Eötvös Loránd Tudományegyetem

Természettudomnyi Kar

Malinoczki Gergely

Galois-elmélet és alkalmazásai

BSc Alkalmazott Matematikus Szakdolgozat

Témavezető:

Somlai Gábor

Algebra és Számelmélet Tanszék

Budapest, 2018

Köszönetnyilvánítás

Köszönettel tartozom a családomnak tamogatásukért, valamint amiért lehetővé tették számomra, hogy egyetemi tanulmányaimra öszpontosítsak. Köszönettel tartozom egykori tanáraimnak, Pelikán Józsefnek és Frenkel Péternek, amiért megszerettették velem az algebrát. Külön köszönet illeti a témavezetőmet, Somlai Gábort, aki rengeteg időt és energiát fordított arra, hogy segítsen megérteni és feldolgozni az anyagot. Mindannyiuk segítségéért hálás vagyok.

Tartalomjegyzék

Bevezetés

A középiskolai matematikaórákon az ember megtanulja a másodfokú egyenlet megoldóképletét, majd az egyetem első évében megtanulja a harmadfokúét (aztán gyorsan el is felejti), hall a negyedfokú egyenlet megoldóképletének létezéséről, illetve arról, hogy magasabb fokú egyenletekhez nincs ilyen megoldóképlet. Nem azért nincs, mert "bénák vagyunk" és még nem találtuk meg, hanem mert mélyebb elvi okai vannak, hogy miért nem is létezhet. Ez az állítás rögtön felkeltette az érdeklődésemet, így sajnálattal fogadtam, amikor kiderült, hogy az alkalmazott matematikus törzsanyagnak nem része ezen témakör tárgyalása. Remek alkalmat biztosított azonban ez a szakdolgozat, hogy egy egyetemi projekt keretein belül tanulhassak olyan matematikát, ami őszinte lelkesedéssel tölt el.

A kezdeti cél tehát a polinomok megoldhatóságának vizsgálata volt. Az ehhez vezető út természetesen a Galois-elméleten keresztül vezet. Ez az elmélet azonban halmaz-, csoport- és gyűrűelméleti ismereteket is igényel, így a tanulás során több egyéb témakör is felmerült, amivel kiegészíthetném a dolgozatot. Végül az eredeti elmélet végtelen bővítésekre való általánosítása mellett döntöttem.

A dolgozat megírásánál végig szem előtt tartottam, hogy ha egy átlagos alkalmazott matematikus BSc-t elvégzett diák meg akarja érteni, akkor azt (a dolgozat végén az inverz Galois-problémára adott példa kivételével) külső segítség nélkül megtehesse. Nem feltételeztem tehát, hogy emlékezne minden egyes algebra órán elhangzott tételre és definícióra, de azt igen, hogy az alapvető algebrai fogalmakkal tisztában van az olvasó.

1. fejezet

Szükséges előismeretek

Ebben a fejezetben elsőként az általános Galois-megfeleltetésekről lesz szó. Bár a fogalom algebrai eredetű, mára egy általánosabb elméletté nőtte ki magát, ami tetszőleges részbenrendezett halmazok közötti bizonyos megfeleltetéspárok vizsgálatát tűzte ki céljául. A dolgozatnak nem célja az általános Galois-megfeleltetések vizsgálata, ez az alfejezet azért került bele, hogy megmutassuk, az általunk tárgyalt Galois-megfeleltetés valójában egy általánosabb fogalom speciális esete.

A második alfejezet a szükséges csoportelméleti fogalmakat tárgyalja. Egyrészt emlékeztetünk az alapvető, mindenki által tanult fogalmakra, másrészt rövid bevezetőt adunk a csoportok feloldhatóságának témakörébe. Ezek után felidézzük a permutációcsoportok fogalmát, és megvizsgáljuk a szimmetrikus csoport feloldhatóságának kérdését.

Végezetül biztosítjuk a végtelen Galois-bővítések vizsgálatához szükséges topológiai hátteret.

1.1. A Galois-kapcsolatokról általában

1.1.1. Definíció. *A $\langle P; \leq \rangle$ részbenrendezett halmazon egy $\varphi : P \to P$ leképezést lezárásnak hívunk, ha a következő két feltétel teljesül:*

1. $x \leq \varphi(x)$ $(x \in P)$
2. $\varphi(\varphi(x)) = \varphi(x)$ $(x \in P)$
3. *Ha* $x \leq y$, *akkor* $\varphi(x) \leq \varphi(y)$ $(x, y \in P)$

1.1.2. Definíció. *Legyen $\langle P; \leq \rangle$ egy részbenrendezett halmaz, és φ ezen egy lezárás. Az $x \in P$ elemet zártnak nevezzük, ha $\varphi(x) = x$.*

1.1.3. Állítás. *Legyen $\varphi : P \to P$ egy lezárás a $\langle P; \leq \rangle$ részbenrendezett halmazon. Ekkor ha $x \leq \varphi(y)$, akkor $\varphi(x) \leq \varphi(y)$ $(x, y \in P)$.*

Bizonyítás. Ha $x \leq \varphi(y)$, akkor a definíció második és harmadik pontja alapján $\varphi(x) \leq \varphi(\varphi(y)) = \varphi(y)$. $\square$

1.1.4. Definíció. *Legyen $\langle P; \leq \rangle$ és $\langle Q; \leq \rangle$ két részbenrendezett halmaz. Az $\alpha : P \to Q$ és $\beta : Q \to P$ leképezéspárt Galois-megfeleltetésnek hívjuk, ha az alábbi feltételek teljesülnek:*

1. *Minden $x \leq y$ P-beli (Q-beli) elemek esetén $\alpha(x) \geq \alpha(y)$ ($\beta(x) \geq \beta(y)$) teljesül.*
2. *Tetszőleges P-beli (Q-beli) x elemre teljesül az $x \leq \beta\alpha(x)$ ($x \leq \alpha\beta(x)$) összefüggés.*

1.1.5. Megjegyzés. A Galois-megfeleltetésekkel kapcsolatos tételek kimondásánál, bizonyításánál általában eseteket kéne megkülönböztetni. A definíció szimmetrikussága miatt ettől nyilván eltekinthetünk, hiszen az egyik irány könnyedén (például a két alaphalmaz felcserélésével) visszavezethető a másikra.

1.1.6. Tétel. *Legyen $\langle P; \leq \rangle$ és $\langle Q; \leq \rangle$ két részbenrendezett halmaz, $\alpha : P \to Q$ és $\beta : Q \to P$ pedig ezeken adott Galois-megfeleltetés. Ekkor az alábbi tulajdonságok teljesülnek:*

1. *Ha $x \leq y$ tetszőleges P-beli elemek, akkor $\beta\alpha(x) \leq \beta\alpha(y)$.*
2. *Bármely $x \in P$ elemre $\alpha\beta\alpha(x) = \alpha(x)$.*
3. *Tetszőleges $x \in P$, $y \in Q$ elemekre $x \leq \beta(y)$ pontosan akkor, ha $y \leq \alpha(x)$.*
4. *Legyen $H \subseteq P$. Amennyiben létezik az $u = \bigvee\{x | x \in H\}$ elem, akkor létezik a $\bigwedge\{\alpha(x) | x \in H\}$ elem is, és megegyezik $\alpha(u)$-val. (Itt $\bigvee$ a legkisebb felső, illetve $\bigwedge$ a legnagyobb alsó korlátot jelöli.)*

Bizonyítás. Ha $x \leq y$, akkor $\alpha(x) \geq \alpha(y)$, és így $\beta\alpha(x) \leq \beta\alpha(y)$, amivel az első állítást beláttuk.

A definíció alapján tudjuk, hogy $x \leq \beta\alpha(x)$. Ha most az egyenlőtlenség mindkét oldalára alkalmazzuk α-t, akkor az egyenlőtlenség megfordul, és így $\alpha(x) \geq \alpha\beta\alpha(x)$-et kapjuk. Másrészt az $\alpha(x)$ Q-beli elemről a definíció kettes pontja alapján tudjuk, hogy $\alpha(x) \leq \alpha\beta\alpha(x)$. A két egyenlőtlenséget összevetve adódik a második állítás.

A harmadik állításnál $x \leq \beta(y)$-ból a definíció egyes pontja alapján $\alpha(x) \geq \alpha\beta(y)$. A definíció második pontja szerint viszont $\alpha\beta(y) \geq y$, és így a reláció tranzitivitását kihasználva $\alpha(x) \geq y$ adódik. A másik irány ugyanígy látható be.

Az utolsó állításnál $u \geq x$ minden $x \in H$ elemre, így definíció szerint $\alpha(u) \leq \alpha(x)$ minden H-beli x-re, vagyis $\alpha(u)$ valóban alsó korlát. Legyen most v az $\alpha(x)$ elemek egy tetszőleges alsó korlátja. Tudva, hogy $v \leq \alpha(x)$, az imént bizonyított állítás szerint $x \leq \beta(v)$. Mivel $\beta(v)$ a H halmaz egy felső korlátja, így biztosan nagyobb vagy egyenlő mint a legkisebb felső korlát, azaz $\beta(v) \geq u$. Ismét az előző pont alapján kapjuk, hogy $\alpha(u) \geq v$, vagyis $\alpha(u)$ tényleg a legnagyobb alsó korlát. $\square$

1.1.7. Állítás. *Legyen $\langle P; \leq \rangle$ és $\langle Q; \leq \rangle$ két részbenrendezett halmaz, $\alpha : P \to Q$ és $\beta : Q \to P$ pedig ezeken adott Galois-megfeleltetés. Ekkor a $\beta\alpha$ ($\alpha\beta$) leképezés egy lezárás P-n (Q-n). Ezt a lezárást a Galois-megfeleltetés által indukált lezárásnak nevezzük.*

Bizonyítás. A Galois-megfeleltetést definiáló második tulajdonság éppen azt mondja ki, hogy $x \leq \beta\alpha(x)$. Az imént bizonyított tétel első pontja éppen azt állítja, hogy ha $x \leq y$, akkor $\beta\alpha(x) \leq \beta\alpha(y)$, míg a második pontja szerint $\alpha\beta\alpha(x) = \alpha(x)$, amiből nyilván $(\beta\alpha)^2(x) = \beta\alpha(x)$, vagyis $\beta\alpha$ valóban lezárás P-n. A másik irány ugyanígy bizonyítható. $\square$

1.1.8. Megjegyzés. Az 1.1.6 tétel második pontja tehát azt mondja ki, hogy egy elemnek és (az indukált lezárásnál) a lezártjának a képe a Galois-megfeleltetésnél ugyanaz.

1.1.9. Tétel. *Legyen ϱ az (A, B) halmazpáron értelmezett tetszőleges reláció, és $\varphi : P(A) \to P(B)$ az a függvény, ami minden $A_1 \in P(A)$ halmazhoz az A_1 összes elemével relációban álló elemek halmazát rendeli, azaz:*

$$\varphi(A_1) = \{b | (a, b) \in \varrho, \forall a \in A_1\}$$

Ekkor φ és φ^{-1} Galois-kapcsolatot létesít a $\langle P(A); \leq \rangle$ és $\langle P(B); \leq \rangle$ részbenrendezett halmazokon, ahol a részbenrendezést a tartalmazással adjuk meg..

Bizonyítás. Legyen $A_1 \subseteq A_2$. Ha $b \in \varphi(A_2)$, akkor minden $a \in A_2$ elemre $(a, b) \in \varrho$. Ekkor viszont $A_1 \subseteq A_2$ miatt minden $a \in A_1$ elemre is fennáll a reláció. Így tehát $\varphi(A_2) \subseteq \varphi(A_1)$, azaz φ teljesíti a definíció első pontját.

Legyen most $a \in A_1$. A $\varphi^{-1}\varphi(A_1)$ halmazban pontosan azok az elemek vannak, amik $\varphi(A_1)$ minden elemével relációban állnak. Az a elem ilyen, hiszen φ definíciója alapján $\varphi(A_1)$-ben pontosan azok az elemek vannak, amik A_1 minden elemével, és így a-val is relációban állnak. Így tehát $A_1 \subseteq \varphi^{-1}\varphi(A_1)$, vagyis φ teljesíti a definíció második pontját is. A bizonyítás ugyanígy megy φ^{-1}-re. $\square$

1.2. Feloldhatóság és a szimmetrikus csoport

Mindenekelőtt emlékeztetünk néhány, a csoportokkal kapcsolatos alapvető fogalomra, tételre. A G csoport egy tetszőleges H részcsoportja szerint bal oldali (jobb oldali) mellékosztályokon a gH alakú (Hg alakú) halmazokat értjük. A G csoportot a bal oldali (jobb oldali) mekllékosztályok azonos elemszámú diszjunkt halmazokra osztják. Ugyanazon H részcsoport esetén azonban a két különböző oldali mellékosztályok általában nem ugyanazt a felosztást adják. Fontos speciális eset, amikor a bal és jobb oldali mellékosztályok megegyeznek:

1.2.1. Definíció. *A G csoport egy N részcsoportját normálosztónak nevezzük, és $N \lhd G$-vel jelöljük, ha minden $g \in G$ elemre $gN = Ng$.*

Ha N a G csoport egy normálosztója, akkor a gN ($g \in G$) alakú mellékosztályokon bevezethetünk egy műveletet, nevezetesen $(g_1N) \cdot (g_2N) = (g_1g_2N)$. Belátható, hogy a művelet eredménye nem függ attól, hogy az egyes mellékosztályokat melyik elemükkel reprezentáljuk, vagyis a definíció valóban értelmes. Az N szerinti mellékosztályok halmaza ezzel a műveletel ellátva csoportot alkot, melyet a G csoport N szerinti faktorcsoportjának hívunk, és G/N-el jelölünk.

1.2.2. Tétel. (Homomorfizmus-tétel) *Tetszőleges $\varphi : G \to \tilde{G}$ homomorfizmus esetén $G/(Ker(\varphi)) \cong Im(\varphi)$.*

1.2.3. Megjegyzés. Itt $Ker(\varphi)$ azon elemek halmazát jelöli, melyek képe φ-nél a $\tilde{G}$ egységeleme. Ez mindig normálosztó G-ben. Azon elemek halmazát, melyek előállnak képként $Im(\varphi)$-vel jelöljük. Ez mindig részcsoport $\tilde{G}$-ban. A fenti izomorfizmust a $\tilde{\varphi}$: $g \cdot Ker(\varphi) \mapsto \varphi(g)$ bijekció hozza létre.

1.2.4. Tétel. (Első izomorfizmust-tétel) *Ha $H \le G$ és $N \lhd G$, akkor*

$$N \lhd HN,\ (H \cap N) \lhd H \text{ és } HN/N \cong H/(H \cap N).$$

1.2.5. Tétel. (Második izomorfizmus-tétel) *Ha $N, M \lhd G$ és $N \le M$, akkor*

$$(M/N) \lhd (G/N) \text{ és } (G/N)/(M/N) \cong G/M.$$

1.2.6. Tétel. (Cauchy-tétel) *Ha a p prímszám osztója a G véges csoport rendjének, akkor G-nek van p-ed rendű eleme.*

Ezek után rátérünk a feloldható csoportok vizsgálatára.

1.2.7. Definíció. *A G csoport részcsoportjainak egy*

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$$

rendszerét a G egy r hosszúságú normálláncának nevezzük, ha minden i-re $G_{i+1} \lhd G_i$. A G_i/G_{i+1} faktorcsoportokat a normállánc faktorainak nevezzük. Egy normállánc valódi, ha $i \neq j$ esetén $G_i \neq G_j$. Az α normállánc a β normállánc finomítása, ha α tartalmazza β minden elemét. Két normálláncot izomorfnak nevezünk, ha faktoraik között van olyan bijekció, aminél az egymásnak megfeleltetett faktorok izomorfak.

1.2.8. Definíció. *A G csoport egy normálláncát kompozícióláncnak nevezzük, ha valódi normállánc, és nincs valódi finomítása.*

1.2.9. Megjegyzés. Tetszőleges G csoport esetén a $G \rhd \{1\}$ egy normállánc. Ha a G csoport nem triviális, de véges, akkor ezt a normálláncot közbülső normálosztók beszúrásával véges sok lépésben kompozíciólánccá finomíthatjuk.

A következő alapvető fontosságú tételt most bizonyítás nélkül közöljük, ugyanis bizonyítása hosszadalmas lenne, illetve további előkészületeket igényelne.

1.2.10. Tétel. (Jordan-Hölder tétel) *Ha a G csoportnak van kompozíciólánca, akkor bármely két kompzícióa izomorf.*

1.2.11. Definíció. *Egy G véges csoportot feloldhatónak nevezünk, ha kompozícióláncainak faktorai prímrendűek.*

1.2.12. Megjegyzés. A Jordan-Hölder tétel szerint tehát a feloldhatóság nem függ attól, hogy melyik kompozícióláncot tekintjük. Más forrásokban esetleg úgy is definiálhatják a feloldhatóságot, hogy van olyan normállánca, melybena faktorok kommutatívak. A két definíció természetesen ekvivalens. Egyrészt ha a faktorok prímrendűek akkor nyilván kommutatívak is. A másik irány bizonyítása már nem ilyen egyszerű, de nagyvonalakban arról van szó, hogy ha M egy normálosztó a G/N faktorcsoportban, akkor M "visszaemelhető" a G csoport egy N-nél bővebb normálosztójává olyan módon, hogy vesszük az M-beli mellékosztályok unióját. (M-ben tehát a G csoport N szerinti mellékosztályai vannak.) A véges Abel-csoportok alaptételének következményeként minden véges Abel-csoport feloldható, így ha G/N kommutatív, akkor ennek létezik prímrendű foktorokból álló kompozíciólánca. Ha most az eredeti normállánc minden egyes kommutatív faktorának legyártjuk ezt a kompozícióláncát, majd ezen kompozícióláncokat "visszaemeljük", akkor az eredeti normállánc egy olyan finomítását kapjuk, melyben már minden faktor prímrendű.

1.2.13. Tétel. *Feloldható csoport minden részcsoportja és faktorcsoportja is feloldható. Ha $N \lhd G$, és N valamint G/N is feloldhatók, akkor G szintén az.*

Bizonyítás. A részcsoportokra vonatkozó állítást a kompozíciólánc hosszára vonatkozó teljes indukcióval bizonyítjuk. Ha ez 1, akkor az állítás triviális. Legyen tehát a

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

a G feloldható csoport egy kompozíciólánca, és $H \leq G$. A fenti láncból G_0-t elhagyva kapjuk, hogy G_1 is feloldható, és így az indukciós feltevés miatt $(G_1 \cap H) \leq G_1$ is az. Elég tehát megmutatni, hogy ennek egy kompozíciólánca kiegészíthető H-nak egy kompozícióláncává. Ehhez arra van szükség, hogy $(G_1 \cap H)$ maximális normálosztó legyen H-ban, és a $H/(G_1 \cap H)$ faktorcsoport vagy triviális, vagy prímrendű legyen. Amennyiben $H \leq G_1$, úgy az állítás nyilván teljesül. Ellenkező esetben, mivel G_1 maxilmális részcsoport G-ben (hiszen prím indexű), ezért $HG_1 = G$, és így az első izomorfizmus-tétel alapján $H/G_1 \cap H) \cong G/G_1$, ami prímrendű.

Tegyük most fel, hogy $N \lhd G$. Ekkor a $G \rhd N$ normállánc kompozícióllánccá finomítható:

$$G = G_0 > G1 > \cdots > G_r = N > \cdots > \{1\}.$$

Mivel $N \lhd G$, így $N \lhd G_i$ $(1 \leq i \leq r)$. A második izomorfizmus-tétel szerint tehát $(G_i/N)/(G_{i+1}/N) \cong G_i/G_{i+1}$. Ez azt jelenti, hogy a G_i/N alakú faktorok G/N-nek egy olyan normállláncát alkotják, aminek faktorai prímrendűek, és így G/N feloldható.

