}\in R$. Egy $\mathbf{A}\in R^{n\times k}$ mátrix transzponáltja legyen az az $\mathbf{A}^T\in R^{n\times k}$ mátrix, melyet úgy kapunk, hogy **A**-t tükrözzük a főátlójára. (Főátló alatt az $a_{i,i}$ alakú elemek egyenesét értjük akkor is, ha ez történetesen nem átlója a mátrix táblázatának.)

Legyen két azonos dimenziójú mátrix összege az a mátrix, amit akkor kapunk, ha a két mátrix elemeit pozíciónként összeadjuk. Ez az összeadás rendelkezik az R feletti összeadás tulajdonságaival, tehát $R^{n\times k}$ erre az összeadásra kommutatív vagy más néven Abel-csoportot alkot. Az additív egység a csupa 0 mátrix.

A és **B** mátrixok szorzatát akkor definiáljuk, ha **A** sorai és **B** oszlopai száma azonos, azaz $\mathbf{A}\in R^{n\times m}, \mathbf{B}\in R^{m\times k}$. Legyen az **AB** szorzat az $n\times k$-as mátrix, melynek i-edik sorának j-edik eleme **A** i-edik sorának és **B** j-edik oszlopának skalárszorzata (a sor e-edik elemét megszorozzuk az oszlop e-edik elemével minden $1\le e<m$-re és a szorzatokat összeadjuk), azaz $(ab)_{ij}=\sum_{e=1}^{m} a_{ie}\cdot b_{ej}$.

A disztributivitás ($\mathbf{A}\cdot(\mathbf{B}+\mathbf{C})=\mathbf{A}\cdot\mathbf{B}+\mathbf{A}\cdot\mathbf{C}$ és $(\mathbf{A}+\mathbf{B})\cdot\mathbf{C}=\mathbf{A}\cdot\mathbf{C}+\mathbf{B}\cdot\mathbf{C}$) egyszerűen következik az R feletti disztributivitásból. A szorzás asszociativitását egyelőre higgyük el. (Bár ki tudnánk számolni, csak hosszú lenne). Kommutatív több okból sem lesz. Egyrészt $\mathbf{A}\cdot\mathbf{B}$ létezéséből nem következik $\mathbf{B}\cdot\mathbf{A}$ létezése, másrészt ha létezik is, akkor sem feltétlenül ugyanakkora, harmadrészt ha **A** és **B** egyaránt $n\times n$-es mátrixok, még akkor is csak egészen kivételes esetben felcserélhetőek.

Megjegyzés: $(\mathbf{A}\cdot\mathbf{B})^T=\mathbf{B}^T\cdot\mathbf{A}^T$, amennyiben ezek értelmesek.

1.9.2 Definíció: $\mathbf{A}\in R^{n\times n}$ nyoma $tr(\mathbf{A})=\sum_{k=1}^{n} a_{kk}$, a főátlóbeli elemek összege. Nyilván $tr(\mathbf{A}+\mathbf{B})=tr(\mathbf{A})+tr(\mathbf{B})$.

Jelölés: $R^{n\times n}$-re inkább az $M_n(R)$ jelölést használjuk.

Tekintsük $M_n(K)$-t valamely K kommutatív test esetében. Ebben van egységelem a szorzásra, mégpedig az az **I** mátrix, melynek főátlójában minden elem 1, minden más pedig 0. Ezek szerint gyűrű. Kérdés, hogy van-e inverz, illetve mikor van inverz.

Ehhez definiáljuk egy $\mathbf{A}\in R^{n\times n}$ mátrix determinánsát, amennyiben R kommutatív.

1.9.3 Definíció: $\mathbf{det}(\mathbf{A})=\sum_{\pi\in S_n}(-1)^{sgn(\pi)}\cdot\prod_{k=1}^{n} a_{k,\pi(k)}$.

Ez azt jelenti, hogy minden lehetséges módon kiválasztunk n elemet a mátrixból úgy, hogy minden sorból és minden oszlopból pontosan egy szerepeljen, a kiválasztott elemeket összeszorozzuk, és a szorzatokat előjelezve összeadjuk. Az előjel pozitív, ha a kiválasztáshoz tartozó permutáció páros és negatív, ha páratlan. (A kiválasztáshoz tartozó permutáció az, ami a sorok felsorolásához hozzárendeli a belőlük kiválasztott elemek oszlopainak felsorolását. Például egy 4×4-es mátrix esetén az $a_{13}, a_{24}, a_{32}, a_{41}$ kiválasztáshoz tartozó permutáció $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$.)

