Eötvös Loránd Tudományegyetem
Természettudományi Kar

Nagy Levente
Matematikus MSc

Noether-probléma és kohomologikus invariánsok

Szakdolgozat

Témavezető:
Szamuely Tamás
MTA Rényi Alfréd Matematikai Kutatóintézet

2011

Tartalomjegyzék

Bevezetés

A Noether-problémán a következő kérdést értjük: legyen k_0 test, G tetszőleges csoport és tegyük fel, hogy adva van $G \xrightarrow{\rho} GL_n(k_0)$ hűséges reprezentáció. Ekkor G természetes módon hat a $k_0(x_1,\ldots,x_n)$ racionális függvénytesten, jelöljük K_ρ-val a $k_0(x_1,\ldots,x_n)^G$ fixtestet.

KÉRDÉS. *A K_ρ test racionális (tiszta transzcendens) bővítése-e k_0-nak?*

Noether motivációja véges csoportra a kérdés vizsgálatában az ún. inverz Galois-probléma volt: előáll-e minden véges G csoport, mint $\mathbb{Q}$ (vagy tetszőleges algebrai számtest) feletti Galois-bővítés Galois-csoportja. A kapcsolatot Noether tétele jelenti, ami azt mondja ki, hogy ha a G véges csoportra és k_0 algebrai számtestre létezik olyan ρ hűséges reprezentáció, hogy K_ρ racionális bővítése k_0-nak, akkor G előáll k_0 felett Galois-csoportként. Sőt, ebben az esetben a G Galois-csoportú bővítéseket még "parametrizálni" is tudjuk, erről szól Saltman tétele generikus Galois-bővítések létezéséről.

Tetszőleges alaptest és véges G csoport esetén $n = 1$-re a válasz mindig pozitív lesz Lüroth tétele szerint: ha $k_0 \subseteq K \subseteq k_0(x)$, ahol $k_0(x)|K$ véges bővítés, akkor $K|k_0$ is racionális bővítés. Általában azonban a Noether-problémára adható válasz erősen függ attól, hogy a k_0 algebrailag zárt-e vagy sem. Ha k_0 algebrailag zárt és 0 karakterisztikájú, akkor $n = 2$-re Castelnuovo egy híres tétele miatt pozitív lesz a válasz a Noether-problémára, de $n \geq 3$ esetén már vannak ellenpéldák (lásd [**7**] 6.6). Ha G-ről azt tesszük fel, hogy kommutatív és az exponense nem osztható az algebrailag zárt k_0 test karakterisztikájával, akkor Fischer tétele (lásd [**7**] Theorem 6.6.8 vagy [**17**] Theorem 6.1) szerint a Noether-problémára igenlő a válasz.

Az előzőtől gyökeresen eltér a $k_0 = \mathbb{Q}$ eset. Swan 1969-ben bizonyította, hogy a Noether-problémára a $\mathbb{Z}/47\mathbb{Z}$ ciklikus csoport esetén nemleges a válasz. Saltman eredménye, hogy hasonló a helyzet a $\mathbb{Z}/8\mathbb{Z}$ csoportra. A szakdolgozat fő témája az ő módszereinek és eredményének általánosítása a [**6**] könyv nyomán. Célunk a következő tétel bizonyítása: ha G olyan csoport, melynek a 2-Sylow-részcsoportja $\mathbb{Z}/2^m\mathbb{Z}$ ($m \geq 3$) ciklikus csoport, akkor G-re $\mathbb{Q}$ felett a Noether-probléma nem igaz.

A 1. fejezetben tárgyaljuk Noether ill. Saltman fent említett eredményeit a Noether-probléma és az inverz Galois-probléma kapcsolatáról ill. az adott G csoportú Galois-bővítések parametrizálásáról. Kiterjesztjük a Galois-bővítés fogalmát kommutatív gyűrűkre, belátjuk számunkra legfontosabb tulajdonságait, majd ezek és a Hilbert irreducibilitási tétel (amit nem bizonyítunk) segítségével belátjuk Noether tételét. Ezután bevezetjük a generikus Galois-bővítés fogalmát adott k_0 testre és G csoportra, definíció szerint ez fogja az adott csoportú Galois-bővítéseket parametrizálni. Ha a Noether-probléma igaz G-re és k_0-ra, ahol k_0 végtelen test, akkor Saltman tétele generikus Galois-bővítések létezését bizonyítja.

A 2. és 3. fejezet a későbbiekhez szükséges homologikus algebrai és algebrai geometriai előismereteket foglalja össze. Röviden áttekintjük a véges és provéges csoportok kohomológiáját, definiáljuk testek Galois kohomológia-csoportjait. Tárgyaljuk a nem-Abel csoport együtthatós kohomológiák elméletét is. A (generikus) Galois-bővítés fogalmát tovább általánosítjuk sémákra, így jutunk el a (verzális) torzorokhoz. Látni fogjuk, hogy a k_0 test feletti G-torzorokat bijekcióba állíthatjuk a $H^1(k_0, G)$ Galois-kohomológia halmazzal.

Az utolsó fejezetben adott G-re és k_0-ra egy újabb, a Noether-problémához szorosan kapcsolódó kérdést kezdünk el vizsgálni, a G ún. racionalitási tulajdonságát k_0 felett. A racionalitási tulajdonság nagy előnye, hogy a torzorokon keresztül vizsgálni tudjuk majd kohomologikus keretek között. Ehhez bevezetjük a kohomologikus invariánsokat, amik a G-torzorokhoz rendelnek kohomológia osztályokat természetes módon. Különösen fontosak lesznek számunkra az ún. nemelágazó kohomologikus invariánsok, melyeket a 3. fejezetben megismert reziduum leképezés segítségével definiálunk. Fagyejev egzakt sorozatának és a Kompatibilitási tétel következményeként azt kapjuk, hogy ha igaz a racionalitási tulajdonság G-re k_0 felett, akkor minden nemelágazó invariáns szükségszerűen konstans. Ezzel a racionalitási tulajdonság eldöntésére kapunk egy szükséges feltételt, amiről egy konkrét példán belátjuk, hogy a $\mathbb{Z}/2^m\mathbb{Z}$ ($m \geq 3$) csoportra és $\mathbb{Q}$ testre nem teljesül, amiből már következni fog a fő eredményünk.

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Szamuely Tamásnak, hogy felhívta a figyelmemet erre az érdekes témára, és hogy észrevételeivel, tanácsaival segített a szakdolgozat elkészítésében.

1. FEJEZET

Noether tétele

A fejezet fő célja Noether a bevezetőben már említett tételének a bizonyítása. Ehhez szükségünk lesz a Galois-bővítés fogalmának általánosítására kommutatív gyűrűkre, így először azt mutatjuk be. Erről az érdekes témáról az olvasó a [**4**] cikkben találhat további részleteket. Ezután rátérünk a tétel bizonyítására, majd a fejezet lezárásaként ismertetjük Saltman tételét generikus Galois-bővítések létezéséről. A fejezet nagy része Swan [**17**] cikkére épül.

1. Kommutatív gyűrűk Galois-bővítései

Tegyük fel, hogy adott $K|F$ Galois-bővítés G Galois-csoporttal és k test. A $K|F$ Galois-bővítésből szeretnénk konstruálni egy k feletti G Galois-csoportú Galois-bővítést, ehhez azonban érdemes a Galois-bővítések fogalmát kiterjeszteni a kommutatív gyűrűk körére. Kommutatív gyűrűk között tenzorszorzással (bázisbővítéssel) már új Galois-bővítéseket tudunk konstruálni, általában azonban ezek nem lesznek testbővítések. A 2. részben látni fogjuk, hogy bizonyos feltételek teljesülése mellett azonban az új bővítés testek Galois-bővítése lesz.

1.1.1. Definíció. *Legyenek $A \subseteq B$ kommutatív gyűrűk, G a B automorfizmusainak véges részcsoportja. Azt mondjuk, hogy B Galois-bővítése A-nak a G csoporttal, ha*

(1) $A = B^G$
(2) *Minden $H \leq G$ részcsoportra és minden $I \subseteq B$ ($I \neq B$) H-stabil ideálra H hűségesen hat B/I-n.*

1.1.2. Definíció. *Legyen B Galois-bővítése A-nak G csoporttal és $b \in B$. Ekkor a $\sum_{g \in G} g(b)$ összeget a b nyomának nevezzük és $tr(b)$-vel jelöljük. Triviális, hogy $tr(b) \in A$.*

1.1.3. Állítás. *Legyen G a B kommutatív gyűrű automorfizmusainak véges részcsoportja és legyen $A = B^G$. Ekkor a következő állítások ekvivalensek.*

(1) *B az A Galois-bővítése G csoporttal.*
(2) *Léteznek olyan $x_i, y_i \in B$ elemek, hogy $\sum x_i g(y_i) = \delta_{g1}$ minden $g \in G$-re, ahol $\delta_{gg'} = 1$, ha $g = g'$ és 0 egyébként.*
(3) *A $h : B \otimes_A B \to \prod_{g \in G} B$ leképezés izomorfizmus, ahol $h(b_1 \otimes b_2)$ g-edik koordinátája $b_1 g(b_2)$.*

Bizonyítás. (3) $\Rightarrow$ (2) : Ha h izomorfizmus, akkor létezik olyan $\sum x_i \otimes y_i$, hogy $h(\sum x_i \otimes y_i) = (1, 0, \ldots, 0)$ és így az x_i, y_i elemek teljesítik (2)-t.