Végezetül tegyük fel, hogy $N \lhd G$ valamint N is és G/N is feloldható. Tekintsük a

$$G = G_0 > \cdots > N = G_s > \cdots > G_r = \{1\}$$

kompozícióláncot. Amennyiben $i \geq s$ úgy N feloldhatósága miatt G_i/G_{i+1} prímrendű. Ha $i < s$, akkor G_i/G_{i+1} a második izomorfizmustétel alapján izomorf $(G_i/N)/(G_{i+1}/N)$-el, ami G/N feloldhatósága miatt prímrendű. Összességében azt kapjuk tehát, hogy G feloldható. $\square$

1.2.14. Definíció. *Egy n elemű halmaz önmagára vett bijektív leképezéseinek (permutációinak) halmazát a függvénykompozícióval ellátva n-ed fokú permutációcsoportnak nevezzük, és S_n-el jelöljük.*

Az egyszerűség kedvéért szokás feltenni, hogy az n elemű hamaz, aminek a permutálásait nézzük az $\{1, 2, \ldots, n\}$ halmaz. A továbbiakban mi is eszerint járunk el.

1.2.15. Definíció. *Ciklusnak nevezzük, és $(a_1 a_2 \ldots a_r)$-el jelöljük azt a permutációt, melynél a_i képe a_{i+1} minden $1 \leq i < r$-re, és a_r képe a_1.*

1.2.16. Állítás. *Minden permutáció egyértelműen felírható idegen ciklusok szorzataként. (Két permutációt idegennek nevezünk, ha nincs olyan elem, amit mind a két ciklus mozgat.)*

1.2.17. Állítás. *Minden permutáció felírható kételemű ciklusok (transzpozíciók) szorzataként. (Ez a felírás általában már nem egyértelmű.)*

1.2.18. Állítás. *Tetszőleges rögzített transzpozíció illetve n-es ciklus generálja S_n-t.*

1.2.19. Állítás. *A $\sigma \in S_n$ permutáció minden transzpozíciók szorzataként való felírásában a tényezők számának paritása azonos.*

Bizonyítás. Tekintsük a következő

$$P(x_1, \ldots, n_n) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (x_i - x_j)$$

polinomot. Ez nem más, mint az $x_1, \ldots, x_n$ változók összes lehetséges módon képzett különbsége, ahol mindig a kisebb indexű tagból vonjuk ki a nagyobbat. Készítsük most el a $P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ polinomot. Ez a polinom csak előjelben különbözhet P-től, hiszen itt is az összes lehetséges módon képzett különbséget szorozzuk össze, csak néhol a nagyobb indexűből vonjuk ki a kisebbet. Ha σ páros sok transzpozíció szorzataként írható fel, akkor a fenti polinomot definiáló szorzatnak páros sok tagja vált előjelet, míg páratlan sok transzpozíció esetén páratlan sok tag változik meg. Ebből következik, hogy σ nem írható fel páros és páratlan sok transzpozíció szorzataként is, hiszen ekkor a fenti polinom egyenlő lenne a mínusz egyszeresével. $\square$

1.2.20. Definíció. *Egy $\sigma \in S_n$ permutációt párosnak nevezünk, ha előáll páros sok transzpozíció szorzataként. Ellenkező esetben páratlan permutációról beszélünk. Az S_n páros permutációinak csoportját n-ed fokú alternáló csoportnak nevezzük, és A_n-nel jelöljük.*

1.2.21. Állítás. *Az n-ed fokú alternáló csoport valóban csoport, sőt ez egy 2 indexű normálosztó S_n-ben.*

Bizonyítás. Az, hogy páros permutációk szorzata és inverze is páros lényegében triviális. Az identikus permutáció felírható 0 db transzpozíció szorzataként, így ez is páros. A normálosztósághoz elég belátni, hogy $|S_n : A_n| = 2$ hiszen kettő indexű részcsoport mindenképp normálosztó. Ehhez tekintsük az $f : S_n \to S_n$, $\sigma \mapsto (12) \circ \sigma$ leképezést. Ez a leképezés bijekció a páros és a páratlan permutációk halmaza között. Páros permutációhoz nyilván páratlant rendel, és fordítva, valamint invertálható is, hiszen kétszer alkalmazva az identitást kapjuk. Ebből tehát következik, hogy ugyanannyi páros permutáció van, mint páratlan, vagyis A_n indexe tényleg kettő. □

A fejezet további részében a célunk S_n kompozícióláncainak vizsgálata. Mivel a kompozícióláncokat normálosztókkal definiáltuk, és a normálosztóknak megvan az a kellemes tulajdonsága, hogy önmagukba konjugálódnak, ezért érdemes megnézni, hogyan kell permutációkat konjugálni. Mivel minden permutáció felírható diszjunkt ciklusok szorzataként, így valójában elég azt megnézni, hogyan kell ciklusokat ciklusokkal konjugálni.

1.2.22. Állítás. *Két permutáció pontosan akkor azonos típusú (azaz a diszjunkt ciklusok szorzatára való felbontásaik között bijekció létesíthető úgy, hogy az egymásnak megfeleltetett ciklusok egyenlő hosszúak legyenek) ha konjugáltak.*

Bizonyítás. Legyen $\sigma,\ \tau \in S_n$, és $1 < k_1 < \cdots < k_r = n$. Tegyük fel, hogy $\sigma = (a_1 \dots a_{k_1}) \dots (a_{k_{r-1}+1} \dots a_{k_r})$, és $\tau = (b_1 \dots b_{k_1}) \dots (b_{k_{r-1}+1} \dots b_{k_r})$. Tekintsük azt a ϱ permutációt, ami minden a_i elemnek b_i-t felelteti meg, és nézzük meg mit csinál a $\varrho^{-1}\tau\varrho$ permutáció az a_i elemmel:

$$\varrho^{-1}\tau\varrho(a_i) = \varrho^{-1}\tau(b_i) = \varrho^{-1}(b_{i+1}) = a_{i+1}$$

feltéve, hogy $i \neq k_j$ valamilyen j-re. Ez utóbbi eset azonban ugyanígy kezelhető, a szétválasztásra csak a jelölés nehézsége miatt volt szükség. Ebből kapjuk tehát, hogy $\varrho^{-1}\tau\varrho = \sigma$, vagyis a két permutáció valóban konjugált.

Legyen megint $\sigma = (a_1 \dots a_{k_1}) \dots (a_{k_{r-1}+1} \dots a_{k_r})$, és $\varrho \in S_n$ tetszőleges. Tekintsük a $\tau = (\varrho(a_1) \dots \varrho(a_{k_1})) \dots (\varrho(a_{k_{r-1}+1}) \dots \varrho(a_{k_r}))$ permutációt. Erre teljesül, hogy $\tau(\varrho(a_i)) = \varrho(\sigma(a_i))$ minden egyes $a_i \in \{1, 2, \dots, n\}$ elemre. Így $\tau\varrho = \varrho\sigma$ azaz $\tau = \varrho\sigma\varrho^{-1}$. Mivel ϱ tetszőleges volt, így valóban σ minden konjugáltja vele azonos típusú. □

1.2.23. Tétel. *Legyen $n \geq 3$ és N az A_n-nek, vagy az S_n-nek egy normálosztója. Ekkor ha N tartalmaz transzpozíciót, akkor $N = S_n$, ha N tartalmaz hármas ciklust, akkor $N = S_n$, vagy $N = A_n$.*

Bizonyítás. Tegyük fel, hogy N tartalmaz transzpozíciót. Mivel N normálosztó, így tartalmazza az adott transzpozíció összes konjugáltját is, ami a 1.2.22 tétel szerint az összes transzpozíciót magában foglalja. A transzpozíciók azonban generálják S_n-net, hiszen minden permutáció előáll ilyenek szorzataként, és így $N = S_n$.

A többi állítás bizonyításához először megmutatjuk, hogy a hármas ciklusok generálják A_n-et. Ehhez persze elég megmutatni azt, hogy két transzpozíció szorzata előáll hármasciklusok szorzataként. Ha a két transzpozíciónak van közös eleme, akkor ez valójában egy hármas ciklus. Pl: $(12)(23) = (123)$. Ha nincsen, akkor két alkalmas transzpozíció beszúrásával a problémát visszavezethetjük az iménti esetre: $(12)(34) = (12)(23)(23)(34) = (123)(234)$. Ha tehát $N \lhd S_n$ és N tartalmaz hármas ciklust, akkor tartalmazza az összeset, és így az ezek által generált A_n-et is. Mivel A_n indexe kettő, ezért őt tartalmazó normálosztó nyilván csak önmaga vagy S_n lehet.

Tegyük most fel, hogy $N \lhd A_n$. Itt vigyázni kell, ugyanis abból hogy a hármas ciklusok konjugáltak S_n-ben, még nem következik, hogy A_n-ben is konjugáltak lennének, hiszen lehet, hogy a konjugáló elem nincs benne A_n-ben. A jelölés egyszerűsítése kedvéért tegyük fel, hogy $(123) \in N$, és legyen (ijk) egy tetszőleges hármas ciklus. Ekkor létezik, $\mu \in S_n$, amire $(ijk) = \mu^{-1}(123)\mu$. Ha μ páros, akkor $(ijk) \in A_n$. Ha páratlan, akkor $\mu(ij)$ páros, és így $(ij)\mu^{-1}(123)\mu(ij) = (ij)(ijk)(ij) = (jik) \in N$. Ekkor persze $(jik)^2 = (ijk)$ is eleme N-nek, és így $N = A_n$. $\square$

S_n feloldhatóságának vizsgálatához még egy tételre van szükségünk, ezt azonban most bizonyítás nélkül közöljük. Bár a bizonyítás nem túlságosan bonyolult, a különböző esetszétválasztások miatt hosszadalmas, és technikai. A bizonyítás megtalálható Fried Ervin [1] könyvében.

1.2.24. Tétel. *Ha $n \geq 5$, és N egy legalább kételemű normálosztó S_n-ben vagy A_n-ben, akkor N tartalmaz egy transzpozíciót vagy egy hármas ciklust.*

1.2.25. Tétel. *Ha $n \leq 4$ akkor S_n feloldható, míg $n \geq 5$ esetén nem az.*

Bizonyítás. Ha $n \geq 5$, és N egy valódi normálosztó S_n-ben, akkor a 1.2.24 tétel szerint $N = A_n$, és A_n-nek csak triviális normálosztói vannak. Így S_n egyetlen kompozíciólánca

$$S_n \rhd A_n \rhd \{1\}.$$

$A_n/\{1\}$ természetesen nem prímrendű, így S_n nem feloldható.

S_4 feloldhatóságának megmutatásához megadunk egy konkrét kompozícióláncot, melynek faktorai prímrendűek:

$$S_4 \rhd A_4 \rhd V \rhd \{(12)(34), id\} \rhd \{id\}$$

Itt V az úgynevezett Klein csoportot jelöli. ($V = \{(12)(34), (13)(24), (14)(23), id\}$) Az, hogy ez részcsoport, könnyen ellenőrizethő, hiszen bármely elem négyzete az identitás, és bármely két identitástól különböző elem szorzata a harmadik. Az, hogy normálosztó a 1.2.22 tétel következménye, hiszen V éppen a két transzpozíció szorzataként előálló permutációkat tartalmazza, és így önmagába konjugálódik.

Ha $n < 4$, akkor

$$S_n \rhd A_n \rhd \{1\}.$$

szintén kompozíciólánc, és a faktorok prímrendűek, hiszen a csoportnak egyszerűen nagyon kevés eleme van. $\square$

1.3. Topológiai alapfogalmak, topologikus csoportok

1.3.1. Definíció. *Az (X, Ω) párt topologikus térnek nevezzük, ha X tetszőleges halmaz, $\Omega \subseteq P(X)$, és a következő tulajdonságok teljesülnek:*

1. $\emptyset, X \in \Omega$
2. *Ha valamilyen A indexhalmazra minden $\alpha \in A$ esetén $U_\alpha \in \Omega$, akkor $\cup_{\alpha \in A} U_\alpha \in \Omega$.*
3. *$U_1, \ldots, U_n$ esetén $\cap_{i=1}^n U_i \in \Omega$.*

1.3.2. Definíció. *Az $U \subseteq X$ halmazt nyíltnak nevezzük, ha $U \in \Omega$. A $B \subseteq X$ halmazt zártnak nevezzük, ha a komplementere nyílt. A zárt halmazok rendszerét Ω'-vel jelöljük.*

1.3.3. Állítás. *A zárt halmazokra a nyílt halmazokéhoz nagyon hasonló tulajdonságok teljesülnek:*

1. $\emptyset, X \in \Omega'$
2. *Ha valamilyen A indexhalmazra minden $\alpha \in A$ esetén $B_\alpha \in \Omega'$, akkor $\cap_{\alpha \in A} B_\alpha \in \Omega'$.*
3. *$B_1, \ldots, B_n$ esetén $\cup_{i=1}^n B_i \in \Omega'$.*

1.3.4. Megjegyzés. X egy tetszőleges részhalmaza lehet nyílt, zárt, mindkettő, vagy egyik sem. Egy topológiát nyilván megadhatunk akár a nyílt, akár a zárt halmazok rendszerével.

1.3.5. Definíció. *Legyen $A \subseteq X$. Ekkor A belsejének nevezzük, és $intA$-val jelöljük az összes A-ban levő nyílt halmaz unióját. Az x pont A-nak belső pontja, ha $x \in intA$.*

1.3.6. Megjegyzés. Mivel nyílt halmazok uniója is nyílt, így $intA$ is nyílt, és nyilván ez a legbővebb A-ban lévő nyílt halmaz. A definícióból az is könnyen látszik, hogy A pontosan akkor nyílt, ha $A = intA$, azaz ha minden pontja belső pont.

1.3.7. Definíció. *Legyen $A \subseteq X$. Ekkor A lezártjának hívjuk, és $\bar{A}$-val jelöljük a legkisebb A-t tartalmazó zárt halmazt.*

1.3.8. Megjegyzés. Ez a lezárás teljesíti a korábban definiált lezárás operációt definiáló három tulajdonságot. Valóban, megmutatható, hogy tetszőleges lezáráshoz található olyan topológia, melyben az adott lezárás épp az imént definiált dolgot jelenti.

1.3.9. Definíció. *Legyen $x \in X$. Egy $U \subseteq X$ halmazt x egy környezetének mondjuk, ha létezik olyan V nyílt halmaz, amire $x \in V \subseteq U$.*

1.3.10. Állítás. *Tetszőleges x elemre $x \in \bar{A}$ pontosan akkor, ha x minden W környezetére $W \cap A \neq \emptyset$.*

Bizonyítás. Azt fogjuk belátni, hogy x nem eleme $\bar{A}$-nak pontosan akkor, ha x-nek van olyan környezete, melynek A-val vett metszete üres. Tegyük fel tehát, hogy x nem eleme $\bar{A}$-nak. Ez ekvivalens azzal, hogy létezik egy A-t tartalmazó F zárt halmaz, melynek nem eleme x. Ekkor viszont F komplementere egy x-et tartalmazó nyílt halmaz, mely nem metszi A-t. □

1.3.11. Definíció. *Egy $\Sigma \subseteq \Omega$ halmazt az (X, Ω) tér bázisának nevezünk, ha a tér minden nyílt halmaza előáll Σ-beli halmazok tetszőleges számosságú uniójaként.*

1.3.12. Definíció. *Egy $B_x \subseteq \Omega$ halmazt az $x \in X$ elem lokális bázisának nevezük, ha B_x minden eleme egy x-et tartalmazó nyílt halmaz, és az x pont minden környezetéhez létezik olyan B beli halmaz, mely része ennek a környezetnek.*

1.3.13. Megjegyzés. Egy tér bázisának az x-et tartalmazó elemei az x-nek lokális bázisát alkotják, illetve a tér összes eleméhez tartozó lokális bázisok uniója a térnek egy bázisát képezik.

1.3.14. Definíció. *Legyenek (X, Ω) és (Y, τ) topologikus terek. Egy $f : X \to Y$ leképezést folytonosnak hívunk, ha minden Y-beli nyílt halmaz ősképe nyílt (X-ben).*

1.3.15. Definíció. *Az $f : X \to Y$ függvény folytonos az $x \in X$ pontban, ha $f(x)$ minden V környezetéhez van olyan U környezete x-nek, amire $f(U) \subseteq V$.*

1.3.16. Állítás. *Egy függvény pontosan akkor folytonos, ha minden pontjában folytonos.*

1.3.17. Definíció. *Legyen f egy bijekció két topologikus tér alaphalmazai között. Ha f és f^{-1} is folytonos, akkor f-et homeomorfizmusnak hívjuk, és azt mondjuk, hogy a két tér homeomorf.*

1.3.18. Definíció. *Legyenek (X, Ω_1) és (Y, Ω_2) adott topologikus terek. Ekkor szorzattopológiának nevezzük az $X \times Y$ halmazon az*

$$\Omega = \{U \times V | U \in \Omega_1, V \in \Omega_2\}$$

bázis által generált topológiát. Ha végtelensok tér szorzatát tekintjük, akkor a báziselemek olyanok, hogy véges sok koordinátában az adott tér tetszőleges nyílt halmazát tekintjük, míg a többi koordinátában az egész teret, mint nyílt halmazt vesszük.

1.3.19. Definíció. *Legyen (X, Ω) egy topologikus tér. Ha $S \subseteq X$, akkor altér-topológiának nevezzük az (S, Ω_S) topológiát, ahol $\Omega_S = \{U \cap S | U \in \Omega\}$.*

1.3.20. Állítás. *Legyen (X, Ω) és (Y, τ) egy-egy topologikus tér, $A \subseteq X$ ellátva az altértopológiával, és $f : X \to Y$ folytonos függvény. Ekkor $F_{|A}$ is folytonos.*

Bizonyítás. Legyen $V \subseteq Y$ nyílt. Ekkor $f_{|A}^{-1}(V) = f^{-1}(V) \cap A$, ami nyílt az altértopológiában, hiszen $f^{-1}(V) \in \Omega$. $\square$

1.3.21. Definíció. *A G csoportot topologikus csoportnak nevezzük, ha adott az alaphalazán egy topológia, és a szorzás, mint $G \times G \to G$ függvény, valamint az inverzképzés, mint $G \to G$ függvény folytonosak. (Ahol $G \times G$ a szorzattopológiát jelöli.)*

1.3.22. Definíció. *Legyenek X, Y, Z topologikus terek. Azt mondjuk, hogy az $F : X \times Y \to Z$ leképezés mindkét változójában külön-külön folytonos, ha az $X \ni x \mapsto F(x, y_0)$, és az $Y \ni y \mapsto F(x_0, y)$ leképezések folytonosak minden rögzített $x_0 \in X$ és $y_0 \in Y$ mellett.*

1.3.23. Állítás. *Ha az $F : X \times Y \to Z$ leképezés folytonos, akkor mindkét változójában folytonos.*

Bizonyítás. Tetszőleges $x \in X$ rögzített elemre legyen F_x az az $\{x\} \times Y$ térből a Z térbe menő leképezés, mely a fenti definícióban szerepel, és legyen $V \subseteq Z$ nyílt. Ekkor $F^{-1}(V)$ nyílt $X \times Y$-ban, és így $F_x^{-1}(V) = F^{-1}(V) \cap (\{x\} \times Y)$ nyílt az altértopológiában, tehát F_x folytonos. $\square$

1.3.24. Következmény. Legyen G egy topologikus csoport, és minden $g \in G$ elemre $f_g : G \to G$, $h \mapsto g \cdot h$, a g-vel való balról szorzás. Ekkor ez egy folytonos leképezés, és mivel permutálja G elemeit, így bijekció is. Mivel ennek az inverze is ilyen alakú, $(f_g^{-1} = f_{g^{-1}})$ így az inverze is folytonos, vagyis f_g homeomorfizmus.

