A magasabbfokú egyenletek megoldhatóságának vizsgálata a zseniális francia matematikus Évariste Galois (1811 -1832) nevéhez fűződik. Munkájában egy olyan fontos kapcsolatot fedezett fel, amely azóta külön önálló életet kezdett élni. Ezt a kapcsolatot *Galois-kapcsolatnak* nevezik; és érdemes arra, hogy megismerjük. Ehhez azonban szükséges, hogy valamit a Galois-elméletből is megtanuljunk. A Galois-elmélet azt vizsgálja, hogy mikor lehet egy egyhatározatlanú magasabbfokú egyenletet gyökjelekkel megoldani. Nem kell megijedni, csak egy egészen elemi példát fogunk tárgyalni. Ez a példa azért lényegében mindent tartalmaz a Galois-elméletből, kivéve a nehézségeket. Általános esetben ugyanis éppen az nehéz, hogy belássuk, mindent hasonlóképpen tehetünk. Ezt megelőzően tárgyalnunk kell a testelméletet is. Pontosabban szólva ennek is csak egészen elemi részeit.

Néhány szó a számtestekről. Számok egy $\mathbb{K}$ halmazát **számtestnek** nevezzük, ha tartalmazza az 1-et és zárt a négy alapműveletre (azaz $\mathbb{K}$-beli számok összege, különbsége, szorzata és hányadosa is $\mathbb{K}$-beli szám – persze 0-val itt sem oszthatunk). A legkisebb számtest a racionális számok $\mathbb{Q}$ számteste; a legnagyobb, amit „mindenki" ismer, a valós számoké. Sokan persze ismerik a komplex számtestet is.

A $\mathbb{K}$ számtestnek egy ϑ számmal való **bővítésén** azt a legszűkebb számtestet értjük, amely $\mathbb{K}$-n kívül a ϑ számot is tartalmazza. Ezt a számtestet $\mathbb{K}(\vartheta)$ jelöli. Könnyen belátható, hogy ilyen mindig létezik (nevezetesen a $\mathbb{K}$-t és a ϑ-t tartalmazó összes számtest közös része). Mi hallgatólagosan mindig feltesszük, hogy $\vartheta \notin \mathbb{K}$; erre tulajdonképpen nem igazán van szükség, de így elkerülhetjük a „vagy–vagy" típusú meggondolásokat.

Csak a legegyszerűbb esettel foglalkozunk, amikor $\vartheta^2 = t \in \mathbb{K}$. Ekkor érvényes az alábbi

Tétel. *Ha* $\vartheta^2 = t \in \mathbb{K}$, *akkor* $\mathbb{K}(\vartheta)$ *minden eleme egyértelműen felírható* $a + b \cdot \vartheta$ *alakban, ahol* a *és* b K *elemein futnak végig.*

Bizonyítás. Az eleve világos, hogy ezeknek a számoknak mind benne kell lenniük a szóban forgó számtestben. Mivel $\mathbb{K}$ számtest és $\vartheta^2 = t \in \mathbb{K}$, azért a kapott számok halmaza zárt az összeadásra, kivonásra és a szorzásra. Ebből következik az egyértelműség is, hiszen ha két ilyen szám különbsége

$$(a + b \cdot \vartheta) - (c + b \cdot \vartheta) = (a - c) + (b - d) \cdot \vartheta = 0,$$

az csak úgy lehetséges ($\vartheta \notin \mathbb{K}$ alapán), ha $a = c$ és $b = d$. Az osztás vizsgálatához vegyük tekintetbe, hogy ha $c + b \cdot \vartheta \neq 0$, akkor

$$N = (c + d \cdot \vartheta) \cdot (c - d \cdot \vartheta) = c^2 - d^2 \cdot t \in \mathbb{K}$$

sem lehet 0, és így az $u = ac - bdt$ és $v = bc - ad$ választással

$$\frac{a + b \cdot \vartheta}{c + d \cdot \vartheta} = \frac{(a + b \cdot \vartheta) \cdot (c - d \cdot \vartheta)}{N} = \frac{u}{N} + \frac{v}{N} \cdot \vartheta \in \mathbb{K},$$

ami az osztásra való zártságot jelenti. Végül $1 = 1 + 0 \cdot \vartheta$ nyilván eleme e halmaznak.□

Számtestek automorfizmusai. Az alábbiakban egyetlen számtestet fogunk vizsgálni: $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$-t (tehát $\mathbb{Q}$-t először $\sqrt{2}$-vel bővítjük, majd az így kapott számtestet $\sqrt{3}$-mal). Ennek elemei a

$$(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

alakú számok, ahol $a, b, c, d \in \mathbb{Q}$. Mindenekelőtt a $\mathbb{K}$ számtesten értelmezett bizonyos függvényeket – úgynevezett $\mathbb{Q}$ *feletti relatív autamorfizmusokat* – fogunk vizsgálni.

Definíció. *Egy, a* $\mathbb{K}$ *számtesten értelmezett* φ *függvényt* $\mathbb{Q}$ *feletti relatív automorfizmusnak nevezünk, ha e függvényre az alábbiak teljesülnek:*

(1) φ $\mathbb{K}$*-t önmagába képezi.*

(2) φ *különböző elemeket különböző elemekre képez.*

(3) φ*-nél minden* $\mathbb{K}$*-beli elem fellép képként.*

(4) φ *összeget és szorzatot tart.*[1]

(5) φ $\mathbb{Q}$ *minden egyes elemét önmagára képezi.*[2]

A $\mathbb{K}$ *számtest* $\mathbb{Q}$ *feletti relatív*[3] *automorfizmusainak halmazát* G*-vel jelöljük.*

A függvények kompozícióját (amit szorzásnak is nevezünk) egymás mellé írással fogjuk jelölni. Így $\varphi\psi$ azt a függvényt jelöli, amely egy tetszőleges x elemet $\varphi(\psi(x))$-be képez. Vigyázzunk, a $\varphi\psi$ és $\psi\varphi$ függvények általában különbözőek!