(2) $\Rightarrow$ (3) : Legyen

$$k : \prod_{g\in G} B \to B \otimes_A B$$
$$(b_g) \mapsto \sum_g \sum_i x_i \otimes g^{-1}(y_i b_g)$$

Ekkor k a h inverze lesz, ugyanis

$$hk((b_g)) = h(\sum_g \sum_i x_i \otimes g^{-1}(y_i b_g)) = \sum_g \sum_i h(x_i \otimes g^{-1}(y_i b_g))$$

és adott $g' \in G$-re a g'-dik koordinátában a következőt kapjuk

$$\begin{aligned}\sum_g \sum_i x_i \cdot g' g^{-1}(y_i b_g) &= \sum_{g\neq g'} \sum_i x_i \cdot g' g^{-1}(y_i) g' g^{-1}(b_g) + \sum_i x_i \cdot y_i b_{g'} = \\ &= \sum_{g\neq g'} g' g^{-1}(b_g) \sum_i x_i \cdot g' g^{-1}(y_i) + b_{g'} \sum_i x_i \cdot y_i = \\ &= 0 + b_{g'} = b_{g'}.\end{aligned}$$

Nézzük most a másik irányt

$$\begin{aligned}kh(b_1 \otimes b_2) = k((b_1 g(b_2))) &= \sum_g \sum_i x_i \otimes g^{-1}(y_i b_1 g(b_2)) = \\ &= \sum_g \sum_i x_i \otimes g^{-1}(y_i b_1) b_2 = (1 \otimes b_2) \sum_g \sum_i x_i \otimes g^{-1}(y_i b_1) = \\ &= (1 \otimes b_2) \sum_i \sum_g x_i \otimes g^{-1}(y_i b_1) = (1 \otimes b_2) \sum_i x_i \otimes tr(y_i b_1) = \\ &= (1 \otimes b_2) \sum_i x_i tr(y_i b_1) \otimes 1 = \\ &= (1 \otimes b_2) \sum_i \sum_g x_i g(y_i) g(b_1) \otimes 1 = \\ &= (1 \otimes b_2) \sum_g (g(b_1) \otimes 1) \sum_i x_i g(y_i) \otimes 1 = \\ &= (1 \otimes b_2)(b_1 \otimes 1) = b_1 \otimes b_2.\end{aligned}$$

(2) $\Rightarrow$ (1) : Mivel $A = B^G$, ezért a definíció második felét kell csak ellenőrizni. Ha B-re és G-re teljesül (2), akkor minden $H \leq G$-re is igaz, így ha I H-stabil valódi ideál, akkor B/I-re és H-ra is igaz lesz a (2) pont ($\overline{x_i} = x_i + I$ és $\overline{y_i} = y_i + I$ elemekkel) . Ha $1 \neq h \in H$ triviálisan hatna B/I-n, akkor

$$0 = \sum \overline{x_i} \cdot h(\overline{y_i}) = \sum \overline{x_i} \cdot \overline{y_i} = 1$$

lenne, ami ellentmondás, mivel I valódi ideál.

(1) $\Rightarrow$ (2) : Legyen $1 \neq g \in G$ egy elem és nézzük a $b - g(b)$ elemek által generált I ideált. Mivel g triviálisan hat B/I-n, ezért $I = B$, azaz léteznek olyan u_i és v_i elemek B-ben, hogy

$$\sum_{i=1}^{k} u_i(v_i - g(v_i)) = 1.$$

Legyen $u_0 = -\sum_{i=1}^{k} u_i \cdot g(v_i)$ és $v_0 = 1$. Ekkor

$$\sum_{i=0}^{k} u_i v_i = -\sum_{i=1}^{k} u_i \cdot g(v_i) + \sum_{i=1}^{k} u_i v_i = 1,$$

illetve g-re

$$\sum_{i=0}^{k} u_i g(v_i) = -\sum_{i=1}^{k} u_i g(v_i) + \sum_{i=1}^{k} u_i g(v_i) = 0.$$

Legyen $z_g = \sum u_i \otimes v_i$ és minden $1 \neq g \in G$-re készítsük el z_g-t. Ha $z = \prod_{g \neq 1} z_g$, akkor $h(z) = (1, 0, \dots, 0)$ lesz. □

1.1.4. KÖVETKEZMÉNY. *Ha B Galois-bővítése A-nak, akkor B végesen generált és projektív, mint A-modulus.*

BIZONYÍTÁS. Legyenek x_i-k és y_i-k ($i = 1, \dots, k$) olyanok, mint az előző állítás (2) pontjában. Nézzük a következő kompozíciót:

$$B \xrightarrow{\phi} A^k \xrightarrow{\psi} B,$$

ahol $\phi(b) = (tr(y_i b))$ és $\psi(a_i) = \sum_i x_i a_i$. Ekkor $\psi\phi = id_B$, mert

$$\psi\phi(b) = \sum_i x_i tr(y_i b) = \sum_i \sum_g x_i g(y_i) g(b) = \sum_g g(b) \sum_i x_i g(y_i) = b.$$

Ebből következik, hogy B végesen generált és projektív. □

1.1.5. PÉLDA.

(1) Legyenek k és K testek. A $K|k$ véges bővítés akkor és csak akkor lesz Galois-bővítés a fenti definíció értelmében, ha Galois-bővítés a szokásos testelméleti értelemben.
(2) Legyen A kommutatív gyűrű és G véges csoport. Ekkor a $\prod_{g \in G} A$ a $g(a_h) = (a_{hg})$ G-hatással Galois-bővítése lesz A-nak: ha minden $g \in G$-re $x_g = y_g = (\delta_{gh})$, akkor ezek az elemek teljesítik a 1.1.3. Tétel (2) pontjának feltételét. Azt mondjuk, hogy B felbomló Galois-bővítése A-nak, ha G-ekvivariánsan izomorf $\prod_{g \in G} A$-val.

Tudjuk, hogy minden $b \in B$-re $tr(b) \in A$. A következő állítás szerint minden A-beli elem elő is áll nyomként.

1.1.6. ÁLLÍTÁS. *Ha B Galois-bővítése A-nak, akkor $tr : B \to A$ szürjektív.*

A bizonyításhoz szükségünk lesz az alábbi lemmára:

1.1.7. LEMMA. *Ha R kommutatív gyűrű, $I \subseteq R$ ideál, M végesen generált R-modulus és $IM = M$, akkor létezik olyan $r \in I$, hogy $(1 - r)M = 0$.*

BIZONYÍTÁS. Ez az "általánosított Cayley-Hamilton-tétel" egy következménye. Lásd [**1**] Corollary 2.5. □

1.1.6. ÁLLÍTÁS BIZONYÍTÁSA. Legyen $I = tr(B)$. Ekkor I ideál lesz A-ban, hiszen összeadásra ás A-beli elemmel való szorzásra is triviálisan zárt. Teljesül még, hogy $IB = B$, hiszen az előbb láttuk, hogy $b = \sum_i x_i tr(x_i b)$. Ha a lemmát alkalmazzuk a B végesen generált modulusra és az I ideálra, akkor azt kapjuk, hogy van olyan $r \in I$, hogy $(1 - r)B = 0$. De $1 \in B$, ezért $r = 1$, vagyis $I = A$. □

A következő állítás segítségével új Galois-bővítéseket konstruálhatunk egy már adott bővítésből ún. bázisbővítés segítségével.

1.1.8. ÁLLÍTÁS. *Legyen B az A Galois-bővítése G csoporttal és legyen adott $A \to C$ gyűrűhomomorfizmus (azaz C egy A-algebra). Ekkor $C \otimes_A B$ a C Galois-bővítése lesz G csoporttal.*

BIZONYÍTÁS. Legyenek $x_i, y_i \in B$ olyan elemek, melyek teljesítik a 1.1.3. Állítás (2) pontját. Ekkor $1 \otimes x_i$ és $1 \otimes y_i$-k is teljesítik azt, így $C \otimes_A B$ Galois-bővítése lesz $(C \otimes_A B)^G$-nek. A természetes $C \to C \otimes_A B$ leképezés injektív lesz, mert ha $b' \in B$ olyan, hogy $tr(b') = 1$, akkor a

$$\begin{aligned} \phi : B &\to A \\ b &\mapsto tr(bb') \end{aligned}$$

leképezésre $\phi\iota = id_A$, ahol ι az A beágyazása B-be. Már csak a $(C \otimes_A B)^G$ gyűrűt kell meghatároznunk. Az előző állítás felhasználásával $(C \otimes_A B)^G = tr(C \otimes_A B) = C \otimes_A tr(B) = C$. □

A 1.1.3. Állítás (3) pontját most már úgy is meg lehet fogalmazni, hogy ha B Galois-bővítése A-nak, akkor az $A \hookrightarrow B$ beágyazásra vonatkozó bázisbővítés után a B egy felbomló Galois-bővítését kapjuk.
A klasszikus Speiser-lemma (lásd 2.9.1. Állítás) is általánosítható kommutatív gyűrűk Galois-bővítéseire.

1.1.9. ÁLLÍTÁS. *Legyen $B|A$ kommutatív gyűrűk Galois-bővítése G csoporttal. Tegyük fel, hogy M olyan B-modulus, amin G szemilineárisan hat, azaz $g(bm) = g(b)g(m)$ minden $b \in B, m \in M$-re. Ekkor a következő leképezés izomorfizmus lesz*

$$\begin{aligned} \phi : B \otimes_A M^G &\to M \\ b \otimes m &\mapsto bm \end{aligned}$$

BIZONYÍTÁS. Legyenek x_i-k és y_i-k olyan B-beli elemek, amelyek teljesítik a 1.1.3. Állítás (2) pontjának feltételét. Az inverz leképezést definiáljuk a következőképpen

$$\begin{aligned} \psi : M &\to B \otimes_A M^G \\ m &\mapsto \sum_i x_i \otimes tr(y_i m). \end{aligned}$$

Ekkor, ha $b \in B$ és $m \in M^G$, akkor

$$\begin{aligned} \psi\phi(b \otimes m) = \psi(bm) &= \sum_i x_i \otimes tr(y_i bm) = \\ &= \sum_i x_i \otimes tr(y_i b)m = \sum_i x_i tr(y_i b) \otimes m = \\ &= (1 \otimes m)(\sum_i x_i tr(y_i b) \otimes 1) = (1 \otimes m)(b \otimes 1). \end{aligned}$$

Másrészt,

$$\phi\psi(m) = \phi(\sum_i x_i \otimes tr(y_i m)) = \sum_i x_i tr(y_i m) = m.$$

□

1.1.10. Állítás. *Legyen B kommutatív gyűrű, F test és tegyük fel, hogy B az F Galois-bővítése G csoporttal. Ekkor B féligegyszerű gyűrű lesz, így izomorf lesz F feletti testek direkt szorzatával. Másképpen B étale algebra lesz F felett.*

Bizonyítás. Tudjuk, hogy B véges dimenziós F-algebra (mert végesen generált F-modulus), így a J Jacobson-radikálja nilpotens lesz. Tegyük fel, hogy $J \neq 0$. Legyen n olyan, hogy $I = J^n \neq 0$, de $I^2 = 0$. I G-stabil ideál, hiszen J is G-stabil. Mivel $I \neq 0$, ezért $I \otimes I \neq 0$, de a 1.1.3. Állítás (3)-beli h izomorfizmus 0-ba viszi, ami ellentmondás. Így B féligegyszerű és ezért $B = B_1 \times \cdots \times B_m$, ahol B_i-k testek. □

2. Noether tétele

Az alábbi tétel bizonyítása a célunk ebben a részben.