1.3.25. Állítás. *Legyen G egy topologikus csoport. Ekkor minden $g \in G$ elem minden V környezetéhez létezik az egységelemnek olyan U környezete, amire $V = gU$ teljesül.*

Bizonyítás. Legyen $U = g^{-1}V$. Mivel $g \in V$ így $1 \in U$. Legyen $W_1 \subseteq V$ egy g-t tartalmazó nyílt halmaz. Jelöljük W_2-vel a W_1 halmaz képét a g^{-1}-zel való balrólszorzásnál. Ekkor $W_2 \subseteq U$, $1 \in W_2$, és W_2 nyílt, hiszen a g^{-1}-zel való balrólszorzás homeomorfizmus. Vagyis U a kívánt tulajdonságú környezete 1-nek. $\square$

1.3.26. Definíció. *Legyen (X, Ω) egy topologikus tér. Ha minden $x, y \in X$ ponthoz létezik olyan $f : X \to X$ homeomorfizmus, melyre $f(x) = y$, akkor azt mondjuk, hogy a tér homogén.*

1.3.27. Állítás. *Minden topologikus csoport homogén.*

Bizonyítás. Legyen G egy topologikus csoport, és $x, y \in G$. Legyen f az yx^{-1} elemmel való balról szorzás. Mint láttuk ez homeomorfizmus, és az x elemet éppen$y$-ba viszi. Mivel x, y tetszőleges volt, így az állítást beláttuk. $\square$

Mivel egy topologikus csoport mindig homogén, így a csoport egy bázisának megadásához elég az egységelemnek egy lokális bázisát megadni. Valóban, tetszőleges x elemhez létezik homeomorfizmus, mely az egységelemet x-be viszi, és ez a leképezés az egységelem egy lokális bázisát az x elem egy lokális bázisába képezi. Ily módon a tér minden eleméhez találtunk egy lokális bázist, és ezek uniója az egész térnek egy bázisa lesz.

1.3.28. Állítás. *Legyen G egy topologikus csoport, és $H \leq G$. Ekkor H az altér-topológiával ellátva szintén topologikus csoport.*

Bizonyítás. A 1.3.20 állítás alapján nyilvánvaló, hiszen H műveletei, a G műveleteinek megszorításai. $\square$

1.3.29. Állítás. *Legyen G egy topologikus csoport, és $H \leq G$. Ekkor $\bar{H}$ is részcsoport, és ha H normálosztó G-ben, akkor $\bar{H}$ is az.*

Bizonyítás. Elég belátni, hogy minden $a, b \in \bar{H}$ esetén $ab^{-1} \in \bar{H}$, hiszen ekkor $1 = aa^{-1} \in \bar{H}$, és így $1a^{-1} = a^{-1} \in \bar{H}$, valamint $a(b^{-1})^{-1} = ab \in \bar{H}$.

Legyen W egy az ab^{-1} elemet tartalmazó nyílt halmaz. Mivel a szorzás folytonos, ennek az ősképe egy nyílt halmaz lesz $G \times G$-ben. Mivel egy a szorzattopológiában nyílt halmaz a G-ben nyílt halmazok direktszorzatának uniójaként áll elő, így létezik $U, V \subseteq G$ nyíltak, hogy U az a-t tartalmazó, V a b-t tartalmazó nyílt halmaz, valamint $U \times V^{-1}$ része az ősképnek, és így $UV - 1 \subseteq W$. Mivel $a, b \in \bar{H}$ így U-nak és V-nek is van közös pontja H-val. Jelöljük ezeket ilyen sorrendben x-szel, és y-nal. Mivel H részcsoport, így $y^{-1} \in H$, és így $xy^{-1} \in H$, azaz $W \cap H \neq \emptyset$. Mivel W tetszőleges környezet volt, így $ab^{-1} \in \bar{H}$. $\square$

1.3.30. Definíció. *Az X tér kompakt, ha minden nyílt fedéséből kiválasztható véges fedés. Az X egy A részhalmazát kompaktnak nevezzük, ha az altértopológia szerint kompakt.*

1.3.31. Állítás. *Ha A egy zárt részhalmaza a kompakt X térnek, akkor A is kompakt.*

Bizonyítás. Tekintsük A-nak egy $\{U_i\}$ nyílt fedését. Ekkor $\{U_i, X \setminus A\}$ egy nyílt fedése X-nek, vagyis kiválasztható belőle véges fedés. Ebből a véges fedésből $X \setminus A$-t elhagyva A-nak egy véges fedését kapjuk. $\square$

1.3.32. Tétel. (Tychonoff tétel) *Kompakt topologikus terek szorzata is kompakt.*

1.3.33. Definíció. *Az X topologikus tér Hausdorff-tér, ha minden $a, b \in X$-nek létezik olyan U_a és U_b környezete, hogy $U_a \cap U_b = \emptyset$.*

1.3.34. Definíció. *Az x topologikus tér összefüggő, ha tetszőleges $X = U \cup V$ nyílt halmazokra való felbontásában U vagy V mindenképpen üres. A tér egy részhalmaza összefüggő, ha az altér topológiában összefüggő.*

1.3.35. Állítás. *Közös ponttal rendelkező összefüggő halmazok uniója is összefüggő.*

1.3.36. Következmény. Tetszőleges $a \in X$-hez létezik legbővebb a-t tartalmazó összefüggő halmaz, hiszen az $\cup\{A | a \in A,$ és A összefüggő$\}$ tartalmazza a-t és összefüggő.

1.3.37. Definíció. *Az X topologikus tér maximális összefüggő halmazait, X komponenseinek nevezzük.*

1.3.38. Definíció. *Az X topologikus teret totálisan összefüggéstelennek nevezzük, ha komponensei az egypontú halmazok*

2. fejezet

Testbővítések

Ebben a fejezetben részben felidézzük, részben továbbmegyünk és mélyebben, vagy más szempontból tárgyaljuk a testbővítések fogalmát. A Galois-megfeleltetések az úgynevezett Galois-bővítések, és ezek automorfizmus csoportjai között jönnek létre. A Galois-bővítések három karakterizáló tulajdonsága, hogy algebraiak, normálisak és szeparábilisek. Ennek megfelelően e három tulajdonság tárgyalása következik most.

2.1. Algebrai bővítések

2.1.1. Definíció. *Az L test a K testnek egy bővítése, ha $K \leq L$. Ezt $L|K$-val is jelöljük. Ha L a legszűkebb olyan test, ami a K-n kívül egy H halmaz elemiet is tartalmazza, akkor azt mondjuk, hogy L a K-nak a H-val való bővítése, és $L = K(H)$-val jelöljük. Amennyiben H egyetlen a elemből áll, úgy egyszerű bővítésről beszélünk, és $K(a)$-val jelöljük.*

2.1.2. Definíció. *tekintsük az $L|K$ testbővítést. L egy tetszőleges a elemét algebrainak nevezzük a K test felett, ha létezik olyan $f \in K[x]$ nem azonosan 0 polinom, melynek a gyöke. Ha a nem algebrai (K-felett), akkor transzcendens.*

2.1.3. Tétel. *A K felett algebrai a elemhez létezik egy egyértelműen meghatározott, irreducibilis, 1 főegyütthatós $f \in K[x]$ polinom, melynek a gyöke. Ha a gyöke egy tetszőleges $g \in K[x]$ polinomnak, akkor $f \mid g$.*

Bizonyítás. Tekintsük azt a $\varphi : K[x] \to K(a)$ homomorfizmust, mely a konstans polinomokhoz a megfelelő K-beli elemeket, x-hez pedig a-t rendeli. (Ez lényegében az a behelyettesítése az adott polinomba. Annak bizonyítása, hogy ez valóban homomorfizmus egyszerű számolás, ettől most eltekintünk.) Ennek a magja pontosan azokból a $K[x]$-beli polinomokból áll, amiknek a gyöke. Mivel egy gyűrűmorfizmus magja csak a gyűrű egy ideálja lehet, és tetszőleges test fölötti polinomgyűrű főideálgyűrű, ezért létezik $f \in K[x]$ amire $Ker(\varphi) = (f)$, és f minimális fokú eleme $Ker(\varphi)$-nek. Mivel f tetszőleges konstansszorosa is ugyanazt az ideált generálja, feltehető, hogy f normált.

Ha f felbomlana a g és h nem konstans polinomok szorzatára, akkor a gyöke lenne legalább az egyik tényezőnek. Ha például $g(a) = 0$ akkor $g \in Ker(\varphi)$, viszont g foka nyilván kisebb mint f foka, ami ellentmond $deg(f)$ minimalitásának, tehát f valóban irreducibilis.

Legyen most g egy tetszőleges $K[x]$-beli polinom, aminek gyöke a. Ez azt jelenti, hogy $g \in Ker(\varphi) = (f)$ azaz g előáll $h \cdot f$ alakban valamilyen $h \in K[x]$ polinomra. Tehát $f \mid g$. $\square$

2.1.4. Definíció. *A fenti f polinomot az a elem minimálpolinomjának nevezzük. Az a fokán a minimálpolinomjának fokát értjük.*

2.1.5. Tétel. *Legyen $K|L$ egy bővítés, és $a \in L$ egy algebrai elem, melynek minimálpolinomja f. Ekkor $K[x]/(f) \cong K(a)$ és az izomorfizmusnál az a elemnek az $x + (f)$, tetszőleges $k \in K$ elemnek pedig a $k + (f)$ maradékosztály felel meg.*

Bizonyítás. Mint láttuk, a $\varphi : K[x] \to K(a)$ "a behelyettesítése" homomorfizmus magja nem más, mint az f által generált ideál. A gyűrűk homomorfizmus-tétele alapján (ami ugyan azt mondja ki, mint a csoportokra vonatkozó tétel, csak normálosztó helyett ideállal) tudjuk, hogy $K[x]/(f) \cong Im(\varphi)$. Az állítás belátásához tehát csak annyi szükséges, hogy $Im(\varphi) = K(a)$ teljesüljön. Az egyik irányú tartalmazás triviális, hiszen $Im(\varphi)$ elemei a hatványainak K-beli együtthatós lineáris kombinációiként állnak elő, így ezek nyilván benne vannak $K(a)$-ban. Ugyanakkor az f irreducibilitása miatt $Im(\varphi)$ test, és tartalmazza az a elemet, így nyilván részteste az a-t és K-t tartalmazó legszűkebb test, vagyis $K(a)$. $\square$

2.1.6. Tétel. *Tetszőleges $f \in K[x]$ irreducibilis polinomhoz létezik olyan egyszerű $K(a)$ bővítés, hogy a az f-nek gyöke.*

Bizonyítás. Mivel f irreducibilis, így $L = K[x]/(f)$ test. Ez a konstans polinomok szerinti maradékosztályok formájában nyilvánvalóan tartalmaz egy K-val izomorf K' résztestet. Tudjuk, hogy $L = K'(x + (f))$ hiszen L minden eleme előáll az x és a konstans polinomok szerinti maradékosztályokból az összeadás, kivonás és szorzás segítségével. Legyen most $N = (L \setminus K') \cup K$ és tekintsük azt az $\eta : L \to N$ leképezést, ami K' elemeihez a megfelelő K-beli elemeket rendeli, L többi elemét pedig fixen hagyja. Mivel ez egy bijekció L és N között, így N-en definiálhatjuk úgy a műveleteket, hogy η izomorfizmus legyen. Ha most az $x + (f)$ maradékosztályt a-val jelöljük, akkor az izomorfizmus miatt $N = K(a)$.

Ahhoz, hogy $f(a) = 0$-t belássuk, vissza kell mennünk az L testbe. Mivel η izomorfizmus, elég azt belátni, hogy $\eta^{-1}(f)$-nek gyöke $\eta^{-1}(a)$, ahol $\eta^{-1}(f)$ azt a polinomot jelöli, amit úgy kapunk, hogy f együtthatóira alkalmazzuk az η^{-1} függvényt. (Ha η izomorfizmus az alaptestek között, akkor ily módon kiterjesztve a polinomgyűrűre szintén izomorfizmust kapunk. Ez nem triviális, de egyszerű számolás után adódik.) Ha az $\eta^{-1}(f)$ polinomba behelyettesítjük az $\eta^{-1}(a) = a = x + (f)$ maradékosztályt, akkor éppen az $f + (f)$ maradéksoztály adódik, ami nem más, mint L nulleleme. $\square$

2.1.7. Megjegyzés. Az is igaz, hogy a K testnek mindig létezik egyszerű transzcendens bővítése. Ennek bizonyítása szintén a polinomgyűrűn keresztül történik, egy hányadostest nevű konstrukció segítségével, ami lényegében annak a módszernek az általánosítása, ahogy az egész számok gyűrűjéből megkapjuk a racionális számtestet.

2.1.8. Tétel. *Legyen L a K testnek egy tetszőleges bővítése, és $a \in L$. Az a elem pontosan akkor algebrai K felett, ha $K(a)$ mint K feletti vektortér (a $K(a)$-beli összeadásra, és a K elemeivel való szorzásra nézve) véges dimenziós. Ez a dimenzió megegyezik az a elem fokával.*

Bizonyítás. Legyen a algebrai K felett, és legyen a minimálpolinomja f, ahol $deg(f) = n$. Az állítás azon része, hogy $K(a)$ vektortér K felett triviális. Mint az korábban láttuk, $K(a) \cong K[x]/(f)$, így elég ez utóbbinak egy n elemű bázisát találni a K test felett. A lineáris függetlenség ebben a gyűrűben azt jelenti, hogy az adott elem semmilyen nem triviális lineáris kombinációja nem lehet osztható f-fel, míg a generátorrendszerség azt, hogy bármilyen $g \in K[x]$ polinomhoz létezik az adott elemeknek olyan lineáris kombinációja, amit g-ből kivonva az eredmény f-fel osztható. Azt állítjuk, hogy az $1, x, \ldots, x^{n-1}$ polinomrendszer kielégíti ezeket a feltételeket. Egyrészt ezek minden lineáris kombinációja egy n-nél kisebb fokú polinom, aminek tehát f nem lehet osztója, másrészt ezekből minden n-nél kisebb fokú polinom kikeverhető, speciálisan g-nek az f-fel vett osztási maradéka is.

Tegyük most fel, hogy $K(a)$ véges dimenziós K felett, és legyen ez a dimenzió n. Ekkor az $1, a, \ldots, a^n$ elem lineárisan összefüggőek, azaz léteznek $b_1, b_1, \ldots, b_n$ K-beli elemek, hogy

$b_0 + b_1 a + \cdots + b_n a^n = 0$, vagyis a gyöke az $f = b_0 + b_1 x + \cdots + b_n x^n$ polinomnak, ami éppen azt jelenti, hogy a algebrai K felett. $\square$

2.1.9. Definíció. *Legyen L a K testnek egy bővítése. Az $L|K$ bővítés fokán L-nek mint K feletti vektortérnek a dimenzióját értjük, és $|L:K|$-val jelöljük. Ha $|L:K|$ véges, akkor véges bővítésről beszélünk.*

2.1.10. Definíció. *Legyen L a K testnek egy bővítése. Ha L minden eleme algebrai K felett, akkor az $L|K$ bővítést algebrainak nevezzük.*

2.1.11. Tétel. (Algebrai bővítések szorzástétele) *Legyenek $K \leq L \leq M$ testek. Ha $|L:K|$ és $|M:L|$ végesek, akkor $|M:K|$ is az, és $|M:K| = |L:K| \cdot |M:L|$.*

Bizonyítás. Legyen $\alpha_1, \ldots, \alpha_n$ L-nek egy K feletti, $\beta_1, \ldots, \beta_k$ M-nek egy L feletti bázisa, és $b \in M$ tetszőleges. Ekkor b felírható $\gamma_1\beta_1 + \cdots + \gamma_k\beta_k$ alakban, ahol $\gamma_i \in L$. Minden egyes γ_i felírható $c_{i,1}\alpha_1 + \cdots + c_{i,n}\alpha_n$ alakban, ahol $c_{i,j} \in K$, ami éppen azt jelenti, hogy $\{\alpha_i\beta_j | i = 1\ldots n, j = 1\ldots k\}$ generátorrendszere M-nek K felett.

A lineáris függetlenség belátásához tegyük fel, hogy ezen elemek valamilyen $d_{i,j} \in K$ együtthatós kombinációja 0. A $\gamma_j = d_{1,j}\alpha_1 + \cdots + d_{n,j}\alpha_j$ jelöléssel $\gamma_1\beta_1 + \cdots + \gamma_k\beta_k = 0$-t kapunk. Mivel a γ-t definiáló összeg minden tagja L-beli, így γ is L beli, és így a β-k lineáris függetlensége miatt minden γ_j együttható 0. Ebből az α-k lineáris függetlensége alapján minden $d_{i,j}$ együttható is 0, vagyis tényleg bázist kaptunk. Mivel a bázis elemszáma megegyezik a vektortér dimenziójával, ezért $|M:K| = n \cdot k$. $\square$

2.1.12. Állítás. *Minden véges bővítés algebrai.*

Bizonyítás. Legyen $L|K$ egy véges bővítés, és $a \in L$. Ekkor $K(a)$ mint vektortér altere L-nek, így maga is véges dimenziós. Mint láttuk, ez éppen azt jelenti, hogy a algebrai K felett. $\square$

2.1.13. Állítás. *Az $L|K$ bővítés pontosan akkor véges, ha léteznek $a_1, \ldots, a_n \in L$, K felett algebrai elemek, amikre $L = K(a_1, \ldots, a_n)$.*

Bizonyítás. Ha L véges bővítése K-nak, akkor létezik $a_1, \ldots, a_n$ véges bázisa, és nyilván $L = K(a_1, \ldots, a_n)$.

A másik irányhoz legyen $L_0 = K$ és $L_i = L_{i-1}(a_i)$ minden $i = 1, \ldots, n$ esetén. Mivel a_i algebrai K felett, így nyilván algebrai a K-nál bővebb L felett is, és így minden $|L_i : L_{i-1}|$ index véges. A szorzástétel alapján tehát $|L:K|$ is véges. $\square$

2.1.14. Következmény. Algebrai elemmel való bővítés algebrai.

2.1.15. Állítás. *Ha L a K-nak, illetve M az L-nek algebrai bővítése, akkor az $M|K$ bővítés is algebrai.*

Bizonyítás. Legyen $a \in M$. Mivel M algebrai L felett, létezik egy $f = b_0 + b_1x + \cdots + b_kx^k \in L[x]$ polinom, aminek a gyöke. Ekkor a algebrai $K(b_0, b_1, \ldots, b_k)$ felett. Mivel $K(b_0, b_1, \ldots, b_k)$ véges sok algebrai elemmel való bővítése K-nak, így véges bővítés, vagyis a szorzástétel alapján $K(b_0, b_1, \ldots, b_k, a)$ is véges. Ez utóbbi bővítésnek tehát minden eleme, speciálisan a is algebrai K felett. $\square$

2.1.16. Következmény. Ha a algebrai K felett, és $b \in K(a)$ akkor b is algebrai K felett, és b foka osztója a fokának.

2.2. Normális bővítés, felbontási test

2.2.1. Definíció. *Legyen $P \subseteq K[x]$. Az $L \geq K$ testet a P polinomhalmaz felbontási testének nevezzük, ha P minden eleme lineáris faktorokra bomlik L felett, és L a K-nak éppen a P-beli polinomok gyökeivel való bővítése.*

2.2.2. Tétel. *Ha $P \subseteq K[x]$ egy véges halmaz, akkor P-nek létezik felbontási teste K felett.*

Bizonyítás. Először tekintsük azt az esetet, amikor P egyetlen f polinomból áll. A bizonyítást ennek a polinomnak a fokára vonatkozó indukcióval végezzük. Az elsőfokú polinomoknak nyilván létezik felbontási teste, és ez megegyezik az alaptesttel. Tegyük fel tehát, hogy tetszőleges test felett az állítás minden n-nél kisebb fokú polinomra igaz, és legyen $deg(f) = n$. Legyen p az f-nek egy K felett irreducibilis faktora. Ekkor K-nak létezik olyan $K(a)$ bővítése, ahol a gyöke p-nek. Ekkor persze a gyöke f-nek is, tehát $f(x) = (x - a)g(x)$ alakba írható, ahol $g(x) \in K[x]$, és $deg(g) = n - 1 \leq n$. Alkalmazható tehát az indukciós feltevés g-re, miszerint g-nek létezik az L felbontási teste $K(a)$ felett, és ez éppen a g gyökeivel való bővítés. Ez az L egyben az f felbontási teste is a K test felett, hiszen L éppen K-nak az f gyökeivel való bővítése.