Tétel. G *a függvények kompozíciójára mint műveletre nézve zárt, és „csoport"-ot alkot. Ez a következőket jelenti:*

(a) *A művelet asszociatív, azaz* $\varphi, \psi, \chi, \in \mathbf{G}$ *esetén* $(\varphi\psi)\chi = \varphi(\psi\chi)$.

[1] Azaz bármely x és $y\mathbb{K}$-beli számok esetén $\varphi(x + y) = \varphi(x) + \varphi(y)$, illetve $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ teljesül.

[2] Ki lehet mutatni, hogy ez az előző tulajdonságokból már következik. Azért tettük mégis fel, mert ha nem $\mathbb{Q}$-ból indulunk ki, akkor már nem feltétlenül igaz.

[3] Az elnevezésben szereplő *relatív* jelző arra utal, hogy ezek a $\mathbb{Q}$ „alaptest"-et elemenként fixen hagyják.

(b) *Létezik egységelem, azaz olyan* $\iota \in \mathbf{G}$*, amelyre minden* $\varphi \in \mathbf{G}$ *esetén* $\iota\varphi = \varphi\iota = \varphi$ *teljesül.*

(c) *Minden* $\varphi \in \mathbf{G}$ *elemnek van inverze, azaz létezik hozzá olyan* $\psi \in \mathbf{G}$ *elem, amelyre* $\varphi\psi = \psi\varphi = \iota$.

Itt $\mathbb{K}$ helyett sok más számtestet is vehetnénk; azokra is igaz volna, hogy a relatív automorfizmusok csoportot alkotnak. A bizonyítást a $\mathbb{K}$ számtestre végezzük, de az utolsó tulajdonság kivételével ezt a specialitást nem használjuk ki. Az utolsó tulajdonságot majd csak akkor mutatjuk meg, ha fel tudjuk írni $\mathbf{G}$ elemeit.

Mindenekelőtt azt kell megmutatni, hogy két $\mathbf{G}$-beli φ és ψ függvény szorzata is eleme $\mathbf{G}$-nek:

(1): Mivel mindkét függvény $\mathbb{K}$-t képezi önmagára, ezért egymás után alkalmazva őket ismét ilyen függvényt kapunk.

(2): Legyenek x, y a $\mathbb{K}$ különböző elemei. Definíció szerint $\psi(x)$ és $\psi(y)$ is különbözőek; tehát $\varphi(\psi(x))$ és $\varphi(\psi(y))$ sem lehetnek egyenlőek.

(3): Tetszőleges $x \in \mathbb{K}$ esetén létezik olyan $y \in \mathbb{K}$ és ehhez olyan $z \in \mathbb{K}$, amelyre $\varphi(y) = x$ és $\psi(z) = y$; hiszen mindkét függvény rendelkezik a kívánt tulajdonsággal. Ebből viszont azonnal következik a $\varphi(\psi(z)) = x$ egyenlőség.

(4): Ha $x, y \in \mathbb{K}$, akkor $\varphi(\psi(x + y)) = \varphi(\psi(x) + \psi(y)) = \varphi(\psi(x)) + \varphi(\psi(y))$. A szorzásra vonatkozó összefüggés ugyanígy bizonyítható.

(5): Ha $x \in \mathbb{Q}$, akkor $\varphi(\psi(x)) = \varphi(x) = x$ bizonyítja, hogy a szorzat is fixen hagyja $\mathbb{Q}$ elemeit.

A szorzás asszociativitásának a bizonyításához azt kell megmutatni, hogy $(\varphi\psi)\chi$ és $\varphi(\psi\chi)$ bármely x elemet ugyanarra képez:

$$((\varphi\psi)\chi)(x) = (\varphi\psi)(\chi(x)) = \varphi(\psi(\chi(x))) = \varphi((\psi\chi)(x)) = (\varphi(\psi\chi))(x).$$

A $\iota(x) = x$ összefüggéssel definiált identikus függvény nyilván rendelkezik az összes megkövetelt tulajdonsággal, így eleme $\mathbf{G}$-nek. Erre viszont triviálisan igaz a $\iota\varphi = \varphi\iota$ összefüggés.

Most pedig megkeressük a $\mathbb{K}$ test összes $\mathbb{Q}$-ra vonatkozó relatív automorfizmusát.

Mint láttuk, $\mathbb{K}$ elemei $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alakú számok, ahol $a, b, c, d, \in \mathbb{Q}$. Legyen $\varphi \in \mathbf{G}$, ekkor a feltett tulajdonságok alapján

$$\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) + \varphi(c)\varphi(\sqrt{3}) + \varphi(d)\varphi(\sqrt{6}) =$$
$$= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{6}) = a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{2})\varphi(\sqrt{3}).$$

Eszerint a φ relatív automorfizmust egyértelműen meghatározza az, ha tudjuk, mibe képezi le$\sqrt{2}$-t és $\sqrt{3}$-at. Mivel $(\sqrt{2})^2 = 2$, ezért $\varphi(\sqrt{2})^2 = \varphi((\sqrt{2})^2) = \varphi(2) = 2$. Két lehetőségünk van tehát: vagy $\varphi(\sqrt{2}) = \sqrt{2}$, vagy $\varphi(\sqrt{2}) = -\sqrt{2}$. Hasonlóképpen két lehetőség adódik $\varphi(\sqrt{3})$-ra; vagy$\sqrt{3}$ vagy $-\sqrt{3}$. Ez összesen négy lehetőséget ad, tehát G-nek legfeljebb négy eleme van.