Ugyanezen mátrix permanense $\mathbf{per}(\mathbf{A})=\sum_{\pi\in S_n}\prod_{k=1}^{n} a_{k,\pi(k)}$.

1.9.4 Állítás: $\forall\mathbf{A}\in M_n(R)$: $\mathbf{per}(\mathbf{A})=\mathbf{per}(\mathbf{A}^T)$, $\mathbf{det}(\mathbf{A})=\mathbf{det}(\mathbf{A}^T)$.

Az első egyenlőség úgy nyilvánvaló, ahogy van, a második pedig abból következik, hogy egy permutáció és az inverze pontosan ugyanakkor páros, tehát a megfelelő szorzatok ugyanolyan előjellel szerepelnek mindkét oldalon. Képlettel:

$$\mathbf{det}(\mathbf{A})=\sum_{\pi\in S_n}(-1)^{sgn(\pi)}\cdot\prod_{k=1}^{n} a_{k,\pi(k)}=\sum_{\pi\in S_n}(-1)^{sgn(\pi^{-1})}\cdot\prod_{k=1}^{n} a^T_{k,\pi(k)}=\sum_{\pi^{-1}\in S_n}(-1)^{sgn(\pi^{-1})}\cdot\prod_{k=1}^{n} a^T_{k,\pi^{-1}(k)}=\mathbf{det}(\mathbf{A}^T).$$

A következő állításoknál a $\mathbf{det}(\mathbf{A})$ definíciójában szereplő, π permutációhoz tartozó $\prod_{k=1}^{n} a_{k,\pi(k)}$ szorzatot $P_\pi(\mathbf{A})$, $(-1)^{sgn(\pi)}$-t s_π.

Megjegyzés: mivel a transzponálástól a determináns értéke nem változik, a most következő állítások sorok helyett oszlopokra is fennállnak.

1.9.5 Állítás: legyen $\mathbf{A}\in M_n(K)$. Ekkor az alábbiak teljesülnek:

(D1) ha **A** valamelyik sora 0, akkor $\mathbf{det}(\mathbf{A})=0$. (Minden – $\mathbf{det}(\mathbf{A})$ definíciójában szereplő – szorzat 0.)

(D2) ha **A** egy sorát megszorozzuk egy $c\in K$ számmal, akkor a determináns értéke c-szeresére változik. (Minden szorzat c-szeresére változik.)

(D3) ha **A** $i-$edik és $j-$edik sorát megcseréljük $(i\neq j)$, akkor determinánsa az ellentettjére változik.

Bizonyítás: jelölje a kapott mátrixot $\mathbf{A}'$. $\mathbf{det}(\mathbf{A})$ és $\mathbf{det}(\mathbf{A}')$ definíciójában ugyanazok a szorzatok szerepelnek, de a megfelelő kiválasztáshoz tartozó permutációk különböznek; ha **A**-nál valamely szorzat a π kiválasztáshoz tartozik, akkor $\mathbf{A}'$-nél a $\sigma=(ij)\cdot\pi$ permutációhoz. Az (ij) transzpozíció páratlan permutáció, így $(-1)^{sgn(\sigma)}=-(-1)^{sgn(\pi)}$. Ebből

$$\mathbf{det}(\mathbf{A}')=\sum_{\sigma\in S_n}s_\sigma P_\sigma(\mathbf{A}')=\sum_{(ij)\cdot\pi\in S_n}s_{(ij)\cdot\pi}P_\pi(\mathbf{A})=\sum_{\pi\in S_n}-s_\pi P_\pi(\mathbf{A})=-\mathbf{det}(\mathbf{A})$$

(D4) ha **A**-ban az i-edik sor a j-edik sor c-szerese $(i\neq j)$, akkor $\mathbf{det}(\mathbf{A})=0$.