1.2.1. Tétel (Noether). *Legyen k algebrai számtest, G véges csoport. Tegyük fel, hogy G hűségesen hat az $x_1, \ldots, x_n$ határozatlanokon. Ha $k(x_1, \ldots, x_n)^G$ racionális k felett, akkor létezik $L|k$ Galois-testbővítés G csoporttal.*

1.2.2. Lemma. *Legyenek K és F testek és tegyük fel, hogy $K|F$ Galois-bővítés G Galois-csoporttal. Legyen $B \leq K$ olyan G-stabil részgyűrű, amire $Frac(B) = K$ és jelöljük A-val B^G-t. Ekkor létezik olyan $s \in A$, $s \neq 0$, hogy $B[s^{-1}]$ az $A[s^{-1}]$ Galois-bővítése lesz G csoporttal.*

Bizonyítás. Legyenek x_i és y_i olyan K-beli elemek, melyek teljesítik az 1.1.3. Állítás (2) feltételét. $Frac(B) = K$ miatt létezik olyan $t \in B$, hogy $x_i, y_i \in B[t^{-1}]$ minden i-re. Legyen $s = \prod_{g \in G} g(t)$. Ekkor $s \in A$ és az x_i, y_i elemek $B[s^{-1}]$-ben is benne vannak, továbbá $B[s^{-1}]^G = A[s^{-1}]$, ezzel készen vagyunk. □

1.2.3. Megjegyzés. A bizonyításból látszik, hogy K minden eleme b/a alakú, ahol $b \in B$ és $a \in A$.

Legyen $K|F$ testek Galois-bővítése, az előző állítás miatt feltehető, hogy léteznek olyan $A \leq F$ és $B \leq K$ olyan részgyűrűk, melyekre $Frac(B) = K$, $B^G = A$ és $B|A$ Galois-bővítés. Tegyük fel, hogy adott $A \to E$ homomorfizmus, ahol E test. Ekkor $E \otimes_A B|E$ Galois-bővítés lesz, azonban láttuk, hogy $E \otimes_A B$ testek szorzata is lehet. Bizonyos feltételek mellett azonban tudjuk garantálni, hogy $E \otimes_A B$ test legyen.

Mivel $K|F$ Galois-testbővítés, ezért létezik $\alpha \in K$, hogy $K = F[\alpha]$. Megfelelő A-beli elemmel szorozva α-t, feltehetjük, hogy $\alpha \in B$ (mert K minden eleme b/a alakú). Legyen $f(x) = \prod_{g \in G}(x - g(\alpha))$ az α minimálpolinomja F felett. Vegyük észre, hogy $f(x) \in A[x]$, ezért az $A \to E$ leképezés az $f(x)$ polinomotegy $g(x) \in E[x]$ polinomba viszi. Ha g irreducibilis, akkor $1 \otimes \alpha \in E \otimes_A B$ elem $n = deg(g) = deg(f) = |K : F|$ fokú testet generál E felett $E \otimes_A B$-ben (és ez a test izomorf $E[x]/(g(x))$-szel). De $|E \otimes_A B : E| = n$, mert $P = Ker(A \to E)$ szerint lokalizálva, $B_{A \setminus P}$ az A_P Galois-bővítése lesz az 1.1.8. Állítás miatt. Cseréljük le ezekre az A-t ill. B-t. Mivel $B_{A \setminus P}$

végesen generált projektív modulus egy lokális gyűrű felett, ezért szabad lesz. Az 1.1.9. Állítást használva K additív csoportjára, azt kapjuk, hogy

$$K \cong B \otimes_A F \cong A^n \otimes_A F \cong F^n$$

és hasonlóan

$$E \otimes_A B \cong E^n,$$

vagyis $|K : F| = |E \otimes_A B : E|$. Így az $1 \otimes \alpha$ elem által generált test $E \otimes_A B$ lesz, tehát $E \otimes_A B$ test lenne, amit szerettünk volna.

A következő tétel segít nekünk megfelelő polinomot találni.

1.2.4. Tétel (Hilbert irreducibilitási tétel). *Legyen k algebrai számtest és $F = k(t_1, \ldots, t_r)$ a k racionális (tiszta transzcendens) bővítése. Legyen $f(x) = f(t_1, \ldots, t_r, x) \in F[x]$ irreduciblis polinom. Ekkor léteznek olyan $a_1, \ldots, a_r \in k$ számok, hogy $f(a_1, \ldots, a_r, x)$ értelmezett és irreducibilis k felett.*

Bizonyítás. Lásd [**15**] Chapter 9. □

Most már bebizonyíthatjuk Noether tételét.

A 1.2.1. Tétel bizonyítása. Alkalmazzuk az előző eredményeket $K = k(x_1, \ldots, x_n)$-re és $F = k(x_1, \ldots, x_n)^G$-re. A feltétel miatt F racionális bővítése k-nak, így a Hilbert irreducibilitási tétel miatt létezik megfelelő $E = k$-ba menő homomorfizmus, és ezzel készen vagyunk. □

3. Saltman tételei

Saltman tételei bizonyos feltételek teljesülése mellett biztosítják olyan, ún. generikus Galois-bővítés létezését, amely adott G csoportú Galois-bővítéseket paraméterezi adott k test felett.

1.3.1. Definíció. *Legyenek A és B kommutatív gyűrűk és tegyük fel, hogy $B|A$ Galois-bővítés G csoporttal. Azt mondjuk, hogy $B|A$ generikus Galois-bővítés a k testre és G csoportra nézve, ha*

1. *$A = k[x_1, \ldots, x_n, h^{-1}]$, ahol x_i-k határozatlanok és $h \in k[x_1, \ldots, x_n]$.*
2. *Ha F tartalmazza k-t és $K|F$ Galois-bővítés G csoporttal (K nem feltétlenül test!), akkor létezik olyan $A \to F$ k-algebra-homomorfizmus, hogy $F \otimes_A B \cong K$ a G hatását megőrizve.*

Tehát egy k-t tartalmazó F test G csoportú Galois-bővítéseit az $A \to F$ homomorfizmusok paraméterezik, vagy másképpen, az x_i-k képei F-ben. A következő tétel Saltman fő eredménye generikus Galois-bővítések létezéséről, lásd [**12**] vagy [**17**].

1.3.2. Tétel. *Legyen k végtelen test. Tegyük fel, hogy G hűségesen hat az $x_1, \ldots, x_n$ határozatlanokon úgy, hogy $k(x_1, \ldots, x_n)^G = k(y_1, \ldots, y_m)$ racionális bővítése k-nak. Ekkor létezik generikus Galois-bővítés k-ra és G-re nézve.*

Legyenek $B_0 = k[x_1, \ldots, x_n]$ és $A_0 = B_0^G$. Tudjuk, hogy létezik olyan $s \in A$, hogy $B = B_0[s^{-1}]$ Galois-bővítése lesz $A = A_0[s^{-1}]$-nek.

1.3.3. Lemma. *Legyenek C és D végesen generált k-algebrák azonos hányadostesttel. Ekkor léteznek olyan $c \in C$ és $d \in D$ nem-nulla elemek, hogy $C[c^{-1}] = D[d^{-1}]$.*

Bizonyítás. Mivel C végesen generált k felett és a C és D hányadosteste azonos, ezért létezik olyan $a \in D$, hogy a C generátorai $D[a^{-1}]$-ban vannak, így $C \subseteq D[a^{-1}]$. Hasonlóan létezik olyan $c \in C$, hogy $D[a^{-1}] \subseteq C[c^{-1}]$. Mivel $C \subseteq D[a^{-1}]$, ezért $c = b/a^m$ alkalmas $b \in D$ elemre és ekkor $C[c^{-1}] = D[(ab)^{-1}]$. □

Az előző lemma miatt feltehető, hogy A $k[y_1, \dots, y_m, s^{-1}]$ alakú, tehát a definíció (1) feltétele teljesül.

1.3.4. Lemma. *Legyen B az A Galois-bővítése G csoporttal. Ekkor B hűen lapos A-modulus.*

Bizonyítás. Láttuk már, hogy B projektív modulus, így lapos is. Jól ismert, hogy B akkor és csak akkor hűen lapos A felett, ha A minden P prímideálja előáll $Q \cap A$ alakban, ahol Q prímideál B-ben. De B végesen generált A-modulus, így B egész A felett és ezzel készen vagyunk. □

1.3.5. Lemma. *Legyen C test. Ha $A \subseteq B$ és $C \subseteq D$ Galois-bővítések ugyanazzal a G Galois-csoporttal és $f : B \to D$ pedig G-ekvivariáns homomorfizmus, akkor az f által indukált $C \otimes_A B \to D$ leképezés izomorfizmus lesz.*

Bizonyítás. Kicserélhetjük a A-t ill. B-t C-re ill. $C \otimes_A B$-re és feltehetjük, hogy f az identitás $A = C$-re megszorítva. Jelöljük $\langle b, b' \rangle$-vel $tr(bb')$-t. Ekkor ez egy $B \to Hom_A(B, A)$ izomorfizmust indukál: elég az A egy hűen lapos bővítésére leellenőrizni ezt és a felbomló Galois-bővítés esetén ez triviális. Mivel f G-ekvivariáns és $f|A = id$, ezért $\langle f(b), f(b') \rangle = \langle b, b' \rangle$, így ha $f(x) = 0$, akkor $\langle x, - \rangle$ eltűnik egész B-n, ezért $x = 0$, tehát f injektív. Dimenzió okok miatt f szürjektív is, azaz f izomorfizmus. □

Térjünk most rá a definíció (2)-beli feltételére: tegyük fel, hogy F tartalmazza k-t és $K|F$ Galois-bővítés G csoporttal, ekkor keresünk olyan $A \to F$ k-algebra-homomorfizmust, hogy $F \otimes_A B \cong K$ a G hatását megőrizve. Ehhez szükségünk van a következő lemmára.