A négy szóba jövő relatív automorfizmus közül egyik a ι identitás, ami minden elemet önmagába visz. Először azt mutatjuk meg, hogy van olyan τ relatív automorfizmus, amely $\sqrt{2}$-t önmagába viszi és $\sqrt{3}$-at a negatívjába. Mint láttuk $\mathbb{K} = \mathbb{L}(\sqrt{3})$, ahol $\mathbb{L} = \mathbb{Q}(\sqrt{2})$. A keresett τ relatív automorfizmusnak $\mathbb{L}$ minden elemét önmagába kell vinnie (tehát ez $\mathbb{L}$-re vonatkozó relatív automorfizmus). Így az $\alpha, \beta \in \mathbb{L}$ elemekre $\tau(\alpha+\beta\sqrt{3}) = \alpha-\beta\sqrt{3}$ kell legyen. A relatív automorfizmusoktól megkövetelt minden tulajdonság teljesülése triviális, kivéve az összeg- és szorzat-tartást. Ehhez tekintsünk még egy elemet: $\gamma+\delta\sqrt{3}$, ahol $\gamma, \delta \in \mathbb{L}$. Az összegre vonatkozó bizonyítás könnyen elvégezhető, a szorzatra vonatkozó pedig itt következik:

$$\tau((\alpha + \beta\sqrt{3})(\gamma + \delta\sqrt{3})) = \tau((\alpha\gamma + 3\beta\delta) + (\alpha\delta + \beta\gamma)\sqrt{3}) = (\alpha\gamma + 3\beta\delta)-$$
$$-(\alpha\delta + \beta\gamma)\sqrt{3} = (\alpha - \beta\sqrt{3})(\gamma - \delta\sqrt{3}) = \tau(\alpha + \beta\sqrt{3}) \cdot \tau(\gamma + \delta\sqrt{3}).$$

$\sqrt{2}$ és $\sqrt{3}$ szimmetrikus szerepe miatt hasonlóképpen beláthatjuk, hogy létezik egy olyan σ relatív automorfizmus is, amely $\sqrt{2}$-t viszi a negatívjába és a $\sqrt{3}$-at hagyja fixen. Azonnal megjegyezzük, hogy ezeknek a relatív automorfizmusoknak a négyzete (azaz önmagával való szorzata) nyilvánvalóan ι. A hiányzó – negyedik — relatív automorfizmus csak az lehet, amit σ és τ szorzataként állíthatunk elő. Ez a szorzat $\sqrt{2}$-t is és $\sqrt{3}$-at is a negatívjába viszi; eszerint a már látottaktól különbözik. Mivel a tényezők sorrendjétől függetlenül ugyanazt a relatív automorfizmust kell kapnunk, ezért egy $\varrho = \sigma\tau = \tau\sigma$ relatív automorfizmushoz jutottunk. Erre is azonnal következik, hogy $\varrho^2 = \iota$. Ezek szerint itt bármely φ relatív automorfizmusra teljesül a $\varphi^2 = \iota$ összefüggés, ami azt jelenti, hogy minden relatív automorfizmusnak van inverze, nevezetesen önmaga. (Ez még hiányzott a tétel bizonyításából.)

Egyébként a még nem vizsgált szorzatokról belátható, hogy $\sigma\varrho = \varrho\sigma = \tau,\ \tau\varrho = \varrho\tau = \sigma$.

Részcsoportok és résztestek. Láttuk, hogy a σ és τ relatív automorfizmusok is fixen hagynak minden olyan $\mathbb{K}$-beli elemet, amely nincs $\mathbb{Q}$-ban. De ϱ is ilyen, mert $\varrho(\sqrt{6}) = \varrho(\sqrt{2} \cdot \sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6})$. Nézzük meg most, hogy melyek az összes olyan elemek, amelyeket ezek a relatív automorfizmusok önmagukra képeznek. Tekintsük evégett

az $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ képét ezeknél a relatív automorfizmusoknál:

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6},$$
$$\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6},$$
$$\varrho(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$

Eszerint:

$$\left.\begin{array}{l}\sigma(\alpha) = \alpha \\ \tau(\alpha) = \alpha \\ \varrho(\alpha) = \alpha\end{array}\right\} \text{ akkor és csak akkor, ha } \left\{\begin{array}{l} b = d = 0 \\ c = d = 0 \\ b = c = 0\end{array}\right\} \text{ azaz, ha } \left\{\begin{array}{l}\alpha \in \mathbb{Q}\left(\sqrt{3}\right) \\ \alpha \in \mathbb{Q}\left(\sqrt{2}\right) \\ \alpha \in \mathbb{Q}\left(\sqrt{6}\right).\end{array}\right.$$

Itt három számtesttel is találkozunk, amelyek a $\mathbb{Q}$ és $\mathbb{K}$ *között* vannak; éppen ezért *közbülső testeknek* nevezik őket. Ezeket a közbülső testeket nemcsak a felsorolt egyes relatív automorfizmusok hagyják elemről elemre fixen, hanem az identikus leképezés is. Így **G**-nek három részhalmaza választható ki: $\mathbf{H}_2 = \{\iota, \tau\}$, $\mathbf{H}_3 = \{\iota, \sigma\}$, $\mathbf{H}_6 = \{\iota, \varrho\}$; amelyek pontosan azokból a relatív automorfizmusokból állnak, amelyek megfelelően a $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ közbülső testek elemeit hagyják fixen.