Bizonyítás: párosítsuk össze a kiválasztásokat úgy, hogy egy párba olyanok kerülnek, melyek csak abban különböznek, hogy e két sorból mit választottunk ki (azaz hogy a megfelelő két oszlop közül melyik melyik sorhoz tartozik). Legyen a megfelelő két permutáció π és $\sigma=(ij)\cdot\pi$. Ekkor $a_{j,m}=c\cdot a_{i,m}$, $\sigma(j)=\pi(i)$, $\sigma(i)=\pi(j)$ és $k\neq i,j$ esetén $\sigma(k)=\pi(k)$, így

$$P_\sigma(\mathbf{A})=\prod_{k=1}^n a_{k,\sigma(k)}=a_{i,\sigma(i)}\cdot a_{i,\sigma(j)}\cdot\prod_{k\neq i,j}a_{k,\sigma(k)}=a_{i,\pi(j)}\cdot c\cdot a_{i,\pi(i)}\cdot(\prod\ldots)=a_{j,\pi(j)}\cdot a_{i,\pi(i)}\cdot(\prod\ldots)=P_\pi(\mathbf{A})$$

Tehát egy pár két eleméhez ugyanaz a szorzat tartozik. Az előjelet meghatározó s_π és s_σ pedig egymás ellentettjei, hiszen az (ij) transzpozíció páratlan permutáció. Így a párosított tagok kiejtik egymást:

$$\mathbf{det}(\mathbf{A})=\sum_{\pi\in A_n}s_\pi\cdot P_\pi(\mathbf{A})+\sum_{\pi\in A_n}s_{\pi\cdot(ij)}\cdot P_{\pi\cdot(ij)}(\mathbf{A})=\sum_{\pi\in A_n}1\cdot P_\pi(\mathbf{A})+\sum_{\pi\in A_n}(-1)\cdot P_\pi(\mathbf{A})=0$$

Ha R test és karakterisztikája nem 2, akkor ez egyszerűbben is kijön: **(D3)** felhasználásával $\mathbf{det}(\mathbf{A})=-\mathbf{det}(\mathbf{A})$, amiből ez esetben következik $\mathbf{det}(\mathbf{A})=0$.

(D5) ha $\mathbf{A}'$ és $\mathbf{A}''$ mátrixok csak az i-edik sorukban különböznek, továbbá **A** az a mátrix, melyben az i-edik sor e két sor összege, a többi sor pedig megegyezik $\mathbf{A}'$ soraival, akkor $\mathbf{det}(\mathbf{A})=\mathbf{det}(\mathbf{A}')+\mathbf{det}(\mathbf{A}'')$.

Bizonyítás: nyilvánvaló, de azért kiszámolom. A disztributivitásból:

$$P_\pi(\mathbf{A})=\prod_{k=1}^n a_{k,\pi(k)}=(a'_{i,\pi(i)}+a''_{i,\pi(i)})\cdot\prod_{k\neq i}a_{k,\pi(k)}=\prod_{k=1}^n a'_{k,\pi(k)}+\prod_{k=1}^n a''_{k,\pi(k)}=P_\pi(\mathbf{A}')+P_\pi(\mathbf{A}'')$$

$$\mathbf{det}(\mathbf{A})=\sum_\pi s_\pi\cdot P_\pi(\mathbf{A})=\sum_\pi s_\pi\cdot[P_\pi(\mathbf{A}')+P_\pi(\mathbf{A}'')]=\sum_\pi s_\pi\cdot P_\pi(\mathbf{A}')+\sum_\pi s_\pi\cdot P_\pi(\mathbf{A}'')=\mathbf{det}(\mathbf{A}')+\mathbf{det}(\mathbf{A}'')$$

(D6) ha **A** i-edik sorához hozzáadjuk a j-ediket, determinánsa változatlan.

Bizonyítás: az új determináns **(D5)** alapján felírható az eredeti mátrix és azon mátrix determinánsának összegeként, melyet úgy kapunk, hogy az i-edik sor helyére a j-ediket írjuk. Ez utóbbi determináns **(D4)** alapján 0.

(D7) ha egy mátrix egy sorához hozzáadjuk a többi sorok konstansszorosainak összegét (lineáris kombinációját, ld. később), akkor a determináns értéke nem változik. (Alkalmazzuk **(D2)**-t és **(D6)**-ot.) Speciálisan, ha valamely sora előáll a többi sor lineáris kombinációjaként, akkor a determináns 0. (Vonjuk ki a lineáris kombinációt; a determináns nem változik és lesz egy csupa 0 sor.)

