I. POLINOMELMÉLET

1. Polinomok gyökei

Ebben a paragrafusban legyen A integritástartomány, amely valamely K test részgyűrűje.

Definíció. *Azt mondjuk, hogy a $c \in K$ elem az $f(x) \in A[x]$* **polinom gyöke**, *illetve hogy az $f(x) = 0$* **algebrai egyenlet gyöke (megoldása)**, *ha $f(c) = 0$.*

Alapvető fontosságú *Bézout* tétele.

1.1.Tétel. *A $c \in A$ elem az $f(x) \in A[x]$ polinom gyöke akkor és csak akkor, ha $f(x) = (x-c)f_1(x)$ valamely $f_1(x) \in A[x]$ polinom esetén.*

Bizonyítás. Legyen a $c \in A$ elem az $f(x) \in A[x]$ polinom gyöke. Maradékosan osztva a $K[x]$ euklideszi gyűrűben az $f(x)$ polinomot az $x - c$ polinommal kapjuk, hogy

$$f(x) = (x-c)q(x) + r(x) \quad \text{és behelyettesítve} \quad 0 = f(c) = (c-c)q(c) + r(c) = r(c).$$

A maradékos osztás definíciója miatt $r(x)$ konstans polinom, de fent láttuk, hogy $r(c) = 0$. Így szükségképpen $r(x)$ a zérus polinom, azaz $x - c$ osztja $f(x)$-et a $K[x]$ gyűrűben. Azonban az $x - c$ polinom főegyütthatója 1, és a maradékos osztás algoritmusában csak ezzel kell osztani. Emiatt a $q(x)$ hányados együtthatói A-beliek lesznek és $f(x) = (x-c)q(x)$.

Megfordítva, ha $f(x) = (x-c)f_1(x)$ teljesül, ahol $f_1(x) \in A[x]$ akkor

$$f(c) = (c-c)f_1(c) = 0. \qquad \square$$

Az alábbi állítás a gyakorlatban jól használható eljárást ad meg.

1.2.Tétel (Horner-elrendezés). *Legyen $c \in A$ elem, $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n \in A[x]$ polinom, és határozzuk meg a $b_0 = a_0$, $b_k = b_{k-1}c + a_k$ $(k = 1, 2, \ldots, n)$ elemeket, és ezekből a $q(x) = b_0x^{n-1} + \cdots + b_{n-2}x + b_{n-1}$ polinomot. Ekkor*

$$f(x) = (x-c)q(x) + b_n, \qquad f(c) = b_n.$$

Bizonyítás. Teljes indukcióval k-ra $(0 \le k \le n-1)$ belátjuk, hogy

$$(x-c)(b_0x^{n-1} + \cdots + b_kx^{n-1-k}) + b_{k+1}x^{n-1-k} = a_0x^n + \cdots + a_{k+1}x^{n-1-k},$$

ami $k = n-1$-re éppen az első állításunkat adja.

$k = 0$ esetén valóban

$$(x-c)b_0x^{n-1} + b_1x^{n-1} = (x-c)a_0x^{n-1} + (ca_0 + a_1)x^{n-1} = a_0x^n + a_1x^{n-1}.$$

Tegyük fel, hogy igaz az állítás $k-1$-re. Ekkor, az indukciós feltételt alkalmazva,

$$(x-c)(b_0x^{n-1} + \cdots + b_{k-1}x^{n-k} + b_kx^{n-1-k}) + b_{k+1}x^{n-1-k} =$$

$$= a_0x^n + \cdots + a_kx^{n-k} - b_kx^{n-k} + (x-c)b_kx^{n-1-k} + b_{k+1}x^{n-1-k} =$$

$$a_0x^n + \cdots + a_kx^{n-k} - cb_kx^{n-1-k} + (cb_k + a_{k+1})x^{n-1-k} = a_0x^n + \cdots + a_{k+1}x^{n-1-k},$$

és az első állítást beláttuk.

Következésképp $f(c) = (c-c)q(c) + b_n = b_n$. $\square$

Definíció. *A $c \in A$ elemet az $0 \neq f(x) \in A[x]$* **polinom k-szoros gyökének** *nevezzük ($k \geq 1$), ha az $(x-c)^k$ polinom osztja az $f(x)$ polinomot, de az $(x-c)^{k+1}$ polinom már nem osztja az $f(x)$ polinomot az $A[x]$ gyűrűben. Azt is mondjuk ilyenkor, hogy a c gyök* **multiplicitása** *k.*

A következő tételben meghatározzuk, hogy az A integritástartomány feletti polinom hogyan bontható fel szorzatra A-beli gyökeinek ismeretében.

1.3.Tétel. *Legyenek a $0 \neq f(x) \in A[x]$ polinom A-beli gyökei a $c_1, \ldots, c_r$ elemek rendre $k_1, \ldots, k_r$ multiplicitással. Ekkor*

$$f(x) = (x-c_1)^{k_1} \cdots (x-c_r)^{k_r} g(x)$$

valamely $g(x) \in A[x]$ polinom esetén, és $g(c_i) \neq 0$ ($1 \leq i \leq r$). Ezt az alakot $f(x)$ (A feletti) **gyöktényezős felbontásának** *nevezzük. Speciálisan, az $f(x)$ polinom A integritástartománybeli gyökeinek száma multiplicitással együtt nem nagyobb, mint $f(x)$ fokszáma.*

Bizonyítás. Indukció r szerint. $r = 1$-re definíció alapján $f(x) = (x-c_1)^{k_1} f_1(x)$, ahol $f_1(x) \in A[x]$. Ha $f_1(c_1) = 0$ akkor Bézout tétele alapján $x - c_1$ osztja az $f_1(x)$ polinomot az $A[x]$ integritástartományban, következésképp $(x-c_1)^{k_1+1}$ osztja az $f(x)$ polinomot, ellentmondás azzal, hogy a c_1 elem k_1-szeres gyök. Így $f_1(c_1) \neq 0$.

Tegyük fel, hogy igaz az állítás $r-1$-re. Az $r = 1$ eset alapján

$$f(x) = (x-c_1)^{k_1} f_1(x),$$

ahol $f_1(x) \in A[x]$, $f_1(c_1) \neq 0$. Integritástartománybeli oszthatósági szabályok alapján a $c_2, \ldots, c_r$ elem az $f_1(x)$ polinom $k_2, \ldots, k_r$-szeres gyöke. Az indukciós feltételt alkalmazva az $f_1(x)$ polinomra és $c_2, \ldots, c_r$ gyökeire

$$f(x) = (x-c_1)^{k_1} (x-c_2)^{k_2} \cdots (x-c_r)^{k_r} g(x),$$

ahol $g(x) \in A[x]$, és a $c_2, \ldots, c_r$ elem nem gyöke a $g(x)$ polinomnak. Mivel a c_1 elem nem gyöke az $f_1(x)$ polinomnak, szükségképpen a $g(x)$ polinomnak sem. A felbontásban a két oldal fokszámát összehasonlítva kapjuk az A-beli gyökök számára vonatkozó korlátot. □

Lényegesen kihasználtuk azt, hogy a polinom gyökei integritástartománybeliek: nemkommutatív gyűrűben, illetve nem zérusosztómentes gyűrűben nemnulla polinomnak lehet végtelen sok gyöke is.

1.4.Következmény. *Két legfeljebb n-edfokú $A[x]$-beli polinom, amely $n+1$ helyen ugyanazt a helyettesítési értéket veszi fel, megegyezik.*

Bizonyítás. Legyen $f(x), g(x) \in A[x]$ két ilyen polinom. Ekkor az $f(x) - g(x)$ polinom fokszáma legfeljebb n, de van $n+1$ gyöke. Ez 1.3 alapján csak akkor lehet, ha $f(x) - g(x)$ a zérus polinom. □

A következő alapvető fontosságú tételnek sokféle bizonyítása ismert. Legtöbbjük analitikus eszközöket használ.

1.5.Tétel (a klasszikus algebra alaptétele). *Tetszőleges, legalább elsőfokú komplex számok teste feletti polinomnak van komplex gyöke.* □

A bizonyítással itt nem foglalkozunk, de részletesen tekintjük az alaptétel folyományait.

1.6.Következmény.

.1 $\mathbb{C}[x]$ *komplex polinomgyűrű irreducibilis elemei pontosan az elsőfokú polinomok.*

.2 Tetszőleges, legalább elsőfokú komplex polinom sorrendtől és egységtényezőtől eltekintve egyértelműen bontható fel elsőfokú komplex polinomok szorzatára.

.3 Tetszőleges n*-edfokú* ($n \geq 1$) *komplex polinomnak multiplicitással együtt pontosan* n *gyöke van.*

.4 $\mathbb{R}[x]$ *valós polinomgyűrű irreducibilis elemei az összes első és bizonyos másodfokú polinomok; a legalább harmadfokú valós polinomok reducibilisek.*

.5 $\mathbb{Q}[x]$ *racionális polinomgyűrűben vannak tetszőlegesen nagy fokszámú irreducibilis polinomok is.*

Bizonyítás. Az 1,2,3. állítások azonnal adódnak a klasszikus algebra alaptételéből, a gyöktényezős felbontásról szóló tételből és a polinomelmélet alaptételéből.

4. Nyilván az elsőfokú polinomok irreducibilisek, és egy másodfokú valós polinom $\mathbb{R}[x]$-ben irreducibilis pontosan akkor, ha nincs valós gyöke. Például $x^2 - 1$ reducibilis és $x^2 + 1$ irreducibilis.

Emlékezzünk vissza, hogy a $^- : \mathbb{C} \to \mathbb{C}$, $a \mapsto \overline{a}$ konjugálás a komplex számok testének automorfizmusa, amely a valós számokat fixen hagyja.

Indirekte bizonyítunk. Legyen $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n \in \mathbb{R}[x]$ legalább harmadfokú polinom, amely irreducibilis. Bézout tétele alapján nem lehet valós gyöke, de az alaptétel miatt van egy $c \in \mathbb{C} \setminus \mathbb{R}$ komplex gyöke. Belátjuk, hogy a $\overline{c}$ konjugált is gyök. Valóban, felhasználva, hogy a konjugálás automorfizmus és $\overline{a_i} = a_i$,

$$f(\overline{c}) = a_0\overline{c}^n + \cdots + a_{n-1}\overline{c} + a_n = \overline{a_0}\overline{c^n} + \cdots + \overline{a_{n-1}c} + \overline{a_n} =$$

$$\overline{a_0c^n + \cdots + a_{n-1}c + a_n} = \overline{f(c)} = \overline{0} = 0.$$

Mivel c és a konjugáltja is gyök, 1.3 alapján az $(x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c} = x^2 - 2\,\mathrm{Re}(c)x + |c|^2 \in \mathbb{R}[x]$ valós polinom osztja $f(x)$-et $\mathbb{C}[x]$-ben. De elvégezve a maradékos osztás algoritmusát látjuk, hogy a hányados polinom együtthatói is valósak, ami ellentmond annak, hogy $f(x)$ irreducibilis.

5. Schönemann-Eisenstein tétele alapján $n \geq 1$ esetén az $x^n - 2$ polinom irreducibilis $\mathbb{Q}[x]$-ben. □

Vegyük észre, hogy a 2.állítás a polinomelmélet alaptételének felel meg a komplex esetben, és a 4.állítás bizonyítása során beláttuk, hogy ha egy komplex szám valós polinomnak gyöke, akkor a konjugáltja is gyöke a polinomnak.

Az alábbi, *Rolle* nevéhez kötődő tétel alkalmas arra, hogy tetszőleges racionális polinom összes racionális gyökét meghatározzuk kizárólag a négy alapművelet felhasználásával.

1.7.Tétel (Rolle). *Legyen* $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ *egész együtthatós polinom,* r, s *nemnulla relatív prím egész számok. Ha az* $\frac{r}{s}$ *racionális szám az* $f(x)$ *polinom gyöke, akkor* r *osztja* a_n*-et és* s *osztja* a_0*-t.*

Bizonyítás. Szorozva s^n-nel

$$0 = a_0\frac{r^n}{s^n} + \cdots + a_{n-1}\frac{r}{s} + a_n \text{-ből } \; 0 = a_0r^n + a_1r^{n-1}s \cdots + a_{n-1}rs^{n-1} + a_ns^n.$$

A második egyenlőségben az r szám osztja a baloldalt, így osztja a jobboldalt is, de mivel ott az utolsó tag kivételével mind az r szám többszöröse, szükségképp r osztja az a_ns^n számot. A feltétel alapján az r és s^n számok relatív prímek, így r osztja az a_n számot.

Hasonlóan érvelve az s számmal kapjuk, hogy s osztja az a_0 számot. □

Következő állításunk polinom gyökei és együtthatói közötti kapcsolatot adja meg.

1.8.Tétel (Viéte-formulák). *Legyen az* $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in A[x]$ *főpolinom összes* $c_1, \ldots, c_n$ *gyöke a* K *testben. Ekkor*

$$a_1 = -(c_1 + \cdots + c_n)$$

$$a_2 = c_1c_2 + \cdots + c_1c_n + \cdots + c_{n-1}c_n, \quad \ldots,$$

$$a_k = (-1)^k \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} c_{i_1}c_{i_2}\cdots c_{i_k}, \quad \ldots,$$

$$a_n = (-1)^n c_1c_2\cdots c_n.$$

Megfordítva, ha $c_1, \ldots, c_n \in K$ *tetszőleges elemek, és az* $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ *főpolinom* a_i *együtthatóit a fenti formulák adják, akkor* $f(x)$ *összes gyöke* $c_1, \ldots, c_n$.

Bizonyítás. 1.3 alapján $f(x) = (x - c_1)\cdots(x - c_n)$ a gyöktényezős felbontás, így

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = (x - c_1)\cdots(x - c_n).$$

Két polinom pontosan akkor egyenlő, ha megfelelő együtthatóik egyenlőek. Elvégezve a jobb oldalon a műveleteket kapjuk a keresett formulákat.

Megfordítva, legyen $c_1, \ldots, c_n \in K$ és $f(x) \in K[x]$ az a főpolinom, amelynek együtthatóit a fenti formulák adják. $c_1, \ldots, c_n$ az $(x - c_1)\cdots(x - c_n)$ polinom gyöke, amelyről a műveletek elvégzése után látjuk, hogy megegyezik $f(x)$-szel. □

2. Gyökképletek

A valós együtthatós másodfokú egyenlet megoldóképlete jól ismert. A komplex eset (a gyökök komplex számok is lehetnek) analóg.

2.1.Tétel. *Az* $ax^2 + bx + c = 0$ *(*$a, b, c \in \mathbb{C}$, $a \neq 0$*) komplex együtthatós másodfokú algebrai egyenlet komplex gyökei*

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \qquad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

ahol $\sqrt{b^2 - 4ac}$ *a* $b^2 - 4ac$ *komplex szám egyik négyzetgyöke. Ha* a, b, c *valós számok akkor* x_1, x_2 *valósak pontosan akkor, ha* $b^2 - 4ac \ge 0$*; ellenkező esetben* $x_2 = \overline{x_1}$.