A csoportnak ezen részhalmazairól azonnal belátható, hogy bármelyikükből véve két elemet, ezek szorzata is ugyanebbe a részhalmazba esik.

Ha egy csoport elemeinek nem üres részhalmaza a csoportban értelmezett szorzásra zárt és maga is csoport erre nézve, akkor e részhalmazt részcsoportnak nevezzük[4].

Látható, hogy a vizsgált **G** csoportnak még két részcsoportja van. Az egyik az egyedül az identitást tartalmazó **E** részcsoport, a másik maga a **G**. Mindkettő triviálisan részcsoport (úgy is nevezik őket, hogy triviális részcsoportok). Nézzük meg, hogy ezeknek elemei melyik testbeli elemeket tartják fixen. Az **E** egyetlen eleme minden $\mathbb{K}$-beli elemet fixen hagy; és $\mathbb{K}$ minden elemét egyedül **E** elemei tartják fixen. A **G** elemeinek a hatását már láttuk, ezek mindegyike csak a $\mathbb{Q}$ elemeit tartja fixen; az pedig, hogy $\mathbb{Q}$ összes elemét fixen hagyja **G** minden eleme, a relatív automorfizmus definíciójából következik.

A **G**-nek több részcsoportja nincs is. Minden részcsoportnak tartalmaznia kell az egységelemet. Ha a **H** részcsoport egyedül az egységelemet tartalmazza, akkor **E**-vel egyenlő. Ha még egy elemet tartalmaz, akkor a $\mathbf{H}_2, \mathbf{H}_3, \mathbf{H}_6$ részcsoportok valamelyike lesz. Amennyiben viszont az egységelemen kívül még két elemet tartalmaz, akkor tartalmazza ezek szorzatát is, azaz a csoport minden elemét, így e részcsoport az egész **G**.

E részcsoportok mindegyikéhez tartozik egy közbülső test, amely azokból az elemekből áll, amelyeket e részcsoport minden eleme fixen hagy. Emellett minden egyes részcsoport pontosan azokból az elemekből áll, amelyek a megfelelő test elemeit fixen hagyják. Táblázatban ábrázolva:

$$\mathbf{E} \Longleftrightarrow \mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\mathbf{H}_2 \Longleftrightarrow \mathbb{Q}(\sqrt{2}) \qquad \mathbf{H}_3 \Longleftrightarrow \mathbb{Q}(\sqrt{3}) \qquad \mathbf{H}_6 \Longleftrightarrow \mathbb{Q}(\sqrt{6})$$
$$\mathbf{G} \Longleftrightarrow \mathbb{Q}$$

Itt a feljebb levő sorban található testek tartalmazzák az alattuk levő sorban szereplőket; míg a csoportoknál éppen fordított a helyzet.

Vannak tehát **részcsoport $\Longleftrightarrow$ közbülső test** párjaink. Látjuk, hogy a részcsoportok közül mindegyik fellép; a közbülső testekről viszont ez egyáltalán nem látható[5] Ennek ellenére ez így van, és ez a Galois-elmélet egyik fontos következménye. Ha már itt tartunk, akkor szóljunk néhány szót arról is, hogy miképpen használja fel a fenti eljárást a Galois-elmélet[6]

Ha egy adott számtestbeli együtthatós egyenletet akarunk megoldani, akkor ezt bővítjük az egyenlet összes gyökével. Ehhez a bővítéshez elkészítjük a relatív automorfizmusok csoportját (ez az egyenlet *Galois-csoportja*). Ez a csoport meghatározható és mindig véges. Ha ebben létezik bizonyos részcsoportokból álló lánc (azaz részcsoportok egymásba skatulyázott sorozata), akkor a gyököket az együtthatókból a négy alapművelet és gyökvonások segítségével kifejezhetjük. (Ha ilyen lánc nem létezik, akkor a gyökök a fenti módon nem fejezhetők ki.) A megfelelő csoportlánchoz tartozó testlánc még azt is elárulja, hogyan lehet ezt a kifejezést megkapni.

Hogy jön létre a kapcsolat. Térjünk most vissza eredeti példánkhoz, és nézzük meg, miképpen jön létre a

részcsoport $\Longleftrightarrow$ közbülső test

[4] Azért kell hozzátenni, hogy maga is csoport az eredeti szorzásra, mert különben nem tudjuk biztosítani azt, hogy az egységelem is és minden elemének az inverze is benne van. A mi esetünkben csak véges csoportok léphetnek fel; amikoris bebizonyítható, hogy ezek már a szorzásra való zártságból következnek.

[5] Legalábbis én nem látok rá semmilyen egyszerű módot.

[6] Az alábbi ismertetés hiányos és pontatlan, de a lényeget tartalmazza.

kapcsolat! Van itt egy számunkra „misztikus” rész; nevezetesen az, hogy minden közbülső test előfordul. A mi példánkon könnyen láthattuk, hogy a párokban minden részcsoport szerepelhet, általában azonban ez sem könnyű. Mindkettőnek a bizonyítása elég sok testelméleti és csoportelméleti ismeretet igényel. Ezeket itt nincs mód tárgyalni.

Van azonban a kapcsolatnak egy másik része, ami viszonylag egyszerű. Nevezetesen az, hogy csak részcsoportok és közbülső testek állíthatók párba. Ennek bizonyítását mindenki maga elvégezheti.