1.9.6 Állítás: legyen $\mathbf{A}\in M_n(K)$. Jelölje $D_{i,j}$ azon $\mathbf{A}_{i,j}$ mátrix determinánsát, melyet úgy kapunk, hogy **A** i-edik sorát és j-edik oszlopát elhagyjuk. Ekkor $\mathbf{det}(\mathbf{A})=\sum_{j=1}^n(-1)^{j-1}a_{1j}D_{1j}$.

Bizonyítás: ha beírjuk mindenhová a determináns definícióját, azt kapjuk, hogy ugyanazok a tagok szerepelnek mindkét oldalon, csak az előjelre kell vigyázni. Az inverziószámok vizsgálatával belátható, hogy az előjelek helyesen vannak.

1.9.7 Definíció: legyen $\mathbf{A}\in M_n(K)$. Ekkor az i-edik sor j-edik eleméhez tartozó előjeles aldeterminánsa $A_{ij}=(-1)^{i+j}D_{ij}$.

1.9.8 Kifejtési tétel: tetszőleges $i,j\in\{1\dots n\}$-re $\mathbf{det}(\mathbf{A})=\sum_{k=1}^{n}a_{ik}A_{ik}=\sum_{k=1}^{n}a_{kj}A_{kj}$. Ezt nevezzük $\mathbf{det}(\mathbf{A})$ i-edik sor ill. oszlop szerinti kifejtésének.

Bizonyítás: az első fele megkapható **1.9.6**-ból úgy, hogy az i-edik sort kicseréljük az előzővel, majd ezt addig ismételgetjük, amíg az első sorig nem jutunk. A második fele az első felének transzponáltja.

1.9.9 Ferde kifejtés tétele: $i\neq k\Rightarrow\sum_{j=1}^{n}a_{ij}A_{kj}=0$ és hasonlóan $\sum_{j=1}^{n}a_{ji}A_{jk}=0$.

Bizonyítás: ez annak a mátrixnak a k-adik sor (oszlop) szerinti kifejtése, amely majdnem **A**, csak a k-adik sor (oszlop) helyére is az i-ediket írtuk. Ez a determináns viszont **(D4)** szerint 0.

1.9.10 Tétel: $\mathbf{det}(\mathbf{AB})=\mathbf{det}(\mathbf{A})\cdot\mathbf{det}(\mathbf{B})$.

Bizonyítás: vegyük azt a $2n\times 2n$-es mátrixot, melynek bal felső negyedébe **A**-t, jobb alsó negyedébe **B**-t, jobb felső negyedébe csupa 0-t, bal alsó negyedébe akármit írunk. Ennek a determinánsában csak azok a tagok lehetnek 0-tól különbözőek, melyek csak **A**-ból és **B**-ből származó tagokat tartalmaznak. Eszerint ezen mátrix determinánsa $\mathbf{det}(\mathbf{A})\cdot\mathbf{det}(\mathbf{B})$. Írjuk a bal alsó sarokba **I** ellentettjét. Ezek után adjuk hozzá a mátrix jobb felébe eső oszlopokhoz az első n oszlopot olyan konstanssal megszorozva, hogy a jobb alsó sarokban végül csupa 0 legyen. (Azaz az $n+j$-edik oszlopból az i-edik oszlop b_{ij}-szeresét.) Szerencsénk van, a jobb felső sarokban éppen **AB** jelenik meg. (Egyszerű, de most nem számolom ki.–) Látható, hogy a kapott mátrix determinánsa $\mathbf{det}(\mathbf{AB})$ lesz, és a determináns értéke végig változatlan maradt **(D7)** szerint. Ezzel az állítást beláttuk.

1.9.11 Következmény: legyen R kommutatív, $\mathbf{A}\in M_n(R)$ és tegyük fel, hogy $\mathbf{det}(\mathbf{A})$-nak nincs inverze R-ben (például $\mathbf{det}(\mathbf{A})=0$). Ekkor akkor **A**-nak sincs, hiszen $\nexists\,\mathbf{A}^{-1}$, ekkor $1=\mathbf{det}(\mathbf{I})=\mathbf{det}(\mathbf{A}\cdot\mathbf{A}^{-1})=\mathbf{det}(\mathbf{A})\cdot\mathbf{det}(\mathbf{A}^{-1})$, $\lightning$.