Bizonyítás. Viéte formuláiból kapjuk, hogy a két gyök x_1 és x_2:

$$x_1 + x_2 = -\frac{b}{a}, \qquad x_1x_2 = \frac{b^2 - (b^2 - 4ac)}{4a^2} = \frac{c}{a}.$$

A valós egyenletre vonatkozó állítások nyilvánvalóak. □

A másodfokú algebrai egyenlet gyökeit az alábbi módszerrel kerestük meg. Az a számmal osztva kapjuk, hogy $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. A binomiális tételből következik, hogy az $y = x + \frac{b}{2a}$ helyettesítéssel az elsőfokú tag kiküszöbölhető:

$$y^2 - \frac{b^2 - 4ac}{4a^2} = 0,$$

ahonnan gyökvonás és visszahelyettesítés után kapjuk a gyököket.

Térjünk át a harmadfokú esetre. A binomiális tételből következik, hogy az $ax^3 + bx^2 + cx + d = 0$ $(a, b, c, d \in \mathbb{C}, a \neq 0)$ harmadfokú algebrai egyenletből a-val való osztás és $y = x + \frac{b}{3a}$ helyettesítés után a másodfokú tag kiküszöbölhető, azaz az egyenlet $x^3 + px + q = 0$ alakra hozható. Ennek a hiányos egyenletnek a gyökeit felírhatjuk gyökképlettel:

2.2.Tétel (Cardano-képlet). *Legyen $p, q \in \mathbb{C}$ komplex számok, $\varepsilon \in \mathbb{C}$ egy primitív harmadik egységgyök, az*

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

komplex harmadik gyökök legyenek úgy megválasztva, hogy $uv = -\frac{p}{3}$ teljesüljön. Ekkor az $x^3 + px + q = 0$ algebrai egyenlet komplex gyökei

$$x_1 = u + v \quad x_2 = u\varepsilon + v\varepsilon^2 \quad x_3 = u\varepsilon^2 + v\varepsilon.$$

Bizonyítás. Először lássuk be, hogy u és v megválasztható a kívánt módon:

$$uv = \sqrt[3]{\left(\frac{q}{2}\right)^2 - \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3} = \sqrt[3]{-\left(\frac{p}{3}\right)^3} = -\frac{p}{3}\varepsilon^k \quad (k = 0, 1, 2).$$

Felhasználva a jól ismert tulajdonságot, hogy $1 + \varepsilon + \varepsilon^2 = 0$, illetve az $uv = -\frac{p}{3}$ feltételt Viéte formuláiból kapjuk, hogy a három gyök x_1, x_2 és x_3:

$$x_1 + x_2 + x_3 = u(1 + \varepsilon + \varepsilon^2) + v(1 + \varepsilon + \varepsilon^2) = 0,$$

$$x_1x_2 + x_1x_3 + x_2x_3 = x_1(x_2 + x_3) + x_2x_3 =$$

$$= (u + v)\left(u(\varepsilon + \varepsilon^2) + v(\varepsilon + \varepsilon^2)\right) + (u\varepsilon + v\varepsilon^2)(u\varepsilon^2 + v\varepsilon) =$$

$$= -(u + v)^2 + u^2 + v^2 + uv(\varepsilon + \varepsilon^2) = -2uv - uv = -3uv = p,$$

$$x_1x_2x_3 = (u + v)(u\varepsilon + v\varepsilon^2)(u\varepsilon^2 + v\varepsilon) = (u + v)(u^2 + v^2 - uv) =$$

$$= u^3 + v^3 + uv^2 + u^2v - u^2v - uv^2 = u^3 + v^3 = -\frac{q}{2} - \frac{q}{2} = -q. \qquad \square$$

Visszahelyettesítés után az általános harmadfokú eyenlet gyökei is felírhatók gyökképlettel.

Az $x^3 + px + q = 0$ egyenlet gyökeit az alábbi módszerrel kerestük meg. Legyen $x = u + v$. Mivel $(u + v)^3 = u^3 + v^3 + 3uv(u + v)$,

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Legyen $3uv + p = 0$. Ekkor $u^3 + v^3 = -q$ és $u^3v^3 = -\left(\frac{p}{3}\right)^3$. Viéte formulái alapján u^3 és v^3 a

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$$

másodfokú egyenlet (az ún. rezolvens) gyökei. 2.1 miatt a rezolvens gyökei

$$z_{1,2} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},$$

azaz $u^3 = z_1$ és $v^3 = z_2$. A harmadik gyökvonásnál válasszuk meg $u_1 = \sqrt[3]{z_1}$ és $v_1 = \sqrt[3]{z_2}$ értékét úgy, hogy az $uv = -\frac{p}{3}$ feltétel teljesüljön (megtehetjük, hiszen tudjuk, hogy $u^3v^3 = -\left(\frac{p}{3}\right)^3$). A feltétel teljesülése végett a harmadik gyökök további értékeit párosítsuk így: $u_2 = u_1\varepsilon$, $v_2 = v_1\varepsilon^2$, illetve $u_3 = u_1\varepsilon^2$, $v_3 = v_1\varepsilon$. Módszerünkkel megkaptuk a gyököket: $x_i = u_i + v_i$ $(i = 1, 2, 3)$.

Fontos speciális eset az, amikor a p és q együttható valós számok:

2.3.Tétel. *Legyen p és q valós számok, $d = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$, és tekintsük az $x^3 + px + q = 0$ valós együtthatós algebrai egyenletet.*

.1 Ha $d > 0$ akkor egy gyök valós, a másik két gyök nem valós komplex, egymás konjugáltjai.

.2 Ha $d = 0$ akkor mindhárom gyök valós, és legalább kettő egybeesik.

.3 Ha $d < 0$ akkor mindhárom gyök valós.

Bizonyítás. Cardano képlete alapján az egyenlet gyökei

$$x_1 = u + v \quad x_2 = u\varepsilon + v\varepsilon^2 \quad x_3 = u\varepsilon^2 + v\varepsilon,$$

ahol ε egy primitív komplex harmadik egységgyök,

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{d}} \;\; v = \sqrt[3]{-\frac{q}{2} - \sqrt{d}}$$

úgy, hogy $uv = -\frac{p}{3}$.

1. Mivel $d > 0$, $-\frac{q}{2} \pm \sqrt{d}$ valós szám, és u választható valósnak. Ekkor v is valós szám mivel uv is valós, és az $x_1 = u + v$ gyök valós. $d > 0$ miatt $u \neq v$ és

$$x_2 - \overline{x_2} = (u\varepsilon + v\varepsilon^2) - (u\varepsilon^2 + v\varepsilon) = u(\varepsilon - \varepsilon^2) + v(\varepsilon^2 - \varepsilon) =$$

$$= (u - v)(\varepsilon - \varepsilon^2) \neq 0,$$

azaz x_2 nem valós komplex szám. Nyilván $x_3 = \overline{x_2}$ konjugált sem valós.

2. Ha $d = 0$ akkor u választható valós számnak, ekkor v is valós mivel uv is valós. Következésképpen $u = v$,

$$x_1 = 2u \in \mathbb{R}, \quad x_2 = x_3 = u(\varepsilon + \varepsilon^2) = -u \in \mathbb{R}.$$

3. Ha $d < 0$ akkor legyen u a három $\sqrt[3]{-\frac{q}{2} + i\sqrt{-d}}$ köbgyök közül az egyik. Mivel a köbgyökök alatt konjugáltak állnak, azonnal látható, hogy a $v = \overline{u}$ konjugált a három $\sqrt[3]{-\frac{q}{2} - i\sqrt{-d}}$ köbgyök közül valamelyik, és

$$uv = u\overline{u} = |u|^2 = \sqrt[3]{\left(\frac{q}{2}\right)^2 - d} = \sqrt[3]{-\left(\frac{p}{3}\right)^3} = -\frac{p}{3}.$$

Így mindhŕom gyök valóban valós:

$$x_1 = u + \overline{u} = 2\,\mathrm{Re}\, u \in \mathbb{R}, \;\; x_2 = u\varepsilon + \overline{u\varepsilon} = 2\,\mathrm{Re}\, u\varepsilon \in \mathbb{R}, \;\; x_3 = u\varepsilon^2 + \overline{u\varepsilon^2} = 2\,\mathrm{Re}\, u\varepsilon^2 \in \mathbb{R}. \qquad \square$$

Nevezetes tény, hogy az $ax^4 + bx^3 + cx^2 + dx + e = 0$ $(a, b, c, d, e \in \mathbb{C}, a \neq 0)$ negyedfokú algebrai egyenletnek is van gyökképlete, azonban ezt nem tárgyaljuk. Felmerül a kérdés, hogy van-e gyökképlete (bizonyos, jól meghatározott értelemben) az ötöd- illetve a magasabbfokú általános algebrai egyenletnek. Erre a kérdésre nemleges választ ad *Ruffini-Abel* tétele.

3. Többszörös gyökök, reciprok egyenlet

Bizonyos speciális magasabbfokú algebrai egyenletek megoldhatók gyökképlettel. két ilyen esetet tárgyalunk ebben a paragrafusban.

Definíció. *Legyen K test, $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n \in K[x]$ polinom. Az $f'(x) = na_0x^{n-1} + \cdots + 2a_{n-2}x + a_{n-1}$ polinomot az $f(x)$ polinom* **deriváltjának** *nevezzük.*

Ez a definíció összhangban va a polinomfüggvények analízisbeli deriváltjával. Egyszerűen látható, hogy a megszokott tulajdonságok teljesülnek az összeg-, skalárszoros- illetve a szorzatpolinom deriváltjára:

$$(\lambda f(x) + \mu g(x))' = \lambda f'(x) + \mu g'(x); \qquad (f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

Egy gyök többszörös voltát jellemezhetjük a deriválttal.

3.1.Tétel. *Legyen K test, $0 \neq f(x) \in K[x]$ polinom, a $c \in K$ elem, az $f(x)$ polinom gyöke. Ekkor a c gyök többszörös (azaz legalább kétszeres) gyöke $f(x)$-nek pontosan akkor, ha c gyöke az $f'(x)$ deriváltpolinomnak is.*

Bizonyítás. A $K[x]$ test fölötti polinomgyűrűben osszuk el maradékosan az $f(x)$ polinomot az $(x-c)^2$ polinommal:

$$f(x) = (x-c)^2 f_1(x) + (x-c)r + s,$$

ahol $f_1(x) \in K[x], r, s \in K$. Az $f(c) = 0$ feltétel miatt $s = 0$, és

$$f(x) = (x-c)^2 f_1(x) + (x-c)r, \quad f'(x) = 2(x-c)f_1(x) + (x-c)^2 f_1'(x) + r, \quad f'(c) = r,$$

ahonnan kapjuk, hogy az $(x-c)^2$ polinom osztja az $f(x)$ polinomot pontosan akkor, ha $f'(c) = r = 0$, ami a többszörös gyök definíciója miatt az állításunkat adja. □

3.2.Állítás. *Legyen $0 \neq f(x) \in \mathbb{C}[x]$ komplex polinom, $k \geq 2$ természetes szám. Ha a c komplex szám az $f(x)$ polinom k-szoros gyöke, akkor c az $f'(x)$ deriváltpolinom $k-1$-szeres gyöke.*

Bizonyítás. Ha c szám k-szoros gyök, akkor $f(x) = (x-c)^k f_1(x)$, ahol $f_1(x)$ komplex polinom és $f_1(c) \neq 0$. Így

$$f'(x) = k(x-c)^{k-1} f_1(x) + (x-c)^k f_1'(x) = (x-c)^{k-1}(kf_1(x) + (x-c)f_1'(x)).$$

Nyilván az $(x-c)^{k-1}$ polinom osztja az $f'(x)$ deriváltpolinomot, de $kf_1(c) + (c-c)f_1'(c) = kf_1(c) \neq 0$ miatt az $(x-c)^k$ polinom már nem osztja az $f'(x)$ deriváltpolinomot. □

Definíció. *Legyen $f(x), g(x) \in \mathbb{C}[x]$. Azt mondjuk, hogy $c \in \mathbb{C}$ az $f(x), g(x)$* **polinomok közös gyöke**, *ha $f(c) = g(c) = 0$.*

Közvetlenül kapjuk az alábbi állítást:

3.3.Állítás. *A $0 \neq f(x), g(x)$ komplex polinomoknak létezik közös komplex gyöke akkor és csak akkor, ha a $d(x) = \text{lnko}(f(x), g(x))$ legnagyobb közös osztó legalább elsőfokú.* □

A többszörös gyökök alábbi jellemzése alapján megkísérelhetjük magasabbfokú algebrai egyenleteknél a többszörös gyökök kiszűrését.

3.4.Tétel. *Legyen $0 \neq f(x) \in \mathbb{C}[x]$ komplex polinom. Ekkor az alábbi állítások teljesülnek:*

.1 az $f(x)$ polinomnak létezik többszörös gyöke akkor és csak akkor, ha a $d(x) = \text{lnko}(f(x), f'(x))$ legnagyobb közös osztó legalább elsőfokú.

.2 a $d(x)$ polinom gyökei az $f(x)$ polinom többszörös gyökei, eggyel kisebb multiplicitással.

.3 az $\frac{f(x)}{d(x)}$ polinom gyökei megegyeznek az $f(x)$ polinom gyökeivel, de mindegyik egyszeres.

Bizonyítás. 1. Nyilvánvaló 3.1-ből és 3.3-ból.

2,3. Legyen

$$f(x) = (x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_r)^{k_r}f_1(x),$$

ahol a $k_i \geq 2$ számok a többszörös gyökök multiplicitásai, $f_1(c_i) \neq 0$ és az $f_1(x)$ polinomnak már nincsenek többszörös gyökei. 3.2 alapján

$$f'(x) = (x-c_1)^{k_1-1}(x-c_2)^{k_2-1}\cdots(x-c_r)^{k_r-1}h(x),$$

ahol a $h(x)$ polinom és az $x-c_i$ gyöktényezők relatív prímek, továbbá 3.1 miatt a $h(x)$ és az $f_1(x)$ polinom szintén relatív prím. Következésképp

$$d(x) = (x-c_1)^{k_1-1}(x-c_2)^{k_2-1}\cdots(x-c_r)^{k_r-1},$$

$$\frac{f(x)}{d(x)} = (x-c_1)(x-c_2)\cdots(x-c_r)f_1(x). \qquad \square$$

Most térjünk át a másik speciális magasabbfokú egyenlettípusra.

Definíció. *Legyen $f(x)$ komplex polinom. Azt mondjuk, hogy az $f(x)=0$ egyenlet* **reciprok egyenlet***, ha teljesül az alábbi két feltétel:*

a.) ha a c komplex szám gyöke az egyenletnek, akkor az $\frac{1}{c}$ reciproka is gyöke;

b.) a c és $\frac{1}{c}$ gyök multiplicitása megegyezik.

A gyökök ismerete nélkül is el tudjuk dönteni, hogy egy egyenlet reciprok egyenlet-e.