Ha most P véges elemszámú halmaz, akkor P helyett tekinthetjük az összes P-beli polinom szorzatát. Ennek a polinomnak az előbbiek alapján létezik felbontási teste, és nyilván megegyezik a P polinomhalmaz felbontási testével, hiszen a szorzatpolinom összes gyökével való bővítés éppen a P összes elemének összes gyökével való bővítés. $\square$

2.2.3. Megjegyzés. Felbontási test akkor is létezik, ha P végtelen számosságú. Ennek egy speciális esete, ha $P = K[x]$. Ekkor a P felbontási testét a K test algebrai lezártjának nevezzük és $\bar{K}$-val jelöljük. Ha K megegyezik az algebrai lezártjával, akkor azt mondjuk, hogy K algebrailag zárt.

2.2.4. Tétel. (Izomorfizmus-kiterjesztési tétel) *Legyen $L|K$ és $N|M$ két testbővítés, $\psi : K \to M$ egy izomorfizmus, valamint $f \in K[x]$ egy irreducibilis polinom. Ekkor $g = \psi(f)$ is irreducibilis $M[x]$-ben, és ha $\alpha \in L$ gyöke f-nek, valamint $\beta \in N$ gyöke g-nek, akkor létezik olyan*

$$\varphi : K(\alpha) \to M(\beta)$$

izomorfizmus, melyre $\varphi(\alpha) = \beta$ és φ megszorítva K-ra egyenlő ψ-vel.

Bizonyítás. Először is g irreducibilis $M[x]$-ben, hiszen ha felbomlana az $r \cdot s$ nem konstans polinomok szorzatára, akkor az izomorfizmus inverzénél f is felbomlana $\psi^{-1}(r) \cdot \psi^{-1}(s)$ nem konstans polinomok szorzatára.

Mivel α-nak f, β-nak g a minimálpolinomja, így $K(\alpha) \cong K[x]/(f)$ és $M(\beta) \cong M[x]/(g)$. Ha tekintjük a $K[x] \to M[x]/(g)$, $h \mapsto \psi(h)+(g)$ leképezést, akkor a homomorfizmus-tétel alapján $K[x]/(f) \cong M[x]/(g)$, ahol a $h + (f)$ maradékosztálynak a $\psi(h) + (g)$ maradékosztály felel meg. (Hiszen a fenti leképezés magja éppen azokból a $h \in K[x]$ polinomokból áll, melyekre $g \mid \psi(h)$ ami pontosan akkor teljesül, ha $f \mid h$, és tetszőleges $h \in M[x]$-re a $h + (g)$ maradékosztály előáll mint $\psi^{-1}(h) \in K[x]$ képe.) A fenti izomorfizmusok kompozícióját véve egy $\varphi : K(\alpha) \to M(\beta)$ izomorfizmust kapunk. Kiindulva α-ból először $x + (f)$-et, innen $x + (g)$-t és végül β-t kapunk. Tetszőleges $k \in K$ elemet φ a neki megfelelő konstans polinom szerinti maradékosztályon keresztül $\psi(k)$-ba viszi. □

2.2.5. Tétel. *Tegyük fel, hogy $L|K$ és $N|M$ két testbővítés, $\psi : K \to M$ izomorfizmus és $f \in K[x]$. Tudjuk továbbá, hogy L felbontási teste f-nek K felett, és N felbontási teste $g = \psi(f)$-nek M felett. Ekkor létezik $\varphi : L \to N$ izomorfizmus, mely K-ra megszorítva egyenlő φ-vel.*

Bizonyítás. A bizonyítást az f fokszáma szerinti indukcióval végezzük. Elsőfokú és konstans polinomokra az állítás triviális. Tegyük fel tehát, hogy $deg(f) = n$, és kisebb fokú polinomokra az állítást már beláttuk. Legyen $p \in K[x]$ egy irreducibilis faktora f-nek, és $\alpha \in L$ a p-nek egy gyöke. (Ilyen α van, hiszen L az f felbontási teste, és p gyökei az L gyökei közül valók.) ugyanígy $\psi(p)$ egy irreducibilis faktora lesz g-nek, és $\psi(p)$-nek létezik egy $\beta \in N$ gyöke. Az izomorfizmus-kiterjesztési tétel miatt ψ-nek létezik egy $\eta : K(\alpha) \to M(\beta)$ kiterjesztése.

Ezen a ponton van két $L|K(\alpha)$ és $N|M(\beta)$ testbővítésünk, és egy $\eta : K(\alpha) \to M(\beta)$ izomorfizmusunk.Tekintsük a $h(x) = f(x)/(x-0) \in K(\alpha)$ polinomot, melynek foka $n-1$. Az L test felbontási teste h-nak $K(\alpha)$ felett, hiszen h-nak a gyökei éppen f-nek az α-tól különböző gyökei, és így $K(\alpha)$-nak h gyökeivel való bővítése megegyezik K-nak f gyökeivel való bővítésével. ugyanígy N felbontási teste $\eta(h(x)) = g(x)/(x-\beta)$-nak $M(\beta)$ felett, és így az indukciós feltevés miatt η kiterjeszthető $L \to N$ izomorfizmussá, ami nyilván ψ-nek is kiterjesztése lesz. $\square$

2.2.6. Következmény. Ha a fenti tételben $K = M$ és ψ az identitás, akkor azt kapjuk, hogy egy adott $f \in K[x]$ polinom K feletti felbontási teste egy a K elemeit fixen hagyó izomorfizmustól eltekintve egyértelmű.

2.2.7. Megjegyzés. Mivel egy véges polinomhalmaz felbontási teste megegyezik a polinomok szorzatának felbontási testével, így egy K-t fixen hagyó izomorfizmus erejéig ez is egyértelmű. Az analóg állítás igaz végtelen számosságú polinomhalmaz esetén is.

2.2.8. Definíció. *Legyen L a K test egy algebrai bővítése, és $a, b \in L$. Ha a és b K feletti minimálpolinomjai megegyeznek, akkor azt mondjuk, hogy a és b konjugáltak K fölött.*

2.2.9. Definíció. *A K test egy algebrai bővítését normálisnak hívjuk, ha minden $a \in L$ elemre L tartalmazza a összes K feletti $\bar{K}$-beli konjugáltját. Más szóval, ha L tartalmazza egy $f \in K[x]$ irreducibilis polinom egy gyökét, akkor az összeset tartalmazza.*

2.2.10. Tétel. *Legyen $L|K$ egy normális bővítés. Ekkor L egy alkalmas K feletti polinomhalmaz felbontási teste. Ha $|L : K|$ véges, akkor a polinomhalmaz is megválasztható végesnek.*

Bizonyítás. A feltétel szerint L minden eleme algebrai K felett. Legyen L' az L elemeihez tartozó minimálpolinomok halmazának felbontási teste. Mivel L normális bővítése K-nak, így L minden elemének minden konjugáltját is tartalmazza, vagyis $L' \leq L$. Másrészt L'-t eleve úgy csináltuk, hogy L minden elemét tartalmazza, tehát $L \leq L'$ és így $L = L'$.

Tegyük most fel, hogy $|L : K|$ véges. Ekkor léteznek $a_1, \ldots, a_n$ algebrai elemek, hogy $L = K(a_1, \ldots, a_n)$. Legyen L' az $a_1, \ldots, a_n$ elemek minimálpolinomjainak felbontási teste. Akárcsak az előbb, most is könnyen látható, hogy $L' = L$. $\square$

A következő tétel bizonyításához szükség lesz a szimmetrikus polinomok fogalmára, illetve a szimmetrikus polinomok alaptételére, melyet most bizonyítás nélkül közlünk.

2.2.11. Definíció. *Az $f \in K[x_1, \dots, x_n]$ polinomot szimmetrikusnak nevezzük, ha a változóit tetszőlegesen permutálva ugyan azt a polinomot kapjuk. $\sigma_k(x_1, \dots, x_n)$-el jelöljük a K-adik elemi szimmetrikus polinomot $(1 \leq k \leq n)$, amit úgy kapunk, hogy az $x_1, \dots, x_n$ határozatlanok közül az összes lehetséges módon kiválasztunk k különbözőt, a kiválasztott elemeket összeszorozzuk, majd az összes ilyen szorzatot összeadjuk. $k = 0$ esetén σ_0-t a konstans 1 polinomnak definiáljuk.*

2.2.12. Tétel. (Szimmetrikus polinomok alaptétele) *Legyen $f \in K[x_1, \dots, x_n]$ egy tetszőleges szimmetrikus polinom. Ekkor egyértelműen létezik egy $F \in K[y_1, \dots, y_n]$ polinom, melyre*

$$f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n).$$

Más szóval minden szimmetrikus polinom felírható az elemi szimmetrikus polinomok polinomjaként.

2.2.13. Tétel. *Legyen $K \leq L$ két test. Ha L egy $P \subseteq K[x]$ polinomhalmaz felbontási teste, akkor a $K|L$ testbővítés normális.*

Bizonyítás. Legyen L a P polinomhalmaz felbontási teste, és $g \in K[x]$ irreducibilis polinom. Tegyük fel, hogy g felbomlik $L[x]$-ben a $g_1, \dots, g_r$ polinomok szorzatára. Nem megy az általánosság rovására, ha feltesszük, hogy minden g_i polinom normált, és fokszám szerint növekvő sorrendben vannak.

Első állításunk, hogy létezik olyan $f \in K[x]$ polinom, aminek M felbontási teste feletti $M[x]$ polinomgyűrű tartalmazza az összes g_i polinomot. Valóban, L minden eleme felírható véges sok P-beli polinomok gyökeinek K-beli együtthatós kombinációjaként, így L minden eleme benne van egy véges polinomhalmaz felbontási testében. Mivel minden g_i polinomnak véges sok együtthatója van, így ezek benne vannak véges sok véges polinomhalmaz uniójának felbontási testében. Mivel véges polinomhalmaz felbontási teste megegyezik egy alkalmasan választott polinom felbontási testével, így ezt az állítást beláttuk.

Megjegyezzük, hogy mivel g_i irreducibilis $L[x]$-ben, így nyilván irreducibilis az ennél szűkebb $M[x]$ polinomgyűrűben is. Legyen tehát $M = K(a_1, \dots, a_n)$, ahol $a_1, \dots, a_n$ az f összes gyöke. $g_i \in M[x]$ miatt g_i minden együtthatója felírható az a_j-k K-beli együtthatós polinomjaként. Mivel ez a felírás nem egyértelmű, rögzítsük a $g_i'(y_1, \ldots, y_n, x)$ polinomokat úgy, hogy minden i-re $g_i'(a_1, \ldots, a_n, x) = g_i(x)$ teljesüljön. Definiáljuk a $G'(y_1, \ldots, y_n, x) \in K[y_1, \ldots, y_n, x]$ polinomot a következőképpen:

$$G'(y_1, \ldots, y_n, x) = \prod_{\sigma \in S_n} g_1(y_{\sigma(1)}, \ldots, y_{\sigma(n)}, x).$$

G' az $y_1, \ldots, y_n$ határozatlanok szimmetrikus polinomja, hiszen ezek tetszőleges permutációja csak a szorzat tényezőit permutálja. Ha tehát most G'-re mint x-nek a polinomjára tekintünk, akkor azt kapjuk, hogy minden együtthatója az y_i-k szimmetrikus polinomja, és így az alaptétel szerint felírható az y_i-k elemi szimmetrikus polinomjainak K-beli együtthatós polinomjaként.

A Viete-formulák alapján az $a_1, \ldots, a_n$ elemek elemi szimmetrikus polinomjai (előjeltől eltekintve) éppen az f együtthatói (feltéve persze, hogy f normált). Így a $G(x) = G'(a_1, \ldots, a_n, x)$ polinom együtthatói mind K-beliek, azaz $G(x) \in K[x]$. Tudjuk továbbá, hogy $g_1(x) \mid G(x)$, hiszen a $G(x)$-et definiáló szorzatban megjelenik g_1 is, amikor σ az identikus permutáció. Azt állítjuk, hogy ebből következik a $g(x) \mid G(x)$ oszthatóság. Valóban, g irreducibilitása miatt g és G legnagyobb közös osztója $K[x]$-ben vagy konstans, vagy g. Ha ez egy c konstans volna, akkor c előállna $q \cdot g + r \cdot G$ alakban, ahol $q, r \in K[x]$. Ekkor viszont $M[x]$-ben is előállna így, ami ellentmondás, hiszen g_1 osztja az iménti összeget, de nem osztja c-t.

Az $M[x]$ polinomgyűrűre visszatérve az imént megállapított oszthatóság alapján minden i-re g_i osztója $G(x)$-nek. Mivel $g_i(x)$ irreducibilis (és így prím is), osztója a $G(x)$-et definiáló összeg egyik tagjának. Ezen tagok mindegyike $g_1(b_1, \ldots, b_n, x)$ alakú, ahol $b_1, \ldots, b_n$ az f gyökeinek felsorolása valamilyen sorrendben. Ennek a foka természetesen megegyezik $g_1(x)$ fokával, ami a feltétel szerint nem nagyobb g_i fokánál. Másrészt az oszthatóság miatt $g_i(x)$ foka nem lehet nagyobb $g_1(b_1 \ldots, b_n, x)$ fokánál, vagyis a két polinom foka megegyezik.

Ott tartunk tehát, hogy tetszőleges $g \in K[x]$ irreducibilis polinomról beláttuk, hogy $L[x]$-ben azonos fokú faktorok szorzatára bomlik. Ekkor ha g-nek van gyöke L-ben, akkor van lineáris faktora is, és így g lineáris faktorokra bomlik, vagyis az $L|K$ bővítés valóban normális. $\square$

2.3. Szeparábilitás

2.3.1. Definíció. *Legyen K egy test és L illetve M két bővítése K-nak. Egy $\tau : L \to M$ homomorfizmust K feletti relatív homomorfizmusnak, vagy K-homomorfizmusnak nevezünk, ha K minden elemét fixen hagyja. Az L-ből M-be menő K-homomorfizmusok halmazát $Hom_K(L, M)$-el jelöljük.*

2.3.2. Állítás. *Legyen $\tau \in Hom_K(L, M)$, $a \in L$ és $f \in K[x]$. Ekkor $\tau(f(a)) = f(\tau(a))$.*

Bizonyítás. Legyen $f = b_0 + b_1x + \cdots + b_nx^n$. Ekkor $\tau(f(a)) = \tau(b_0 + b_1a + \cdots + b_na^n) = \tau(b_0) + \tau(b_1)\tau(a) + \cdots + \tau(b_n)\tau(a)^n = b_0 + b_1\tau(a) + \cdots + b_n\tau(a)^n = f(\tau(a))$. □

2.3.3. Tétel. *Legyen $K(a)|K$ és $L|K$ két testbővítés. Ekkor az a leképezés, ami tetszőleges $\tau : K(a) \to L$ K-homomorfizmushoz hozzárendeli $\tau(a)$-t egy bijekció $Hom_K(K(a), L)$ és a L-ben lévő K-feletti konjugáltjai között.*

Bizonyítás. Jelölje a minimálpolinomját f. Először is be kell látnunk, hogy a fenti leképezés tényleg az említett $\{\beta \in L|f(\beta) = 0\}$ halmazba képez. Az előző állításunk szerint $f(\tau(a)) = \tau(f(a)) = \tau(0) = 0$, vagyis a leképezés tényleg értelmes.

Az injektivitás a következőképpen látható be: $K(a)$ minden eleme előáll $g(a)$ alakban, ahol $g \in K[x]$. (Hiszen $K(a)$ izomorf $K[x]/(f)$-el, és így az adott elemnek megfelelő maradékosztály egy reprezentáns eleme jó lesz g-nek.) Ha tehát $\tau_1(a) = \tau_2(a)$ akkor $\tau_1(g(a)) = g(\tau_1(a)) = g(\tau_2(a)) = \tau_2(g(a))$ vagyis $\tau_1 = \tau_2$.

A szürjektivitáshoz tegyük fel, hogy $\beta \in L$ és $f(\beta) = 0$. Legyen $\varphi : K[x] \to L$ a "β behelyettesítése" homomorfizmus. $f(\beta) = 0$ alapján $f \in Ker(\varphi)$. Mivel f irreducibilis, így (f) maximális ideál. $Ker(\varphi)$ nyilván nem az egész $K[x]$, de tartalmazza (f)-et, így valójában megegyezik (f)-el. A homomorfizmus-tétel szerint tehát $Im(\varphi) \cong K[x]/(f)$, ami viszont izomorf $K(a)$-val. Az izomorfizmusok kompozíciójánál az a képe az $x + (f)$ maradékosztályon keresztül éppen β, így kaptunk egy $K(a) \to L$ homomorfizmust, ami a-t β-ba viszi. □

2.3.4. Következmény. A fenti tételből adódik, hogy a $K(a) \to L$ K-homomorfizmusok számára felső korlát a minimálpolinomjának, vagyis a-nak a foka. A bizonyítás során az is kijött, hogy a konjugáltjai éppen a lehetésges képei a $\tau \in Hom_K(K(a), L)$ homomorfizmusoknál, illetve, hogy egy ilyen homomorfizmus a-t mindenképpen valamelyik konjugáltjába viszi, és minden konjugálthoz létezik is olyan homomorfizmus, aminél a képe az adott konjugált.

2.3.5. Definíció. *Legyen $L|K$ egy testbővítés. Az $a \in L$ elemet szeparábilisnek nevezzük (K felett), ha K-feletti minimálpolinomjának K egyetlen bővítésében sem léteznek többszörös gyökei.*

2.3.6. Állítás. *Egy $a \in \bar{K}$ elem pontosan akkor szeparábilis K felett, ha $|Hom_K(K(a), \bar{K})| = deg(a)$.*

Bizonyítás. Az előző tétel szerint $|Hom_K(K(a), \bar{K})| = |\{\beta \in L | f(\beta) = 0\}|$, ahol f az a minimálpolinomja. Ez utóbbi halmaz mérete pontosan akkor lesz $deg(a)$, ha f-nek csupa különböző gyökei vannak, azaz a szeparábilis. $\square$

Az imént bizonyított tétel azt mutatta meg, hogy a K testnek egy egyszerű bővítését hányféleképpen ágyazhatjuk be egy K-t tartalmazó M testbe úgy, hogy K fixen marad. A következő tétel annak megmutatására szolgál, hogy ha már egy $L \geq K$ testet beágyaztunk M-be egy τ homomorfizmus segítségével, akkor ezt a beágyazást hányféleképpen terjeszthetjük ki L-nek egy egyszerű bővítésére.

2.3.7. Tétel. *Legyenek $K \leq L \leq L(a)$ és $K \leq M$ testbővítések, ahol a algebrai L felett, és legyen a minimálpolinomja L felett f. Tetszőleges rögzített $\tau \in Hom_K(L, M)$ homomorfizmus mellett az a*

$$\{\rho \in Hom_K(L(a), M) | \rho_{|L} = \tau\} \to \{\beta \in M | \tau(f)(\beta) = 0\}$$

leképezés, amely egy ilyen ρ-hoz az a-nál vett képét rendeli, az bijekció.

Bizonyítás. Először most is azt kell belátnunk, hogy ez a leképezés tényleg az adott halmazba képez. Az $f(a) = 0$ azonosságra alkalmazva ρ-t $\rho(f(a)) = 0$ adódik. Mivel ρ megszorítva L-re egyenlő τ-val, és f együtthatói L-beliek, így ez a kifejezés tovább egyenlő $\tau(f)(\rho(a))$-val.