1.9.12 Inverz mátrix előállítása: legyen R egységelemes, kommutatív gyűrű, $\mathbf{A}\in M_n(R)$ egy invertálható determinánsú mátrix, determinánsát jelölje A.

Legyen az $\mathbf{A}^*$ mátrix i-edik sorának k-adik eleme A_{ki}. Ekkor $\mathbf{A}\cdot\frac{\mathbf{A}^*}{A}$ m-edik sorának l-edik eleme $\sum_{k=1}^{n}a_{mk}\cdot\left(\frac{1}{A}\cdot a^*_{kl}\right)=\frac{1}{A}\cdot\sum_{k=1}^{n}a_{mk}\cdot A_{kl}$, ami $m=l$ esetén $\frac{1}{A}\cdot A=1$, különben 0 a sor szerinti kifejtési tétel ill. ferde kifejtési tétel szerint. Tehát ez a mátrix **I**. Az oszlop szerinti kifejtések alapján ugyanígy $\frac{\mathbf{A}^*}{A}\cdot\mathbf{A}=\mathbf{I}$. Tehát $\frac{\mathbf{A}^*}{A}=\mathbf{A}^{-1}$.

1.9.13 Állítás: legyenek $a_1,a_2,\dots,a_{n-1},a_n$ K különböző elemei. Legyen az **A** mátrixban $a_{ij}=a_i^{j-1}$. (Ez egy ún. Vandermonde-determináns.) Ekkor $\mathbf{det}(\mathbf{A})=\prod_{1\le i<j\le n}(a_j-a_i)$.

Bizonyítás: teljes indukció n-re. Vonjuk le az első sort az összes többiből. Az első oszlopban minden 0 lesz, kivéve $a_{11}=1$. A kapott determináns értéke az első oszlop szerint kifejtve A_{11}, elég tehát az utolsó $(n-1)$ sor és oszlop alkotta aldeterminánst vizsgálnunk. Ebben az i-edik sor j-edik eleme $a_{i+1}^j-a_1^j=(a_{i+1}-a_1)(a_1^{j-1}+a_1^{j-2}a_{i+1}+\dots+a_1a_{i+1}^{j-2}+a_{i+1}^{j-1})$. Osszunk le $1\le i\le(n-1)$-re az i-edik sort $(a_{i+1}-a_1)$-el. Ezzel a determináns értékét $\prod_{i=2}^{n}(a_i-a_1)$-el osztottuk. A kapott **B** mátrixban $b_{ij}=(a_1^{j-1}+a_1^{j-2}a_{i+1}+\dots+a_{i+1}^{j-1})$. (Az i-edik elem az első oszlopban 1, a másodikban a_1+a_{i+1}, a harmadikban $a_1^2+a_1a_{i+1}+a_{i+1}^2$, stb.) Vonjuk ki az első oszlop a_1-szeresét az összes többi oszlopból, majd a kapott mátrix második oszlopának a_1-szeresét a későbbi oszlopokból, stb., végül az utolsóelőtti oszlop a_1-szeresét az utolsóból. Ezt végigcsinálva látható, hogy $b_{ij}=a_{i+1}^{j-1}$ lesz. Ezen determináns értéke az indukciós feltevés szerint $\prod_{2\le i<j\le n}(a_j-a_i)$. A determináns csak a leosztásnál változott – ld. **(D7)** –, azaz $\mathbf{det}(\mathbf{A})=\left(\prod_{i=2}^{n}(a_i-a_1)\right)\cdot\left(\prod_{2\le i<j\le n}(a_j-a_i)\right)=\prod_{1\le i<j\le n}(a_j-a_i)$. Ezzel az állítást beláttuk.

1.9.14 Állítás: legyen az **A** mátrixban a főátlón minden elem a, a többi elem mind b. Ekkor $\mathbf{det}(\mathbf{A})=(a-b)^{n-1}(a+b(n-1))$.