3.5.Tétel. *Az $a_0x^n + \cdots + a_{n-1}x + a_n = 0$ ($a_i \in \mathbb{C}$) egyenlet reciprok egyenlet akkor és csak akkor, ha*

az együtthatók vagy szimmetrikusak, azaz $a_0 = a_n, a_1 = a_{n-1}, \ldots,$

vagy antiszimmetrikusak, azaz $a_0 = -a_n, a_1 = -a_{n-1}, \ldots$

Bizonyítás. Az egyenlet reciprok egyenlet pontosan akkor, ha

$$a_0x^n + \cdots + a_{n-1}x + a_n = a_0(x-c_1)(x-c_2)\cdots(x-c_n) = a_0(x-\frac{1}{c_1})(x-\frac{1}{c_2})\cdots(x-\frac{1}{c_n}),$$

ami, a_0-lal való leosztás után, Viéte formulái alapján, illetve közös nevezőre hozva, majd ismét Viéte formulái alapján, ekvivalens azzal, hogy

$$\frac{a_1}{a_0} = -(c_1+\cdots+c_n) = -(\frac{1}{c_1}+\cdots+\frac{1}{c_n}) = -\frac{c_2\cdots c_n + c_1c_3\cdots c_n + \cdots + c_1\cdots c_{n-1}}{c_1\cdots c_n} =$$

$$= \frac{a_{n-1}/a_0}{a_n/a_0} = \frac{a_{n-1}}{a_n}, \ \ldots,$$

$$\frac{a_k}{a_0} = (-1)^k \sum_{1\leq i_1<\cdots<i_k\leq n} c_{i_1}\cdots c_{i_k} = (-1)^k \sum_{1\leq i_1<\cdots<i_k\leq n} \frac{1}{c_{i_1}\cdots c_{i_k}} =$$

$$= (-1)^k \frac{1}{c_1\cdots c_n} \sum_{1\leq i_1<\cdots<i_{n-k}\leq n} c_{i_1}\cdots c_{i_{n-k}} = \frac{a_{n-k}/a_0}{a_n/a_0} = \frac{a_{n-k}}{a_n}, \ \ldots,$$

és végül

$$\frac{a_n}{a_0} = (-1)^n c_1\cdots c_n = (-1)^n \frac{1}{c_1\cdots c_n} = \frac{a_0}{a_n},$$

ami pontosan azt jelenti, hogy $(\frac{a_n}{a_0})^2 = 1$, azaz $\frac{a_n}{a_0} = \pm 1$, $a_0 = \pm a_n$. A fenti $\frac{a_k}{a_0} = \frac{a_{n-k}}{a_n}$ egyenlőségekbe ezt beírva kapjuk, hogy $a_k = \pm a_{n-k}$, azaz az együtthatók vagy szimmetrikusak, vagy antiszimmetrikusak. $\square$

3.6.Következmény. *Az $f(x) = 0$ komplex együtthatós n-edfokú egyenlet reciprok egyenlet akkor és csak akkor, ha $f(x) = \pm x^n f(\frac{1}{x})$ (az előjel pozitív illetve negatív annak megfelelően, hogy az egyenlet együtthatói szimmetrikusak illetve antiszimmetrikusak). Továbbá,*

1. *ha n páratlan és az együtthatók szimmetrikusak, akkor $f(-1) = 0$ (az „$x + 1$ eset”);*
2. *ha n páratlan és az együtthatók antiszimmetrikusak, akkor $f(1) = 0$ (az „$x - 1$ eset”);*
3. *ha n páros és az együtthatók antiszimmetrikusak, akkor $f(1) = f(-1) = 0$ (az „$x^2 - 1$ eset”).*

Bizonyítás. A tétel első állítása nyilvánvaló 3.5-ből, x^n-t kiemelve. A másik háromból lássuk be az elsőt, a többi hasonlóan igazolható.

Legyen n páratlan és az együtthatók szimmetrikusak. A fenti jellemzés alapján $f(-1) = (-1)^n f(\frac{1}{-1}) = -f(-1)$ azaz $2f(-1) = 0$, ahonnan nyilván $f(-1) = 0$ következik. □

3.7.Állítás. *Legyen $f(x) = 0$ reciprok egyenlet. Ekkor a páratlan szimmetrikus, páratlan antiszimmetrikus illetve a páros antiszimmetrikus esetekben az $x + 1$, $x - 1$, illetve az $x^2 - 1$ gyöktényezőkkel egyszerűsítve az $f(x) = 0$ egyenletet páros fokszámú szimmetrikus egyenletet kapunk.*

Bizonyítás. A paritásra vonatkozó állítás világos. A szimmetriára vonatkozó három eset közül lássuk be az elsőt, a többi hasonlóan igazolható:

$$f_1(x) = \frac{f(x)}{x+1} = \frac{x^n f(\frac{1}{x})}{x+1} = \frac{x^{n-1} f(\frac{1}{x})}{1+\frac{1}{x}} = x^{n-1} f_1(\frac{1}{x}),$$

azaz 3.6 jellemzése alapján az $\frac{f(x)}{x+1}$ polinom együtthatói szimmetrikusak. □

Könnyen látható, hogy a $2n$ fokszámú szimmetrikus egyenlet x^n-nel való leosztás után az $y = x + \frac{1}{x}$ új ismeretlen bevezetésével visszavezethető n-edfokúra. Tegyük fel, hogy az $y_1, \dots, y_n$ gyököket meghatároztuk (például, ha $n \leq 4$, gyökképlet segítségével.) Ekkor az $y_i = x + \frac{1}{x}$ $(1 \leq i \leq n)$ egyenletet beszorozva x-szel kapjuk a másodfokú $x^2 - y_i x + 1 = 0$ egyenletet, amelynek x_{2i-1}, x_{2i} gyökeit a gyökképletből kapjuk. Viéte formulái alapján $x_{2i-1} x_{2i} = 1$, azaz valóban x_{2i-1} és x_{2i} egymás reciprokai.

4. A többhatározatlanú polinomgyűrű

Ebben a paragrafusban legyen A egy integritástartomány.

Definíció. *Legyen $x_1, \dots, x_n$ határozatlan, $A[x_1]$ a szokásos egyhatározatlanú polinomgyűrű. Legyen*

$$A[x_1, x_2] = (A[x_1])[x_2], \dots, A[x_1, \dots, x_n] = (A[x_1, \dots, x_{n-1}])[x_n].$$

*Ekkor $A[x_1, \dots, x_n]$-t n-**határozatlanú polinomgyűrű**nek nevezzük.*

4.1.Tétel. *Az $A[x_1, \dots, x_n]$ n-határozatlanúM polinomgyűrű integritástartomány.*

Bizonyítás. Az állítás következik abból a jól ismert tételből, hogy integritástartomány feletti egyhatározatlanú polinomgyűrű integritástartomány. □

Az $A[x_1, \dots, x_n]$ n-határozatlanúM polinomgyűrű elemei az $f(x_1, \dots, x_n)$ n-határozatlanú polinomok. Az $x_1^{k_1} \cdots x_n^{k_n}$ $(k_i \geq 0, x_i^0 = 1)$ alakú elemeket **egytag**oknak, a $k_1 + \cdots + k_n$ számot az **egytag fokszámának**, az $k_1 + 2k_2 + \cdots + nk_n$ számot az **egytag súlyának** nevezzük. Minden n-határozatlanú polinom egytagok A-lineáris kombinációja. **Polinom fokszáma** illetve **súlya** alatt értjük a benne szereplő egytagok fokszámának illetve súlyának maximumát. Polinomok összeadásának elvégzése világos, a szorzást az egytagok szorzásának

$$x_1^{k_1} \cdots x_n^{k_n} \cdot x_1^{l_1} \cdots x_n^{l_n} = x_1^{k_1+l_1} \cdots x_n^{k_n+l_n}$$

szabálya és a disztributív törvények alapján végezhetjük el.

Emlékezzünk vissza, hogy egy H halmaz esetén az összes $H \to H$ bijektív leképezés, azaz H permutációi halmazát $\mathrm{Sym}(H)$-val, $H = \{1, 2, \dots, n\}$ esetén S_n-nel jelöltük. S_n a kompozíciószorzás műveletére nézve csoportot alkot, az n-edfokú szimmetrikus csoportot, elemeinek száma $n!$.

Definíció. *Legyen $\pi \in S_n$ permutáció, $\widetilde{\pi} : A[x_1, \dots, x_n] \to A[x_1, \dots, x_n]$, $f(x_1, \dots, x_n) \mapsto f(x_{\pi(1)}, \dots, x_{\pi(n)})$. Az $f(x) \in A[x_1, \dots, x_n]$ polinomot* **szimmetrikus polinom***nak nevezzük, ha minden $\pi \in S_n$ permutáció esetén $\widetilde{\pi}(f(x)) = f(x)$. Az*

$$s_1(x_1, \dots, x_n) = x_1 + \dots + x_n,$$

$$s_2(x_1, \dots, x_n) = x_1x_2 + x_1x_3 + \dots + x_1x_n + \dots + x_{n-1}x_n, \ \dots,$$

$$s_k(x_1, \dots, x_n) = \sum_{1 \le i_1 < \dots < i_k \le n} x_{i_1} \cdots x_{i_k}, \ \dots,$$

$$s_n(x_1, \dots, x_n) = x_1 \cdots x_n$$

*polinomokat n-***határozatlanú elemi szimmetrikus polinomok***nak nevezzük.*

A Viéte-formulák a fenti jelöléssel így írhatók: $a_k = (-1)^k s_k(c_1, \dots, c_n)$. Nyilván $x_n = 0$ helyettesítéssel $s_k(x_1, \dots, x_{n-1}, 0)$ $(1 \le k \le n-1)$ az összes $n-1$-határozatlanú elemi szimmetrikus polinom. Ha $f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ akkor az elemi szimmetrikus polinomok $x_k = s_k$ behelyettesítése után kapott $f(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n))$ polinom szimmetrikus, foka megegyezik $f(x_1, \dots, x_n)$ súlyával. Ennek az állításnak a megfordítása lesz az alaptétel.

4.2.Tétel. *Az $A[x_1, \dots, x_n]$ n-határozatlanúM polinomgyűrűben a szimmetrikus polinomok részgyűrűt alkotnak.*

Bizonyítás. Legyen $\pi \in S_n$ permutáció, $\widetilde{\pi} : A[x_1, \dots, x_n] \to A[x_1, \dots, x_n]$, $f(x_1, \dots, x_n) \mapsto f(x_{\pi(1)}, \dots, x_{\pi(n)})$. Könnyen látható, hogy $\widetilde{\pi}$ gyűrűk homomorfizmusa.

Valóban, be kell látni, hogy szimmetrikus polinomok összege, additív inverze és szorzata is szimmetrikus polinom. Ha f és g szimmetrikus polinom, akkor tetszőleges $\pi \in S_n$ esetén

$$\widetilde{\pi}(f+g) = \widetilde{\pi}(f) + \widetilde{\pi}(g) = f + g, \quad \widetilde{\pi}(-f) = -\widetilde{\pi}(f) = -f,$$

$$\widetilde{\pi}(fg) = \widetilde{\pi}(f)\widetilde{\pi}(g) = fg. \qquad \square$$

4.3.Tétel (szimmetrikus polinomok alaptétele). *Legyen $f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ m-edfokú szimmetrikus polinom. Ekkor egyértelműen létezik $g(y_1, \dots, y_n) \in A[y_1, \dots, y_n]$ m súlyú polinom úgy, hogy $f(x_1, \dots, x_n) = g\left(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)\right)$.*

Bizonyítás. Alkalmazzuk az alábbi jelöléseket:

$$\underline{x} = x_1, \dots, x_n \quad \underline{y} = y_1, \dots, y_n$$

$$s_k = s_k(x_1, \dots, x_n)\ (1 \le k \le n), \quad s_k^0 = s_k(x_1, \dots, x_{n-1}, 0)\ (1 \le k \le n-1).$$

Egzisztencia. Indukció n és m szerint. Ha $n = 1$ akkor tetszőleges m-re $f(x_1) = f(s_1(x_1))$ mivel $s_1(x_1) = x_1$. Tegyük fel, hogy n-nél kisebb határozatlanú szimmetrikus polinomokra igaz az állítás. Az n-határozatlanú esetben m szerinti indukciót alkalmazunk. $m = 0$-ra nyilvánvaló, tegyük fel, hogy m-nél kisebb fokszámú szimmetrikus polinomokra igaz az állítás.

Legyen $f(\underline{x})$ m-edfokú szimmetrikus polinom. Az indukciós feltétel szerint

$$f(x_1,\dots,x_{n-1},0)=g_1(s_1^0,\dots,s_{n-1}^0),$$

ahol $g_1(y_1,\dots,y_{n-1})\in A[y_1,\dots,y_{n-1}]$ m-nél nem nagyobb súlyú, és az előző észrevétel alapján s_k^0 $(1\le k\le n-1)$ az összes $n-1$-határozatlanú elemi szimmetrikus polinom. Következésképp $g_1(s_1,\dots,s_{n-1})$ foka legfeljebb m, és

$$f_1(\underline{x})=f(\underline{x})-g_1(s_1,\dots,s_{n-1})$$

m-nél nem nagyobb fokszámú szimmetrikus polinom. Mivel $f_1(x_1,\dots,x_{n-1},0)=0$, nyilván x_n osztja az $f_1(\underline{x})$ polinomot. De $f_1(\underline{x})$ szimmetrikus, így az $s_n=x_1\cdots x_n$ elemi szimmetrikus polinom is osztja az $f_1(\underline{x})$ polinomot, azaz

$$f_1(\underline{x})=s_nf_2(\underline{x}),$$

ahol $f_2(\underline{x})$ legfeljebb $m-n$ fokszámú szimmetrikus polinom. Ezért az indukciós feltétel alapján létezik legfeljebb $m-n$ súlyú $g_2(\underline{y})$ polinom úgy, hogy

$$f_2(\underline{x})=g_2(s_1,\dots,s_n).$$

Világos, hogy

$$g(\underline{y})=g_1(y_1,\dots,y_{n-1})+y_ng_2(\underline{y})$$

súlya legfeljebb m, és $f(\underline{x})=g(s_1,\dots,s_n)$ miatt a súly pontosan m.

Unicitás. Tegyük fel, hogy létezik $g_1(\underline{y})$, $g_2(\underline{y})$ különböző polinom úgy, hogy

$$f(\underline{x})=g_1(s_1,\dots,s_n)=g_2(s_1,\dots,s_n).$$

Ekkor $(g_1-g_2)(s_1,\dots,s_n)=0$ és $g_1-g_2\neq 0$. Indukcióval n szerint belátjuk, hogy ha $g(\underline{y})\neq 0$ akkor $g(s_1,\dots,s_n)\neq 0$ (0 a zérus polinomot jelöli).

$n=1$-re az állítás világos, tegyük fel, hogy igaz n-nél kisebb határozatlanú polinomokra. Legyen $g(\underline{y})$ a legkisebb fokszámú nemzérus polinom, hogy $g(s_1,\dots,s_n)=0$. Nyilván

$$g(\underline{y})=g_0(y_1,\dots,y_{n-1})+g_1(y_1,\dots,y_{n-1})y_n+\cdots+g_k(y_1,\dots,y_{n-1})y_n^k. \qquad (*)$$

Ha $g_0(y_1,\dots,y_{n-1})=0$ akkor $g(\underline{y})=h(y_1,\dots,y_n)y_n$, azaz

$$0=g(s_1,\dots,s_n)=h(s_1,\dots,s_n)s_n,$$

amiből 4.1 miatt $h(s_1,\dots,s_n)=0$ következik, ellentmodásban azzal, hogy $h(\underline{y})$ fokszáma eggyel kisebb, mint $g(\underline{y})$ fokszáma, hiszen feltettük, hogy $g(\underline{y})$ a legkisebb fokszámú ilyen polinom.