Eleve az sem világos, hogy vannak párba állítható „valamik”. Hiszen gondoljuk el, hogy miképpen lehet egy ilyen párt megtalálni (ahogy tulajdonképpen tettük is). Kiindulunk egy számhalmazból, és tekintjük az őket fixen hagyó függvényeket. Azután vesszük azokat a számokat, amelyeket ezek a függvények mind fixen hagynak. Aztán meg azokat a függvényeket, amelyek ennek az újabb számhalmaznak az elemeit fixálják, és így tovább. Egyáltalán nem világos, hogy ez az eljárás egyszer véget fog érni. Persze az is lehet, hogy az eljárás véget ér, és ennek bizonyos testelméleti vagy/és csoportelméleti okai vannak.

Nos a mi célunk éppen annak a megmutatása, hogy az eljárás „mindig” véget ér, és ez a dolgok „természetéből” következik. Pontosabban szólva azért történik mindez, mert bizonyos relatív automorfizmusok bizonyos számokat „tisztelnek”; azaz e számokat fixen hagyják. A „tisztelnek” szót azért használjuk, mert nem az fontos igazán, hogy „fixen hagyják”, hanem csak az, hogy valami kapcsolat van közöttük. Amiket keresünk, azok meg olyan részhalmazokból álló párok, amelyben a függvények pontosan azok, amelyek a halmaz számait „tisztelik”, a számok meg pont azok, amelyeket a felsorolt függvények mind „tisztelnek”.

A Galois-kapcsolat. Fogalmazzuk meg matematikai módon azt, amivel foglalkozni akarunk. Mindenekelőtt adott két halmaz $\mathbf{G}$ és $\mathbb{K}$. Az előbbinek az elemeit görög, az utóbbiét latin kisbetűkkel fogjuk jelölni. Valamilyen módon adott egy $\leftrightarrow$ „kapcsolat”, amely bizonyos módon párba állítja a $\mathbf{G}$ egy-egy elemét $\mathbb{K}$ egy-egy elemével. Ilyen módon $\varphi \leftrightarrow x$ alakú párok keletkeznek. Pontosabban:

Tekintsük az összes (φ, x) alakú párok halmazát, ahol $\varphi \in \mathbf{G}$ és $x \in \mathbb{K}$. Tekintsük e párhalmaz egy tetszőleges, de rögzített $\mathcal{S}$ részhalmazát. Azt, hogy $(\varphi, x) \in \mathcal{S}$, úgy jelöljük, hogy[7] $\varphi \leftrightarrow x$.

Az $\mathcal{S}$ indukálta $\mathcal{G}$ Galois-kapcsolaton azoknak a $\mathbf{H} \Longleftrightarrow \mathbb{L}$ $(\mathbf{H} \subseteq \mathbf{G},\ \mathbb{L} \subseteq \mathbb{K})$ pároknak a halmazát értjük, amelyekre:

$$\begin{array}{rl} \varphi \in \mathbf{H} & \text{akkor és csak akkor, ha minden} \quad x \in \mathbb{L}\text{-re} \quad \varphi \leftrightarrow x; \\ x \in \mathbb{L} & \text{akkor és csak akkor, ha minden} \quad \varphi \in \mathbf{H}\text{-ra} \quad \varphi \leftrightarrow x. \end{array}$$

Mindenekelőtt érdemes megfigyelni, hogy a fenti megfogalmazásban a $\mathbf{G}$ és a $\mathbb{K}$ halmazok szerepe szimmetrikus. Ezért elég mindent „egyoldalúan” bizonyítani; a szimmetrikus állítás ugyanúgy igaz.

Először azt fogjuk megnézni, hogy mi történik akkor, ha egy részhalmazból kiindulva a $\leftrightarrow$ reláció „mentén” ide-oda „szaladgálunk”. Ehhez két jelölésre van szükségünk, annak megfelelően, hogy a kiinduló ($\mathbb{K}$-beli) halmazból Balra($\mathbf{G}$-be) megyünk, vagy $\mathbf{G}$-beli halmazból kiindulva megyünk Jobbra ($\mathbb{K}$-ba):

Legyen $\mathbb{L} \subseteq \mathbb{K}$, illetve $\mathbf{H} \subseteq \mathbf{G}$.$\mathbb{L}^B$, illetve $\mathbf{H}^J$ az alábbi halmazokat jelöli:

$$\begin{array}{rl} \alpha \in \mathbb{L}^B & \text{akkor és csak akkor, ha minden} \quad x \in \mathbb{L}\text{-re} \quad \alpha \leftrightarrow x; \\ x \in \mathbf{H}^J & \text{akkor és csak akkor, ha minden} \quad \alpha \in \mathbf{H}\text{-ra} \quad \alpha \leftrightarrow x. \end{array}$$

Definíció szerint $\mathbf{H} \Longleftrightarrow \mathbb{L}$ pontosan azt jelenti, hogy $\mathbf{H} = \mathbb{L}^B$ és $\mathbf{H}^J = \mathbb{L}$. Most azt fogjuk megnézni, hogy az $\mathcal{S}$ indukálta $\mathcal{G}$ Galois-kapcsolatnak milyen elemi tulajdonságai vannak. Érdemes megfigyelni, hogy a továbbiakban már nem térünk vissza az $\mathcal{S}$ kapcsolatra, hanem minden tulajdonságra a most bebizonyítandó alaptulajdonságokból következtetünk majd.