Az injektivitás a következőképpen látható be: Ha $\rho_1(a) = \rho_2(a)$ akkor $\rho_{1|L} = \rho_{2|L}$ miatt $\rho_1 = \rho_2$ $L(a)$-n is.

A szürjektivitáshoz megjegyezzük, hogy f irreducibilitásából következik, hogy $\tau(f)$ is irreducibilis, így ha β gyöke $\tau(f)$-nek, akkor neki ez is a minimálpolinomja. Mint azt tudjuk, $L(a) \cong L[x]/(f)$ és $\tau(L)(\beta) \cong \tau(L)[x]/(\tau(f))$. Ugyanakkor nyilván $L[x]/(f) \cong \tau(L)[x]/(\tau(f))$, így ezen izomorfizmusok megfelelő sorrendben vett kompozíciója éppen egy $L(a) \to \tau(L)(\beta)$ homomorfizmust ad, ahol a képe β. $\square$

2.3.8. Következmény. Legyen $L|K$ és $M|K$ két testbővítés. Ekkor $|Hom_K(L, M)| \leq |L : K|$, amennyiben ez az index véges.

Bizonyítás. Mivel $|L : K|$ véges, így léteznek $a_1, \dots, a_n$ elemek, hogy $L = K(a_1, \dots, a_n)$. A bizonyítást n szerinti indukcióval végezzük. $n = 1$-re az állítás már beláttuk. Legyen tehát $n \geq 2$, és tegyük fel, hogy minden n-nél kissebb számra már készen vagyunk. Legyen $L' = K(a_1, \dots, a_{n-1})$. Az indukciós feltevés szerint legfeljebb $|L' : K|$-féleképpen választhatunk tetszőleges $L' \to M$ K-homomorfizmust, és ezt legfeljebb $|L : L'|$-féleképpen terjeszthetjük ki $L \to M$ homomorfizmussá. Ebből tehát $|Hom_K(L, M)| \leq |L' : K| \cdot |L : L'| = |L : K|$. $\square$

2.3.9. Definíció. *Egy véges $L|K$ bővítés szeparábilis, ha L minden eleme szeparábilis K felett.*

2.3.10. Állítás. *Legyen $L|K$ egy bővítés, és $a \in L$ szeparábilis. Ekkor $K(a)$ minden eleme szeparábilis.*

Bizonyítás. Legyen $\beta \in K(a)$. Mivel a szeparábilis $K(\beta)$ felett is (hiszen a $K(\beta)$ feletti minimálpolinomja osztója a K feletti minimálpolinomnak, így ha utóbbinak nincsenek többszörös gyökei, akkor az előbbinek sem lehetnek), így tetszőleges $\tau \in Hom_K(K(\beta), \bar{K})$ homomorfizmus $|K(a) : K(\beta)|$-féleképpen terjeszthető ki $K(a) \to \bar{K}$ K-homomorfizmussá. Innen $|Hom_K(K(a), \bar{K})| = |K(a) : K(\beta)| \cdot |Hom_K(K(\beta, \bar{K})|$. Mivel a szeparábilis K felett, így itt a bal oldal egyenlő $|K(a) : K|$-val. A szorzástétel alapján, ha most mindkét oldalt leosztjuk $|K(a) : K(\beta)|$-val, akkor $|Hom_K(K(\beta, \bar{K})| = |K(\beta) : K|$-t kapunk, ami éppen azt jelenti, hogy β szeparábilis K felett. $\square$

2.3.11. Következmény. Egy a elem pontosan akkor szeparábilis a K test felett, ha a $K(a)|K$ bővítés szeparábilis.

2.3.12. Állítás. *Az $L|K$ véges bővítés pontosan akkor szeparábilis, ha $|Hom_K(L, \bar{K})| = |L : K|$.*

Bizonyítás. Legyen $a \in L$. Tetszőleges $\tau \in Hom_K(K(a), \bar{K})$ homomorfizmus legfeljebb $|L : K(a)|$-féleképpen terjed ki $L \to \bar{K}$ homomorfizmussá. $|Hom_K(L, \bar{K})| = |L : K|$ alapján tehát legalább $|L : K|/|L : K(a)| = |K(a) : K|$ különböző $K(a) \to \bar{K}$ homomorfizmus létezik, ami az iménti következmény alapján éppen azt jelenti, hogy a szeparábilis K felett.

Tegyük most fel, hogy az $L|K$ bővítés szeparábilis. Mivel L véges bővítés, így léteznek $a_1 \dots, a_n \in L$ elemek, hogy $L = K(a_1, \dots, a_n)$. A bizonyítást n szerinti indukcióval végezzük. Az $n = 1$ esetet már korábban beláttuk. Ha tehát n-nél kisebb számokra az állítást már tudjuk, akkor legyen $L' = K(a_1, \ldots, a_{n-1})$. Mivel a szeparábilis K felett, így szeparábilis a nála bővebb L' test felett is. Tudjuk, hogy tetszőleges $\tau \in Hom_K(L', \bar{K})$ homomorfizmus annyiféleképpen terjed ki $L \to \bar{K}$ K-homomorfizmussá ahány konjugáltja van a-nak $\bar{K}$-ban. Az a elem szeparábilitása és $\bar{K}$ algebrai zártsága miatt ez a szám éppen $deg(\tau(f)) = deg(f) = |L : L'|$ ahol f az a-nak L feletti minimálpolinomja. Ezek alapján $|Hom_K(L, \bar{K})| = |Hom_K(L', \bar{K})| \cdot |L : L'|$, ami az indukciós feltevés miatt nem más mint, $|L' : K| \cdot |L : L'| = |L : K|$. $\square$

2.3.13. Állítás. *Legyen $K \leq L \leq M$ bővítések egy lánca. Az $M|K$ bővítés pontosan akkor szeparábilis, ha az $M|L$ és $L|K$ bővítések szeparábilisek.*

Bizonyítás. Legyen $\beta \in M$ és f a minimálpolinomja L felett. Azt szeretnénk belátni, hogy $|Hom_K(L\beta), \bar{K})| = |L(\beta) : K|$, hiszen ekkor $L(\beta)$ minden eleme, speciálisan β is szeparábilis K felett. Mivel $L|K$ szeparábilis, így $|Hom_K(L, \bar{K})| = |L : K|$, tehát csak arra van szükségünk, hogy tetszőleges $\tau : L \to \bar{K}$ K-homomorfizmus éppen $|L(\beta) : L|$-féleképpent terjedjen ki $L(\beta) \to \bar{K}$ homomorfizmussá. Mivel β szeparábilis L felett, így f-nek nincsenek többszörös gyökei, és így $\tau(f)$-nek sincsenek. Ezek szerint tehát (felhasználva $\bar{K}$ algebrai zártságát) τ éppen $deg(\tau(f)) = deg(f) = |L(\beta) : L|$-féleképpen terjed ki $L(\beta)$-ra.

Mivel M minden eleme szeparábilis K fölött, így nyilván $L \leq M$ minden eleme is az, vagyis az $L|K$ bővítés szeparábillis. Az $M|L$ bővítés szeparábilitásához arra van szükség, hogy $|Hom_L(M, \bar{L})| = |M : L|$ teljesüljön. Feltehető, hogy $L \leq \bar{K}$, és $\bar{L} = \bar{K}$. Mivel L szeparábilis, ezért $|Hom_K(L, \bar{K})| = |L : K|$. Ahhoz, hogy $|Hom_K(M, \bar{K})| = |M : K|$ teljesüljön, arra van szükség, hogy tetszőleges $\tau \in Hom_K(L, \bar{K})$ homomorfizmus éppen $|M : K|/|L : K| = |M : L|$-féleképpen terjedjen ki $M \to \bar{K}$ K-homomorfizmussá. Speciálisan $\tau = id_L$ is ennyiféleképpen terjed ki, ami épp azt jelenti, hogy $|Hom_L(M, \bar{K})| = |M : L|$. $\square$

2.3.14. Következmény. A K test egy tetszőleges M bővítésének azon elemei, melyek szeparábilisek a K fölött résztestet alkotnak.

Bizonyítás. Ha α és β eleme M-nek, és szeparábilisek K felett, akkor az imént bizonyított állítás alapján $K(\alpha)(\beta)$ szeparábilis bővítés. Ennek tehát minden eleme, speciálisan $\alpha \pm \beta$, $\alpha \cdot \beta$, és $\beta \neq 0$ esetén α/β is szeparábilis. $\square$

2.3.15. Definíció. *A K testet tökéletesnek nevezzük, ha minden egyszerű algebrai bővítése szeparábilis. Más szóval a $K[x]$-beli irreducibilis polinomoknak $\bar{K}$-ban nincsenek többszörös gyökeik.*

2.3.16. Definíció. *A K test karakterisztikájának nevezzük azt a legkisebb n számot, amire teljesül, hogy K egységelemét n-szer összeadva K nulleleme adódik. Ezt a számot $char(K)$-val jelöljük. Ha ilyen szám nem létezik, akkor azt mondjuk, hogy K nullkarakterisztikájú.*

2.3.17. Megjegyzés. Ha $char(K)$ véges, akkor nyilván prímszám, hiszen ha összetett szám lenne, és előállna $p \cdot q$ alakban, akkor $p \cdot q = 0$, és a testek nullosztómentessége miatt vagy p vagy q nulla kellene legyen, ám mindketten kisebbek $p \cdot q$-nál, ami ellentmond a karakterisztika minimalitásának.

2.3.18. Állítás. *Minden nullkarakterisztikájú test tökéletes.*

Bizonyítás. Mivel egy $a \in K$ elem pontosan akkor többszörös gyöke egy $f \in K[x]$ polinomnak, ha gyöke a deriváltnak, ez azt is jelenti, hogy az f polinomnak pontosan akkor vannak többszrös gyökei, ha a deriváltjával vett legnagyobb közös osztója nem konstans. Mivel f irreducibilis, ez csak úgy lehetséges, ha a deriváltja 0. Nullkarakterisztikájú test esetében azonban nem konstans polinom deriváltja nyilván nem lehet 0, így az állítást beláttuk. □

2.3.19. Megjegyzés. Az is igaz, hogy minden véges test tökéletes, ennek bizonyításához azonban le kéne írnunk, hogy hogyan is néznek ki pontosan a véges testek, és ez a jelenlegi dolgozatnak nem célja.

2.3.20. Tétel. *Minden véges szeparábilis bővítés egyszerű.*

Bizonyítás. A bizonyítást csak végtelen testekre végezzük el. Mivel az $L|K$ bővítés véges, így léteznek $a_1, \ldots, a_n \in L$ elemek, amikre $L = K(a_1, \ldots, a_n)$. Legyen az $L|K$ bővítés foka d és $Hom_K(L, \bar{K}) = \{\tau_1, \ldots, \tau_d\}$. Célunk olyan $\alpha \in L$ elemet találni, melyre a $\tau_1(\alpha), \ldots \tau_d(\alpha)$ elemek mind különbözőek. Valóban, mivel τ α-t mindenképp egy konjugáltjába viszi, ez azt jelentené, hogy α minimálpolinomjának a foka legalább d. Mivel $|L : K| = d$, $|K(\alpha) : K| \geq d$ és $K(\alpha) \leq L$ így $K(\alpha) = L$ adódna.

Legyen $f(x) = \sum_{i=1}^{n} \alpha_i x^i \in L[x]$.Ha $j \neq k$, akkor létezik olyan i index, amire $\tau_j(\alpha_i) \neq \tau_k(\alpha_i)$, különben τ_j és τ_k megegyezne az α_i-k által generált testen, azaz L-en. Ez azt jelenti, hogy a $\tau_j(f)$ polinomok mind különbözőek, hiszen bármely kettőhöz van olyan i, hogy x^i együtthatója eltér. Definiáljuk $P(x) \in \bar{K}[x]$-et a következőképpen:

$$P(x) = \prod_{1 \le j < k \le d} \tau_j(f(x)) - \tau_k(f(x)).$$

Az előbbeik alapján ez nem a 0 polinom, így K végtelensége alapján létezik $\beta \in K$, hogy $P(\beta) \neq 0$. Ha $P(\beta) \neq 0$, akkor az őt definiáló szorzat egyik eleme sem lehet 0, azaz $\tau_j(f(\beta)) \neq \tau_k(f(\beta))$, így $\alpha = f(\beta)$ választás jó lesz. $\square$

3. fejezet

Galois-elmélet

3.1. Klasszikus Galois-elmélet

3.1.1. Definíció. *Legyen N a K testnek egy algebrai bővítése. Ekkor $G(N|K)$-val jelöljük és a bővítés Galois-csoportjának hívjuk, a $(Hom_K(N,N),\circ)$ csoportot, ahol $\circ$ a függvény-kompozíció művelete. Ha a bővítést egyetlen polinom felbontási testeként hoztuk létre, akkor a polinomhoz tartozó Galois-csoportról beszélünk.*

3.1.2. Állítás. *$G(N|K)$ tényleg csoport.*

Bizonyítás. A műveletre való zártság és az asszociativitás nyilvánvaló, az egységelem pedig az identitás. Mivel minden $\tau \in Hom_K(N,N)$ homomorfizmus injektív (hiszen tetszőleges testhomomorfizmus az), így az inverz létezéséhez csak azt kell belátni, hogy szürjektív is. Legyen $a \in N$ tetszőleges. Ennek csak véges sok konjugálja létezik, így csak véges sok konjugáltja lehet N-ben. Legyenek ezek $\{a = a_1, \ldots, a_k\}$. Mivel τ minden N-beli elemet egy konjugáltjába visz, és injektív, így valójában permutálja az $\{a_1, \ldots, a_k\}$ halmaz, tehát ennek minden eleme, speciálisan a is előáll képként. □

3.1.3. Definíció. *Az $N|K$ véges bővítésről azt mondjuk, hogy Galois-bővítés, ha $|G(N|K)| = |N : K|$.*

3.1.4. Állítás. *A (véges) Galois-bővítések éppen a véges, normális, szeparábilis bővítések.*

Bizonyítás. Tegyük fel, hogy az $N|K$ véges bővítés Galois. Ekkor $|N : K| = |G(N|K)| = |Hom_K(N,N)| \leq |Hom_K(N,\bar{K}| \leq |N : K|$, vagyis végig egyenlőség van. Így $|N : K| =$

$|Hom_K(N, \bar{K})|$ ami éppen azt jelenti, hogy $N|K$ szeparábilis. Mivel véges és szeparábilis, így egyszerű, vagyis létezik $a \in N$, amire $N = K(a)$. Legyen a minimálpolinomja $f \in K[x]$. N tartalmazza a összes (K feletti) konjugáltját, hiszen a-nak legfeljebb $deg(f) = deg(a) = |K(a) : K|$ darab konjugáltja lehet, ugyanakkor különböző $\tau \in G(N|K)$ automorfizmusok a-t különböző konjugáltjába viszik, és ezen automorfizmusok száma éppen $|N : K|$. Ha tehát a konjugáltjait $a = a_1, \ldots, a_n$-el jelöljük, akkor $N = K(a) = K(a_1, \ldots, a_n)$ adódik, vagyis N az f polinom K feletti felbontási teste, és így normális bővítés.

Legyen most $N|K$ véges, normális, szeparábilis. Mivel szeparábilis és véges, ezért megint csak létezik $a \in N$, hogy $N = K(a)$. Az a elem szeparábilitása miatt $deg(a) = |Hom_K(K(a), \bar{K})|$. Mivel a bővítés normális, ezért minden $\tau \in Hom_K(K(a), \bar{K})$ homomorfizmus tekinthető $Hom_K(K(a), K(a))$-belinek is, hiszen τ az a-t egy konjugáltjába viszi, de $K(a)$ az összes ilyet tartalmazza. Ez éppen azt jelenti, hogy $|N : K| = |Hom_K(N, N)| = |G(N|K)|$. $\square$

3.1.5. Megjegyzés. A Galois-bővítéseket tehát úgy is definiálhattuk volna, mint algebrai, normális és szeparábilis bővítések. Ennek a definíciónak az az előnye, hogy ez végtelen bővítésekre is működik.

Tekintsük azt a $\varrho \subseteq G(N|K) \times N$ relációt, aminek egy (σ, a) pár pontosan akkor eleme, ha $\sigma(a) = a$. Mint azt az első fejezetben láttuk, ez indukál egy Galois-megfeleltetést $G(N|K)$ és N részhalmazai között. Az $X \subseteq G(N|K)$ halmaz képét $\Delta(X)$-el jelöljük, és ez azon N-beli elemeket tartalmazza, amit minden X-beli relatív automorfizmus helyben hagy. Az $Y \subseteq N$ halmaz képét $H(Y)$-al jelöljük, és ez azon $G(N|K)$-beli automorfizmusokat tartalmazza, amik Y minden elemét helybenhagyják.

3.1.6. Állítás. *A $G(N|K)$ és N közötti Galois-megfeleltetés által indukált lezárásban a $P(N)$-beli zárt halmazok küzbülső testek, és a $P(G(N|K))$-beli zárt halmazok pedig részcsoportok.*

Bizonyítás. Elég azt belátni, hogy relatív automorfizmusok egy adott $X \subseteq G(N|K)$ részhalmaza által helybenhagyott N-beli elemek testet alkotnak, illetve, hogy tetszőleges $Y \subseteq N$ halmazt elemenként fixen hagyó automorfizmusok csoportot alkotnak. Mind a két állítás egyszerű következménye a homomorfizmusok művelettartásának. $\square$

Mivel a Galois-megfeleltetés egy bijekciót ad az általa indukált lezárás zárt halmazai között, így a továbbiakban az iménti állítás megfordítása a cél, vagyis, hogy minden részcsoport és minden közbülső test valóban zárt is. Ez az állítás azonban csak véges bővítésekre igaz. A következő fejezet elején mutatunk egy példát, ami ezt illusztrálja, most azonban folytassuk ennek az állításnak a bizonyítását véges bővítésekre.

3.1.7. Állítás. *Legyen $N|K$ egy Galois-bővítés. Ekkor a $G(N|K)$ csoporthoz tartozó közbülső test K.*

Bizonyítás. Azt kell belátni, hogy N egyetlen K-n kívüli elemét sem hagyja $G(N|K)$ minden eleme fixen. Mivel a bővítés szeparábilis, így minden a elemnek van önmagától különböző konjugáltja, és mivel normális, N tartalmazza is ezeket. A 2.3.4 következmény szerint létezik olyan $K(a) \to N$ homomorfizmus, ami a-t egy tetszőleges konjugáltjába viszi, és a 2.3.7 tétel szerint ez kiterjeszthető $N \to N$ homomorfizmussá. Így tetszőleges K-n kívül a elemhez találtunk olyan automorfizmus, ami őt nem hagyja fixen. □

3.1.8. Állítás. *Legyen $N|K$ egy szeparábilis bővítés. Ekkor ha $\Delta(G(N|K)) = K$, akkor a bővítés normális.*

Bizonyítás. Tegyük fel, hogy $\Delta(G(N|K)) = K$, és van olyan $a \in N$, melynek N nem tartalmazza az összes (a felbontási test feletti) konjugáltját. Jelöljük $a = a_1, \dots, a_k$-val az a-nak N-beli konjugáltjait, és n-nel az a elem fokát K fölött. A feltételek szerint tehát $k < n$. Tekintsük az $f = \prod_{i=1}^{k}(x - a_i)$ polinomot. Ennek a polinomnak az együtthatói éppen az $a_1, \dots, a_n$ elemek elemi szimmetrikus polinomjai, így minden $\sigma \in G(N|K)$ automorfizmusra $\sigma(f) = f$. Mivel a feltétel szerint ez a tulajdonsága csak a K-beli elemeknek van meg, így $f \in K[x]$. Ám f definíciója alapján a gyöke f-nek, ami ellentmondás, hiszen f foka kisebb, mint a minimálpolinomjának a foka. □

3.1.9. Megjegyzés. A fenti két állítás következménye a Galois-bővítéseknek egy újabb ekvivalens definíciója: Az $N|K$ algebrai bővítés Galois, ha szeparábilis, és $\Delta(G(N|K)) = K$.