Azaz $g_0(y_1,\dots,y_{n-1})\neq 0$. (*)-ból $y_k=s_k$ majd $x_n=0$ helyettesítéssel $g_0(s_1^0,\dots,s_{n-1}^0)=0$ adódik, ellentétben az indukciós feltétellel.

□

4.4.Következmény. *Legyen K test, az $f(x)\in K[x]$ polinom összes gyöke $c_1,\dots,c_n$, amelyek valamely N testben vannak, amelynek K részteste. Ha $h(x_1,\dots,x_n)\in K[x_1,\dots,x_n]$ tetszőleges szimmetrikus polinom, akkor $h(c_1,\dots,c_n)\in K$.*

Bizonyítás. Alkalmazzuk 4.3 bizonyításának jelöléseit. 4.3 miatt $h(\underline{x})=g(s_1,\dots,s_n)$, ahol $g(\underline{y})\in K[\underline{y}]$. Mivel $f(\underline{x})\in K[\underline{x}]$, Viéte formulái alapján $s_k(c_1,\dots,c_n)\in K$ minden $1\le k\le n$-re. Következésképp

$$h(c_1,\dots,c_n)=g\left(s_1(c_1,\dots,c_n),\dots,s_n(c_1,\dots,c_n)\right)\in K. \qquad \square$$

II. CSOPORTELMÉLET

5. A csoport fogalma

Definíció. *Legyen $G \neq \emptyset$ egy halmaz, $* : G \times G \to G$ művelet a G halmazon. A $(G, *)$ algebrai struktúrát* **félcsoport***nak nevezzük, ha a $*$ művelet asszociatív. Ha a $(G, *)$ félcsoportban létezik neutrális elem, akkor a $(G, *)$ struktúrát* **monoid***nak nevezzük. Azt mondjuk, hogy a $(G, *)$ monoid* **csoport***, ha G minden elemének létezik inverze a $*$ műveletre nézve. Ha a $(G, *)$ csoportban a $*$ művelet kommutatív, akkor a $(G, *)$ struktúrát* **kommutatív vagy Abel-csoport***nak nevezzük.*

A $(G, +)$ additív csoportban, azaz ahol a csoportművelet a $+$ összeadás, a neutrális elemet **nullelemnek** *nevezzük és 0-val jelöljük, továbbá az $a \in G$ inverz elemét $-a$-val jelöljük.*

A $(G, \cdot)$ multiplikatív csoportban, azaz ahol a csoportművelet a $\cdot$ szorzás, a neutrális elemet **egységelemnek** *nevezzük és 1-gyel jelöljük, továbbá az $a \in G$ elem inverzét a^{-1}-gyel jelöljük.*

A G halmaz számosságát a **csoport rendjének** *nevezzük, és* **véges***, ill.* **végtelen csoport***ról beszélünk aszerint, hogy a számosság véges ill. végtelen.*

Az, hogy a $(G, *)$ rendezett pár csoport, részletesen azt jelenti, hogy:
- $G \neq \emptyset$ egy halmaz;
- $* : G \times G \to G$ egy leképezés;
- $a * (b * c) = (a * b) * c$ minden $a, b, c \in G$ elemre;
- létezik $e \in G$ elem úgy, hogy $a * e = e * a = a$ minden $a \in G$ elem esetén;
- minden $a \in G$ elemhez létezik $a' \in G$ elem úgy, hogy $a * a' = a' * a = e$.

A továbbiakban, ha másképpen nem jelezzük, a csoportművelet a szorzás lesz, amelyet egymásutánírással jelölünk, és $(G, \cdot)$ csoport helyett röviden G csoportról beszélünk.

Az asszociativitás legegyszerűbb következményei az alábbiak.

5.1. Állítás. *Legyen $(G, \cdot)$ félcsoport. Ekkor:*

.1 Tetszőleges számú tényezőből álló szorzat értéke független a zárójelezéstől.

.2 Ha G monoid, egyetlen neutrális elem van G-ben, és ha az $a \in G$ elemnek létezik a^{-1} inverze, akkor az egyértelmű.

.3 G invertálható elemei (az úgynevezett **egyégek***), csoportot alkotnak (a G monoid úgynevezett* **egységcsoport***ját), amelyet $U(G)$-vel jelölünk.*

Bizonyítás. 1. Legyen az $a_1, \dots, a_n \in G$ elemek tetszőlegesen zárójelezett szorzata t_n, és legyen $l_n = (\dots((a_1a_2)a_3)\dots)a_n$ a balrarendezett szorzat. Indukcióval n szerint belátjuk, hogy $t_n = l_n$. $n = 3$ esetén az állítás éppen a szorzás asszociativitása. Tegyük fel, hogy n-nél kisebb tényezős szorzatok ($n > 3$) tetszőlegesen zárójelezhetők. Ha $t_n \neq l_n$ akkor $t_n = t_k u$, ahol u az $a_{k+1}, \dots, a_n$ elemek valamely szorzata. Indukció alapján $t_k = l_k$ és $u = a_{k+1}(a_{k+2}(\dots(a_{n-1}a_n)\dots))$, azaz az asszociativitás többszöri alkalmazásával

$$t_n = l_k(a_{k+1}(a_{k+2}(\dots(a_{n-1}a_n)\dots))) = (l_ka_{k+1})(a_{k+2}(a_{k+3}(\dots(a_{n-1}a_n)\dots))) =$$

$$l_{k+1}(a_{k+2}(\dots(a_{n-1}a_n)\dots)) = \dots = l_{n-2}(a_{n-1}a_n) = l_{n-1}a_n = l_n.$$

2. Legyen e, f neutrális elem. Ekkor mivel f neutrális elem, $ef = e$, de mivel e is neutrális elem, $ef = f$, azaz $e = f$. Ha $aa^{-1} = a^{-1}a = e$ és $ab = ba = e$, akkor $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}e = a^{-1}$.

3. Ha a neutrális elem e, $g, h \in U(G)$, inverzeik g^{-1}, h^{-1}, akkor $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$, és hasonlóan $(h^{-1}g^{-1})(gh) = e$, azaz gh is invertálható

elem, és $U(G)$ a szorzásra nézve zárt, és így algebrai struktúra. Nyilván $e \in U(G)$, és a szorzás asszociativitása öröklődik, vagyis $U(G)$ monoid. A $gg^{-1} = g^{-1}g = e$ tulajdonság szimmetriája miatt g^{-1} inverze g, és $U(G)$ csoport. $\square$

Csoportokra számtalan példát ismerünk. Néhány ezek közül:

1. Végtelen Abel-csoportok a végtelen gyűrűk additív csoportjai: $(\mathbb{Z}, +)$ az egész számok additív csoportja, $(\mathbb{Q}, +)$, a racionális számok additív csoportja, $(\mathbb{R}, +)$ a valós számok additív csoportja, $(\mathbb{C}, +)$ a koimplex számok additív csoportja, $(\mathbb{Z}[x], +)$ az egész együtthatós polinomok additív csoportja, $(\mathbb{Q}[x], +)$ a racionális együtthatós polinomok additív csoportja, $(\mathbb{R}[x], +)$ a valós együtthatós polinomok additív csoportja, $(\mathbb{C}[x], +)$ a komplex együtthatós polinomok additív csoportja, $(M_n(\mathbb{R}), +)$ a valós matrixok additív csoportja.
2. Végtelen Abel-csoportok a végtelen test feletti véges (nemnulla) dimenziós, illetve a végtelen dimenziós vektorterek additív csoportjai: $(\mathbb{R}^n, +)$ a valós rendezett szám n-esek additív csoportja, $Z_p[x]$ a p prímelemű test feletti polinomok additív csoportja.
3. Végtelen Abel-csoportok a végtelen K testek (azaz multiplikatív félcsoportjaik) $U(K) = K \setminus \{0\}$ egység- (multiplikatív) csoportjai, pld. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
4. Véges Abel-csoportok a véges K testek $U(K) = K \setminus \{0\}$ multiplikatív csoportjai, például $K = Z_p$ p prímelemű test, az egészek maradékosztálygyűrűje modulo p;
5. Lehet véges Abel csoport egy végtelen integritástartomány (azaz az integritástartomány multiplikatív félcsoportjának) egységcsoportja: $U(\mathbb{Z}) = \{-1, 1\}$, $U(Z_p[x]) = Z_p \setminus \{0\}$;
6. $n > 2$ esetén véges nem-Abel csoport az $\{1, 2, \ldots, n\}$ elemek összes ismétlés nélküli permutációinak $(S_n, \circ)$ csoportja, az **n-edfokú szimmetrikus csoport**, amelynek rendje $n!$, ahol a csoportművelet a leképezések $\circ$ kompozíciószorzása;
7. $n > 1$ esetén véges illetve végtelen nem-Abel csoport az $M_n(K)$ véges illetve végtelen K test feletti ($K = Z_p$ illetve $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$) teljes matrixgyűrű (multiplikatív félcsoportjának) $\mathrm{GL}_n(K)$ egységcsoportja, az ún. **teljes lineáris csoport**, amelynek elemei az invertálható, azaz nemnulla determinánsú matrixok. Véges nemkommutatív csoport a szabályos n-szög ($n \geq 3$) szimmetriáinak (a síkidomot önmagára képező egybevágósági transzformációinak) csoportja, a $2n$ edrendű D_n diédercsoport, amelyet n elforgatás és n tükrözés alkot, és ahol a csoportművelet a leképezések kompozíciószorzása.
8. Legyen A egy halmaz, az úgynevezett **ábécé**, elemei a **betűk**. Képezzünk a betűkből (véges hossszú) szavakat, ezek közötti művelet legyen a **konkatenáció**, az egymásutánírás, amelyet asszociatívnak tekintünk. Kaptuk az úgynevezett **szabad félcsoportot**. Bővítsük ki az A ábécét újabb betűkkel az $A \cup A^{-1}$ ábécévé, ahol $A^{-1} = \{a^{-1} | \, a \in A\}$. Tekintsük az $A \cup A^{-1}$ ábécé betűiből képzett szavak W halmazát, amelybe beleértjük az üres szót is. Egy W-beli szót **redukált alakú**nak nevezünk, ha benne nem áll egymás mellett a illetve a^{-1} alakú betű. Tetszőleges W-beli szóhoz tartozik redukált alakú szó, az aa^{-1} illetve $a^{-1}a$ alakú szórészletek helyébe az üres szót írva, esetleg több lépésben. Legyen F a redukált alakú szavak halmaza (az üres szóval együtt). Két F-beli szó konkatenáltja legyen az egymásutánírt szó (ami W eleme) redukált alakja (ez már biztosan F-beli), a konkatenációt ismét asszociatívnak tekintve. Ekkor a konkatenáció művelet a redukált alakú szavak F halmazán, amely erre a műveletre nézve csoport (ellenőrizze!), amelyet az A ábécé feletti **szabad csoport**nak nevezünk.

Definíció. *Legyen $(G, *)$ csoport, $H \subseteq G$ részhalmaz. Ha a H halmaz csoport a $*$ leképezésnek a $H \times H$ szorzathalmazra történő leszűkítésére nézve, akkor azt mondjuk, hogy H a G* **részcsoportja**. *Az e neutrális elemből álló egyelemű $\{e\}$ részcsoportot* **triviális részcsoport***nak nevezzük.*

A részstruktúra fogalmával már találkoztak, például a vektorterek esetén: ott a részstruktúra a lineária altér. Speciálisan a lineáris altér a vektorok additív csoportjának részcsoportja is. Egyéb példák:

.1 A páros számok a $(\mathbb{Z}, +)$ csoport részcsoportját alkotják. Azok a törtek, amelyeknek nevezője 2-hatvány, a racionális számok $(\mathbb{Q}, +)$ additív csoportjának részcsoportját alkotják. Az $a_1 + a_2\sqrt{2}$ alakú valós számok halmaza, ahol $a_1, a_2 \in \mathbb{Q}$, a valós számok $(\mathbb{R}, +)$ csoportjának részcsoportja. A racionális valós és képzetes résszel rendelkező komplex számok halmaza a komplex számok $(\mathbb{C}, +)$ csoportjának részcsoportja.

.2 A 2 egész kitevős hatványai a nemnulla racionális számok $U(\mathbb{Q})$ multiplikatív csoportjának részcsoportját alkotják. Az $a_1 + a_2\sqrt{2}$ alakú nemnulla valós számok halmaza, ahol $a_1, a_2 \in \mathbb{Q}$, a nemnulla valós számok $U(\mathbb{R})$ multiplikatív csoport részcsoportját alkotják. A nemnulla komplex számok $U(\mathbb{C})$ multiplikatív csoportjának részcsoportjai: az olyan (nemnulla) komplex számok halmaza, amelyeknek argumentuma fokban kifejezve egész szám; az 1 abszolútértékű komplex számok; az n-edik komplex egységgyökök $(n \geq 2)$.

A részcsoport tulajdonság könnyen ellenőrizhető:

5.2.Állítás. *A G csoport $\emptyset \neq H \subseteq G$ részhalmaza részcsoport akkor és csak akkor, ha $a^{-1}b \in H$ minden $a, b \in H$ elem esetén.*

Bizonyítás. Ha H részcsoport, akkor zárt a szorzásra és az inverzképzésre nézve, és nyilván $a^{-1}b \in H$ minden $a, b \in H$ esetén.

Megfordítva, legyen $a \in H$ tetszőleges elem. Ekkor $a^{-1}a = 1 \in H$, $a^{-1}1 = a^{-1} \in H$, és ha $b \in H$ akkor $(a^{-1})^{-1}b = ab \in H$. Mivel az asszociativitás öröklődik, beláttuk, hogy H csoport. □

5.3.Állítás. *Legyen G csoport. Ha $I \neq \emptyset$ egy halmaz, H_i $(i \in I)$ a G részcsoportja akkor a $\cap_{i\in I} H_i$ metszet is részcsoport. Továbbá, ha A a G halmaz részhalmaza, akkor $\langle A\rangle = \cap\{H$ részcsoportja a Gcsoportnak $\mid A \subseteq H\}$ részcsoport, a legszűkebb részcsoportja a G csoportnak, amely tartalmazza az A részhalmazt.*

Bizonyítás. Legyen $H = \cap_{i\in I} H_i$. Mivel minden i-re $1 \in H_i$, $1 \in H$ és $H \neq \emptyset$. Alkalmazzuk 5.2-t. Ha $a, b \in H$ akkor minden i-re $a, b \in H_i$. H_i részcsoport volta miatt $a^{-1}b \in H_i$ minden i-re, és $a^{-1}b \in H$. A másik állítás most már nyilvánvaló. □

Definíció. *Az $\langle A\rangle$ részcsoportot az A* **részhalmaz által generált csoport***nak nevezzük, és azt is mondjuk, hogy A a $\langle A\rangle$* **csoport generátorrendszere***.*

Könnyen látható, hogy

$$\langle A\rangle = \{a_1^{\delta_1} a_2^{\delta_2} \cdots a_l^{\delta_l} \mid a_i \in A,\ \delta_i \in \{1, -1\},\ l \in \mathbb{N}^+\}.$$

Az egész számok additív csoportját generálja az $\{1\}$ egyelemű halmaz, az ilyen csoportokra a következő paragrafusban visszatérünk. A nemnulla racionális számok multiplikatív csoportjának nincsen véges generátorrendszere.