Bizonyítás: vonjuk ki első oszlopából a másodikat, majd a másodikból a harmadikat, stb., végül az utolsóelőttiből az utolsót. Ekkor az minden $1\le i\le(n-1)$-re az i-edik oszlop i-edik eleme $a-b$, $i+1$-edik eleme $b-a$, máshol pedig 0 lesz; az utolsó oszlop változatlanul marad. Adjuk hozzá az első sort a másodikhoz, a másodikat a harmadikhoz, stb., az utolsóelőttit az utolsóhoz. Így az utolsó oszlopban a b-k összeadódnak és végül $a_{nn}=a+b(n-1)$ lesz, az első $n-1$ oszlopban a főátló alatti $(b-a)$-k eltűnnek, így a főátló alatt csupa 0 lesz. A determináns képletében csak a főátlón lévő elemek szorzata nem lesz 0, azaz $\mathbf{det}(\mathbf{A})=\prod_{i=1}^{n}a_{ii}=(a-b)^{n-1}(a+b(n-1))$. A valós számok felett két különböző nemnegatív számra tehát soha nem lesz 0.

1.9.15 Definíció: blokkrendszernek nevezünk egy v elemű X alaphalmaz b elemű részhalmazrendszerét, ahol minden részhalmaz k elemű, minden X-beli elem pontosan r részhalmazban van benne és bármely két részhalmaz metszete λ elemű. ($v,k,\lambda,r,b\in\mathbb{Z}^+$) Megköveteljük továbbá, hogy $k<v$ is fennálljon.

Nyilván minden blokkrendszerben $bk=rv$, $(v-1)\lambda=r(k-1)$ és $\lambda<r$.

1.9.16 Fischer tétele: egy blokkrendszerben $b\geq v$.

Bizonyítás: legyen az $\mathbf{A}\in\mathbb{R}^{b\times v}$ mátrixban $a_{ij}=1$, ha az alaphalmaz j-edik eleme benne van az i-edik részhalmazban és 0, ha nincs. Tekintsük a $\mathbf{B}=\mathbf{A}^T\cdot\mathbf{A}$ mátrixot. b_{ii} az **A** mátrix i-edik oszlopában szereplő egyesek száma lesz, tehát azon részhalmazok száma, amelyben az alaphalmaz i-edik eleme szerepel, azaz r. b_{ij} **A** i-edik és j-edik oszlopának skalárszorzata, tehát azon sorok száma **A**-ban, amelyekben mindkét oszlopban egyes van. Ez azon részhalmazok száma, melyekben az alaphalmaz i-edik és j-edik eleme együtt szerepel, azaz λ. A kapott négyzetes mátrixban tehát a főátlón r, mindenhol máshol λ van. Mivel $0<\lambda<r$, ennek determinánsa az előző állítás szerint nem 0.

↑ $b<v$, ekkor **A** „lapos" mátrix, azaz hozzá lehet venni néhány 0 sort úgy, hogy négyzetes legyen. Ettől $\mathbf{A}^T\cdot\mathbf{A}$ nem változik, másrészt a kapott $\mathbf{A}_0$ és $\mathbf{A}_0^T$ mátrixok determinánsa 0 lesz, mert lesz 0 soruk illetve oszlopuk. Azaz $0\neq\mathbf{det}(\mathbf{A}^T\cdot\mathbf{A})=\mathbf{det}(\mathbf{A}_0)\cdot\mathbf{det}(\mathbf{A}_0^T)=0$, ↯. Tehát b nem lehet kisebb v-nél.

1.9.17 Cramer-szabály: ha az **A** mátrix determinánsa nem 0, akkor pontosan egy megoldása van annak az n egyenletből álló lineáris egyenletrendszernek, amelyben az i-edik egyenlet $\sum_{j=1}^n a_{ij}x_j=b_i$.

Megjegyzés: ezt az egyenletet a jövőben $x\mathbf{A}=b$ alakban írjuk, ahol $x=(x_1,x_2,\ldots,x_n)$ és $b=(b_1\ldots b_n)$.

Bizonyítás: legyen $A=\mathbf{det}(\mathbf{A})$, A_k pedig annak az $\mathbf{A}_k$ mátrixnak a determinánsa, amelyet úgy kapunk, hogy **A**-ban a_{ik} helyére b_i-t írunk minden i-re. Azt állítjuk, hogy egy x_k sorozat megoldás $\Leftrightarrow x_k=\frac{A_k}{A}$.