3.1.10. Állítás. *Legyen $N|K$-egy Galois-bővítés. Ekkor tetszőleges L közbülső testre N normális bővítése L-nek, $H(L) = G(N|L)$, és $\Delta(H(L)) = L$.*

Bizonyítás. Mivel N ugyannak a polinomhalmaznak a felbontási teste L felett, mint K felett, így $N|L$ normális. A második állítás nyilvánvaló, hiszen mind a két csoportban N-nek pontosan azok az automorfimusai vannak, amik L-et fixen hagyják. Tudjuk, hogy $N|L$ normális, és mivel tetszőleges $a \in N$ elem L feletti minimálpolinomja osztója a K feletti minimálpolinomjának, így szeparábilis is, tehát Galois. Így a tétel már bizonyított része alapján $H(L) = G(N|L)$, és így $\Delta(H(L)) = \Delta(G(N|L))$. A 3.1.7 állítás következtében ez utóbbi éppen L-lel egyenlő. □

3.1.11. Következmény. A Galois-bővítéseknél minden közbülső test zárt.

3.1.12. Tétel. (A Galois-elmélet alaptétele) *Legyen $N|K$ egy véges Galois-bővítés. Ekkor a Galois-megfeleltetésben minden közbülső test, és minden részszoport zárt, továbbá, ha $L \leq N$ és $H \leq G(N|K)$ egymásnak megfeleltetett elemek, akkor $|L : K| = |G(N|K) : H|$, és $|H| = |N : L|$.*

Bizonyítás. Legyen L egy közbülső test. A 2.3.13 tétel miatt N szeparábilis bővítése L-nek, és így az imént bizonyított állítás, valamint a 2.3.12 tétel miatt $|H(L)| = |G(N|L)| = |N : L|$. Ugyanakkor $N|K$ szeparábilitása miatt $|G(N|K)| = |N : K|$, így ebből a két egyenlőségből, a csoportokra vonatkozó Lagrange-tételből, illetve az algebrai bővítések szorzástételéből adódik, hogy

$$|G : H(L)| = |L : K|.$$

Legyen most $H \leq G(N|K)$. A Galois-megfeleltetések definíciójából adódóan $H \subseteq H(\Delta(H))$, vagyis

$$|H| \leq |H(\Delta(H))|.$$

Mivel N szeparábilis bővítése K-nak, így a 2.3.20 tétel miatt létezik $a \in N$, elem, amire $N = K(a)$. Jelöljük most H elemeit $\sigma_1, \dots, \sigma_K$-val, és tekintsük a $g(x) = \prod_{i=1}^{k}(x - \sigma_i(a))$ polinomot. Erre H-nak egy tetszőleges σ elemét alkalmazva visszakapjuk a g polinomot, hiszen a tényezők sorrendtől eltekintve ugyanazok maradnak ($\sigma H = H$ miatt). Ez azt jelenti, hogy $g(x) \in \Delta(H)[x]$. Mivel az identitás eleme H-nak így a gyöke g-nek, és így az a elem $\Delta(H)$ feletti minimálpolinomja osztója g-nek. Az oszthatóság következménye, hogy az említett minimálpolinom legfeljebb k-ad fokú, és így $N = (\Delta(H))(a)$, és a 2.1.8 tétel szerint

$$|N : \Delta(H)| \leq k = |H|.$$

A most bizonyított egyenlőtlenségeket összevetve adódik, hogy

$$|H| \leq |H(\Delta(H))| = |N : \Delta(H)| \leq |H|.$$

Itt tehát végig egyenlőség áll. Mivel $H \subseteq H(\Delta(H))$ így az elemszámok egyenlősége a két csoport egyenlőségét jelenti, vagyis a Galois-megfeleltetésben H valóban zárt. □

3.1.13. Állítás. *Legyen $N|K$ egy véges Galois-bővítés. Legyenek továbbá H_1 és H_2 a Galois-csoport részcsoportjai, L_1 és L_2 közbülső testek, és jelöljük $[L_1, L_2]$-vel a legszűkebb L_1-et és L_2-t is tartalmazó közbülső testet. Ekkor igazak a következő összefüggések:*

1. $H(L_1 \cap L_2) = \langle H(L_1), H(L_2) \rangle$
2. $H([L_1, L_2]) = H(L_1) \cap H(L2)$
3. $\Delta(H_1 \cap H_2) = [\Delta(H_1), \Delta(H_2)]$
4. $\Delta(\langle H_1, H_2 \rangle) = \Delta(H_1) \cap \Delta(H_2)$

Bizonyítás. A második állítással kezdünk. A 1.1.6 tétel negyedik pontja szerint $H(L_1 \cup L_2) = H(L_1) \cap H(L_2)$. (Hiszen a részhalamzok tartalmazásra vett részbenrendezésénél a legkisebb felső korlát az unió, míg a legnagyobb alsó korlát a metszet.) Azt kell tehát még belátnunk, hogy $H(L_1 \cup L_2) = H[L_1, L_2])$. Ez azonban rögtön adódik a 1.1.8 megjegyzésből, hiszen épp most láttuk be, hogy a megfeleltetésben a zárt halmazok pontosan a közbülső testek, így tetszőleges részhalmaz lezártja az őt tartalmazó legszűkebb közbülső test. A négyes állítás ugyanígy bizonyítható.

Felhasználva az iménti egyenlőséget, és a részcsoportok zártságát, tudjuk, hogy $H_1 \cap H_2 = H(\Delta(H_1)) \cap H(\Delta(H_2)) = H([\Delta(H_1), \Delta(H_2)])$. Innen az egyenlőség mindkét oldalára alkalmazva Δ-t, a $\Delta(H(L)) = L$ összefüggés alapján $\Delta(H_1 \cap H_2) = [\Delta(H_1), \Delta(H_2)]$. Az első állítás bizonyítása ezzel analóg módon történik. $\square$

3.1.14. Tétel. *Legyen $N|K$ egy Galois-bővítés, valamit az L közbülső test és a $H \leq G(N|K)$ részcsoport egymásnak megfeleltetett elemek. Ekkor L pontosan akkor normális bővítése K-nak, ha $H \lhd G(N|K)$, és ebben az esetben $G(L|K) \cong G(N|K)/H$.*

Bizonyítás. Legyen L normális bővítés, $a \in L$ valamint $\sigma \in H$ és $\tau \in G(N|K)$ tetszőleges. Mivel L normális bővítés, így $\tau(a) \in L$, hiszen τ az a-t egy konjugáltjába viheti csak, ám L az a összes konjugáltját tartalmazza. Így ezt az elemet σ helyben hagyja, majd τ^{-1} visszaviszi a-ba, vagyis összességében $(\tau^{-1}\sigma\tau)(a) = a$, és így H normálosztó $G(N|K)$-ban.

Tegyük most fel, hogy $a \in L$, és létezik a-nak olyan b konjugáltja, ami nem eleme L-nek. Ekkor létezik olyan $\sigma \in H$ automorfizmus, ami b-t nem hagyja helyben. A 2.3.4 következmény és az izomorfizmus kiterjesztési tétel miatt létezik továbbá olyan $\tau \in G(N|K)$ automorfizmus, ami a-t b-be viszi. Ekkor $(\sigma\tau)(a) \neq b$, és így $(\tau^{-1}\sigma\tau)(a) \neq a$, hiszen τ^{-1} injektív.

Az izomorfizmus bizonyításához tekintsük azt a $\varphi : G(N|K) \to G(L|K)$ homomorfizmust, mely minden $\sigma \in G(N|K)$ elemhez hozzárendeli az L-re való megszorítását. (Ez a definíció értelmes, hiszen az $L|K$ bővítés normális, vagyis N minden automorfizmusánál L-beli elem képe szintén L-beli elem.) Ennek a homomorfizmusnak a magja éppen H, és így a homomorfizmus-tétel szerint $G(N|K)/H$ izomorf $G(L|K)$ egy részcsoportjával. Azonban $G(N|K)/H$ elemszáma egyenlő a $|G(N|K) : H|$ indexszel, ami az alaptétel szerint nem más mint $G(L|K)$ elemszáma, vagyis az említett részcsoport valójában az egész csoport. $\square$

3.1.15. Állítás. *Legyen $N|K$ egy Galois-bővítés, és L_1, L_2 közbülső testek. Ekkor:*

1. *ha L_2 normális bővítése L_1-nek, akkor $G(L_2|L_1) \cong G(N|L_1)/G(N|L_2)$*
2. *ha az $[L_1, L_2]|L_1$ és az $L_2|(L_1 \cap L_2)$ bővítések normálisak, akkor $G([L_1, L_2]|L_1) \cong G(L_2|(L_1 \cap L_2))$.*

Bizonyítás. Jelöljük $G(N|L_1)$-et H_1-el, és $G(N|L_2)$-t H_2-vel. Ekkor $L_2 \geq L_1$ miatt $H_2 \leq H_1$, és mivel az $L_2|L_1$ bővítés normális, így a 3.1.14 tétel miatt $G(L_2|L_1) \cong H_1/H_2$.

Legyen M a legkisebb $[L_1, L_2]$-t tartalmazó normális bővítése $(L_1 \cap L_2)$-nek. Mivel az eredeti bővítés szeparábilis, így $N|(L_1 \cap L_2)$ is az, és $M \leq N$ miatt $M|(L_1 \cap L_2)$ is, vagyis ez utóbbi bővítés Galois. Alkalmazhatjuk tehát a tétel első pontját, miszerint $G(M|L_1)/G(M|[L_1, L_2]) \cong G([L_1, L_2]|L_1)$, valamint $G(M|(L_1 \cap L_2)/G(M|L_2) \cong G(L_2|(L_1 \cap L_2))$. A 3.1.13 állítás szerint $G(M|(L_1 \cap L_2) \cong \langle G(L1|(L_1 \cap L_2)), G(L_2|(L_1 \cap L_2)\rangle$ és $G(M|[L_1, L_2]) \cong G(L_1|(L_1 \cap L_2)) \cap G(L_2|(L_1 \cap L_2))$. Ezt, és az első izomorfizmustételt felhasználva kapjuk, hogy a fent említett faktorcsoportok izomorfak, ami bizonyítja az állítást. $\square$

3.2. Végtelen Galois-elmélet

Mint láttuk a véges Galois-bővítések esetében a Galois-megfeleltetés által indukált lezárás szerinti zárt részhalmazai a Galois-csoportnak, éppen a részcsoportok voltak. Végtelen bővítés esetében azonban nem ez a helyzet. Tekintsük ugyanis $\mathbb{Q}$-nak a prímszámok négyzetgyökeivel való bővítését. Ekkor a Galois-csoportnak egy részcsoportját alkotják azok az automorfizmusok, melyek véges sok gyököt a negatívjukba visznek, míg a többieket helybenhagyják. Az ehhez a csoporthoz tartozó közbülső test maga $\mathbb{Q}$, ám a $\mathbb{Q}$-hoz tartozó csoport (tehát az egész Galois-csoport) tartalmaz újabb elemeket is, például azt az automorfizmust, mely minden gyököt a negatívjába visz. Annak érdekében, hogy megtudjuk, mely részcsoportok lesznek a megfeleltetés szerint zártak, értelmezünk egy olyan topológiát a Galois-csoporton, ami azt tudja, hogy ezen topológia szerinti zárt részcsoportok éppen a megfeleltetés által indukált lezárás szerinti zárt részcsoportok lesznek.

Mielőtt belekezdenénk, emlékeztetünk a Galois-bővítés azon definíciójára, mely végtelen bővítés esetén is értelmes.

3.2.1. Definíció. *Az $N|K$ végtelen algebrai bővítést Galois-bővítésnek nevezzük, ha szeparábilis, és $\Delta(G(N|K)) = K$.*

3.2.2. Definíció. *Legyen I egy olyan részbenrendezett halmaz, amelyben bármely két elemnek van közös felső korlátja. Az $(X_i, \phi_{ij})_I$ inverzrendszer egy topologikus terek $\{X_i | i \in I\}$ halmazából, és az őket összekötő folytonos függvények $\{\phi_{ij} : X_i \to Xj | j \leq i \in I\}$ halmazából álló pár, amire a következő tulajdonságok teljesülnek:*

1. *ϕ_{ii} az identitás minden $i \in I$ esetén.*
2. *$\phi_{ik} = \phi_{jk} \circ \phi_{ij}$ minden $k \leq j \leq i \in I$ esetén.*

3.2.3. Megjegyzés. Ha az inverzrendszer minden X_i eleme egy topologikus csoport, akkor a ϕ_{ij} függvényeknek csoporthomomorfizmusoknak kell lenniük.

3.2.4. Definíció. *Az $(X_i, \phi_{ij})_I$ inverzrendszer inverzlimesze az $X = \prod_{i \in I} X_i$ szorzattopológia következő módon definiált altere:*

$$\varprojlim (X_i, \phi_{ij})_I = \{a \in X | a_j = \phi_{ij}(a_i), \forall j \leq i \in I\}$$

3.2.5. Állítás. *Amennyiben az $(X_i, \phi_{ij})_I$ inverzrendszer minden eleme egy topologikus csoport, úgy az inverzlimesze is az.*

Bizonyítás. Az állítjuk, hogy a szorzattopológián a csoportműveletek folytonosak. Ehhez persze elég belátni, hogy a szorzattopológia egy bázisának minden elemének ősképe nyílt (mind a csoportszorzás, mind a csoport inverzképzése szerint). Ez viszont rögtön következik abból, hogy ennek a bázisnak minden eleme direktszorzat alakú, és így az ősképet koordinátánként vehetjük.

Mivel tehát a szorzattopológia egy topologikus csoport, és az inverzlimesz ennek egy részhalmaza, így elég belátni, hogy az inverzlimesz zárt a csoportműveletekre, és tartalmazza az egységelemet. Mivel ϕ_{ij} csoporthomomorfizmus, így az egységelem képe szintén egységelem, vagyis $\phi_{ij}(e_i) = e_j$, azaz e eleme az inverzlimesznek. Legyen most $x, y \in \varprojlim (X_i, \phi_{ij})_I$. Mivel a szorzást koordinátánként végezzük, és ϕ_{ij} homomorfizmus, ezért $(xy)_j = \phi_{ij}((xy)_i)$, vagyis az inverzlimesz zárt a szorzásra nézve. Hasonlóan látható be, hogy zárt az inverzképzésre is, tehát részcsoport. $\square$

3.2.6. Állítás. *Az $(X_i, \phi_{ij})_I$ inverzrendszer inverzlimesze zárt részcsoportja a $\prod_{i \in I} X_i$ szorzattopológiának.*

Bizonyítás. Azt kell belátnunk, hogy ha g nem eleme az inverzlimesznek, akkor van olyan nyílt környezete, melynek metszete a limesszel üres. A feltevésünk szerint léteznek olyan i, j indexek, melyekre $\phi_{ij}(x_i) \neq x_j$. Legyen U az a részhalmaza a szorzattopológiának, melyben azok az elemek vannak, melyeknek i-edik koordinátája g_i és j-edik koordinátája g_j. Ez a szorzattopológia értelmezése alapján nyílt, a konstrukció alapján egyik eleme sem lehet benne az inverzlimeszben, és persze tartalmazza g-t, vagyis ez egy megfelelő környezet. $\square$

3.2.7. Következmény. Az inverzlimesz nyílt részcsoportjai éppen a véges indexű zárt részcsoportok.

Bizonyítás. Az inverzrendszer elemei véges topológiák, így ezek nyilván kompaktak. Tychonoff tétele alapján tehát a szorzattopológia is kompakt. Mivel az inverzlimesz egy zárt részcsoport, így ezen az altértopológia is kompakt. Tekintsünk most egy tetszőleges U nyílt részcsoportot. Ennek a komplementere előáll gU alakú mellékosztályok uniójaként, melyek az elemmel való szorzás folytonossága révén maguk is nyíltak. Ez azt jelenti, hogy U egyben zárt is, és mivel az U szerinti mellékosztályok egy nyílt fedését adják a csoportnak, így a kompaktság miatt véges indexű is. Hasonlóan, ha V egy véges indexű zárt részcsoport, akkor a komplementere is zárt (hiszen előáll végessok zárt részhalmaz uniójaként) és így V egyben nyílt is. $\square$

3.2.8. Definíció. *A G topologikus csoportot provégesnek nevezzük, ha izomorf egy olyan $(G_i, \phi_{ij})_I$ inverzrendszer inverzlimeszével, melyben minden G_i egy véges diszkrét topologikus csoport.*

3.2.9. Tétel. *A G topologikus csoport pontosan akkor provéges, ha Hausdorff, kompakt, és totálisan összefüggéstelen.*

3.2.10. Definíció. *Legyen $N|K$ egy Galois-bővítés. Ekkor a $G(N|K)$ csoporton értelmezett Krull topológiának nevezzük azt a topológiát, melynél a véges indexű normálosztók alkotják az egységelemnek egy lokális bázisát.*

3.2.11. Tétel. *Legyen $N|K$ egy végtelen Galois-bővítés. Ekkor $G(N|K)$ ellátva a Krull topológiával Hausdorff, kompakt, és teljesen összefüggéstelen.*

A fenti két tétel összerakásával adódik, hogy egy végtelen Galois-bővítés Galois-csoportja provéges. Ennél azonban sokkal többet mond az az út, ha megmutatjuk, hogy adott Galois-csoport milyen inverzrendszer inverzlimeszével izomorf. Ehhez legyen megint $N|K$ egy Galois-bővítés. Az inverzrendszer elemei legyenek K-nak N-ben lévő véges Galois-bővítéseihez tartozó Galois-csoportok. Ha $L \leq M$ ilyen bővítések, akkor legyen $\phi : G(M|K) \to G(L|K)$ az a homomorfizmus, ami M minden automorfizmusához hozzárendeli az L-re való megszorítását. (Ennek van értelme, hiszen M minden automorfizmusa L-et önmagára képezi. Ez valójában éppen az a homomorfizmus, mely létrehozza a 3.1.14 tételben látott bijekciót.) Mivel a provéges csoportok definíciójában az inverzrendszer minden elemét a diszkrét topológiával láttuk el, így a folytonosságra vonatkozó feltétel triviálisan teljesül.

Azt kell még belátni tehát, hogy a Galois-csoport izomorf ezen rendszer inverzlimeszével. A limesznek az elemei úgy néznek ki, hogy minden koordinátájuk egy adott közbülső véges Galois-bővítésnek egy automorfizmusa. Legyen tehát ψ az a leképezés, ami N tetszőleges relatív automorfizmusához hozzárendeli a limesznek azt az elemét, melynek az L közbülső testhez tartozó koordinátája az adott $G(N|K)$-beli elem L-re vett megszorítása. Ez természetesen injektív hiszen ha N két automorfizmusa nem egyezik meg, akkor lesz olyan véges közbülső bővítés, hogy arra megszorítva sem egyeznek meg.

A szürjektivitás a következőképpen mutatható meg: A limesz tetszőleges σ eleméhez úgy találunk őségképet, hogy minden $a \in N$ elemre megnézzük, hogy σ egy a-t tartalmazó véges közbülső bővítéshez tartozó kordinátája hova viszi a-t, és ez az elem lesz a-nak a képe a keresendő automorfizmusnál is. Ez a definíció értelmes hiszen az inverzlimeszben szereplő csoportokat összekötő homomorfizmusok biztosítják, hogy σ minden a-t tartalmazó bővítéshez tartozó koordinátája ugyan oda vigye a-t.