Alaptétel. Az alábbiak érvényesek:

1. *Ha $\mathbb{M} \subseteq \mathbb{L} (\subseteq \mathbb{K})$, akkor $\mathbb{M}^B \supseteq \mathbb{L}^B$. Hasonlóképpen, ha $\mathbf{S} \subseteq \mathbf{H} (\subseteq \mathbf{G})$, akkor $\mathbf{S}^J \supseteq \mathbf{G}^J$.*
2. *Ha $\mathbb{L} \subseteq \mathbb{K}$, akkor $(\mathbb{L}^B)^J \supseteq \mathbb{L}$. Hasonlóképpen, ha $\mathbf{H} \subseteq G$, akkor $(\mathbf{H}^J)^B \supseteq \mathbf{H}$.*

Bizonyítás. Tegyük fel, hogy $\mathbb{M} \subseteq \mathbb{L}$ és legyen $\varphi \in \mathbb{L}^B$. Ez azt jelenti, hogy bármely $\mathbb{L}$-beli x elemre igaz a $\varphi \leftrightarrow x$ összefüggés. Mivel $\mathbb{L}$ tartalmazza $\mathbb{M}$-et, ezért a $\varphi \leftrightarrow x$ összefüggés eleve igaz $\mathbb{M}$-beli x-ekre is; vagyis $\mathbb{L}^B$ elemei $\mathbb{M}^B$-nek is elemei. A szimmetria miatt az 1. alatti másik állítás is igaz.

A 2. alatti állítás kimutatására – ugyancsak a szimmetria miatt – elég annyit bizonyítani, hogy tetszőleges $\mathbf{H} \subseteq \mathbf{G}$ esetén $(\mathbf{H}^J)^B \supseteq \mathbf{H}$ is igaz.

Vegyünk tehát egy $\mathbf{H}$-beli x elemet. $\mathbf{H^J}$ definíciója szerint minden $\mathbf{H^J}$-beli φ-re teljesül a $\varphi \leftrightarrow x$ összefüggés. Ez viszont éppen azt jelenti, hogy x-nek hozzá kell tartoznia a $(\mathbf{H}^J)^B$ halmazhoz. □

Az alaptétel 1. pontját kétszer alkalmazva azt látjuk, hogy „nagyobb halmazból nagyobba jutunk”. A 2. pont pedig azt mondja, hogy a kiindulási halmaz „növekszik”. Ez azt sugallja, hogy „ide-oda menve” egyre nagyobb halmazhoz jutunk, „láncreakció” lép fel, az eljárás „megszalad”. Szerencsére az 1. pont tartalmaz egy „negatív visszacsatolást” is azáltal, hogy egy lépés után megfordul a tartalmazás iránya. Ezt mutatja meg az alábbi tétel előállítása, míg a második ennek egy egyszerű, de fontos következménye:

Következmény. *A fenti Galois-kapcsolatra az alábbiak teljesülnek:*

[7] Ezt a kapcsolatot tekinthetjük gráfnak, amelynek szögpontjai a $\mathbf{G}$ és $\mathbb{K}$ halmazok egyesítésének elemei, élei pedig az $\mathcal{S}$ halmaz elemei. Ez egy úgynevezett páros gráf, ami azt jelenti, hogy bármelyik szögpontból kiindulva csak úgy érhetünk önmagába vissza, ha páros sok élen megyünk keresztül. Tulajdonképpen bármely páros gráfot tekinthetnénk kiindulási alapnak.

1. $((\mathbf{H}^J)^B)^J = \mathbf{H}^J$ és $((\mathbb{L}^B)^J)^B = \mathbf{L}^B$.

2. $\mathbf{H} \subseteq \mathbb{L}^B$ akkor és csak akkor igaz, ha $\mathbf{H}^J \supseteq \mathbb{L}$.

Bizonyítás. Az alaptétel 2. pontja szerint $(\mathbf{H}^J)^B \supseteq \mathbf{H}$, amiből a tétel 1. pontja alapján$((\mathbf{H}^J)^B)^J \subseteq \mathbf{H}^J$ következik. Ha viszont az alaptétel 2. pontját alkalmazzuk az $\mathbf{L} = \mathbf{H}^J$ elemre, akkor azt kapjuk, hogy $((\mathbf{H}^J)^B)^J \supseteq \mathbf{H}^J$. Ezekből pedig azonnal adódik a vizsgált két halmaz egyenlősége. (A másik két halmaz egyenlősége a szimmetria miatt igaz.)

Ugyancsak a szimmetria miatt elég a 2. ponthoz annyit bizonyítani, hogy $\mathbf{H} \subseteq \mathbb{L}^B$ esetén $\mathbf{H}^J \supseteq \mathbb{L}$ is igaz. Ha $\mathbf{H} \subseteq \mathbb{L}^B$ igaz, akkor e következmény 1. pontját valamint az alaptételt felhasználva

$$\mathbf{H}^J = ((\mathbf{H}^J)^B)^J \supseteq (((\mathbb{L}^B)^J)^B)^J = [((\mathbb{L}^B)^J)^B]^J = (\mathbf{L}^B)^J \supseteq \mathbb{L},$$

amivel állításunkat bizonyítottuk. □

A fentiek szerint a „jobb oldali felső indexben" felváltva szereplő B és J betűk közül legfeljebb kettőnek kell fellépnie. Amennyiben több lép fel, akkor – mint éppen láttuk – vagy csak az „első", vagy az „első kettő" marad meg. Ennek megfelelően nincs szükség zárójelezésre; például $(((\mathbb{L}^B)^J)^B)^J$ helyett azt írhatjuk, hogy $\mathbb{L}^{BJBJ}$.