1.3.6. Lemma (Kuyk). *Legyen F végtelen test és tegyük fel, hogy K az F Galois-bővítése G csoporttal. Tegyük fel, hogy a G csoport hat az $X = \{x_1, \dots, x_n\}$ véges halmazon. Ha $0 \neq s \in F[x_1, \dots, x_n]$, akkor létezik olyan $f : X \to K$ G-ekvivariáns leképezés, hogy $s(f(x_1), \dots, f(x_n)) \in K$ invertálható.*

Bizonyítás. [**17**] Lemma 4.5. □

A lemma miatt létezik G-ekvivariáns $B \to K$ leképezés, amire a 1.3.5. Lemmát alkalmazva kapjuk a keresett $F \otimes_A B \xrightarrow{\cong} K$ izomorfizmust, így a $B|A$ generikus Galois-bővítés lesz k-ra és G-re.

2. FEJEZET

Kohomológia-elméletek

A Noether-probléma további tanulmányozásához szükségünk lesz bizonyos homologikus algebrai és ehhez kapcsolódó előismeretekre. A fejezetben ezeket ismertetjük: először a véges csoportok, majd a provéges csoportok kohomológia-elméletét mutatjuk be, ezután definiáljuk az ún. nem-Abel együtthatós első kohomológia-halmazt. Ebben a fejezetben található meg a reziduum leképzés általános konstrukciója, amit aztán majd tovább vizsgálunk lokális testek kohomológiájának esetén. Az utolsó három részben olyan, önmagukban is érdekes eredményeket mutatunk be, amik a szakdolgozat későbbi részében elő fognak kerülni. A téma nagysága miatt lehetetlen lenne mindent teljes részletességgel tárgyalni, így sok helyen fogunk hivatkozni a [**7**] és [**14**] könyvekre.

1. Csoportok kohomológiája

Legyen G csoport és tekintsük a $\mathbb{Z}G$ csoportalgebra feletti (bal oldali) modulusok ${}_{\mathbb{Z}G}Mod$ kategóriáját. Ennek a kategóriának az objektumait G-modulusoknak, a morfizmusokat pedig G-homomorfizmusoknak fogjuk nevezni. Az A_1 és A_2 közötti G-homomorfizmusok halmazát $Hom_G(A_1, A_2)$-vel jelöljük. Az A G-modulusra tekinthetünk úgy is, mint egy Abel-csoportra, amin adott a G (bal oldali) hatása. Azt mondjuk, hogy az A triviális G-modulus, ha a G minden eleme triviálisan hat az A-n.
Először definiáljuk tetszőleges gyűrű felett egy kolánc-komplexus kohomológiáját.

2.1.1. Definíció. *Legyen R gyűrű. Tegyük fel, hogy minden $n \in \mathbb{Z}$-re adott M^n R-modulus és $\delta^n : M^n \to M^{n+1}$ R-modulus-homomorfizmus. Azt mondjuk, hogy $M^\bullet = (M^n, \delta^n)$ kolánc-komplexus, ha $\delta^{n+1} \circ \delta^n = 0$ minden n-re.*

2.1.2. Megjegyzés. Az R gyűrű feletti kolánc-komplexusok is kategóriát alkotnak: az objektumok az $M^\bullet$ kolánc komplexusok, egy $\phi^\bullet : M^\bullet \to N^\bullet$ kolánc-leképezés pedig nem más, mint $\phi^n : M^n \to N^n$ modulus-homomorfizmusok családja melyekre teljesül, hogy a következő diagram kommutatív lesz minden n-re.

$$\begin{array}{ccc} M^n & \xrightarrow{\delta^n_M} & M^{n+1} \\ {\scriptstyle \phi^n}\downarrow & & {\scriptstyle \phi^{n+1}}\downarrow \\ N^n & \xrightarrow{\delta^n_N} & N^{n+1} \end{array}$$

Értelemszerűen lehet definiálni kolánc-komplexusok rövid egzakt sorozatát is.

2.1.3. DEFINÍCIÓ. *Ha R gyűrű és $M^\bullet = (M^n, \delta^n)$ kolánc-komplexus R felett, akkor legyen $Z^n(M^\bullet) = ker(\delta^n)$, $B^n(M^\bullet) = im(\delta^{n-1})$ és $H^n(M^\bullet) = Z^n(M^\bullet)/B^n(M^\bullet)$. Az első modulus elemeit a kociklusoknak, a második elemeit pedig kohatároknak nevezzük. A $H^n(M^\bullet)$ modulust hívjuk az $M^\bullet$ komplexus n-dik kohomológiájának.*

Belátható, hogy ha $\phi^\bullet : M^\bullet \to N^\bullet$ kolánc-leképzés, akkor $\phi^\bullet$ indukál a kohomológiák között is egy leképezést. A következő tétel alapvető fontosságú a homologikus algebrában.

2.1.4. TÉTEL. *Legyen*

$$0 \to L^\bullet \to M^\bullet \to N^\bullet \to 0$$

R feletti kolánc-komplexusok rövid egzakt sorozata. Ekkor létezik a következő hosszú egzakt sorozat

$$\ldots \to H^n(L^\bullet) \to H^n(M^\bullet) \to H^n(N^\bullet) \xrightarrow{d} H^{n+1}(L^\bullet) \to \ldots,$$

ahol a d leképezés az ún. összekötő homomorfizmus és minden más leképezést pedig a kolánc-leképezések indukálnak.

2.1.5. DEFINÍCIÓ. *Legyen R gyűrű és M R-modulus. Ha létezik olyan egzakt sorozat*

$$\ldots \to P_2 \to P_1 \to P_0 \to M \to 0,$$

hogy a P_n modulusok projektívek minden $n \leq 0$-ra, akkor ezt az M egy projektív feloldásának nevezzük.

Belátható, hogy minden R-modulusnak létezik projektív feloldása (sőt, szabad modulusokból álló feloldása is).

2.1.6. DEFINÍCIÓ. *Legyen G csoport, A G-modulus és legyen $P^\bullet$ a $\mathbb{Z}$, mint triviális G-modulus egy projektív feloldása. Nézzük a következő $Hom_G(P^\bullet, A)$ Abel-csoportokból álló kolánc-komplexust:*

$$Hom_G(P_0, A) \to Hom_G(P_1, A) \to Hom_G(P_2, A) \to \ldots$$

A $H^n(Hom_G(P^\bullet, A))$ $(n \geq 0)$ kohomológia-csoportot a G csoport n-dik A együtthatós kohomológia-csoportjának nevezzük és $H^n(G, A)$-val jelöljük.

A következő állítások jól ismertek.

2.1.7. ÁLLÍTÁS.

(1) *$H^n(G, A)$ izomorfia erejéig független a $P^\bullet$ projektív feloldás választásától.*
(2) *$H^0(G, A) = A^G = \{a \in A : g(a) = a \text{ minden } g \in G\text{-re}\}$.*
(3) *Minden $A \to B$ G-homomorfizmus indukál $H^n(G, A) \to H^n(G, B)$ homomorfizmust.*
(4) *Ha adott G-modulusok rövid egzakt sorozata*

$$0 \to A \to B \to C \to 0,$$

akkor létezik a következő hosszú egzakt sorozat

$$\ldots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \xrightarrow{d} H^{n+1}(G, A) \to \ldots$$

Az alacsony dimenziós kohomológiák kiszámításához kiváló segítséget nyújtanak az ún. inhomogén koláncok. Legyen $C^n(G,A) = \{f : G^n \to A$ függvény$\}$, ez Abel-csoport lesz a pontonkénti összeadással, és definiáljuk a $\delta^n : C^n(G,A) \to C^{n+1}(G,A)$ leképezést a következőképpen

$$\begin{aligned}\delta^n(f)(g_1,g_2,\dots,g_{n+1}) = g_1(f(g_2,\dots,g_{n+1}))\\ + \sum_{j=1}^{n}(-1)^j f(g_1,\dots,g_jg_{j+1},\dots,g_{n+1})\\ + (-1)^{n+1} f(g_1,\dots,g_n).\end{aligned}$$

Jelöljük $Z^n(G,A)$-val a $ker(\delta^n)$-t és $B^n(G,A)$-val az $im(\delta^{n-1})$-t, ezek részcsoportok lesznek $C^n(G,A)$-ban. Ekkor a $Z^n(G,A)/B^n(G,A)$ faktorcsoport izomorf lesz a fent definiált $H^n(G,A)$ kohomológia-csoporttal. A $C^n(G,A)$, $Z^n(G,A)$ ill. $B^n(G,A)$ csoportok elemit n-koláncoknak, n-kociklusoknak ill. n-kohatároknak nevezzük.

2.1.8. PÉLDA.

(1) Az $n = 0$ esetben $C^0(G,A) = A$. Legyen $a \in C^0(G,A)$ egy elem, ekkor $\delta^0(a)(g) = g(a) - a$. Ebből következik az előző állítás (2) pontja: $H^0(G,A) = A^G$.
(2) Az előző pontban láttuk, hogy $f \in B^1(G,A)$, ha $f(g) = g(a) - a$ alakú valamilyen $a \in A$-ra. Egy 1-kolánc pontosan akkor lesz 1-kociklus, ha $f(g_1g_2) = g_1(f(g_2)) + f(g_1)$. Érdemes megemlíteni, hogy ha G triviálisan hat az A-n, akkor $H^1(G,A) = Hom(G,A)$.

Legyen H a G csoport részcsoportja. A következőkben a H és G kohomológia-csoportjai közötti kapcsolatot fogjuk vizsgálni.

2.1.9. DEFINÍCIÓ. *Legyen H a G részcsoportja. A $\mathbb{Z}G$ csoportalgebra additív csoportján H természetes módon hat balról és így H-modulust kapunk. Ha A egy H-modulus, akkor a*

$$M_H^G(A) = Hom_H(\mathbb{Z}G, A)$$

Abel-csoport G-modulus lesz a következő hatással

$$g_1(\phi(g_2)) = \phi(g_2g_1).$$

Ha $H = 1$ (ekkor A egyszerűen csak egy Abel-csoport), akkor az előző G-modulust $M^G(A)$-val fogjuk jelölni és az A-hoz tartozó koindukált modulusnak nevezzük.

2.1.10. ÁLLÍTÁS (Shapiro-lemma). *Ha H a G részcsoportja és A pedig H-modulus, akkor létezik természetes izomorfizmus*

$$H^n(G, M_H^G(A)) \xrightarrow{\cong} H^n(H,A)$$

minden $n \geq 0$-ra. Speciálisan, $H^n(G, M^G(A)) = 0$ minden $n > 0$-ra.