6.Lagrange tétele. Ciklikus csoport.

Definíció. *Legyen G csoport, H részcsoportja. Ha $a \in G$, akkor az*

$$aH = \{ah \mid h \in H\} \text{ ill. } Ha = \{ha \mid h \in H\}$$

halmazokat a H részcsoport a elem szerinti **bal- illetve jobboldali mellékosztály***ainak, a halmazok $|aH|$ ill. $|Ha|$ számosságát a* **mellékosztályok rendjének** *nevezzük.*

A mellékosztályokkal már találkoztak a lineáris algebrában: a V vektortér $a + H$ lineáris sokasága a vektorok $(V, +)$ additív csoportja H részcsoportjának mellékosztálya. További példák:

1. Az egész számok $(\mathbb{Z}, +)$ csoportjában a páros számok részcsoportjának két mellékosztálya van: a páros illetve a páratlan számok halmaza. A $\mathbb{Z}$ részcsoport mellékosztályai a racionális számok $(\mathbb{Q}, +)$ additív csoportjában $r + \mathbb{Z}$ alakúak, $0 \leq r < 1$ racionális szám, azaz egy mellékosztályban az ugyanannyi törtrészű racionális számok vannak.
2. a nemnulla komplex számok $U(\mathbb{C})$ csoportjában az 1 hosszú komplex számok E részcsoportjának mellékosztályai rE alakúak, ahol r pozitív valós szám, rE elemei az r hosszú komplex számok.

A mellékosztályok alapvető tulajdonságai a következők.

6.1.Állítás. *Legyen G csoport, H részcsoportja. Ekkor:*

1. *$aH = bH$ akkor és csak akkor, ha $b \in aH$;*
2. *az $\{aH \mid a \in G\}$ baloldali mellékosztályok a G halmaz osztályozását adják;*
3. *hasonló állítások érvényesek a jobboldali mellékosztályokra is.*

Bizonyítás. 1. Legyen $aH = bH$. Ekkor $b = b1 \in bH = aH$.

Megfordítva, legyen $b \in aH$. Ekkor $b = aw$ valamely $w \in H$ elemre, és $a = bw^{-1}$. Ha $ah \in aH$ akkor $ah = (bw^{-1})h = b(w^{-1}h) \in bH$, azaz $aH \subseteq bH$. Ha $bh \in bH$ akkor $bh = (aw)h = a(wh) \in aH$, azaz $bH \subseteq aH$.

2. $a = a1 \in aH$ miatt $G = \cup_{a \in G} aH$. Az első állítás miatt pedig ha $c \in aH \cap bH$ akkor $cH = aH$ és $cH = bH$, azaz $aH = bH$.

3. Nyilvánvaló. □

Alapvető tulajdonságokat ad meg az

6.2.Tétel (Lagrange). *Legyen G véges csoport, H részcsoportja. Ekkor:*

1. *$|aH| = |bH|$ és $|aH| = |Hb|$ minden $a, b \in G$ elem esetén;*
2. *a H részcsoport rendje osztja a G részcsoprt rendjét;*
3. *a H részcsoport szerinti bal- és jobboldali mellékosztályok száma megegyezik, amelyet a H* **részcsoport G-beli indexének** *nevezünk és $|G : H|$-val jelölünk;*
4. *$|G| = |H| \cdot |G : H|$.*

Bizonyítás. 1. Legyen $\varphi : aH \to bH, ah \mapsto bh$ leképezés. φ nyilván szürjektív. Legyen $\varphi(ah_1) = \varphi(ah_2)$, azaz $bh_1 = bh_2$. Szorozva b^{-1}-gyel balról kapjuk, hogy $h_1 = h_2$, és $ah_1 = ah_2$. Beláttuk, hogy φ injektív. Így φ bijekció. Hasonlóan látható be, hogy a $\psi : aH \to Hb$, $ah \mapsto hb$ leképezés is bijekció.

2,3,4. Az első állítást összevetve 6.1.2-vel és 6.2.3-mal kapjuk, hogy az összes mellékosztály rendje megegyezik a $|H|$ renddel, és a bal- ill. a jobboldali mellékosztályok száma $\frac{|G|}{|H|} = |G : H|$. □

Definíció. *Legyen G csoport. Ha létezik, az $a \in G$* **elem rendjének** *nevezzük azt a legkisebb n pozitív egészet, amelyre $a^n = 1$, ebben az esetben az $n = |a|$ jelölést alkalmazzuk és azt mondjuk, hogy a* **végesrendű elem**. *Ellenkező esetben* **végtelenrendű elem***ről beszélünk. Ha a G csoportnak létezik egyelemű $\{a\}$ generátorrendszere, akkor* **ciklikus csoport***nak nevezzük és a $G = \langle a \rangle$ jelölést alkalmazzuk.*

A nemnulla racionális számok multiplikatív csoportjában az 1-et és a -1-et kivéve minden elem végtelen rendű; az összes komplex egységgyök csoportjában minden elem végesrendű. Az $\langle a \rangle$ ciklikus csoport véges ill. végtelen rendű aszerint, hogy az a elem véges ill. végtelen rendű, továbbá $|\langle a \rangle| = |a|$. A véges esetben $\langle a \rangle = \{1, a, a^2, \dots, a^{|a|-1}\}$, a végtelen esetben $\langle a \rangle = \{1, a, a^{-1}, a^2, a^{-2}, \dots, a^n, a^{-n}, \dots\}$.

Végtelen ciklikus csoportra példa $(\mathbb{Z}, +) = \langle 1 \rangle = \{0, 1, -1, 2, -2, \dots, n, -n, \dots\}$, véges n-edrendűre $(Z_n, +) = \langle 1 \rangle = \{0, 1, 2, \dots, n-1\}$, illetve az n-edik komplex egységgyökök multiplikatív csoportja,melynek generátora bármely primitív n-edik komplex egységgyök.

6.3.Következmény. *Véges csoport elemének rendje osztja a csoport rendjét.*

Bizonyítás. Véges csoport a elemének $|a|$ rendje szükségképpen véges, és mivel $|a| = |\langle a \rangle|$, az állítás 6.2.2 miatt világos. □

A végesrendű elemek két egyszerű tulajdonsága az alábbi.

6.4.Lemma. *Legyen G csoport, $a \in G$, $|a| = n \in \mathbb{N}^+$ végesrendű elem. Ekkor:*
1. *ha $t \in \mathbb{Z}$ egész szám és $a^t = 1$ akkor n osztja t-t;*
2. *ha $k \in \mathbb{N}^+$ pozitív egész akkor $|a^k| = \frac{n}{\text{lnko}(k,n)}$.*

Bizonyítás. 1. Legyen $t = rn + q$, $0 \le q < n$ maradékos osztás. Ekkor $1 = a^t = a^{rn+q} = (a^n)^r a^q = a^q$, ami $q < n$ miatt csak akkor lehetséges, ha $q = 0$, azaz $t \mid n$.

2. Legyen $|a^k| = l$, $\frac{n}{\text{lnko}(k,n)} = m$. Mivel $(a^k)^{\frac{n}{\text{lnko}(k,n)}} = (a^n)^{\frac{k}{\text{lnko}(k,n)}} = 1$, az első állítás miatt $l \mid m$. Továbbá, $1 = (a^k)^l = a^{kl}$ miatt $n \mid kl$, amiből $m = \frac{n}{\text{lnko}(k,n)} \mid \frac{k}{\text{lnko}(k,n)} l$. Nyilván m és $\frac{k}{\text{lnko}(k,n)}$ relatív prímek, és így kaptuk, hogy $m \mid l$. □

A paragrafus utolsó tétele a ciklikus csoportokról szól.

6.5.Tétel.
1. *Prímszámrendű csoport ciklikus.*
2. *Ciklikus csoport tetszőleges részcsoportja ciklikus.*
3. *Legyen G véges n-edrendű ciklikus csoport, l az n rendet osztó pozitív egész. Ekkor a G csoportban egy és csak egy l-edrendű részcsoport létezik.*
4. *Legyen $\langle a \rangle$ véges n-edrendű ciklikus csoport, $k \in \mathbb{N}^+$ pozitív egész. Ekkor $\langle a \rangle = \langle a^k \rangle$ akkor és csak akkor, ha k és n relatív prímek. Emiatt az n-edrendű ciklikus csoport generátorainak száma $\varphi(n)$, ahol φ az Euler-féle függvény.*

Bizonyítás. 1. A G p prímszámrendű csoportban 6.3 miatt az elemek rendje 1 vagy p. Mivel $G \neq \{1\}$, lennie kell p rendű elemnek, amely által generált részcsoport rendje p, vagyis az egész G.

2. Legyen H nemtriviális részcsoportja a $G = \langle a \rangle$ ciklikus csoportnak, $l = \min\{i \in \mathbb{N}^+ \mid a^i \in H\}$. Belátjuk, hogy $H = \langle a^l \rangle$. Az $\langle a^l \rangle \subseteq H$ tartalmazás világos. Legyen $a^i \in H$, $i = lq + r$, $0 \le r < l$ maradékos osztás. Ekkor $a^i = a^{lq+r} = (a^l)^q a^r \in H$, ahonnan $a^r \in H$ következik. Mivel l minimális, ez csak $r = 0$ esetén lehetséges, azaz $a^i = (a^l)^q \in \langle a^l \rangle$, és a másik $H \subseteq \langle a^l \rangle$ tartalmazás is teljesül.

3. Egzisztencia. Legyen $G = \langle a \rangle$. 6.4.2 miatt az $\langle a^{\frac{n}{l}} \rangle$ részcsoport rendje l. Az unicitás a második állítás konstrukciójából nyilvánvaló.

4. 6.4.2 miatt az a^k elem rendje n akkor és csak akkor, ha a k és n számok relatív prímek. Az ilyen $0 \leq k \leq n-1$ számok száma éppen $\varphi(n)$. $\square$

7. Nevezetes részcsoportok

Nemkommutatív csoportban lényeges az elemek közötti úgynevezett konjugáltsági reláció, és az ehhez a fogalomhoz szorosan kapcsolódó speciális részcsoport, a normálosztó.

Definíció. *Legyen G csoport, $a, b \in G$, N részcsoportja a G csoportnak. Ha létezik $g \in G$ elem úgy, hogy $b = g^{-1}ag$, akkor azt mondjuk, hogy a b elem az a* **elem konjugáltja**. *Ha minden $g \in G$ elemre $gN = Ng$, akkor az N részcsoportot a G csoport* **normális részcsoport***jának vagy* **normálosztó***jának nevezzük.*

A konjugátsággal kapcsolatos legfontosabb tulajdonság az alábbi.

7.1.Állítás. *A konjugáltsági reláció ekvivalencia reláció a G halmazon, amelynek ekvivalencia osztályait* **konjugált osztályok***nak nevezzük.*

Bizonyítás. Reflexivitás. Nyilván $1^{-1}a1 = a$.
Szimmetria. Ha $b = g^{-1}ag$ akkor $a = gbg^{-1} = (g^{-1})^{-1}bg^{-1}$.
Tranzitivitás. Ha $b = g^{-1}ag$ és $c = h^{-1}bh$ akkor $c = (h^{-1}g^{-1})a(gh) = (gh)^{-1}a(gh)$. $\square$

A normális részcsoportokat jellemezhetjük az alábbi módon.

7.2.Tétel. *Legyen G csoport, N a G csoport részcsoportja. Ekkor az alábbi állítások ekvivalensek:*
(i) *N normálosztó a G csoportban;*
(ii) *$g^{-1}ag \in N$ tetszőleges $a \in N$, $g \in G$ elemre;*
(iii) *az N halmaz konjugált osztályok uniójaként áll elő.*

Bizonyítás. (i)$\Longrightarrow$(ii) Mivel $ag \in gN = Ng$, $ag = ga_1$ valamely $a_1 \in N$ elem esetén, azaz $g^{-1}ag = g^{-1}ga_1 = a_1 \in N$.
(ii)$\Longrightarrow$(iii) Nyilvánvaló.
(iii)$\Longrightarrow$(i) Lássuk be először, hogy a $gN \subseteq Ng$ tartalmazás teljesül. Legyen $ga \in gN$ tetszőleges elem. Ekkor $gag^{-1} = a_1 \in N$ és $a = g^{-1}a_1g$ teljesül, így kapjuk, hogy $ga = gg^{-1}a_1g = a_1g \in Ng$.
Most lássuk be, hogy a másik irányú $Ng \subseteq gN$ tartalmazás teljesül. Legyen $ag \in Ng$. Ekkor $g^{-1}ag = a_2 \in N$ és $a = ga_2g^{-1}$, így $ag = ga_2g^{-1}g = ga_2 \in gN$. $\square$

Abel-csoport tetszőleges részcsoportja normálosztó. A D_n diédercsoportban az elforgatások 2-indexű részcsoportot alkotnak, amely normálosztó, mivel teljesül az alábbi állítás: 2 indexű részcsoport normálosztó. Valóban, legyen a G csoportban H 2-indexű részcsoport. Ha $g \in G \setminus H$, 6.1.2 és 6.1.3 miatt $G = H \cup gH = H \cup Hg$, azaz $gH = G \setminus H = Hg$. Ha $g \in H$, akkor nyilván $gH = H = Hg$. További példa 2-indexű részcsoportra az S_n szimmetrikus csoportban a páros permutációk részcsoportja, amely így normálosztó (lásd lentebb). A $\mathrm{GL}_n(K)$ teljes lineáris csoportban normálosztót alkotnak az 1 determinánsú matrixok, az úgynevezett speciális lineáris csoportot.

Két fontos speciális részcsoport a centralizátor és a centrum.

Definíció. *Legyen G csoport, $H \subseteq G$ részhalmaz. Azt mondjuk, hogy a*

$$C_G(H) = \{c \in G \mid hc = ch \text{ minden } h \in H\text{-ra}\}$$

halmaz a H részhalmaz **centralizátora** *a G csoportban. Speciálisan, a $C_G(G)$ halmazt a G csoport* **centrumának** *nevezzük és $\zeta(G)$-vel jelöljük.*

A $\zeta(G)$ centrum G azon elemeinek a halmaza, amelyek minden elemmel felcserélhetőek. Mivel ha c centrumbeli elem és $g \in G$ akkor $g^{-1}cg = c$, a centrum az egyelemű konjugált osztályok uniója. Nyilván G Abel-csoportban $\zeta(G) = G$. Az S_n szimmetrikus csoportban ($n \geq 3$) és a D_p (p páratlan prím) diédercsoportban a centrum az egyelemű triviális részcsoport. A $\mathrm{GL}_n(K)$ teljes lineáris csoportban a centrum a skaláris matrixok csoportja.