Tetszőleges $\mathbb{L} \subseteq \mathbb{K}$, illetve $\mathbf{H} \subseteq \mathbf{G}$ esetén a $\mathbb{L}^{BJ}$, illetve $\mathbf{H}^{JB}$ halmazt az eredeti megfelelő halmazok (*Galois-)lezártjának* nevezzük. Ha egy részhalmaz lezártja önmaga, akkor azt mondjuk, hogy ez egy *zárt részhalmaz.*

Foglaljuk össze, hogy mit tudunk a Galois-kapcsolatról:

Bármely $\mathbb{L} \subseteq \mathbb{K}$, illetve $\mathbf{H} \subseteq \mathbf{G}$ esetén $\mathbb{L}^B$, illetve $\mathbf{H}^J$ zárt halmazok; továbbá minden zárt halmaz ilyen alakú. Pontosan akkor kapunk egy $\mathbf{H} \Longleftrightarrow \mathbb{L}$ Galois-kapcsolatbeli párt, ha ezek mindketten zárt halmazok, továbbá $\mathbf{H} = \mathbb{L}^B$ és $\mathbf{H}^J = \mathbb{L}$. Minden ilyen párt a két részhalmaz bármelyike egyértelműen meghatározza.

Néhány további fontos tulajdonság. Mint láttuk, a $\mathbf{H} \subseteq \mathbf{G}$ részhalmaz lezártja $\mathbf{H}^{JL}$, ami az eredeti részhalmazt tartalmazó zárt halmaz. Ha azonban erre a „lezárt" szót használjuk, akkor ez azt sugallja, hogy a $\mathbf{H}$-t tartalmazó legkisebb zárt halmazról van szó. Ez valóban így igaz. Tekintsünk ugyanis egy $\mathbf{H}$-t tartalmazó zárt halmazt, amely – mint láttuk $-\mathbb{L}^B$ alakban írható. A feltett $\mathbf{H} \subseteq \mathbb{L}^B$ összefüggésből $\mathbf{H}^J \supseteq \mathbb{L}$, ebből pedig $\mathbf{H}^{JB} \subseteq \mathbb{L}^B$ következik; mint sejtettük.

A következőkben azt mutatjuk meg, hogy két zárt halmaz közös része is zárt halmaz. Jelölje $\mathbf{H}_1 \cap \mathbf{H}_2$ a $\mathbf{H}_1$ és $\mathbf{H}_2$ zárt halmazok közös részét. Az eleve biztos, hogy $\mathbf{H}_1 \cap \mathbf{H}_2 \subseteq (\mathbf{H}_1 \cap \mathbf{H}_2)^{JB}$. Tekintettel viszont arra, hogy $\mathbf{H}_1 \cap \mathbf{H}_2$ benne van a $\mathbf{H}_1$ és $\mathbf{H}_2$ halmazok mindegyikében, ezért $(\mathbf{H}_1 \cap \mathbf{H}_2)^{JB}$ is benne van a $(\mathbf{H}_1)^{JB}$ és $(\mathbf{H}_2)^{JB}$ halmazok mindegyikében. Feltételünk szerint ezek az eredeti $\mathbf{H}_1$ és $\mathbf{H}_2$ halmazok. Így $(\mathbf{H}_1 \cap \mathbf{H}_2)^{JB}$ benne van e két halmaz közös részében is; amit az eredeti tartalmazással összevetve a két halmaz egyenlőségét nyerjük. Ez pedig éppen azt jelenti, hogy a $\mathbf{H}_1 \cap \mathbf{H}_2$ halmaz megegyezik saját lezártjával – tehát zárt. Megjegyezzük, hogy ugyanígy bizonyítható, hogy akármennyi véges számú zárt halmaz közös része is zárt; és annak a bizonyítása sem okoz komoly nehézséget, ha itt végtelen sok halmazt engedünk meg[8].

A közös résszel ellentétben zárt halmazok egyesítése nem feltétlenül zárt. (Ez a bevezető példánkban valóban elő is fordult.) Tekintsük most a $\mathbf{H}_1$ és a $\mathbf{H}_2$ zárt halmazok $\mathbf{H}_3 = \mathbf{H}_1 \cup \mathbf{H}_2$ egyesítési halmazát. Ez nem kell, hogy zárt legyen, de lezártja, $(\mathbf{H}_3)^{JB}$ biztosan tartalmazza az eredeti két halmazt. Azt is belátjuk viszont, hogy ez a legkisebb zárt halmaz, amely az eredeti két halmazt tartalmazza. Ha ugyanis egy zárt halmaz az eredeti két halmaz mindegyikét tartalmazza, akkor tartalmazza egyesítésüket is; márpedig azt láttuk, hogy egy halmazt tartalmazó minden zárt halmaz tartalmazza e halmaz (jelen esetben tehát $\mathbf{H}_3$) lezártját is.

Érdemes itt megjegyezni, hogy ezek az eredmények természetesen alkalmazhatóak a kiindulópontul szolgáló Galois-elméletben. Ezáltal számos olyan információhoz jutottunk a testekről, illetve a csoportokról, amelyekhez nem is nagyon kellett a testek, illetve a csoportok „milyenségét" ismerni.

Az alábbiakban egy másik olyan jelenséget említünk meg (részletes tárgyalásra itt sem kerülhet sor), amelyben ugyancsak természetesen lép fel egy Galois-kapcsolat.

Polinomok és gyökök. Tulajdonképpen mondhattunk volna polinomok helyett függvényeket is; de a polinomok vizsgálata is igen sok gondot okoz. Valójában még az elsőfokú polinomok esete sem egyszerű. (Természetesen nem egyetlen ismeretlenre gondolunk.)

Nézzünk egy nagyon egyszerű példát. A „második" halmaz legyen $\mathbb{V}^2$, ami a valós számpárok halmazát jelöli. Az „első" halmaz elemei pedig a kétváltozós valós együtthatós polinomok $\mathbb{V}[x, y]$ halmaza. Esetünkben is az történik, hogy az első halmaz elemei „hatnak" a második halmaz elemein. A „hatás" a behelyettesítés. A $p(x, y)$ polinom az (a, b) valós számpárból a $p(a, b)$ számot „csinálja". A kiinduló példánktól eltérően most $p(a, b) \notin \mathbb{V}^2$. Ennek ellenére itt is van egy igen speciális és nagyon fontos hatás, nevezetesen, amikor az eredmény 0.