A most következők tárgyalásmódja a [**11**]. könyv 1.5. részét követi.
Most legyen G és G' két csoport, A egy G-modulus és A' egy G'-modulus. Tegyük fel, hogy a $\phi : G' \to G$ és a $f : A \to A'$ leképezések csoporthomomorfizmusok. Azt mondjuk, hogy ϕ és f kompatibilisek, ha

$$f(\phi(g')(a)) = g'(f(a))$$

minden $g' \in G'$ és $a \in A$-ra.

2.1.11. Állítás. *Ha G és G' két csoport, A G-modulus, A' G'-modulus, $\phi : G' \to G$ és $f : A \to A'$ kompatibilis homomorfizmusok, akkor az alábbi leképezés*

$$f_* : H^n(G, A) \to H^n(G', A')$$
$$a \mapsto f_*(a)_{g'_1,\ldots,g'_n} = f(a_{\phi(g'_1),\ldots,\phi(g'_n)})$$

homomorfizmus lesz.

Az előző állítás segítségével definiálhatunk néhány nevezetes leképezést.

2.1.12. Konstrukció.

(1) Tegyük fel, hogy H részcsoportja G-nek és A pedig G-modulus. Legyen ϕ a $H \hookrightarrow G$ beágyazás és f pedig az id_A leképezés. Ezek a leképezések triviálisan kompatibilisek és az előző állítás segítségével kapott
$$Res : H^n(G, A) \to H^n(H, A)$$
homomorfizmust ($n \geq 0$) megszorítási leképezésnek nevezzük. Könnyen látszik, hogy az $a : G^n \to A$ kociklus képe ennél a leképezésnél a $a|_{H^n}$ megszorított leképezés lesz.

(2) Legyen most H normális részcsoportja G-nek. Ha A egy G-modulus, akkor A^H G/H-modulus lesz a $(gH)(a) = g(a)$ hatással. Válasszuk ϕ-nek a $G \to G/H$ projekciót és f-nek az $A^H \to A$ beágyazást. Triviális, hogy ezek kompatibilisek. Az ezek által indukált
$$Inf : H^n(G/H, A^H) \to H^n(G, A)$$
homomorfizmust ($n \geq 0$) inflációs leképezésnek nevezzük. Az $a : (G/H)^n \to A^H$ kociklus képe a $g_1, \ldots, g_n$ elemeken az $a_{g_1H,\ldots,g_nH}$ értéket veszi fel.

(3) Legyen továbbra is H normálosztó G-ben és A egy G-modulus. Ha rögzítünk egy $g \in G$ elemet, akkor az ezzel az elemmel való konjugálás ($h \mapsto g^{-1}hg$) indukál egy $H \to H$ automorfizmust, válasszuk ezt ϕ-nek. Definíció szerint a g-vel való hatás A-n nem más, mint egy $A \to A$ automorfizmus, legyen ez az f. A ϕ és f leképezések kompatibilisek, az így kapott
$$g_* : H^n(H, A) \to H^n(H, A)$$
homomorfizmust ($n \geq 0$) a g elemmel való konjugálásnak nevezzük. Ha $a \in H^n(H, A)$, akkor könnyen kiszámolható, hogy $g_*(a)_{h_1,\ldots,h_n} = g(a_{g^{-1}h_1g,\ldots,g^{-1}h_ng})$ lesz a konjugált kociklus, így ellenőrizhető, hogy 1_* az identitás lesz és $(gh)_* = g_*h_*$, azaz G hatását kaptuk $H^n(H, A)$-n. Belátható, hogy a H-beli elemek triviálisan hatnak $H^n(H, A)$-n, így értelmezhető a G/H csoport hatása is rajta. Ezt a hatást nevezzük konjugált hatásnak.

Létezik még egy negyedik nevezetes leképezés is, azonban ennek a definiálása eltér az előzőektől.

2.1.13. Konstrukció. Legyen H véges indexű részcsoportja G-nek és A egy G-modulus. A H bal oldali mellékosztályaiból válasszunk egy teljes reprezentáns-rendszert, legyenek ezek $t_1, \dots, t_m$. Ha $\psi : \mathbb{Z}G \to A$ egy H-homomorfizmus, akkor definiálható a következő leképezés

$$\begin{aligned} \psi_H^G : \mathbb{Z}G &\to A \\ x &\mapsto \sum_{j=1}^{m} t_j \psi(t_j^{-1} x), \end{aligned}$$

ami független a t_i-k választásától, továbbá G-homomorfizmus lesz. Az így kapott

$$\begin{aligned} M_H^G(A) = Hom_H(\mathbb{Z}G, A) &\to Hom_G(\mathbb{Z}G, A) \cong A \\ \psi &\mapsto \psi_H^G \end{aligned}$$

leképezés a G hatásával is kommutál, így a Schapiro-lemma segítségével kapjuk a

$$Cor : H^n(H, A) \to H^n(G, A)$$

($n \geq 0$) komegszorítási leképezést. Ez is felírható explicite a kociklusok szintjén.

A következő állítások szükségesek lesznek a reziduum leképezés megkonstruálásához (lásd 3.4. rész), de önmagukban is érdekesek.

2.1.14. Állítás. *Legyen H normális részcsoport G-ben és tegyük fel, hogy*

$$0 \to A \to B \to C \to 0$$

G-modulusok rövid egzakt sorozata. Ekkor a következő hosszú egzakt sorozat

$$\cdots \to H^n(H, A) \to H^n(H, B) \to H^n(H, C) \to H^{n+1}(H, A) \to \dots$$

G/H-modulusok egzakt sorozata lesz, ahol a kohomológia-csoportokat a G/H konjugált hatásával látjuk el.

Bizonyítás. [**7**] Lemma 3.3.13 □

2.1.15. Állítás. *Legyen G csoport és H normális részcsoportja G-nek, A egy G-modulus. Ekkor minden $n > 0$-ra $H^n(H, M^G(A)) = 0$.*

Bizonyítás. [**7**] Lemma 3.3.15 □

2.1.16. Állítás. *Tegyük fel, hogy H normális részcsoportja G-nek és legyen A egy G-modulus. Ekkor létezik egy olyan*

$$\tau : H^1(H, A)^{G/H} \to H^2(G/H, A^H)$$

természetes leképezés úgy, hogy a következő sorozat egzakt lesz

$$\begin{aligned} 0 \to H^1(G/H, A^H) \xrightarrow{Inf} H^1(G, A) \xrightarrow{Res} H^1(H, A)^{G/H} \xrightarrow{\tau} \\ \xrightarrow{\tau} H^2(G/H, A^H) \xrightarrow{Inf} H^2(G, A) \end{aligned}$$

A τ leképezést transzgressziós leképezésnek nevezzük.

Bizonyítás. [**7**] Proposition 3.3.14 □

2.1.17. ÁLLÍTÁS. *Tegyük fel, hogy H normális részcsoportja G-nek és legyen A egy G-modulus. Ha $n > 1$ és minden $1 \leq j \leq n-1$-re $H^j(H, A)$ triviális, akkor létezik*

$$\tau_n : H^n(H, A)^{G/H} \to H^{n+1}(G/H, A^H)$$

természetes leképezés úgy, hogy a következő sorozat egzakt lesz

$$0 \to H^n(G/H, A^H) \xrightarrow{Inf} H^n(G, A) \xrightarrow{Res} H^n(H, A)^{G/H} \xrightarrow{\tau_n}$$

$$\xrightarrow{\tau_n} H^{n+1}(G/H, A^H) \xrightarrow{Inf} H^{n+1}(G, A)$$

BIZONYÍTÁS. [**7**] Proposition 3.3.17 □

A csoportok kohomológiájának lezárásaként ejtünk néhány szót az ún. cup-szorzatról (vagy csészeszorzatról). A fogalmat kociklusok szintjén tárgyaljuk csak (követve a [**11**] 1.4. részét), azonban van másfajta definiálásra is lehetőség (lásd [**7**]. 3.4. rész).

Legyen G csoport. Ha A és B két G-modulus, akkor az $A \otimes_{\mathbb{Z}} B$ tenzorszorzat is ellátható G-modulus struktúrával: $g(a \otimes b) = g(a) \otimes g(b)$.

2.1.18. ÁLLÍTÁS. *Ha $n, m \geq 1$ egészek és $a \in H^n(G, A)$, $b \in H^m(G, B)$ két kociklus, akkor a következő*

$$a \cup b : G^{n+m} \to A \otimes_{\mathbb{Z}} B$$
$$(g_1, \ldots, g_{n+m}) \mapsto a_{g_1,\ldots,g_n} \otimes (g_1 \ldots g_n)(b_{g_{n+1},\ldots,g_{n+m}})$$

leképezés $(n+m)$-kociklus lesz. Ennek a kociklusnak a kohomológia osztálya csak az a és b kociklusok kohomológia osztályától függ és így egy $\mathbb{Z}$-bilineáris

$$\cup : H^n(G, A) \times H^m(G, B) \to H^{n+m}(G, A \otimes_{\mathbb{Z}} B)$$

leképezést kapunk.

2.1.19. DEFINÍCIÓ. *Az előző állításban szereplő*

$$\cup : H^n(G, A) \times H^m(G, B) \to H^{n+m}(G, A \otimes_{\mathbb{Z}} B)$$

leképezést nevezzük cup-szorzásnak. Ha adott C G-modulus és

$$\psi : A \otimes_{\mathbb{Z}} B \to C$$

G-homomorfizmus, akkor a

$$H^n(G, A) \times H^m(G, B) \xrightarrow{\cup} H^{n+m}(G, A \otimes_{\mathbb{Z}} B) \xrightarrow{\psi_*} H^{n+m}(G, C)$$

kompozíciót (a ψ leképezésre nézre) relatív cup-szorzatnak nevezzük.

2. Provéges csoportok

A provéges csoportok és kohomológiájuk tárgyalása javarészt a [**7**] könyv 4. fejezetének első három részén alapul.