Láttuk tehát, hogy adott bővítéshez tartozó Galos-csoport izomorf a bővítésből gyártott inverzlimesszel, ám ennél több is igaz. A Galois-csoporton már értelmeztük a Krull topológiát, az inverzlimeszen pedig természetes módon adódik egy topológia az altértopológia formájában. A következő állításunk ezek viszonyáról szól:

3.2.12. Állítás. *Legyen $N|K$ egy Galois-bővítés. Ekkor a $G(N|K)$ csoport ellátva a Krull topológiával homeomorf a fent látott inverzlimesszel ellátva az altér topológiával.*

Bizonyítás. Mivel az izomorfizmust már beláttuk, így az egyszerűbb tárgyalhatóság kedvéért úgy teszünk, mintha a Krull-topológia is a limeszen lenne értelmezve. Mivel az egységelem lokális bázisa már meghatározza a topológiát egy topologikus csoporton, így elég azt belátnunk, hogy minden az altértopológia szerint nyílt halmaz, mely tartalmazza az egységelemet, tartalmaz egyben egy véges indexű normálosztót, valamint minden normálosztó tartalmaz egy az altértopológia szerint nylít halmazt.

Egy ilyen nyílt halmaz elemei úgy néznek ki, hogy véges sok i indexre van meghatározva, hogy az i-edik koordinátán milyen automorfizmus állhat, ezeken kívül tetszőleges. Tekintsük tehát azon inverzlimeszbeli elemeket, melyeknek ezen i koordinátáiban az identitás áll, egyébként pedig akármi. Először is ez nyilván részcsoport, és része az imént kiválasztott halmaznak. Másodszor ez normálosztó, hiszen a konjugálást koordinátánként végezzük, és az identitásnak a konjugáltja önmaga, míg a többi koordinátán nincs megkötés, hogy az adott automorfizmusnak milyen másik automorfizmusba szabad konjugálódnia. Végül pedig véges indexű, hiszen indexe éppen a megfelelő inverzrendszerbeli G_i csoportok rendjének maximuma. Így tehát tetszőleges limeszbeli nylít halmazban találtunk véges indexű normálosztót.

A másik irányhoz megmutatjuk, hogy a véges indexű normálosztók eleve nyíltak. Vegyük észre, hogy a 3.1.14 tételben sehol nem használtuk ki a bővítés végességét, így ez az eredmény végtelen bővítésekre is áll. Eszerint egy H véges indexű normálosztó pontosan azokat a $G(N|K)$-beli elemeket tartalmazza, melyek egy adott L véges normális bővítést elemenként fixálnak. Ennek a H halmaznak az inverzlimeszben az a halmaz felel meg, melynek elemei úgy néznek ki, hogy az L-hez és az összes résztestéhez tartozó koordinátában az identitás szerepel, egyébként pedig akármi, amit az inverzlimesz definíciója megenged. Ez viszont éppen annak a szorzattopológiában nyílt halmaznak a metszete az inverzlimesszel, mely elemeinek az imént említett koordinátáiban az identitás áll, egyébként pedig akármi, és így definíció alapján nyílt az altértopológiában. □

3.2.13. Tétel. (Végtelen Galois-elmélet alaptétele) *Legyen $N|K$ egy végtelen Galois-bővítés. Ekkor a Galois-megfeleltetés által indukált lezárásban N zárt részhalmazai a közbülső testek, míg $G(N|K)$ zárt részhalmazai a Krull-topológia szerinti zárt részcsoportok lesznek. Ennek megfelelően kapunk egy bijekciót az $N|K$ bővítés közbülső bővítései, és a $G(N|K)$ csoport zárt részcsoportjai között.*

Bizonyítás. Megmutatjuk, hogy ha L egy tetszőleges közbülső bővítés, akkor $G(N|L)$ zárt részcsoport. Először tegyük fel, hogy $L|K$ véges bővítés. Legyen M egy L-et tartalmazó véges Galois-bővítés. Mint azt korábban már említettük, a 3.1.14 tétel eredménye végtelen bővítésekre is áll. Eszerint tehát $G(M|K)$ izomorf $G(N|K)$ egy fakrtoával, és persze részcsoportként tartalmazza $G(M|L)$-et. Legyen U_L a $G(N|K)$-ből $G(M|K)$-ba menő természetes homomorfizmusnál vett ősképe $G(M|L)$-nek. Mivel ez a homomorfizmus folytonos, és $G(M|K)$-n a diszkrét topológia van, így U_L nyílt. Az U_L csoportban pontosan azok az elemek vannak, melyeket M-re megszorítva egy L-et fixen hagyó automorfizmust kapunk, így nyilván $U_L = G(N|L)$. Legyen most L egy tetszőleges közbülső bővítés. Ekkor L felírható, mint véges L_i bővítések uniója. Az imént látottak alapján minden i-re $G(N|L_i)$ nyílt részcsoportja $G(N|K)$-nak, és így a 3.2.7 következmény miatt zárt is. Ezek metszete éppen $G(N|L)$, ami így szintén zárt.

Most megmutatjuk, hogy tetszőleges $H \leq G(N|K)$-ra $H(\Delta(H)) = \bar{H}$. Jelöljük a H elemei által fixált testet L-lel. Ekkor $H \leq G(N|L)$, és mint láttuk ez utóbbi csoport zárt, így $\bar{H} \leq G(N|L)$ is teljesül. A másik irányú tartalmazáshoz legyen $\sigma \in G(N|L)$ és legyen U_M a σ lokális bázisának egy tetszőleges eleme, mely az $M|L$ véges Galois-bővítésnek megfelelő normálosztó. Legyen $\varphi : G(N|L) \to G(M|L)$ a két csoport közötti természetes homomorfizmus. Azt állítjuk, hogy $\varphi(H) = G(M|L)$. Valóban, ha $\varphi(H)$ valódi részcsoportja $G(M|L)$-nek, akkor a véges Galois-elmélet alaptétele alapján M-nek az L-nél egy bővebb résztestét fixálja, és ekkor H elemei a K-nak szintlén egy L-nél bővebb résztestét fixálják, ami ellentmond L definíciójának. A szürjektivitás miatt tehát létezik $\tau \in H$, amire $\varphi(\tau) = \varphi(\sigma)$. A természetes homomorfizmus definícióját figyelembe véve azt kaptuk, hogy $H \cap \sigma U_M \neq \emptyset$. Mivel U_M tetszőleges volt, így azt kaptuk, hogy a H halmaz σ minden környezetébe belemetsz, vagyis $\sigma \in \bar{H}$, és így $G(N|L) \leq \bar{H}$. Vagyis a megfeleltetés által indukált lezárás zárt halmazai éppen a zárt részcsoportok.

Végezetül $\Delta(H(L)) = L$ a 3.1.11 következmény szerint. $\square$

4. fejezet

Alkalmazások

4.1. Az általános n-ed fokú polinom gyökjelekkel való megoldhatósága

A továbbiakban a célunk annak a vizsgálata, hogy egy adott polinom gyökei mikor fejezhetőek ki az együtthatók segítségével a négy alapművelet és a gyökvnás felhasználásával. Megjegyezzük, hogy nyilván elég csak prímkitevőjű gyökvonásokkal dolgozni, hiszen ezek egymásutáni végrehajtásával tetszőleges kitevőjű gyökvonás elvégezhető. Ahhoz, hogy az együtthatókból alkotott valamilyen gyökkifejezéssel további számolásokat tudjunk végezni, az adott kifejezést hozzá kell vennünk az együtthatók által generált testhez, és itt jön be a képbe a testbővítésk fogalma. Egy polinom egy gyöke akkor lesz gyökkifejezése az együtthatóknak, ha az alaptest véges sok speciális típusú bővítésével egy olyan testhez jutunk, amely már tartalmazza az említett gyököt. Hogy mik ezek a speciális típusú bővítések, azt a következőképpen formalizálhatjuk:

4.1.1. Definíció. *A K test felett gyökjelekkel elérhetőnek nevezzük a K testet, továbbá ha az L test gyökjelekkel elérhető, akkor az $L(b)$ test is az, amennyiben b egy L felett irreducibilis, szeparábilis, prím fokú $x^p - a$ alakú polinom gyöke.*

Vagyis az a-ból való p-edik gyökvonás valójában az $x^p - a$ alakú polinom egy gyökével való bővítésnek felel meg. Első feladatunk tehát az ilyen alakú bővítések megértése lesz. Mivel a véges testek vizsgálata kimaradt a dolgozatból, így a véges karakterisztikájú testek feletti polinomok megoldhatóságának kérdésével sem foglalkozunk. A továbbiakban ezért külön említés nélkül feltesszük, hogy nullkarakterisztikájú test fölött dolgozunk, illetve hogy p valamilyen prímszámot jelöl.

4.1.2. Állítás. *A K test felett az $x^p - 1$ polinom szeparábilis és Galois-csoportja ciklikus.*

Bizonyítás. Legyen L az $x^p - 1$ polinom felbontási teste, és $\varepsilon \in L$ ennek a polinomnak egy 1-től különböző gyöke. (Ilyen van, hiszen könnyen ellenőrizhető például deriválással vagy maradékos osztással, hogy az 1 nem többszörös gyök.) Ekkor $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ mind különböző elemek, hiszen ha lenne köztük két azonos, akkor ezek kitevőinek különbsége nem 1 (hiszen $\varepsilon \neq 1$), viszont osztója lenne p-nek, ami nyilván lehetetlen. Ugyanakkor ezek is gyökei a vizsgált polinomnak, vagyis ezek éppen ε konjugáltjai lesznek, és így a bővítés szeparábilis. Mivel $L = K(\varepsilon)$, így a test egy relatív automorfizmusának megadásához elég ε képét megadni. Ha $\sigma_i(\varepsilon) = \varepsilon^i$ és $\sigma_j(\varepsilon) = \varepsilon^j$, akkor $\sigma_i\sigma_j(\varepsilon) = (\varepsilon^i)^j = \varepsilon^{i \cdot j}$, amiből triviálisan következik, hogy a Galois-csoport a *mod p* vett redukált maradékosztályok multiplikatív csoportjával izomorf. $\square$

4.1.3. Definíció. *Az $x^p - 1$ polinom gyökeit p-edik egységgyököknek, míg az 1-től különböző gyökeit p-edik primitív egységgyököknek hívjuk.*

4.1.4. Tétel. *Amennyiben K tartalmazza az összes p-edik egységgyököt, úgy az $x^p - a \in K[x]$ polinom vagy irreducibilis, vagy lineáris faktorokra bomlik.*

Amennyiben K nem tartalmaz primitív p-edik egységgyököt, úgy $x^p - a$ vagy irreducibilis, vagy felbomlik egy irreducibilis és egy elsőfokú faktor szorzatára.

Bizonyítás. Tegyük fel, hogy K tartalmazza a p-edik egységgyököket, és $x^p - a$ reducibilis. Ha van egy b gyöke K-ban, akkor minden ε (p-edik) egységgyökre εb is gyök lesz, és így a polinom lineáris faktorokra bomlik. Ha nincs lineáris faktora, akkor tekintsük egy tetszőleges komponensét. Ez a kompnens $x - \varepsilon b$ alakú tényezők szorzataként áll elő, konstans tagja tehát εb^k alakú. Mivel ez egy $K[x]$-beli polinom, így $\varepsilon b^k \in K$. Felhasználva, hogy k és p relatív prímek, léteznek olyan r és s egészek, hogy $rk = sp + 1$, azaz $(\varepsilon b^k)^r = \varepsilon^r b^{sp+1} = \varepsilon^r a^s b$. Átrendezve az egyenletet $\varepsilon^r b = (\varepsilon b^k)^r a^{-s} \in K$ adódik, vagyis $x^p - a$-nak mégis csak van lineáris faktora K fölött, és így alkalmazható az iménti gondolatmenet.

Tegyük most fel, hogy K nem tartalmaz primitív p-edik egységgyököt. Az előző gondolatmenet alapján, ha $x^p - 1$ nem irreducibilis, akkor van egy lineáris faktora. Ha ezzel leosztva a maradék nem irreducibilis, akkor ennek is van egy lineáris faktora. Ekkor viszont az $x^p - a$ polinomnak már két gyöke is van a K testben, melyek mindegyike $\varepsilon_1 b$ és

$\varepsilon_2 b$ alakú. Ezek hányadosa azonban egy primitív egységgyök lenne ami ellentmond annak a feltételnek, hogy K nem tartalmaz primitív p-edik egységgyököket. $\square$

4.1.5. Megjegyzés. Ezzel minden eshetőséget lefedtünk, hiszen mint láttuk, ha K tartalmaz egy primitív p-edik egységgyököt, akkor az összeset tartalmazza. A tétel arra is magyarázatot ad, hogy a gyökjelekkel való elérhetőség definíciójában miért tettük fel, hogy az $x^p - a$ polinom irreducibilis. Ennek az összes gyökével bővítve ugyanis a p-edik egységgyökök mindenképpen bekerülnek a testbe, akár irreducibilis a polinom, akár nem. Így megtehetjük, hogy először ezekkel bővítjük a testet. Ha már viszont a p-edik egységgyököket tartalmazza a test, akkor $x^p - a$ polinom vagy irreducibilis, vagy lineáris faktorokra bomlik, amely esetben nincs értelme a gyökeivel bővíteni.

4.1.6. Tétel. *Legyen $N|K$ egy p-ed fokú bővítés, ahol K tartalmazza a p-edik egységgyököket, és tegyük fel, hogy $G(N|K)$ ciklikus. Ekkor $N = K(b)$, ahol b az $x^p - a \in K[x]$ irreducibilis polinom gyöke.*

Bizonyítás. Legyen $G(N|K)$ egy generátoreleme σ és rögzítsünk egy K-n kívüli c elemet, valamit egy ε primitív p-edik egységgyököt. Készítsük el, az úgynevezett Lagrange-féle rezolvenst:

$$(\varepsilon, c) = c + \varepsilon^{-1}\sigma(c) + \cdots + \varepsilon^{-(p-1)}\sigma^{p-1}(c)$$

és tekintsük ezek

$$c' = (\varepsilon, c) + (\varepsilon^2, c) + \cdots + (\varepsilon^p, c)$$

összegét. Ez utóbbi összeg a Lagrange-rezolvens definícióját behelyettesítve, majd a $\sigma^i(c)$-k szerint csoportosítva a következő alakú:

$$\sum_{i=0}^{p-1}(\varepsilon^{-i} + \varepsilon^{-2i} + \cdots + \varepsilon^{-pi})\sigma(c)$$

Ha $i \neq 0$ akkor a mértani sorozat összegképlete alapján $\sigma(c)$ együtthatója 0, míg $i = 0$ esetén p. Így $c' = pc \neq 0$ adódik, hiszen nullkarakterisztikájú test felett dolgozunk. Mivel c nem eleme K-nak, így c'-sem, és így az őt definiáló összeg legalább egy tagja is K-n kívüli. Ez nem lehet az $(1, c)$ hiszen ezt σ fixen hagyja, tehát a keresett b elem (ε, c) alakú lesz valamilyen ε primitív p-edik egységgyökkel. A feltétel szerint K tartalmazza az egységgyököket, ezért

$$\sigma(b) = \sum_{i=0}^{p-1} \varepsilon^{-i}\sigma^{i+1}(c) = \varepsilon \cdot \sum_{i=1}^{p} \varepsilon^{-i}\sigma^{i}(c) = \varepsilon \cdot (\varepsilon, c) = \varepsilon b$$

Innen az $a = b^p$ elemre

$$\sigma(a) = \sigma(b^p) = \sigma(b)^p = (\varepsilon b)^p = b^p = a$$

vagyis $a \in K$. Kaptuk tehát, hogy b az $x^p - a \in K[x]$ polinom gyöke. Mivel b nem eleme K-nak, és a szorzástétel miatt a foka osztója a bővítés fokának, így csak $N = K(b)$ lehetséges. Az $x^p - a$ polinom nyilván nem bomlik lineáris faktorokra K felett, így a 4.1.4 tétel miatt irreducibilis. $\square$

4.1.7. Állítás. *Legyen $M|K$ véges Galois-bővítés, ahol M tartalmazza a p-edik egységgyököket. Ekkor K-nak az a legszűkebb M-et tartalmazó normális bővítése, mely tartalmazza az $x^p - a \in M[x]$ irreducibilis polinom gyökeit, az M felett gyökjelekkel elérhető.*

Bizonyítás. Mivel M normális bővítése K-nak, így a 2.2.10 tétel szerint tehát létezik olyan $f \in K[x]$, amire M éppen f felbontási teste K felett. Jelöljük $a = a_1, \ldots, a_k$-val az a összes K feletti konjugáltját, és legyen $g(x) = \prod_{i=1}^{k}(x^p - a_i)$. A már többször alkalmazott gondolatmenet alapján, ennek a polinomnak az együtthatói éppen az a_i-k elemi szimmetrikus polinomjai, melyeket M minden automorfizmus helyben hagy. Mivel a 3.1.7 állítás szerint ez a tulajdonsága csak K-nak van meg, így $g \in K[x]$. Legyen tehát N az $f(x) \cdot g(x)$ polinom felbontási teste K felett. Ekkor persze N normális bővítése K-nak és $M \leq N$. Legyen most $M_0 = M$, és M_{i+1} az M_i test bővítése az $x^p - a_{i+1}$ polinom egy gyökével. Mivel M_i tartalmazza a p-edik egységgyököket, így a 4.1.4 tétel szerint $x^p - a_{i+1}$ vagy irreducibilis M_i felett, vagy lineáris faktorokra bomlik. Mindkét esetben M_{i+1} gyökjelekkel elérhető lesz M_i felett, és így $N = M_k$ is gyökjelekkel elérhető $M = M_0$ felett. $\square$

4.1.8. Tétel. *Legyen $f \in K[x]$ egy irreducibilis (a nullkarakterisztika miatt rögtön szeparábilis) polinom, és tegyük fel, hogy f egy gyöke eleme a K felett gyökjelekkel elérhető L testnek. Ekkor f Galois-csoportja feloldható.*

Bizonyítás. Az f polinom felbontási teste része tetszőleges L-et tartalmazó normális bővítésnek. Mivel a 3.1.14 tétel alapján f Galois-csoportja megegyezik egy a felbontási testet tartalmazó normális bővítés Galois-csoportjának bizonyos faktorcsoportjával, és feloldható csoport faktorcsoportja is feloldható, így elég egy L-et tartalmazó normális bővítést találni, melynek Galois-csoportja feloldható.

Legyen $|L : K| = k$ és M_0 a K-nak az a bővítése, amit úgy kapunk, hogy k minden p prímosztójára K-t bővítjük a p-edik egységgyökökkel. Ez a bővítés normális, hiszen

$x^p - a \in K[x]$ alakú polinomok szorzatának felbontási teste, és szeprábilis is, mivel ennek a szorzatpolinomnak nincsenek többszörös gyökei. Azt állítjuk, hogy ekkor $G(M_0|K)$ feloldható. Létezik ugyanis testeknek egy

$$K \leq K_1 \leq K_2 \leq \dots K_r = M_0$$

lánca, ahol K_{i+1} valamilyen $x^p - a \in K_i[x]$ alakú polinom felbontási teste K_i felett. A $G(K_r|K_{r-1})$ csoport a 4.1.2 tétel szerint ciklikus, és így feloldható. Tegyük fel tehát, hogy $G(K_r|K_i)$ feloldható. A 3.1.15 állítás értelmében $G(K_i|K_{i-1}) \cong G(K_r|K_{i-1})/G(K_r|K_i)$. Itt $G(K_i|K_{i-1})$ ciklikus, és így feloldható, valamint az indukciós feltevés szerint $G(K_r|K_i)$ szintén feloldható. Így a 1.2.13 tétel alapján $G(K_r|K_{i-1})$ is, és végül $G(M_0|K)$ is feloldható.

A gyökjelekkel való elérhetőség definíciója alapján létezik testeknek egy olyan $K = L_0 \leq \dots \leq L_n = L$ lánca, hogy $L_{i+1} = L_i(\vartheta_{i+1})$, ahol ϑ_i az $x^{p_i} - a_i \in L_{i-1}[x]$ irreducibilis, prím fokú polinom gyöke. A továbbiakban ha M_i már megvan, akkor ennek úgy szeretnénk egy M_{i+1}, K felett normális bővítését találni, hogy $L_{i+1} \leq M_{i+1}$ teljesüljön, valamint $G(M_{i+1}|K)$ feloldható legyen, hiszen ekkor M_n éppen olyan bővítés lesz, amit keresünk.