A centralizátor és a centrum legegyszerűbb tulajdonságait foglalja össze a

7.3.Tétel. *Legyen G csoport, H részhalmaza a G halmaznak. Ekkor:*
.1 a $C_G(H)$ centralizátor a G csoport részcsoportja;
.2 $\zeta(G)$ centrum a G csoport normálosztója;
.3 Ha a G csoport véges, akkor a G csoport a eleme konjugált osztályának a rendje megegyezik a $C_G(\{a\}) = C_G(a)$ centralizátor indexével a G csoportban.

Bizonyítás. 1. Nyilván $1 \in C_G(H)$, így az nemüres halmaz, alkalmazzuk az 5.2 állítást. Legyen $a, b \in C_G(H)$, $h \in H$. Ekkor $a^{-1}bh = a^{-1}hb = a^{-1}(ha)a^{-1}b = a^{-1}(ah)a^{-1}b = ha^{-1}b$, azaz $a^{-1}b \in C_G(H)$.

2. Az első állítás miatt a centrum részcsoport, és mivel az egyelemű konjugált osztályok uniója, a 7.2 állításból kapjuk, hogy normálosztó.

3. $g^{-1}ag = h^{-1}ah$ pontosan akkor, ha $(gh^{-1})a = a(gh^{-1})$, azaz $g \in C_G(a)h$. Ez 6.1 alapján akkor és csak akkor teljesül, ha $C_G(a)g = C_G(a)h$, ahonnan az állítás következik. □

8. Faktorcsoport, homomorfizmus

A normálosztó segítségével konstruálhatunk egy új, egyszerűbb csoportot.

8.1.Tétel. *Legyen G csoport, N a G csoport normálosztója, $G/N = \{aN \mid a \in G\}$ a mellékosztályok halmaza. Ekkor G/N csoport az $(aN)(bN) = abN$ műveletre nézve, ezt a csoportot a G csoport N normálosztó szerinti* **faktorcsoport***jának nevezzük.*

Bizonyítás. Lássuk be először, hogy a G/N halmazon a szorzás jóldefiniált. Legyen $aN = cN$, $bN = dN$. Ekkor 6.1 miatt $c \in aN$, $d \in bN$, $c = ag_1$, $d = bg_2$ valamely $g_1, g_2 \in N$ elemre. Így $cd = ag_1bg_2 = ab(b^{-1}g_1b)g_2 \in abN$ 7.2 alapján, és ismét 6.1 miatt $cdN = abN$, azaz $(cN)(dN) = cdN = abN = (aN)(bN)$.

Asszociativitás. A G csoportbeli asszociativitást alkalmazva $aN(bNcN) = (aN)(bcN) = a(bc)N = (ab)cN = (abN)(cN) = (aNbN)cN$.

Nyilván N neutrális elem, és aN inverze $a^{-1}N$. □

Csoportok közötti speciális leképezések a homomorfizmusok, azaz olyan leképezések, ahol a leképezés és a művelet sorrendje felcserélhető.

Definíció. *Legyen $(G, *)$ és $(H, \circ)$ csoport. A $\varphi : G \to H$ leképezést* **homomorfizmus***nak nevezzük, ha minden $a, b \in G$ elemre $\varphi(a * b) = \varphi(a) \circ \varphi(b)$. Az injektív homomorfizmust* **monomorfizmus***nak, a szürjektívet* **epimorfizmus***nak, a bijektívet* **izomorfizmus***nak, a $G \to G$ izomorfizmust* **automorfizmus***nak nevezzük. Ha létezik $G \to H$ izomorfizmus, akkor azt mondjuk, hogy G és H* **izomorf csoportok***, és a $G \cong H$ jelölést alkalmazzuk. Ha $\varphi : G \to H$ homomorfizmus és H neutrális eleme e, akkor a $\mathrm{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e\}$ halmazt a φ* **homomorfizmus magjának** *nevezzük.*

Homomorfizmusokkal már találkoztunk a lineáris algebrában: vektortér lineáris transzformációja az additív csoport homomorfizmusa. További példák:

1. A determinánsfüggvény az általános lineáris csoport epimorfizmusa a test egységcsoportjába, magja az 1 determinánsú matrixok részcsoportja.
2. A $(\mathbb{Z},+)\to(\mathbb{Z},+)$, $a\mapsto ma$ leképezés monomorfizmusa az egészek additív csoportjának, képe az $m\mathbb{Z}$ részcsoport. Az $U(\mathbb{C})\to U(\mathbb{C})$, $a\mapsto a^n$ ($n>1$ egész) leképezés a nemnulla komplex számok multiplikatív csoportjának epimorfizmusa, magja az n-edik komplex egységgyökök részcsoportja. A $(\mathbb{Z},+)\to(\mathbb{Z}_m,+)$, $a\mapsto\overline{a}$ leképezés epimorfizmus az egészek és a modulo m maradékosztályok additív csoportjai között, magja $m\mathbb{Z}=\langle m\rangle$.
3. A $\cong$ izomorfia reláció ekvivalencia reláció, ekvivalencia osztályait a csoportok izomorfiaosztályainak nevezzük. Izomorf csoportok adott n számra az n-edrendű ciklikus csoportok, például a modulo n maradékosztályok $(Z_n,+)$ csoportja és az n-edik komplex egységgyökök multiplikatív csoportja. Izomorf csoportok továbbá az S_3 szimmetrikus csoport és a D_3 diédercsoport, amint azt a szabályos háromszög szimmetriáinak permutáció-prezentációja mutatja. Két n-elemű halmaz permutációinak csoportjai izomorfak. Abel-csoport automorfizmusa az inverzképzés. A komplex konjugálás a a komlex számok $(\mathbb{C},+)$ additív csoportjának és a nemnulla komplex számok $U(\mathbb{C})$ csoportjának automorfizmusa is. Tetszőleges G csoport automorfizmusa adott $g\in G$ elemre az $x\mapsto g^{-1}xg$ konjugálás (ami Abel-esetben az identikus leképezés).

A homomorfizmusok legalapvetőbb tulajdonságait taglalja a

8.2.Állítás. *Legyen G és H csoport, $\varphi:G\to H$ homomorfizmus, $g\in G$ tetszőleges elem. Ekkor:*

.1 $\varphi(1)=1$*;*

.2 $\varphi(g^{-1})=\varphi(g)^{-1}$*;*

.3 ha A a G csoport részcsoportja akkor a $\varphi(A)$ képe a H csoport részcsoportja;

.4 a $\mathrm{Ker}(\varphi)$ *mag a G csoport normálosztója;*

.5 φ monomorfizmus akkor és csak akkor ha $\mathrm{Ker}(\varphi)=\{1\}$.

Bizonyítás. 1. A $\varphi(g)=\varphi(1g)=\varphi(1)\varphi(g)$ egyenlőséget beszorozva $\varphi(g)^{-1}$-gyel jobbról kapjuk, hogy $1=\varphi(1)$.

2. Az előző állítást felhasználva $1=\varphi(1)=\varphi(gg^{-1})=\varphi(g)\varphi(g^{-1})$, ezt az egyenlőséget beszorozva $\varphi(g)^{-1}$-gyel balról kapjuk, hogy $\varphi(g)^{-1}=\varphi(g^{-1})$.

3. Nyilván 1. miatt $1=\varphi(1)\in\varphi(A)=B$, így ez nemüres halmaz. Alkalmazzuk az 5.2 állítást; legyen $b,d\in B$. Ekkor létezik $a,c\in A$ elem úgy, hogy $b=\varphi(a)$, $d=\varphi(c)$, és 2-t felhasználva $b^{-1}d=\varphi(a^{-1})\varphi(c)=\varphi(a^{-1}c)\in B$, hiszen $A\le G$ miatt $a^{-1}c\in A$.

4. Az 1.állítás miatt $1\in\mathrm{Ker}(\varphi)$, így ez nemüres halmaz. Alkalmazzuk az 5.2 állítást, hogy belássuk, $\mathrm{Ker}(\varphi)$ részcsoportja a G csoportnak. Legyen $a,b\in\mathrm{Ker}(\varphi)$. Ekkor $\varphi(a^{-1}b)=\varphi(a)^{-1}\varphi(b)=1\cdot 1=1$, és $a^{-1}b\in\mathrm{Ker}(\varphi)$.

Ha $g\in G, a\in\mathrm{Ker}(\varphi)$ akkor $\varphi(g^{-1}ag)=\varphi(g)^{-1}\varphi(a)\varphi(g)=\varphi(g)^{-1}\varphi(g)=1$, azaz $g^{-1}ag\in\mathrm{Ker}(\varphi)$, és 7.2 alapján $\mathrm{Ker}(\varphi)$ normálosztó.

5. Ha φ monomorfizmus, akkor nyilván $\mathrm{Ker}(\varphi)=\{1\}$. Megfordítva, ha $\varphi(a)=\varphi(b)$ akkor $1=\varphi(a)\varphi(b)^{-1}=\varphi(ab^{-1})\in\mathrm{Ker}(\varphi)=\{1\}$, azaz $ab^{-1}=1$, $a=b$. □

Nagyjelentőségű az alábbi

8.3.Tétel. *Legyen G, H csoport, $\varphi:G\to H$ homomorfizmus.*

.1 **(homomorfia-tétel)** *A* $G/\mathrm{Ker}(\varphi)$ *faktorcsoport és az* $\mathrm{Im}(\varphi)$ *kép izomorfak.*

.2 Ha N a G csoport normálosztója akkor a $\psi:G\to G/N$, $a\mapsto aN$ leképezés epimorfizmus, amelyet **természetes epimorfizmus***nak nevezünk.*

Bizonyítás. 1. Jelölje N a $\mathrm{Ker}(\varphi)$ magot, és legyen $\widetilde{\varphi}:G/N\to\mathrm{Im}(\varphi)$, $aN\mapsto\varphi(a)$ leképezés. Lássuk be először, hogy $\widetilde{\varphi}$ jóldefiniált. Legyen $aN=bN$, ekkor $a^{-1}b\in N$, és $1=\varphi(a^{-1}b)=\varphi(a)^{-1}\varphi(b)$ miatt $\varphi(a)=\varphi(b)$.

Nyilván $\widetilde{\varphi}(aNbN) = \widetilde{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \widetilde{\varphi}(a)\widetilde{\varphi}(b)$ miatt a $\widetilde{\varphi}$ leképezés homomorfizmus. Világos, hogy szürjektív. Ha $aN \in \operatorname{Ker}\widetilde{\varphi}$ akkor $1 = \widetilde{\varphi}(aN) = \varphi(a)$ miatt $a \in \operatorname{Ker}(\varphi) = N$, és $aN = N$. 8.2.5 alapján a $\widetilde{\varphi}$ leképezés injektív.

2. $\psi(ab) = abN = aNbN = \psi(a)\psi(b)$ miatt ψ homomorfizmus. A szürjektivitás nyilvánvaló. □

A $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ leképezés, amely 0-t rendel a páros és 1-et rendel a páratlan számokhoz, az egészek és a modulo 2 maradékosztálygyűrű additív csoportjai közötti epimorfizmus, magja a páros számok $2\mathbb{Z}$ csoportja. Így a $\mathbb{Z}/2\mathbb{Z}$ faktorcsoport másodrendű ciklikus csoport.

A $\varphi : \mathbb{Q} \to [0,1) \cap \mathbb{Q}$ leképezés, amely a racionális számhoz a törtrészét rendeli, az additív csoportok epimorfizmusa (a képnél az összeadást „modulo 1" kell érteni), magja az egész számok csoportja, így a $\mathbb{Q}/\mathbb{Z}$ csoport izomorf a racionális számok modulo 1 vett additív csoportjával.

A deriválás epimorfizmusa a $K[x]$ polinomgyűrű additív csoportjának, magja a test additív csoportja, így a $K[x]/K$ és a $K[x]$ csoportok izomorfak.

Az $U(\mathbb{C}) \to U(\mathbb{C})$, $a \mapsto a^n$ ($n > 1$ egész) leképezés a nemnulla komplex számok multiplikatív csoportjának epimorfizmusa, magja az n-edik komplex egységgyökök E_n részcsoportja, így az $U(\mathbb{C})/E_n$ és az $U(\mathbb{C})$ csoportok izomorfak.

A nemnulla komplex számok és a pozitív valós számok multiplikatív csoportja között az abszolútérték képzése epimorfizmus, magja az 1 hosszú komplex számok C_1 csoportja, így az $U(\mathbb{C})/C_1$ fakorcsoport izomorf a $\mathbb{R}^+$ multiplikatív csoporttal.

9. Permutációk

A csoportelmélet alkalmazásainál fontos a szimmetrikus csoport, amelynek elemeit az alább ismertetendő módon rendszerezhetjük.

9.1.Állítás. *Legyen $\mathcal{N} = \{1, 2, \dots, n\}$ halmaz, a $\sigma : \mathcal{N} \to \mathcal{N}$ permutáció az S_n n-edfokú szimmetrikus csoport eleme, és*

$$\Sigma = \{(i,j) \in \mathcal{N} \times \mathcal{N} \mid \textit{létezik } l \in \mathbb{Z} : j = \sigma^l(i)\}$$

Ekkor Σ ekvivalencia reláció az N halmazon, amely ekvivalencia osztályairól azt mondjuk, hogy a σ **permutáció pályái**.

Bizonyítás. Reflexivitás. σ^0 az identikus permutáció, és minden $i \in \mathcal{N}$ számra $\sigma^0(i) = i$.

Szimmetria. Legyen $(i,j) \in \Sigma$. Ekkor $j = \sigma^l(i)$, és mivel a σ^l leképezés inverze σ^{-l}, $i = \sigma^{-l}(j)$, azaz $(j,i) \in \Sigma$.

Tranzitivitás. Legyen $(i,j) \in \Sigma$, $(j,k) \in \Sigma$. Ekkor $j = \sigma^l(i)$ és $k = \sigma^m(j)$, és $\sigma^{l+m}(i) = \sigma^m(j) = k$ miatt $(i,k) \in \Sigma$. □

Definíció. *A σ permutáció pályájának számosságát a* **pálya hosszának**, *az 1 hosszúakat* **triviális pályák***nak nevezzük. Az egyetlen nemtriviális pályával rendelkező permutációt* **ciklus***nak, a nemtriviális pályája hosszát a* **ciklus hosszának** *nevezzük. A 2 hosszú ciklusokat* **transzpozíciók***nak nevezzük. Azt mondjuk, hogy két ciklus* **diszjunkt**, *ha nemtriviális pályáik diszjunktak.*

Legyen $\sigma \in S_n$ l hosszú ciklus és $\{i_1, i_2, \dots, i_l\}$ a nemtriviális pályája úgy, hogy $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \dots, \sigma(i_{l-1}) = i_l$. Nyilván $\sigma(i_l) = i_1$, és ekkor a $\sigma = (i_1\, i_2 \dots i_l)$ jelölést alkalmazzuk. Világos, hogy $(i_1\, i_2 \dots i_l) = (i_2\, i_3 \dots i_l\, i_1) = \dots = (i_l\, i_1\, i_2 \dots i_{l-1})$ és a σ permutáció rendje l. A permutációkat előállíthatjuk a következő módon.