2.2.1. DEFINÍCIÓ. *Azt mondjuk, hogy $(G_\alpha, \phi_{\alpha\beta})$ csoportok inverz rendszere, ha teljesíti a következőket:*

(1) *adott $(P, \leq)$ részbenrendezett halmaz úgy, hogy minden $\alpha, \beta \in P$-re létezik olyan $\gamma \in P$, hogy $\alpha \leq \gamma$ és $\beta \leq \gamma$;*
(2) *minden $\alpha \in P$-re adott G_α csoport*

(3) *minden* $\alpha \leq \beta$ *elempárra* $\phi_{\alpha\beta} : G_\beta \to G_\alpha$ *homomorfizmus úgy, hogy ha* $\alpha \leq \beta \leq \gamma$, *akkor* $\phi_{\alpha\gamma} = \phi_{\alpha\beta}\phi_{\beta\gamma}$ *ill.* $\phi_{\alpha\alpha} = id_{G_\alpha}$.

2.2.2. Definíció. *Legyen* $(G_\alpha, \phi_{\alpha\beta})$ *csoportok inverz rendszere. Azt mondjuk, hogy* G *az inverz rendszer inverz limesze, ha* G *a* $\prod_\alpha G_\alpha$ *csoport azon* (g_α) *elemeiből áll, melyekre* $\phi_{\alpha\beta}(g_\beta) = g_\alpha$. *Az inverz limeszt* $\varprojlim G_\alpha$*-val jelöljük.*

2.2.3. Megjegyzés.

(1) Inverz rendszereket tetszőleges kategóriában lehet definiálni. Tetszőleges kategóriában inverz rendszer inverz limeszét univerzális objektumként lehet definiálni (de nem feltétlenül létezik).
(2) Az inverz limesz konstrukciójából látszik, hogy minden $\alpha \in P$-re létezik kanonikus leképezés $\varprojlim G_\alpha$-ból G_α-ba, ez nem más, mint az α-dik koordinátára vetítés. Ennek a leképezésnek a magját U_α-val jelöljük.

2.2.4. Definíció. *Azt mondjuk, hogy* G *provéges csoport, ha véges csoportok inverz limesze. Ha* p *prímszám, akkor pro-*p*-csoporton* p*-csoportok inverz limeszét értjük.*

2.2.5. Megjegyzés. Ha a véges csoportokat ellátjuk a diszkrét topológiával, akkor minden provéges csoporton indukálódik topológia. Belátható, hogy ez a topológia teljesen összefüggéstelen kompakt Hausdorff-topológia lesz. Sőt, a topologikus csoportok között a provéges csoportok pont az előző tulajdonságú topologikus csoportok lesznek.

2.2.6. Példa.

(1) Minden G véges csoport provéges csoport: tetszőleges P indexhalmazt választva minden $\alpha \in P$-re legyen $G_\alpha = G$ és a homomorfizmusokat válassszuk a G identitásának.
(2) Ha G csoport, akkor elkészíthetjük a G provéges lezártját. Legyen P a G véges indexű normálosztóinak a halmaza és a részben rendezés legyen a következő: ha N_α, N_β két normálosztó, akkor $N_\alpha \leq N_\beta$, ha $N_\beta \subseteq N_\alpha$. Ha $N_\alpha \leq N_\beta$, akkor létezik a $\phi_{\alpha\beta} : G/N_\beta \to G/N_\alpha$ leképezés. Könnyen ellenőrizhető, hogy ez valóban inverz rendszer lesz és ennek a rendszernek az inverz limeszét nevezzük a G provéges lezártjának. Jelölése: $\widehat{G}$. Fontos példa az, ha G-nek a $(\mathbb{Z}, +)$ csoportot választjuk.
(3) Nézzük továbbra is $(\mathbb{Z}, +)$-t, de most csak a p-hatvány indexű részcsoportokat vegyük be az inverz rendszerbe. Ennek a rendszernek az inverz limeszeként kapott csoportot $\mathbb{Z}_p$-vel jelöljük és belátható, hogy izomorf lesz a p-adikus egészek additív csoportjával.
(4) Legyen G provéges csoport és p prímszám. Azt mondjuk, hogy az S pro-p-csoport a G pro-p-Sylow-részcsoportja, ha S indexe a G minden véges faktorában relatív prím p-hez. Belátható, hogy adott p-re mindig létezik pro-p-Sylow-részcsoport és a pro-p-Sylow-részcsoportok konjugáltak G-ben.

Újabb példa előtt szükségünk lesz néhány testelméleti fogalomra.

2.2.7. DEFINÍCIÓ. *Legyen $K|k$ testbővítés és jelöljük $Aut(K|k)$-val a K azon automorfizmusainak a csoportját, melyek fixen hagyják a k minden elemét. Azt mondjuk, hogy a $K|k$ bővítés Galois-bővítés, ha $K|k$ algebrai bővítés és minden $x \in K \backslash k$ elemhez van olyan $g \in Aut(K|k)$ automorfizmus, hogy $g(x) \neq x$ (azaz $K^{Aut(K|k)} = k$). Ha $K|k$ Galois-bővítés, akkor $Aut(K|k)$ helyett $Gal(K|k)$-t írunk, ezt nevezzük a bővítés Galois-csoportjának.*

Belátható, hogy $K|k$ algebrai bővítés akkor és csak akkor Galois-bővítés, ha szeparábilis és normális, vagyis véges bővítésekre az előző definíció a klasszikus definícióval ekvivalens.

2.2.8. PÉLDA. Az egyik legfontosabb példa végtelen Galois-bővítésre a k test k_s szeparábilis lezártja, azaz k egy fix algebrai lezártjában lévő szeparábilis elemek részteste. A $Gal(k_s|k)$ csoportot a k abszolút Galois-csoportjának nevezzük. A $Gal(k_s|k)$ csoportot néha Γ_k-val fogjuk jelölni.

2.2.9. ÁLLÍTÁS. *Legyen $K|k$ Galois-bővítés. Ekkor az $L|k$ véges Galois-részbővítések $Gal(L|k)$ Galois-csoportjai a $\phi_{ML} : Gal(M|k) \to Gal(L|k)$ szürjekciókkal inverz rendszert alkotnak és ennek a rendszernek az inverz limesze izomorf lesz $Gal(K|k)$-val, speciálisan $Gal(K|k)$ provéges csoport lesz.*

Vizsgáljuk most azt a kérdést, hogy tetszőleges testbővítés esetén van-e leképezés a testek abszolút Galos-csoportjai között.

2.2.10. ÁLLÍTÁS. *Legyen k és k' két test és tegyük fel, hogy $K|k$ és $K'|k'$ két (nem feltétlenül véges) Galois-bővítés. Legyen $\iota : k \to k'$ homomorfizmus.*

(1) *Ha $\phi_1, \phi_2 : K \to K'$ olyan homomorfizmusok, hogy $\phi_i|_k = \iota$ (azt mondjuk, hogy a ϕ_i kiterjeszti ι-t), akkor minden $g' \in Gal(K'|k')$-re egyértelműen létezik olyan $g \in Gal(K|k)$, hogy a következő diagram kommutatív*
$$\begin{array}{ccc} K & \xrightarrow{g} & K \\ {\scriptstyle\phi_1}\downarrow & & {\scriptstyle\phi_2}\downarrow \\ K' & \xrightarrow{g'} & K' \end{array}$$
Speciálisan, létezik olyan $g \in Gal(K|k)$, hogy $\phi_1 = \phi_2 \circ g$.

(2) *Az előző pontban legyen $\phi_1 = \phi_2 = \phi$. Az előző pont miatt tudjuk, hogy minden $g' \in Gal(K'|k')$-re egyértelműen létezik $\overline{\phi}(g') \in Gal(K|k)$ úgy, hogy $g' \circ \phi = \phi \circ \overline{\phi}(g')$. Ekkor a következő*
$$\overline{\phi} : Gal(K'|k') \to Gal(K|k)$$
$$g' \mapsto \overline{\phi}(g')$$
leképezés folytonos csoport-homomorfizmus lesz.

(3) *Ha ϕ' egy másik kiterjesztése ι-nak, akkor létezik $g \in Gal(K|k)$ úgy, hogy $\phi = \phi' \circ g$. Ekkor $\overline{\phi'} = g \circ \overline{\phi} \circ g^{-1}$, azaz tetszőleges kiterjesztésre a Galois-csoportok közötti leképezés konjugálás erejéig egyértelmű.*

BIZONYÍTÁS. [**2**] Proposition I.2.9. és Corollary I.2.10. □

2.2.11. KÖVETKEZMÉNY. *Tegyük fel, hogy k és k' két test és adott $\iota : k \to k'$ homomorfizmus. Legyen k_s ill. k'_s a k ill. k' egy-egy rögzített szeparábilis lezártja. Ekkor létezik olyan $\phi : k_s \to k'_s$ homomorfizmus ami kiterjeszti ι-t.*

2.2.12. Következmény. *Legyen $K|k$ tetszőleges testbővítés. Ekkor konjugálás erejéig egyértelműen létezik $\Gamma_K \to \Gamma_k$ folytonos csoporthomomorfizmus.*

3. Provéges csoportok kohomológiája és Galois-kohomológia

Provéges csoportok esetén érdemes módosítani a kohomológia-csoportok definícióját. Az elmélet felépítésére kétféle, ekvivalens lehetőség van. Az egyik lehetőség az, hogy a provéges csoport feletti folytonos modulusok kategóriájában építjük fel a kohomológia-elméletünket. A másik mód alapgondolata az, hogy a provéges csoportok kohomológiáját meghatározza a véges faktorok kohomológiája. Mi az utóbbi felépítést fogjuk követni.

Legyen $G = \varprojlim G_\alpha$ provéges csoport. Azt mondjuk, hogy A diszkrét folytonos G-modulus, ha G folytonosan hat rajta, vagyis a $G \times A \to A$ hatás folytonos leképezés. Ez ekvivalens azzal, hogy minden $a \in A$-ra az a elem stabilizátora nyílt G-ben. Legyen $G_\alpha = G/U_\alpha$ (ez véges csoport!) és nézzük az A^{U_α} modulust, erre G_α-modulusként is tekinthetünk. Ha $\alpha \leq \beta$, akkor létezik $\phi_{\alpha\beta} : G_\beta \to G_\alpha$ leképezés és ez indukálja következő inflációs leképezést az n-dik kohomológiák között minden $n \geq 0$-ra

$$Inf_\alpha^\beta : H^n(G_\alpha, A^{U_\alpha}) \to H^n(G_\beta, A^{U_\beta})$$

Mivel $\phi_{\alpha\gamma} = \phi_{\alpha\beta}\phi_{\beta\gamma}$ teljesül, ha $\alpha \leq \beta \leq \gamma$, ezért az indukált inflációs leképezések is teljesíteni fognak egy azonosságot

$$Inf_\alpha^\gamma = Inf_\beta^\gamma Inf_\alpha^\beta$$

Mielőtt folytatnánk, szükségünk lesz a következő fogalomra.