Definiáljuk tehát M_{i+1}-et úgy, mint M_i-nek a legszükkeb K felett normális, az $x^{p_{i+1}} - a_{i+1} \in M_i[x]$ polinom egy ϑ_{i+1} gyökét tartalmazó bővítését. A 4.1.7 állítás szerint M_{i+1} gyökjelekkel elérhető M_i felett, így ugyanúgy ahogy az $M_0|K$ bővítés esetén beláttuk, hogy a Galois-csoportja feloldható, be lehet látni, hogy a $G(M_{i+1}|M_i)$ csoport feloldható, és szintén ugyanez a technika alkalmazható annak bizonyítására, hogy $G(M_{i+1}|K)$ feloldható. (Annyi különbséggel, hogy a $G(M_j|M_{j-1})$, $j \leq i$ csoportok feloldhatósága nem a csoport ciklikusságának, hanem a korábban bizonyított lépéseknek a következménye.) $\square$

4.1.9. Tétel. *Ha $f(x)$ egy olyan polinom a (nullkarakterisztikájú) K test felett, melynek Galois-csoportja feloldható, akkor a felbontási teste része egy a K felett gyökjelekkel elérhető testnek.*

Bizonyítás. Legyen az f felbontási teste K felett N_0 és az $N_0|K$ bővítés foka n. Legyen M az a test, amit úgy kapunk, hogy n minden p prímosztójára K-t bővítjük a p-edik egységgyökökkel. Ez természetesen gyökjelekkel elérhető. Legyen most N az f felbontási teste M felett. Mivel $N_0 \leq N$, így elég annak belátása, hogy N gyökjelekkel elérhető a K test felett, amihez elég, hogy N gyökjelekkel elérhető M felett. A 3.1.15 állítás második pontja szerint (ahol N_0-ra és M-re mint egy tetszőleges őket tartalmazó Galois-bővítés közbülső testeire tekintünk) $G([N_0, M]|M) \cong G(N_0|(N_0 \cap M))$. Ez utóbbi csoport azonban a feloldható $G(N_0|K)$ csoport egy részcsoportja, és így maga is feloldható. Mivel $[N_0, M] = N$ így azt kaptuk, hogy $G(N|M)$ izomorf egy feloldható csoporttal, tehát ő is az. A bizonyításból az is kijött, hogy $G(N|M)$ rendjének minden prímosztója osztója $G(N_0|K)$ rendjének is, hiszen előbbi izomorf az utóbbinak egy részcsoportjával. Ez azt jelenti, hogy M tartalmazza a p-edik egységgyököket $|G(N|M)|$ minden p prímosztójára.

Most rátérünk annak bizonyítására, hogy N gyökjelekkel elérhető M felett. Legyen $G = G(N|M)$, és tekintsük ennek egy kompozícióláncát:

$$G = G_0 \rhd \dots G_i \rhd G_{i+1} \rhd \dots \rhd G_r = \{1\}.$$

Minden i-re jelöljük Δ_i-vel a $\Delta(G_i)$ testet. A 3.1.14 tétel szerint mivel $G_{i+1} \lhd G_i$ így Δ_{i+1} normális bővítése Δ_i-nek, és $G(\Delta_{i+1}|\Delta_i) \cong G_i/G_{i+1}$, ami a feloldhatóság miatt prímrendű. Ezen a ponton a 4.1.6 tétel minden feltétele teljesül, így alkalmazhatjuk a $\Delta_{i+1}|\Delta_i$ bővítésre, kapva ezzel, hogy a $\Delta_0 \leq \dots \leq \Delta_r$ testlánc éppen egy olyan lánc, ami bizonyítja N gyökjelekkel való elérhetőségét M felett. $\square$

4.1.10. Definíció. *A K test feletti általános n-ed fokú polinomnak nevezzük az*

$$x^n + y_{n-1}x^{n-1} + \dots + y_1 x + y_0 \in K(y_0, \dots, y_{n-1})[x]$$

polinomot, ahol y_i transzcendens elem a K felett.

Az, hogy az y_i elemek trnaszcendensek K felett, szemléletesen azt jelenti, hogy az algebrai elemekkel ellentétben nem áll fenn semmilyen összefüggés az y_i-k és a test elemei között. Ez ezért jó, mert így ezekkel az elemekkel tisztán formális számolást végezhetünk, melynek eredménye igaz marad akkor is, ha ezek helyére más elemeket helyettesítünk (mindaddig, amíg figyelünk rá, hogy helyettesítés után ne történjen nullával való osztás). Innen látszik, hogy az általános n-ed fokú polinom $K(y_0 \dots y_{n-1})$ test feletti felbontási testének gyökjelekkel való elérhetősége egy olyan megoldóképletet biztosítana tetszőleges n-ed fokú polinomra, mely csak az együtthatók ismeretében meg tudná határozni a polinom gyökeit. Ezen a ponton már minden eszköz rendelkezésünkre áll, hogy megmutassuk, ez milyen n-ek esetén lehetséges.

4.1.11. Tétel. *Az általános n-ed fokú polinom felbontási teste $n \leq 4$ esetén gyökjelekkel elérhető, míg $n \geq 5$ esetén gyökjelekkel nem elérhető.*

Bizonyítás. Azt fogjuk megmutatni, hogy az általános n-ed fokú polinom felbontási testének Galois-csoportja S_n. Mivel a 4.1.8 és a 4.1.9 tételek szerint a gyökjelekkel való elérhetőség ekvivalens a Galois-csoport feloldhatóságával, így az állítás rögötn adódik az első fejezetben S_n feloldhatóságáról látottak alapján.

Jelöljük most K'-vel a $K(y_0, \dots, y_{n-1})$ testet, valamit σ_i-vel az $x_1, \dots, x_n$ határozatlanok i-edik elemi szimmetrikus polinomját. Tekintsük a következő

$$\varphi : K(y_0, \dots, y_{n-1}) \to K(\sigma_1, \dots, \sigma_n) \leq K(x_1, \dots, x_n)$$

homomorfizmus, mely a K test elemeit fixen hagyja, és minden egyes y_i-t a $(-1)^{n-i}\sigma_{n-1}$ elembe visz. Ez testhomomorfizmus lévén injektív, és $K(\sigma_1, \dots, \sigma_n)$ minden eleme előáll képként, így valójában izomorfizmus. Az izomorfizmus-kiterjesztési tétel következtében az általános n-ed fokú polinom K'-feletti, és a képének a $K(\sigma_1, \dots, \sigma_n)$ feletti felbontási teste izomorf, sőt kölcsönösen egyértelmű megfeleltetés áll a két polinom gyökei között. Jelöljük az általános n-ed fokú polinom gyökeit $u_1, \dots, u_n$-el. Mivel e polinom képének minden együtthatója az x_i-k elemi szimmetrikus polinomja (a megfelelő előjelekkel), így a kép gyökei maguk az $x_1, \dots, x_n$ elemek, és így a kép felbontási teste nem más, mint $K(x_1, \dots, x_n)$. Ebből kapjuk, hogy a $G(K'(u_1, \dots, u_n))$ és a $G(K(x_1, \dots, x_n)|K(\sigma_1, \dots, \sigma_n))$ csoportok izomorfak. Ez utóbbi csoport azonban éppen S_n, hiszen az $x_1, \dots, x_n$ elemek különböző permutációi a $K(x_1, \dots, x_n)$ test különböző automorfizmusait adják, ám a $K(\sigma_1, \dots, \sigma_n)$ test minden elemét fixen hagyják. □

Ezzel tehát beláttuk, hogy nincs olyan megoldóképlet, ami minden ötödfokú egyenlet megoldására alkalmas lenne. Ettől függetlenül persze előfordulhat, hogy minden egyes ötödfokú egyenlethez külön-külön találhatunk olyan módszert, aminek segítségével a gyökei az együtthatókból gyökvonások segítségével előállíthatók, ám sajnos nem ez a helyzet. A fejezet lezárásaként érdekességképpen megmutatjuk, hogy létezik olyan racionális együtthatós ötödfokú polinom, melynek gyökei nem gyökkifejezések a racionális test felett.

4.1.12. Állítás. *Ha az $f(x) \in \mathbb{Q}[x]$ irreducibilis polinomnak három valós és két komplex gyöke van $\mathbb{C}$-ben, akkor Galois-csoportja izomorf S_5-el, ennek megfelelően felbontási teste gyökjelekkel nem elérhető.*

Bizonyítás. Jelöljük f felbontási testét n-nel. A Galois-csoport nyilván része lesz S_5-nek. Mivel S_5-öt generálja egy transzpozíció és egy ötös ciklus, így elég megmutatni, hogy ezek benne vannak a Galois-csoportban. Legyen a az f-nek egy valós gyöke. Ekkor f irreducibilitása alapján $|K(a) : K| = 5$. Mivel f felbontási teste $K(a)$-nak is bővítése, így az algebrai bővítések szorzástétele alapján N foka K felett osztható öttel. Az $N|K$

bővítés normális (hiszen felbontási test), és szeparábilis (hiszen $\mathbb{Q}$ tökéletes), és így Galois-csoportjának rendje megegezik a bővítés fokával. Ez azt jelenti, hogy a Galois-csoport rendje osztható öttel, és így Cauchy tétele alapján a csoportnak van ötödrendű eleme, ami csak egy öt hosszú ciklus lehet. Transzpozíciót találni még egyszerűbb, hiszen az az automorfizmus, ami a valós gyököket fixen hagyja, és a két komplex gyököt egymásba viszi épp ilyen. $\square$

Nincs más hátra tehát, mint találni egy a fenti állítás feltételeit kielégítő polinomot. Azt állítjuk, hogy az $f(x) = x^5 - 4x + 2$ polinom ilyen. A Schönemann-Eisenstein-kritérium alapján a polinom irreducibilis. Mivel $f(-2) < 0$, $f(-1) > 0$, $f(1) < 0$ és $f(2) > 0$, így a polinomnak van legalább három valós gyöke. Mivel a deriváltnak $(5x^4 - 4)$ csak két valós gyöke van, így az eredetinek legfeljebb három. Vagyis a polinomnak pontosan három valós, és így pontosan 2 komplex gyöke van.

4.2. Inverz Galois probléma és a kvaternió csoport

Az inverz Galois probléma azzal a kérdéssel foglalkozik, hogy minden véges csoport előállítható-e mint a racionális számok testének valamely bővítésének Galois-csoportja. Ennek egyik speciális esete volt az, amikor S_5-öt előállítottuk, mint egy a racionális számok teste feletti polinom Galois-csoportja. Bár részeredmények születtek a témában, az alapkérdés még mindig megoldatlan. Ebben a fejezetben felsorolunk néhányat ezek közül az eredmények közül, majd konstruálunk egy olyan bővítést, melynek Galois-csoportja izomorf a 8 elemű kavternió csoporttal, Dean [7] cikke alapján. A fejezet megértéséhez szükség van a Sylow részcsoportok fogalmának ismeretére. Az ezzel kapcsolatos tudnivalók megtalálhatók Fried Ervin [1] könyvében.

4.2.1. Tétel. (Kronecker-Weber) *Minden véges Abelcsoport előáll, mint $\mathbb{Q}(\varepsilon)$ egy résztestének Galois-csoportja, valamilyen ε egységgyökre.*

4.2.2. Tétel. *Minden $1 \leq n$-re S_n és A_n előáll, mint alkalmas racionális együtthatós polinom Galois-csoportja.*

Az első példa ilyen polinomra Schur-tól származik.[8] A következő nagy előrelépés a témában A. Scholz-nak [9] és H. Reichard-nak [10] köszönhető:

4.2.3. Tétel. *Tetszőleges páratlan p prímre minden p csoport előáll mint a racionális számok megfelelő bővítésének Galois-csoportja.*

Végezetül megemlítjük Shafarevich tételét. [11]

4.2.4. Tétel. *Minden véges feloldható csoport előáll $\mathbb{Q}$ egy alkalmas bővítésének Galois-csoportjaként.*

Most rátérünk egy olyan bővítés megkonstruálására, melynek Galois-csoportja a kvaternió csoport. Először belátjuk, hogy a keresett polinom foka legalább 8. Legyen $p \in \mathbb{Q}[x]$ egy n-ed fokú polinom, ami irreducibilis $\mathbb{Q}$ felett. A polinom felbontási testének Galois-csoportja p gyökeit permutálja, és a gyökök permutációja egyértelműen meghatároz minden Galois csoportbeli elemet. Így a Galois csoport az S_n szimmetrikus csoport részcsoportjának is tekinthető. A kvaterniócsoport 8 elemű, így mind a Galois csoport, mind az azt tartalmazó szimmetrikus csoport 2-Sylow részcsoportjában benne van.

4.2.5. Lemma. *S_n szimmetrikus csoport 2-Sylow részcsoportja nem tartalmaz a kvaterniócsoporttal izomorf részcsoportot, ha $n \leq 7$.*

Bizonyítás. Elég az állítást $n = 7$-re belátni, hisz S_m részcsoportja S_n-nek, ha $m \leq n$. Sőt, a 2-Sylow részcsoportja S_7-nek és S_6-nak izomorfak egymással. Ismert tény [4], hogy S_n szimmetrikus csoport 2-Sylow részcsoportja egy erdő automorfizmus csoportja. Ezek az erdők teljes bináris fák diszjunkt uniói, és az n kettes számrendszerbeli felírása határozza meg, hogy mekkora fákra van szükség. Egy ilyen fa minden automorfizmusa leírható a leveleken indukált permutációval. S_6 esetében ez 4+2, azaz egy négylevelű és egy kétlevelű teljes bináris fa uniójának automorfizmus csoportjáról van szó. A részfák automorfizmus csoportjának direkt összege a 2-Sylow részcsoport.

A 4 csúcsú teljes bináris fa automorfizmus csoportjának van olyan másodrendű eleme, ami csak két levelet kicserél, amiknek van közös szomszédja a fában, illetve egy másik olyan, ami a fa két oldalát kicseréli. Ezek szorzata egy negyedrendű elem, míg fordított sorrendben szorozva őket az iménti elem inverzét kapjuk. Ez éppen a diéder csoport karakterizáló tulajdonsága, ennek a fának az automorfizmus csoportja tehát a diéder csoport. Így S_6-é $D_4 \times C_2$ csoporttal izomorf, ahol C_2 a 2 rendű ciklikus csoport (melynek hat negyedrendű eleme van). Ebben összesen 4 negyedrendű elem van, ráadásul bármely kettő felcserélhető. Így ebben a csoportban nem található a kvaterniócsoporttal izomorf részcsoport. $\square$

Most keresünk egy olyan valós számot, mely felbontási testének Galois-csoportja a kvaternió csoporttal izomorf. Legyen s a $(2+\sqrt{2})(3+\sqrt{3})$ egyik négyzetgyöke.

4.2.6. Lemma. $s \notin \mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))$

Bizonyítás. Legyen σ a $\mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))$ testnek azon automorfizmusa, ami $\sqrt{3}$-at helyben hagyja, $\sqrt{2}$-t pedig elviszi a -1-szeresébe. Ekkor

$$\frac{\sigma(s)^2}{s^2} = \frac{2-\sqrt{2}}{2-\sqrt{2}} = 3-2\sqrt{2} = (1-\sqrt{2})^2.$$

Azt kapjuk, hogy

$$\frac{\sigma(s)}{s} = \pm(1-\sqrt{2}) \tag{4.1}$$

Tegyük fel indirekt, hogy $s \in \mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))$. Ekkor alkalmazhatjuk σ-t az egyenlet mindkét oldalára. Kapjuk, hogy $\frac{\sigma^2(s)}{\sigma(s)} = \pm(1+\sqrt{2})$. Beírva a 4.1 egyenlőség alapján, hogy $\sigma(s) = s \pm (1-\sqrt{2})$, azt kapjuk, hogy $\sigma^2(s) = -s$. Ez viszont ellentmond annak, hogy σ egy másodrendű testautomorfizmusa $\mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))$-nak. $\square$

A 4.2.6 lemma alapján tudjuk, hogy s nincs benne a $\mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))$ testben, de egy másodfokú bővítésben nyilván benne van. Így a szorzástétel alapján $\mathbb{Q}$ feletti foka 8, és Galois-csoportjának rendje is ennyi. Legyen p a $(2+\sqrt{2})(3+\sqrt{3})$ szám $\mathbb{Q}$ feletti minimálpolinomja, aminek foka 4. Ekkor a nyolcadfokú $p(x^2)$ polinomnak gyöke lesz s, így ez a minimálpolinom. Ennek minden α gyökének a -1-szerese is gyöke. Ráadásul a $\mathbb{Q}(s)$ automorfizmusainak megszoritasai a $\mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))$ testre kiadják a $\sqrt{2}$ és $\sqrt{3}$ előjelét megváltoztató négy automorfizmust. Ez alapjána polinom többi gyökei tehát a következők: $\pm(2\pm\sqrt{2})(3\pm\sqrt{3})$.

$G(\mathbb{Q}((2+\sqrt{2})(3+\sqrt{3}))|\mathbb{Q})$ a Klein csoporttal izomorf, így $G(\mathbb{Q}(s)|\mathbb{Q})$ nem lehet a 8 elemű ciklikus csoporttal izomorf. Jelölje π azt a testautomorfizmust, amire

$$\pi(s) = \pi(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}) = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}. \tag{4.2}$$

Belátjuk, hogy ez egy negyedrendű automorfizmus. A fenti alapján, ha nem negyedrendű, akkor a rendje csak kettő lehet. Ekkor $\pi(s)s$-et π fixen hagyja, tehát

$$\pi\left(\sqrt{(2+\sqrt{2})(2-\sqrt{2})}(3+\sqrt{3})\right) = \pi(\sqrt{2}(3+\sqrt{3})) = \sqrt{2}(3+\sqrt{3}). \tag{4.3}$$

Négyzetre emelve (4.3)-at, és kihasználva, hogy π a racionális számokat helyben hagyja, azt kapjuk, hogy $\pi(\sqrt{3}) = \sqrt{3}$. Ezt visszaírva kapjuk, hogy $\pi(\sqrt{2} = \sqrt{2})$.

Négyzetre emelve a (4.2) egyenletet

$$\pi((2+\sqrt{2})(3+\sqrt{3})) = (2-\sqrt{2})(3+\sqrt{3}),$$

adódik, ami ellentmond annak, hogy π fixen hagyja $\sqrt{2}$-t, $\sqrt{3}$-at és a racionális számokat.

Ezzel analóg számolással megmutatható, hogy azon automorfizmusok, melyek s-et nem önmagába vagy a mínusz egyszeresébe viszik, szintén negyedrendűek. Az elemrendek alapján a Galois-csoport csak a kavetrniócsoport lehet.

Irodalomjegyzék

[1] Fried Ervin, Algebra II., Nemzeti Tankönyvkiadó, 2002

[2] Kiss Emil, Bevezetés az algebrába, Typotex, 2007

[3] Szamuely Tamás, Galois groups and fundamental groups

[4] P. Cameron, Permutation groups 1999

[5] Szűcs András, Topológia

[6] Zabradi Gergely, internetes jegyzet (http://zabradi.web.elte.hu/Jegyzetek/szeparabilis.pdf)

[7] R. A. Dean, A rational polynomial whose group is the quaternions. The Amer. Math. Monthly,

[8] Schur, Gleichungen ohne Affekt, Sitzungsberichte Akad. Berlin (1930),

[9] Scholz, Konstruktion algebraischer Zahlkorper mit belieb iger Gruppe von Primzahlpoten-zordnung I, Math (1937)

[10] H. Reichardt, Konstruktion von Zahlkorpern mit gegebener G aloisgruppe von Primzahlpotenzordnung, J. Reine Angew. Math.

[11] R. Shafarevich, Construction of fields of algebraic number s with given solvable Galois group