9.2.Tétel. *Minden $1 \neq \sigma \in S_n$ permutáció sorrendtől eltekintve egyértelműen bontható fel diszjunkt ciklusok szorzatára.*

Bizonyítás. Legyen a σ permutáció egy pályája $P = \{i_1, i_2, \dots, i_l\}$ úgy, hogy $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \dots, \sigma(i_{l-1}) = i_l$ Ekkor nyilván a σ permutáció ugyanúgy hat a P pálya elemein, mint az $(i_1\, i_2 \dots i_l)$ ciklus.

Mivel a P_j pályák az $\{1, 2, \dots, n\}$ halmaz osztályozását adják, és a σ permutáció ugyanúgy hat a P_j pálya elemein, mint valamely σ_j ciklus, $\sigma = \sigma_1\sigma_2\cdots\sigma_r$, ahol a σ_j permutációk egyértelműen meghatározott diszjunkt ciklusok, amelyek egymással felcserélhetőek. □

9.3.Következmény.

.1 A ciklusok generálják az S_n csoportot;

.2 A transzpozíciók generálják az S_n csoportot;

.3 Ha a $\sigma \in S_n$ permutáció diszjunkt ciklusok szorzatára való felbontása $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ akkor $|\sigma| = \mathrm{lkkt}(|\sigma_1|, \dots, |\sigma_r|)$.

Bizonyítás. 1. 9.2 alapján minden permutáció ciklusok szorzata.

2. Nyilvánvaló 1-ből és abból, hogy $(i_1\, i_2 \dots i_l) = (i_1\, i_2)(i_2\, i_3)\cdots(i_{l-1}\, i_l)$.

3. Legyen $m = \mathrm{lkkt}(|\sigma_1|, \dots, |\sigma_r|)$. Mivel diszjunkt ciklusok egymással felcserélhetőek,

$$\sigma^m = (\sigma_1\sigma_2\cdots\sigma_r)^m = \sigma_1^m\sigma_2^m\cdots\sigma_r^m = 1\cdot 1\cdots 1 = 1.$$

Másrészről ha $0 < l < m$ akkor valamely i indexre a $|\sigma_i|$ rend nem osztja l-et, és ezért $\sigma_i^l \neq 1$. Mivel a σ_i ciklusok diszjunktak, σ^l sem lehet 1. □

A permutációk konjugálása elvégezhető az alábbi egyszerű módszerrel, egyúttal megkapjuk a permutációk konjugált osztályokba való sorolását is.

9.4.Állítás. *Legyen $\sigma = (i_1 \dots i_l) \in S_n$ ciklus, $\tau \in S_n$ permutáció. Ekkor $\tau^{-1}\sigma\tau = (\tau^{-1}(i_1)\dots\tau^{-1}(i_l))$. Következésképp az S_n csoport egy konjugált osztálya azokból a permutációkból áll, amelyeknek diszjunkt ciklusok szorzatára való felbontásaiban a megegyező hosszúságú ciklusok száma ugyanannyi.*

Bizonyítás. Legyen $P = \{i_1, \dots, i_l\}$. Ha $\tau(j) \notin P$ akkor $\tau^{-1}\sigma\tau(j) = \tau^{-1}\tau(j) = j$. Legyen $\tau(j) = i_k \in P$, azaz $j = \tau^{-1}(i_k)$. Ha $k < l$ akkor $\tau^{-1}\sigma\tau(j) = \tau^{-1}\sigma(i_k) = \tau^{-1}(i_{k+1})$, és ha $k = l$ akkor $\tau^{-1}\sigma\tau(j) = \tau^{-1}\sigma(i_l) = \tau^{-1}(i_1)$.

Legyen $\sigma = \sigma_1\cdots\sigma_r$, $\tau \in S_n$, a σ_i-k diszjunkt ciklusok. Ekkor

$$\tau^{-1}\sigma\tau = (\tau^{-1}\sigma_1\tau)(\tau^{-1}\sigma_2\tau)\cdots(\tau^{-1}\sigma_r\tau)$$

diszjunkt ciklusok szorzatára való felbontás, és $\tau^{-1}\sigma_i\tau$ hossza ugyanannyi, mint σ_i hossza.

Másrészről, ha

$$\sigma = (i_1 \dots i_{l_1})(i_{l_1+1} \dots i_{l_2})\cdots(i_{l_s+1} \dots i_n),$$

$$\delta = (j_1 \dots j_{l_1})(j_{l_1+1} \dots j_{l_2})\cdots(j_{l_s+1} \dots j_n)$$

diszjunkt ciklusok szorzatára való felbontás, kiegészítve a nem mozgatott elemekkel, akkor a

$$\tau = \begin{pmatrix} j_1 j_2 \dots j_{l_1} \dots j_n \\ i_1 i_2 \dots i_{l_1} \dots i_n \end{pmatrix}$$

permutációra $\delta = \tau^{-1}\sigma\tau$. □

A permutáció paritásának fogalmát vezetjük be a következő tételben.

9.5.Állítás. *Legyen* $f : S_n \to \mathbb{Q}$,

$$f\left(\begin{pmatrix} 12\dots n \\ i_1 i_2 \dots i_n \end{pmatrix}\right) = \prod_{s\neq t} \frac{s-t}{i_s - i_t}.$$

Ekkor $f : S_n \mapsto U(\mathbb{Z})$ *epimorfizmus,* A_n*-nel jelölt magja* $\frac{n!}{2}$ *rendű normálosztó, amelyet* n**-edfokú alternáló csoport***nak, elemeit* **páros permutáció***knak nevezünk. Továbbá, a páros permutációk transzpozíciók szorzatára történő tetszőleges felbontásában a tényezők száma páros.*

Bizonyítás. Legyen

$$\tau = \begin{pmatrix} 12\dots n \\ i_1 i_2 \dots i_n \end{pmatrix},\ \sigma = \begin{pmatrix} i_1 i_2 \dots i_n \\ j_1 j_2 \dots j_n \end{pmatrix}.$$

Ekkor

$$\sigma\tau = \begin{pmatrix} 12\dots n \\ j_1 j_2 \dots j_n \end{pmatrix},\ f(\sigma\tau) = \prod_{s\neq t} \frac{s-t}{j_s - j_t}$$

és

$$f(\sigma)f(\tau) = \prod_{s\neq t} \frac{i_s - i_t}{j_s - j_t} \prod_{s\neq t} \frac{s-t}{i_s - i_t} = f(\sigma\tau).$$

9.3.2 alapján legyen $\sigma = \tau_1\tau_2\cdots\tau_r = (i_1 i_2)(i_3 i_4)\cdots(i_{2r-1} i_{2r})$. Ekkor

$$f(\sigma) = f(\tau_1)\cdots f(\tau_r) = \frac{i_1 - i_2}{i_2 - i_1}\frac{i_3 - i_4}{i_4 - i_3}\cdots\frac{i_{2r-1} - i_{2r}}{i_{2r} - i_{2r-1}} = (-1)^r.$$

Azaz valóban $f : S_n \mapsto U(\mathbb{Z})$ epimorfizmus. 8.3.1 alapján $S_n/A_n \cong U(\mathbb{Z})$, azaz $n!/|A_n| = 2$ □

Könnyen látható, hogy az $f(\sigma)$ értékében szereplő $\frac{s-t}{i_s - i_t}$ tört pontosan akkor negatív, ha az (s,t) pár a permutációban inverziót alkot, azaz az $f(\sigma)$ érték pontosan akkor pozitív illetve negatív, ha a permutációban szereplő inverziók száma páros illetve páratlan.

Definíció. *Az* $S_n \setminus A_n$ *halmaz elemeit* **páratlan permutáció***knak nevezzük. Az* S_n *n-edfokú szimmetrikus csoport részcsoportjait* n**-edfokú permutációcsoport***oknak nevezzük.*

Alapvető fontosságú az alábbi tétel, mely szerint bármely véges csoport előállítható permutációcsoportként. (Ez igaz tetszőleges csoportra is.)

9.6.Tétel (Cayley). *Tetszőleges n-edrendű véges csoport izomorf egy n-edfokú permutációcsoporttal.*

Bizonyítás. Legyen $\varphi : G \to \mathrm{Sym}(G)$,

$$g \mapsto l_g = \begin{pmatrix} g_1\, g_2 \dots g_n \\ gg_1\, gg_2 \dots gg_n \end{pmatrix}.$$

Ekkor $\varphi(gh)(x) = l_{gh}(x) = ghx = gl_h(x) = l_g(l_h(x))$, azaz φ homomorfizmus. Ha $g \neq 1$ akkor $l_g(1) = g1 = g \neq 1$, azaz φ magja $\{1\}$. 8.2.5 miatt φ monomorfizmus, és a G csoport izomorf a $\varphi(G)$ csoporttal, amely a $\mathrm{Sym}(G) \cong S_n$ szimmetrikus csoport részcsoportja. □

10. Direkt szorzat, véges Abel-csoportok alaptétele

10.1.Tétel. *Legyen $G_1, G_2, \dots, G_n$ csoport. Ekkor a*

$$G = G_1 \times \cdots \times G_n = \{(g_1, \dots, g_n) \mid g_i \in G_i \ (i = 1, \dots, n)\}$$

halmaz a $(g_1, \dots, g_n)(h_1, \dots, h_n) = (g_1h_1, \dots, g_nh_n)$ műveletre nézve csoport, amelyet a G_i csoportok (külső) **direkt szorzatának** *nevezünk.*

Bizonyítás. Az asszociativitás nyilvánvaló, $(1, 1, \dots, 1)$ egységelem, ha g_i iverze g_i^{-1} akkor $(g_1, \dots, g_n)$ inverze $(g_1^{-1}, \dots, g_n^{-1})$. □

Definíció. *Legyen G csoport, $G_1, \dots, G_n$ a G normális részcsoportjai. Azt mondjuk, hogy a G csoport a G_i normális részcsoportok* **belső direkt szorzata**, *ha $G = \langle \cup_{i=1}^n G_i \rangle$ és minden k-ra $G_k \cap \langle \cup_{i \neq k} G_i \rangle = \{1\}$.*

10.2.Állítás. *A G csoport a $G_1, \dots, G_n$ normálosztóinak belső direkt szorzata akkor és csak akkor, ha G izomorf a $G_1, \dots, G_n$ csoportok (külső) direkt szorzatával.*

Bizonyítás. Legyen először a G csoport a $G_1, \dots, G_n$ normálosztóinak belső direkt szorzata.

Lássuk be, hogy különböző normálosztókhoz tartozó elemek egymással felcserélhetőek. Valóban, legyen $a \in G_i$, $b \in G_j$ $(i \neq j)$. Ekkor egyrészt $a^{-1}(b^{-1}ab) \in G_i$, másrészt $(a^{-1}b^{-1}a)b \in G_j$, azaz $a^{-1}b^{-1}ab \in G_i \cap G_j = \{1\}$, ahonnan $ab = ba$ következik.

Mivel a G_i normálosztók generálják az egész csoportot, tetszőleges a elem felírható a normálosztók elemeinek szorzataként. A felcserélhetőség miatt a szorzat tényezőinek rendezése után a felírás $a = a_1a_2 \cdots a_n$ alakot ölt, ahol $a_i \in G_i$. Ez a felírás egyértelmű, mert ha $a = a_1'a_2' \cdots a_n'$ is teljesül, ahol $a_i' \in G_i$, akkor $a = a_1a_2 \cdots a_n = a_1'a_2' \cdots a_n'$, amelyből a felcserélhetőség miatt ${a_k{a_k'}^{-1}} \in \langle \cup_{i \neq k} G_i \rangle$, ami a $G_k \cap \langle \cup_{i \neq k} G_i \rangle = \{1\}$ feltétel miatt csak akkkor lehetséges, ha minden k-ra $a_k = a_k'$. Ha $a = a_1a_2 \cdots a_n$ és $b = b_1b_2 \cdots b_n$ ilyen felírás, akkor a felcserélhetőség miatt $ab = a_1b_1a_2b_2 \cdots a_nb_n$ szintén a keresett alakú felírás. Az egyértelműség miatt a $\varphi : G \to G_1 \times \cdots \times G_n$, $a \mapsto (a_1, a_2, \dots, a_n)$ leképezés homomorfizmus, amely nyilván injektív és szürjektív is.

Legyen most G izomorf a $G_1, \dots, G_n$ csoportok (külső) direkt szorzatával, ahol az izomorfizmust a ψ leképezés adja, és legyen H_i a direkt szorzat azon elemeinek a halmaza, amely elem n-esek i-edik tagja tetszőleges eleme a G_i csoportnak, a többi 1. Nyilván a külső direkt szorzat a H_i normálosztóinak belső direkt szorzata, és ugyanez fennáll a G csoportra és a G_i csoportokkal azonosítható $\psi^{-1}(H_i)$ normálosztóira. □

Ebben a paragrafusban a cél a véges Abel-csoportok felépítésének teljes megadása a direkt szorzat fogalmának segítségével.

Az elsődleges struktúrális tételünk a következő.

10.3.Tétel (a primér felbontás tétele). *Legyen G véges n-edrendű Abel-csoport, n prímtényezős felbomtása $n = p_1^{k_1} \cdots p_r^{k_r}$, ahol $p_1, \dots, p_r$ különböző prímek. Ekkor a G csoport p_i-hatványrendű elemei egy $p_i^{k_i}$-rendű G_{p_i} részcsoportot alkotnak és $G = G_{p_1} \times \cdots \times G_{p_r}$ direkt szorzat.*

Bizonyítás. Legyen p az n egy prímosztója, és lássuk be, hogy G_p a G csoport részcsoportja. $1 \in G_p$ miatt $G_p \neq \emptyset$, alkalmazzuk 5.2-t. Legyen $a, b \in G_p$, $|a| = p^{l_1}$ és $|b| = p^{l_2}$ az elemek rendjei, $l = \max\{l_1, l_2\}$. Ekkor $(a^{-1}b)^{p^l} = (a^{p^l})^{-1}b^{p^l} = 1 \cdot 1 = 1$, és $a^{-1}b \in G_p$.

Lássuk be, hogy a G_{p_i} részcsoportok generálják a G csoportot. Legyen $g \in G$ t-rendű elem. 6.3 miatt $t = p_1^{i_1}p_2^{i_2} \cdots p_r^{i_r}$, és legyen $t_j = \frac{t}{p_j^{i_j}}$. Ekkor $g_j = g^{t_j}$ rendje $p_j^{i_j}$ és $g_j \in G_{p_j}$. Mivel $h = g_1g_2 \cdots g_r = g^{t_1+t_2+\cdots+t_r}$ és $\text{lnko}(t, t_1 + t_2 + \cdots + t_r) = 1$, 5.5.4 miatt $g \in \langle h \rangle \subseteq \langle \cup_j G_{p_j} \rangle$.