Legyen (x_j) megoldás. Szorozzuk meg az i-edik egyenletet A_{ik}-val és a kapott egyenleteket adjuk össze. A bal oldalon x_j együtthatója $\sum_{i=1}^n a_{ij}\cdot A_{ik}$ lesz, ami a kifejtési és ferde kifejtési tételek szerint $j=k$ esetén A, egyébként 0. A jobb oldalon $\sum_{i=1}^n b_i\cdot A_{ik}$ áll, ami éppen $\mathbf{det}(\mathbf{A}_k)$ kifejtése a k-adik oszlop szerint. Az egyenlet tehát az alábbi roppant bonyolult alakot ölti: $x_k\cdot A=A_k$, amiből $x_k=\frac{A_k}{A}$.

Legyen most $x_k=\frac{A_k}{A}$. Vegyük az i-edik egyenletet és szorozzuk meg A-val: $\sum_{k=1}^n(a_{ik}A_k)=b_iA$. Most $\mathbf{A}_k$-t fejtsük ki a k-adik oszlopa szerint minden k-ra. Azt kapjuk, hogy $\sum_{k=1}^n\left(a_{ik}\cdot\sum_{j=1}^n b_jA_{jk}\right)=b_iA$. Rendezzük ezt át a b_j-k szerint: $\sum_{j=1}^n(b_j\cdot\sum_{k=1}^n a_{ik}\cdot A_{jk})=b_iA$. A bal oldalon b_j együtthatója a kifejtési és ferde kifejtési tételek szerint $j=i$ esetén A, egyébként 0, az egyenlet tehát teljesül. Azaz ha az x_k sorozat az, amit megadtunk, akkor valóban megoldás.

1.9.18 Definíció: az $x\mathbf{A}=b$ egyenletrendszer homogén, ha $b=0$.

1.9.19 Következmény: ha egy n egyenletből álló n ismeretlenes homogén lineáris egyenletrendszer mátrixának determinánsa nem 0, akkor csak triviális megoldása van ($x=0$). Ugyanis csak egy megoldás lehet, $x=0$ pedig nyilván jó.

A Cramer-szabály a gyakorlatban szinte teljességgel alkalmatlan egyenletrendszerek elfogadható idő alatt történő megoldására. Ha erre van szükség, akkor a Gauss -féle eliminációs módszert szokás használni:

Tegyük fel, hogy az egyenletrendszer determinánsa nem 0. Ekkor válasszuk ki egy sorát, melyben x_n együtthatója nem 0. Feltehetjük, hogy ez az utolsó. Vonjuk ki az utolsó sort az összes többiből ennek annyiszorosát, hogy x_n együtthatója mindenütt másutt kiessen (az i-edik sorból $\frac{a_{i1}}{a_{n1}}$-szeresét). A kapott egyenletrendszer ekvivalens lesz az eredetivel. Ezek után az első $n-1$ sorból vegyünk egy olyat, amelyben x_{n-1} együtthatója nem 0 (ha ilyen nincs, akkor az egyenletrendszer determinánsa 0 volt, mert menet közben nem változott – ld. **(D7)** – és egy ilyen egyenletrendszernek feltűnően 0), nevezzük ezt el $(n-1)$-edik sornak, majd ennek segítségével ejtsük ki az x_{n-1}-es tagokat a többi sorból. Folytassuk ezt addig, amíg x_j-nek csak a j-edik sorban lesz nem 0 együtthatója. Az egyenletrendszer i-edik sora ekkor $a^*_{i,i}\cdot x_i=b^*_i$ lesz, amiből x_i meghatározható.

A Lagrange-féle interpolációs feladat: legyenek $a_1,\ldots,a_{n+1}$ egy K test különböző elemei, továbbá $b_1,\ldots,b_{n+1}$ a test tetszőleges elemei. Keressük azon K feletti legfeljebb n-edfokú $f(x)=\sum_{k=0}^n c_kx^k$ polinomokat, melyekre $f(a_i)=b_i$.

1.9.20 Állítás: pontosan egy ilyen polinom van.

Bizonyítás: a fenti jelölésekkel $f(x)$ pontosan akkor megoldás, ha $i\in\{1\ldots n+1\}$ esetén $\sum_{k=0}^n c_ka_i^k=b_i$. Ez egy $n+1$ ismeretlenes, $n+1$ egyenletből álló lineáris egyenletrendszer, amelynek determinánsa egy Vandermonde-determináns, azaz nem 0. A Cramer-szabály szerint tehát pontosan egy ilyen polinom van.