2.3.1. Definíció. *Azt mondjuk, hogy $(A_\alpha, \psi_{\alpha\beta})$ Abel-csoportok direkt rendszere, ha teljesíti a következőket:*

(1) *adott $(P, \leq)$ részbenrendezett halmaz úgy, hogy minden $\alpha, \beta \in P$-re létezik olyan $\gamma \in P$, hogy $\alpha \leq \gamma$ és $\beta \leq \gamma$;*
(2) *minden $\alpha \in P$-re adott A_α Abel-csoport*
(3) *minden $\alpha \leq \beta$ elempárra $\psi_{\alpha\beta} : A_\alpha \to A_\beta$ homomorfizmus úgy, hogy ha $\alpha \leq \beta \leq \gamma$, akkor $\psi_{\alpha\gamma} = \psi_{\beta\gamma}\psi_{\alpha\beta}$ ill. $\psi_{\alpha\alpha} = id_{G_\alpha}$.*

Könnyen látható, hogy az $(H^i(G_\alpha, A^{U_\alpha}), Inf_\alpha^\beta)$ rendszer minden $i \geq 0$-ra direkt rendszer lesz az előző definíció értelmében.

2.3.2. Definíció. *Legyen $(A_\alpha, \psi_{\alpha\beta})$ Abel-csoportok direkt rendszere. Azt mondjuk, hogy A a direkt rendszer direkt limesze, ha A a $\oplus_\alpha A_\alpha$ Abel-csoport azon részcsoportja szerint vett faktora, mely részcsoportot az $a_\beta - \psi_{\alpha\beta}(a_\alpha)$ alakú elemek generálnak. Az A direkt limeszt $\varinjlim A_\alpha$-val is jelölhetjük.*

Ezen fogalmak segítségével már definiálhatjuk provéges csoportok (folytonos) kohomológia-csoportjait.

2.3.3. Definíció. *Legyen $G = \varprojlim G_\alpha$ provéges csoport és A diszkrét folytonos G-modulus. Adott $n \geq 0$-ra definiáljuk az n-dik A együtthatós $H^n(G, A)$ (folytonos) kohomológia-csoportot úgy, mint a $(H^n(G_\alpha, A^{U_\alpha}), Inf_\alpha^\beta)$ direkt rendszer direkt limeszét.*

2.3.4. MEGJEGYZÉS. Hasonlóan a véges csoportok esetéhez, a provéges csoportok kohomológiáját is lehet definiálni n-kociklusok segítségével. Legyen G provéges csoport, A diszkrét folytonos G-modulus és jelöljük $C^n(G,A)$-val a *folytonos* $G^n \to A$ leképezések halmazát. A véges esethez hasonlóan definiálható a $\delta^n : C^n(G,A) \to C^{n+1}(G,A)$ leképezés, a $Z^n(G,A) = ker(\delta^n)$ n-kociklusok csoportja és a $B^n(G,A) = im(\delta^{n-1})$ n-kohatárok csoportja. Ekkor belátható, hogy a $Z^n(G,A)/B^n(G,A)$ faktorcsoport izomorf lesz a $H^n(G,A)$ kohomológia-csoporttal.

Különösen fontos lesz az alábbi speciális eset.

2.3.5. DEFINÍCIÓ. *Legyen k test. Láttuk, hogy $\Gamma_k = Gal(k_s|k)$ provéges csoport. Ha A folytonos Γ_k-modulus, akkor a $H^n(\Gamma_k, A)$ (folytonos) kohomológia-csoportot a k test n-edik Galois kohomológia-csoportjának nevezzük és $H^n(k,A)$-val jelöljük.*

Mivel a provéges csoportok (folytonos) kohomológiája szorosan kapcsolódik a véges csoportokéhoz, ezért nem meglepő, hogy a véges esetben megismert fogalmaknak és állításoknak van párjuk a folytonos kohomológiában, most ezeket fogjuk áttekinteni.

2.3.6. ÁLLÍTÁS. *Legyen G provéges csoport és tegyük fel, hogy*

$$0 \to A \to B \to C \to 0$$

folytonos G-modulusok rövid egzakt sorozata. Ekkor a létezik a következő hosszú egzakt sorozat

$$\cdots \to H^n(H,A) \to H^n(H,B) \to H^n(H,C) \to H^{n+1}(H,A) \to \dots$$

2.3.7. KONSTRUKCIÓ.

(1) Legyen G provéges csoport,A folytonos G-modulus és tegyük fel, hogy H zárt részcsoportja G-nek. Ekkor létezik a következő

$$Res : H^n(G,A) \to H^n(H,A)$$

ún. folytonos megszorítási leképezés, amit a véges esetben már megismert

$$H^n(G/U_\alpha, A^{U_\alpha}) \xrightarrow{Res_\alpha} H^n(H/(H \cap U_\alpha), A^{U_\alpha})$$

megszorítási leképezések direkt limeszeként definiálunk.

(2) Legyen G proveges csoport,A folytonos G-modulus és tegyük fel, hogy H nyílt részcsoportja G-nek. Ekkor létezik a következő

$$Cor : H^n(H,A) \to H^n(G,A)$$

ún. folytonos komegszorítási leképezés, amit a véges esetben már megismert

$$H^n(H/(H \cap U_\alpha), A^{U_\alpha}) \xrightarrow{Cor_\alpha} H^n(G/U_\alpha, A^{U_\alpha})$$

komegszorítási leképezések direkt limeszeként definiálunk.

(3) Legyen G proveges csoport, A folytonos G-modulus és tegyük fel, hogy H zárt, normális részcsoportja G-nek. Ekkor létezik a következő

$$Inf : H^n(G/H, A^H) \to H^n(G,A)$$

ún. folytonos inflációs leképezés, amit a véges esetben már megismert

$$H^n(G/HU_\alpha, A^{HU_\alpha}) \xrightarrow{Inf_\alpha} H^n(G/U_\alpha, A^{U_\alpha})$$

inflációs leképezések direkt limeszeként definiálunk.

2.3.8. Megjegyzés. Az előző konstrukciókat mind megkaphattuk volna a véges esethez hasonlóan a 2.1.11. Állítás folytonos változatának felhasználásával.

A következő három állítás a 2.1.15, 2.1.16. és 2.1.17. Állítások folytonos változatai (lásd [**7**] Proposition 4.3.5)

2.3.9. Állítás. *Legyen G csoport és H zárt, normális részcsoportja G-nek, A folytonos G-modulus. Ekkor minden $n > 0$-ra $H^n(H, M^G(A)) = 0$.*

2.3.10. Állítás. *Tegyük fel, hogy H zárt, normális részcsoportja G-nek és legyen A folytonos G-modulus. Ekkor létezik olyan*

$$\tau : H^1(H, A)^{G/H} \to H^2(G/H, A^H)$$

természetes leképezés úgy, hogy a következő sorozat egzakt lesz

$$0 \to H^1(G/H, A^H) \xrightarrow{Inf} H^1(G, A) \xrightarrow{Res} H^1(H, A)^{G/H} \xrightarrow{\tau}$$
$$\xrightarrow{\tau} H^2(G/H, A^H) \xrightarrow{Inf} H^2(G, A).$$

A τ leképezést (folytonos) transzgressziós leképezésnek nevezzük.

2.3.11. Állítás. *Tegyük fel, hogy H zárt, normális részcsoportja G-nek és legyen A folytonos G-modulus. Ha $n > 1$ és minden $1 \leq j \leq n-1$-re $H^j(H, A)$ triviális, akkor létezik*

$$\tau_n : H^n(H, A)^{G/H} \to H^{n+1}(G/H, A^H)$$

természetes leképezés úgy, hogy a következő sorozat egzakt lesz

$$0 \to H^n(G/H, A^H) \xrightarrow{Inf} H^n(G, A) \xrightarrow{Res} H^n(H, A)^{G/H} \xrightarrow{\tau_n}$$
$$\xrightarrow{\tau_n} H^{n+1}(G/H, A^H) \xrightarrow{Inf} H^{n+1}(G, A).$$

A következőkben egy fontos, a provéges csoportok kohomológiájához kapcsolódó fogalmat vizsgálunk (lásd [**7**] 6.1). Ha A Abel-csoport, akkor jelöljük $A\{p\}$-vel az A p-hatvány rendű elemeinek részcsoportját.

2.3.12. Definíció. *Legyen G provéges csoport és p prímszám. Azt mondjuk, hogy a G p-kohomologikus dimenziója $\leq n$, ha $H^i(G, A)\{p\} = 0$ minden $i > n$-re és minden A folytonos torzió G-modulusra. A G csoport $cd_p(G)$ p-kohomologikus dimenzióján azt a legkisebb n pozitív egész számot értjük, amelyre G p-kohomologikus dimenziója $\leq n$. Ha nem létezik ilyen n, akkor azt mondjuk, hogy a p-kohomologikus dimenzió végtelen ($cd_p(G) = \infty$). A G csoport $cd(G)$ kohomologikus dimenzióján a $cd_p(G)$ számok szuprémumát értjük, ahol p befutja az összes prímszámot.*

2.3.13. Példa. Legyen $\widehat{\mathbb{Z}}$ a $\mathbb{Z}$ provéges lezártja. Ekkor megmutatható, hogy $cd_p(\widehat{\mathbb{Z}}) = 1$ minden p prímre.

2.3.14. ÁLLÍTÁS. *Legyen G provéges csoport és tegyük fel, hogy H zárt részcsoportja G-nek. Ekkor minden p prímszámra $cd_p(H) \leq cd_p(G)$. Ha H képének indexe a G minden véges faktorában relatív prím p-hez, akkor $cd_p(H) = cd_p(G)$. Speciálisan, ha G_p a G pro-p-Sylow-részcsoportja, akkor $cd_p(G) = cd_p(G_p)$.*

BIZONYÍTÁS. [**7**] Lemma 6.1.4 □

4. Reziduum leképezés konstrukciója általánosan

Legyen G provéges csoport és $H \leq G$ olyan zárt normális részcsoportja, amire $cd(H) \leq 1$. Minden A torzió G-modulusra és minden $n \geq 1$-re konstruálunk

$$H^n(G,A) \xrightarrow{r} H^{n-1}(G/H, H^1(H,A))$$

leképezést, melynek később egy speciális esetben fontos szerepe lesz.