Legyen $H = \langle \cup_{j \neq i} G_{p_j} \rangle$ és $g \in G_{p_i} \cap H$, $n_i = \frac{n}{p_i^{k_i}}$. Mivel $g \in H$, $g = g_1 g_2 \cdots g_{i-1} g_{i+1} \cdots g_r$, ahol $g_k \in G_{p_k}$, és

$$g^{n_i} = g_1^{n_i} g_2^{n_i} \cdots g_{i-1}^{n_i} g_{i+1}^{n_i} \cdots g_r^{n_i} = 1 \cdot 1 \cdots 1 = 1$$

és 6.4.1 miatt g rendje osztja n_i-t. Mivel g rendje p_i-hatvány, és $\text{lnko}(n_i, p_i) = 1$, ez csak akkor lehet, ha $g = 1$. Kaptuk, hogy $G = G_{p_1} \times \cdots \times G_{p_r}$ direkt szorzat.

Lássuk be végül indukcióval r szerint, hogy a G_{p_i} csoport rendje $p_i^{k_i}$. $r = 1$ esetén ez világos. Indukció alapján a $H = G_{p_1} \times \cdots \times G_{p_{r-1}}$ részcsoport rendje osztja $\frac{n}{p_r^{k_r}}$-t, $G = H \times G_{p_r}$, és ekkor szükségképpen a H részcsoport rendje $\frac{n}{p_r^{k_r}}$, a G_{p_r} részcsoport rendje $p_r^{k_r}$. □

Az alaptétel bizony´ásában lényeges szerepet tölt be az alábbi két lemma.

10.4.Lemma. *Legyen p prímszám, G p-hatványrendű nem ciklikus Abel-csoport. Ha a a G csoport maximális rendű eleme, akkor létezik $b \in G$ p-rendű elem, hogy $b \notin \langle a \rangle$.*

Bizonyítás. Legyen az a elem rendje p^t. Ha $t = 1$ akkor az állítás teljesül. Legyen $t > 1$. Alkalmazzunk indukciót a csoport rendje szerint. A $G/\langle a^{p^{t-1}} \rangle$ faktorcsoport nem lehet ciklikus, mert ekkor a G csoport is ciklikus lenne. Ha az $\overline{a}$ elem p^{t-1} rendje nem maximális a faktorcsoportban, akkor létezik egy $c \in G$ elem, hogy rendje p^t, és $\langle a \rangle \cap \langle c \rangle = \{1\}$; ekkor $b = c^{p^{t-1}}$ a keresett p-rendű elem. Ellenkező esetben indukció alapján létezik egy $d \in G$ elem, hogy a $\overline{d} \notin \langle \overline{a} \rangle$ elem rendje p. Ha a d elem rendje is p, akkor ez a keresett elem. Ha nem, akkor rendje p^2, $a^{p^{t-1}} = d^p$ feltehető és $b = a^{p^{t-2}} d^{-1}$ a keresett p-rendű elem. □

10.5.Lemma. *Prímhatványrendű Abel-csoportban maximális rendű elem által generált ciklikus részcsoport direkt faktor.*

Bizonyítás. Ha a csoport ciklikus, nincs mit belátni. Ha nem, alkalmazzunk indukciót a csoport rendjére. Az előző lemma alapján ha a a G csoport maximális rendű eleme, legyen $b \in G$ p-rendű elem, hogy $b \notin \langle a \rangle$. Ekkor indukció alapján a $G/\langle b \rangle$ faktorcsoport felbomlik $\overline{a} \times \overline{B}$ direkt szorzatra, ahol B a G csoport b elemet tartalmazó részcsoportja. Nyilván a G csoport direkt felbontása $\langle a \rangle \times B$. □

Összevetve a primér felbontás tételét a két lemmával, kapjuk az alábbi struktúra–tételt.

10.6.Tétel (véges Abel-csoportok alaptétele). *Minden véges Abel-csoport felbomlik prímhatványrendű ciklikus csoportok direkt szorzatára.*

Bizonyítás. A második lemma alapján indukciót alkalmazva a rendre az állítás teljesül prímhatványrendű Abel-csoportokra. A primér felbontás tétele adja a teljes állítást. □

Az egyértelműséget bizonyítás nélkül közöljük.

10.7.Tétel (unicitás). *Ha G véges Abel-csoport,*

$$G = \langle a_1 \rangle \times \cdots \times \langle a_r \rangle = \langle b_1 \rangle \times \cdots \times \langle b_s \rangle$$

a G csoport két direkt felbontása prímhatványrendű ciklikus csoportok direkt szorzatára, akkor $r = s$ és létezik $\sigma \in S_r$ permutáció úgy, hogy $|a_i| = |b_{\sigma(i)}|$ minden $1 \leq i \leq r$ esetén. □

11. A p^2, $2p$, 8-adrendű csoportok

11.1.Tétel. *Legyen p prímszám, G p^2-rendű csoport. Ekkor G Abel-csoport.*

Bizonyítás. Tegyük fel, hogy a G csoport nemkommutatív. 7.3.3 miatt a G csoport konjugált osztályainak rendje 1 vagy p, és összegük p^2. Mivel $\{1\}$ konjugált osztály, lennie kell még egy másik egyelemű osztálynak, azaz a centrum rendje p, mivel nem lehet az egész G csoport.

Legyen $Z = \langle a\rangle$ a G csoport p-rendű centruma. Nyilván létezik $b \notin Z$ p-rendű elem G-ben, ekkor $G/Z = \langle bZ\rangle$ ciklikus p-rendű csoport, és $G = Z \cup bZ \cup \cdots \cup b^{p-1}Z$ mellékosztályok diszjunkt uniója, azaz tetszőleges elem a^ib^j alakú. De ekkor $(a^ib^j)(a^kb^l) = (a^kb^l)(a^ib^j)$, és a G csoport Abel-féle, ellentmondás. □

11.2.Lemma. *Ha egy G csoportban minden elem rendje osztja 2-t, akkor a G csoport Abel-féle.*

Bizonyítás. Legyen $a, b \in G$ tetszőleges elem. Ekkor $a^2 = 1$, $b^2 = 1$ és $abab = (ab)^2 = 1$, ahonnan $ab = ba$ következik. □

11.3.Tétel. *Legyen $p \neq 2$ prímszám, G nemkommutatív, $2p$-rendű csoport. Ekkor G izomorf a $D_p = \langle a, b \,|\, a^p = 1,\ b^2 = 1,\ ba = a^{p-1}b\rangle$ diédercsoporttal.*

Bizonyítás. A G csoportban az elemek rendje 6.3 miatt 1, 2 vagy p. Mivel G nemkommutatív csoport, 11.2 alapján van benne p-rendű a elem. Mivel az $\langle a\rangle$ ciklikus részcsoport indexe 2, normálosztó. Nyilván létezik $b \notin \langle a\rangle$ elem. $b^2 \in \langle a\rangle$ miatt a b elem rendje 2. Mivel a $\langle a\rangle$ ciklikus részcsoport normálosztó, $bab = a^k$, $1 \leq k \leq p-1$. Mivel $a = b(bab)b = ba^kb = (bab)^k = a^{k^2}$, $k^2 \equiv 1 (\mathrm{mod}\, p)$. A Z_p maradékosztálygyűrű test, benne az $x^2 - 1$ polinomnak két gyöke van, és $k = 1$ vagy $k = p-1$. Ha $bab = a$ akkor $ba = ab$ és a G csoport kommutatív, ami nem lehet, így $k = p-1$, és a G csoport izomorf a D_p diédercsoporttal. □

11.4.Tétel. *Legyen G nemkommutatív, 8-adrendű csoport. Ekkor a G csoport vagy a $D_4 = \langle a, b \,|\, a^4 = 1,\ b^2 = 1,\ ba = a^3b\rangle$ diédercsoporttal, vagy a $Q = \langle a, b \,|\, a^4 = 1,\ b^2 = a^2,\ ba = a^b\rangle$ kvaterniócsoporttal izomorf.*

Bizonyítás. A G csoportban nincsenek 8-adrendű elemek, mivel ekkor G ciklikus lenne. Ha a G csoportban minden elem rendje osztaná 2-t, akkor 11.2 miatt Abel-féle lenne, ami lehetetlen. Ezért a G csoport tartalmaz 4-edrendű a elemet. Nyilván létezik $b \notin \langle a\rangle$ elem, rendje 2 vagy 4. Mivel az $\langle a\rangle$ ciklikus részcsoport indexe 2, normálosztó, és $G/\langle a\rangle = \langle b\langle a\rangle\rangle$ faktocsoport másodrendű ciklikus csoport. Ezért $b^2 \in \langle a\rangle$ és $b^2 = 1$ vagy $b^2 = a^2$, b^2 és a felcserélhetőek. Így, mivel $\langle a\rangle$ normálosztó, $a = b^{-1}(b^{-1}ab)b = b^{-1}a^kb = (b^{-1}ab)^k = a^{k^2}$, azaz $k^2 \equiv 1 (\mathrm{mod}\, 4)$, $k = 1$ vagy $k = 3$. $k = 1$ esetén $ba = ab$ miatt a G csoport Abel-féle lenne, ami lehetetlen, ezért $k = 3$.

Ha $b^2 = 1$, akkor a G csoport a D_4 diédercsoporttal, ha $b^2 = a^2$, akkor a Q kvaterniócsoporttal izomorf. □

12. Az S_4 szimmetrikus és az A_5 alternáló csoportok

Definíció. *A G csoport G_i részcsoportjainak*

$$G_0 = \langle 1\rangle \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

véges láncát **feloldólánc***nak, a G csoportot* **feloldható***nak nevezzük, ha a G_i csoport normálosztó a G_{i+1} csoportban és a G_{i+1}/G_i faktorcsoportok $(1 \leq i \leq n-1)$ Abel-félék.*

Minden G Abel-csoport feloldható, feloldólánca $\langle 1\rangle \subset G$, ennek faktora a G Abel-csoport. A $D_n = \langle a, b \,|\, a^n = 1,\ b^2 = 1,\ b^{-1}ab = a^{-1}\rangle$ $(n > 2)$ $2n$-edrendű diédercsoport nemkommutatív és feloldható, feloldólánca $\langle 1\rangle \subset \langle a\rangle \subset D_n$, ennek faktorai n-rendű és másodrendű ciklikus csoportok.

12.1.Tétel. *Az S_4 negyedfokú szimmetrikus csoport feloldható, feloldólánca $\langle 1\rangle \subset \langle a\rangle \subset K_4 \subset A_4 \subset S_4$, ahol $a = (12)(34)$, $b = (13)(24)$, $K_4 = \langle a, b\rangle$.*

Bizonyítás. Nyilván $ab = ba = (14)(23)$, és $K_4 = \{1, a, b, ab\}$ 4-edrendű Abel-csoport, így az $\langle a\rangle$ másodrendű ciklikus csoport normálosztó a K_4 csoportban. 9.3 miatt az S_4 csoportban $K_4 = \{1\} \cup \{a, b, ab\}$ konjugált osztályok uniója, így normálosztó az S_4 szimmetrikus csoportban, és ezért az A_4 alternáló csoportban is. 9.4 miatt az A_4 12-edrendű alternáló csoport normálosztó az S_4 csoportban. A feloldólánc faktorainak rendjei rendre 2, 2, 3, 2 prímek, és a faktorok ciklikusak. □

12.2.Lemma. *Feloldható csoport részcsoportja és faktorcsoportja feloldható.*

Bizonyítás. Legyen H a G feloldható csoport részcsoportja, N a normálosztója, a G csoport feloldólánca $\{G_i\}$. Könnyen látható, hogy $\{H \cap G_i\}$ a H részcsoport feloldólánca. Ha $\psi : G \to G/N$ a ternészetes epimorfizmus, akkor $\{\psi(G_i)\}$ a faktorcsoport feloldólánca. □

Teljesül még az is, hogy ha egy csoport normálosztója és eszerinti faktorcsoportja is feloldható, akkor maga a csoport is feloldható.

Az egyenletek gyökképlettel történő megoldhatósága vizsgálatánál alapvető a

12.3.Tétel. *Az A_5 alternáló csoport, és következésképp $n \geq 5$ esetén az S_n szimmetrikus csoport nem feloldható.*

Bizonyítás. Lássuk be, hogy az A_5 alternáló csoport egyedüli normálosztói $\langle 1\rangle$ és A_5.

9.4 alapján az S_5 szimmetrikus csoportban a páros paritású elemek konjugált osztályai $L_1 = \{1\}$, L_2 a 3-hosszú ciklusok, L_3 az 5-hosszú ciklusok, L_4 a két diszjunkt transzpozíció szorzatai. Nyilván $|L_1| = 1$, $|L_2| = 20$, $|L_3| = 24$, $|L_4| = 15$.

Nyilván $K_1 = L_1$ az A_5 csoportban is konjugált osztály.

7.5 alapján a $C_{S_5}((123))$ centralizátor indexe 20, rendje 6, és $C_{S_5}((123)) = \langle (123)\rangle \times \langle (45)\rangle$. Innen $C_{A_5}((123)) = C_{S_5}((123)) \cap A_5 = \langle (123)\rangle$, azaz a (123) ciklus A_5 csoportbeli osztályának rendje 20, és $K_2 = L_2$ A_5 csoportbeli konjugált osztály.

7.5 alapján a $C_{S_5}((12345))$ centralizátor indexe 24, rendje 5, és $C_{S_5}((12345)) = \langle (12345)\rangle = C_{A_5}((12345))$, azaz az (12345) ciklus A_5 csoportbeli osztályának rendje 12, és $L_3 = K_3 \cup K_4$ két 12-edrendű A_5 csoportbeli konjugált osztály uniója.

7.5 alapján a $C_{S_5}((12)(34))$ centralizátor indexe 15, rendje 8, és $C_{S_5}((12)(34)) = \langle (13)(24), (12)\rangle$ a D_4 diédercsoporttal izomorf. Innen $C_{A_5}((12)(34)) = C_{S_5}((12)(34))) \cap A_5 = \langle (12)(34)\rangle \times \langle (13)(24)\rangle$, azaz az (12)(34) permutáció A_5 csoportbeli osztályának rendje 15, és $K_5 = L_4$ A_5 csoportbeli konjugált osztály.

Láttuk, hogy az A_5 alternáló csoport konjugált osztályainak rendje $1, 20, 12, 12, 15$. Tegyük fel, hogy N normálosztó az A_5 csoportban. Ekkor 5.2 miatt az N normálosztó rendje $1, 2, 4, 5, 6, 10, 15, 30$ vagy 60 lehet, és 7.2 miatt a normálosztó előáll konjugált osztályok uniójaként. Az osztályok rendjeit figyelembe véve ez csak akkor lehetséges, ha az N normálosztó rendje 1 vagy 60.

Így az A_5 csoportnak nem lehet normállánca, és az A_5 csoport nem feloldható. Mivel $n \geq 5$ esetén az S_n szimmetrikus csoport tartalmaz az A_5 csoporttal izomorf részcsoportot, 12.2 miatt nem lehet feloldható. □

Azt mondjuk, hogy egy csoport egyszerű, ha benne csak a két triviális normálosztó van, az egyelemű részcsoport és az egész csoport. Nyilván ilyenek a prímrendű ciklikus csoportok, és Abel-csoportok között más egyszerű csoport nincsen. Nemkommutatív egyszerű csoport nyilván nem lehet feloldható. Az előbb beláttuk, hogy az A_5 alternáló csoport egyszerű csoport. Igaz az a tény, hogy $n \geq 5$ esetén az n-edfokú alternáló csoport egyszerű csoport.