Esetünkben tehát egy $p \leftrightarrow P$ kapcsolatból indulunk ki, ahol p egy kétváltozós polinom, P a sík egy pontja, ahol a p polinom a 0 értéket veszi fel. Ez az $\mathcal{S}$ kiinduló kapcsolat, amelyből meg kell csinálni a megfelelő $\mathcal{G}$ Galois-kapcsolatot.

A Galois-kapcsolatnál itt bizonyos $\mathfrak{P}$ polinomhalmazok és bizonyos Σ ponthalmazok[9] felelnek meg egymásnak (most többváltozós polinomokra és „többdimenziós tér"-beli pontokra is gondolunk). A fellépő ponthalmazokat *algebrai alakzatoknak, algebrai sokaságoknak* vagy *algebrai varietásoknak* nevezik (azért, mert algebrai „kifejezések"

[8] Meg kell fontolni, mi történik, ha a szereplő halmazok közös része üres. Ha végignézünk a bizonyításokon, láthatjuk, hogy az üres halmazt sehol sem zártuk ki. Esetünkben azt kaphatjuk, hogy az üres halmaz is zárt! Érdemes meggondolni, hogy ez mit jelent.

[9] $\mathfrak{P}$ Az egy gót nagy P betű, Σ pedig nem „szumma-jel", hanem egy görög nagy szigma betű.

gyökhalmazaként vannak definiálva). Ezeknek a leírása igen fontos és roppant nehéz. Éppen ezért hasznos az a leírás, amivel a Galois-megfeleltetés áttranszformálja őket a polinomok körébe.

Ennél a Galois-kapcsolatnál olyan $\mathfrak{P}$ polinomhalmazok jönnek szóba, amelyek a következő tulajdonságokkal rendelkeznek:

(1) Bármely két $\mathfrak{P}$-beli polinom összege is $\mathfrak{P}$-ben van.
(2) Egy $\mathfrak{P}$-beli polinomnak egy tetszőleges polinommal való szorzata is $\mathfrak{P}$-ben van.
(3) Ha egy polinom valamelyik hatványa $\mathfrak{P}$-beli, akkor ez a polinom is $\mathfrak{P}$-ben van.

Azt, hogy minden ilyen halmaz elő is fordul, „Hilbert-féle nullhelytétel"-nek nevezik, de ez csak akkor igaz, ha a valós számtest helyett a komplex számtestet vesszük.

És még vannak más lehetőségek is. A matematikában számos helyen alkalmazzák a Galois-kapcsolatot. Tudatos alkalmazásra azonban csak olyankor kerül sor, amikor a vizsgált matematikai ágak önmagukon belül is sok fontos információt nyújtanak. Ez azt jelenti, hogy előtte „bele kell mélyülni" a speciális anyagba.

A Galois-kapcsolat használható azonban sok egyszerű esetben is. A következőkben arra adunk példát, miképpen lehetséges ez például „adatok kezelésénél".

Adva van *objektumoknak* egy $\mathbb{K}$ halmaza, amelyek bizonyos *tulajdonságokkal* rendelkeznek vagy nem rendelkeznek. Jelölje $\mathbf{G}$ a felsorolt tulajdonságok halmazát. Itt is azonnal adódik egy $\mathcal{S}$ kapcsolat: $\varphi \leftrightarrow x$ azt jelenti, hogy az x objektum rendelkezik a φ tulajdonsággal.

A felépíthető Galois-kapcsolatról tudjuk, hogy **tulajdonsághalmaz** $\Longleftrightarrow$ **objektumhalmaz** párokból áll. Ez tehát megmondja „analizálja", hogy melyek az „összetartozó" tulajdonságok, illetve „összetartozó" objektumok (nevezetesen éppen a zárt tulajdonsághalmazok, illetve zárt objektumhalmazok). Való igaz, hogy ez az „összetartozó" szónak elég önkényes definíciója; de nem hiszem, hogy ennél jobbat ki lehet találni.

Teljesen precíz viszont az a kérdés, hogy bizonyos megadott tulajdonságokból mely további tulajdonságok következnek. A $\mathbf{H}$ tulajdonsághalmaz elemeiből pontosan azok a tulajdonságok következnek, amelyek $\mathbf{H}^{JB}$ elemei. De megállapíthatók olyan dolgok, hogy például az α és β tulajdonságok ekvivalensek (mit jelenthet ez?); és ebben az esetben bármelyikük elhagyható. Hasonlóképpen ekvivalens objektumok közül is elég csak egyet figyelembe venni. Ezáltal az egész adatrendszer csökkenthető; és így jobban áttekinthetővé válik.

Természetesen nem szabad azt gondolni, hogy ezáltal az egész kérdéskör nagyon egyszerűvé lesz. Számítógépre azért ennél az adatfeldolgozásnál is szükség van; de az összefüggések sokkal képszerűbbekké válnak.

Végezetül szeretném megjegyezni, hogy a matematikában számos ilyen kapcsolatféle létezik. Ezek segítségével bizonyos struktúrafajtán belül megoldhatatlan kérdéseket „átfordítottak" másik (egyszerűbb) struktúrafajtára, s az ott kapott választ visszafordítva az eredeti problémára, sikerült választ kapni. Nem vállalkozhatunk azonban arra, hogy itt ilyen példákat mutassunk; mert ezek hátterében nehéz matematikai elméletek állnak.

Fried Ervin