Ágyazzuk be az A modulust az $M^G(A)$ koindukált modulusba és nézzük a következő egzakt sorozatot

$$0 \to A \to M^G(A) \to C \to 0. \tag{4.1}$$

Természetesen ez az egzakt sorozat tekinthető H-modulusok egzakt sorozatának is, ezért létezik a következő hosszú egzakt sorozat

$$\cdots \to H^n(H,A) \to H^n(H, M^G(A)) \to H^n(H,C) \to H^{n+1}(H,A) \to \ldots \tag{4.2}$$

A 2.3.9. Állítás miatt $H^n(H, M^G(A)) = 0$ minden $n \geq 1$-re, ezért

$$H^n(H,C) \cong H^{n+1}(H,A)$$

minden $n \geq 1$-re, de $cd(H) \leq 1$, ezért az utóbbi 0 lesz, vagyis $H^n(H,C) = 0$, ha $n \geq 1$.

Mivel $H^n(H,C) = 0$, ha $n \geq 1$, ezért a 2.3.11. Állítás feltételei teljesülnek C-re, ezért vehetjük az állításból kapott egzakt sorozatot $n \geq 2$-re

$$0 \to H^n(G/H, C^H) \xrightarrow{Inf} H^n(G,C) \xrightarrow{Res} H^n(H,C)^{G/H} \xrightarrow{\tau_n}$$
$$\xrightarrow{\tau_n} H^{n+1}(G/H, C^H) \xrightarrow{Inf} H^{n+1}(G,C).$$

De $H^n(H,C) = 0$, ezért a

$$H^n(G/H, C^H) \xrightarrow{Inf} H^n(G,C)$$

leképezés izomorfizmus lesz $n \geq 2$-re. Célszerű itt eltolni az indexeket eggyel, ezért azt kapjuk, hogy

$$H^{n-1}(G/H, C^H) \xrightarrow{Inf} H^{n-1}(G,C)$$

izomorfizmus lesz, ha $n \geq 3$. A 2.3.10. Állítás miatt hasonló igaz $n = 2$-re is.
Most nézzük a (4.1) G-modulusok egzakt sorozatához tartozó hosszú egzakt sorozatot

$$\cdots \to H^n(G,A) \to H^n(G, M^G(A)) \to H^n(G,C) \to H^{n+1}(G,A) \to \ldots$$

A Shapiro-lemma miatt $H^n(G, M^G(A)) = 0$, ha $n \geq 1$, ezért

$$H^{n-1}(G, C) \cong H^n(G, A),$$

ha $n \geq 2$. Ezt és az előbbi izomorfizmust összevetve adódik a következő izomorfizmus $n \geq 2$-re

$$H^n(G, A) \cong H^{n-1}(G/H, C^H) \tag{4.3}$$

A (4.2) hosszú egzakt sorozatból kapunk $C^H = H^0(H, C) \to H^1(H, A)$ leképezést és a 2.1.14. Állítás miatt ez G/H-morfizmus lesz. Ezért ez minden $n \geq 1$-re indukál leképezést

$$H^{n-1}(G/H, C^H) \to H^{n-1}(G/H, H^1(H, A)) \tag{4.4}$$

2.4.1. Definíció. *A (4.3) izomorfizmus és a (4.4) leképezés kompozíciójaként kapott*

$$r_n : H^n(G, A) \to H^{n-1}(G/H, H^1(H, A))$$

leképezést, ahol $n \geq 2$, reziduum leképezésnek nevezzük. Az $n = 1$ esetben a 2.3.10. Állításbeli megszorítási leképezés lesz az r_1 reziduum leképezés.

2.4.2. Megjegyzés. Rögzítsük a p prímszámot és tegyük fel, hogy $cd_l(H) \leq 1$ minden $l \neq p$ prímre. Ha A olyan torzió G-modulus, melynek nincsen nemtriviális p-hatvány rendű eleme, akkor a reziduum leképezések definiálhatóak az előzőhöz hasonlóan.

2.4.3. Állítás. *Ha G provéges csoport, H zárt, normális részcsoportja, melyre $cd(H) \leq 1$ és A folytonos torzió G-modulus, akkor létezik a következő, $H^1(G, A)$-tól kezdődő hosszú egzakt sorozat*

$$\ldots \to H^n(G/H, A^H) \xrightarrow{Inf} H^n(G, A) \xrightarrow{r_n} H^{n-1}(G/H, H^1(H, A)) \to$$
$$\to H^{n+1}(G/H, A^H) \to \ldots$$

Bizonyítás. [**7**] Proposition 6.8.2. □

5. Lokális testekről

Ebben a részben összefoglaljuk azokat az eredményeket, amiket a következő részben, a reziduum leképezés konstrukciójához fel fogunk használni. A most következő állítások, tételek bizonyítása (és még sokkal több) megtalálható a [**16**] könyvben, a kíváncsi olvasó minden részletet megtalálhat ott.

2.5.1. Definíció. *Legyen K test. Azt mondjuk, hogy a $v : K \to \mathbb{Z} \cup \{\infty\}$ leképezés diszkrét értékelés, ha*

(1) *$v : K^\times \to \mathbb{Z}$ szürjektív homomorfizmus*
(2) *$v(0) = \infty$*
(3) *$v(x + y) \geq min(v(x), v(y))$*

2.5.2. Állítás. *Legyen K test és v diszkrét értékelés K-n.*

(1) *$R_v := \{x \in K : v(x) \geq 0\}$ integritási tartomány lesz K-ben és a hányadosgyűrűje K-val egyenlő.*
(2) *$\mathfrak{p}_v := \{x \in K : v(x) > 0\}$ maximális ideál lesz R_v-ben, sőt ez lesz az egyetlen maximális ideál, azaz R_v lokális gyűrű.*
(3) *R_v főideálgyűrű*

2.5.3. DEFINÍCIÓ. *Az előbbi állításbeli R_v-t a v diszkrét értékelés értékelésgyűrűjének nevezzük, $\mathfrak{p}_v$-t pedig az értékelésideálnak. Az $R_v/\mathfrak{p}_v$ hányadost pedig az értékelés maradéktestének nevezzük (ez tényleg test, mivel $\mathfrak{p}_v$ maximális ideál).*

2.5.4. ÁLLÍTÁS. *Az R integritási tartományra a következő tulajdonságok ekvivalensek:*

(1) *Egyértelműen létezik $K = Frac(R)$-n olyan v diszkrét értékelés, hogy $R = R_v$*
(2) *R lokális főideálgyűrű, de nem test*
(3) *R Noether-gyűrű, integrálisan zárt és egyetlenegy nem-0 prímideálja van*

Legyen K test, v diszkrét értékelés K-n és $0 < c < 1$ valós szám. Ekkor definiálható a következő, ún. indukált értékelés:

$$|x|_v := c^{v(x)}$$

Belátható, hogy az indukált értékelés ekvivalencia erejéig független a c választásától, ahol $|\ |_1$ és $|\ |_2$ ekvivalensek, ha létezik olyan $d > 0$ valós szám, hogy $|\ |_2 = |\ |_1^d$. A következő állítás foglalja össze a $|\ |_v$ értékelés (könnyen bizonyítható) tulajdonságait.

2.5.5. ÁLLÍTÁS. *Legyen K test, v diszkrét értékelés K-n és legyen $|\ | = |\ |_v$ az indukált értékelés. Ekkor igazak a következők:*

(1) $|0| = 0$ *és* $|x| = 0$ *akkor és csak akkor, ha* $x = 0$
(2) $|xy| = |x||y|$ *minden* $x, y \in K$*-ra*
(3) $|x + y| \leq |x| + |y|$

A $|\ |_v$ értékelés toplógiát indukál K-n, sőt metrika is definiálható a szokásos módon: minden $x, y \in K$-ra legyen $d(x, y) = |x - y|$.

2.5.6. DEFINÍCIÓ. *Legyen K test, v diszkrét értékelés K-n és legyen $|\ | = |\ |_v$ az indukált értékelés. Azt mondjuk, hogy K teljes (v-re nézve), ha K teljes metrikus tér a fent definiált metrikával.*

2.5.7. DEFINÍCIÓ. *Legyen K test és v diszkrét értékelés K-n. Jelöljük K_v-vel a K teljes burkát a v által indukált metrika szerint. Ekkor K_v test lesz, ami tartalmazza K-t és v kiterjed a K_v-re diszkrét értékeléssé.*

Tegyük fel, hogy adott a (K, v) test (véges vagy végtelen) Galois-bővítése. Természetes kérdés, hogy kiterjeszthető-e a v a nagyobb testre és ha igen, akkor hányféleképpen ill. milyen kapcsolat van a kiterjesztett értékelések között. Először a véges Galois-bővítések esetét nézzük meg.

2.5.8. ÁLLÍTÁS. *Legyen K test, v diszkrét értékelés K-n és $L|K$ véges Galois-bővítés.*

(1) *Ha adott v diszkrét értékelés K-n, akkor az kiterjeszthető L-re w diszkrét értékelésként.*
(2) *Csak véges sok w kiterjesztése van v-nek.*
(3) *Ha K teljes v-re nézve, akkor v egyértelműen terjeszthető ki L-re.*
(4) *A w kiterjesztéseken a $Gal(L|K)$ Galois-csoport tranzitívan hat a $g(w) = w \circ g$ hatással. Adott w kiterjesztésre jelöljük Dec_w-vel a w stabilizátorát a $Gal(L|K)$ hatására nézve.*

(5) *Minden w kiterjesztésre $L_w|K_v$ Galois-bővítés lesz és ennek a bővítésnek a Galois-csoportja izomorf lesz Dec_w-vel.*
(6) $\mathfrak{p}_w \cap K = \mathfrak{p}_v$
(7) *Létezik $k(w)|k(v)$ testbővítés és ez normális bővítés lesz.*
(8) *Ha $k(w)|k(v)$ szeparábilis, akkor $k(w)|k(v)$ Galois-bővítés lesz.*

A végtelen Galois-bővítések közül csak a K szeparábilis lezártjának esetére lesz szükségünk.

2.5.9. Állítás. *Legyen K test v diszkrét értékeléssel. Rögzítsük a K egy K_s szeparábilis lezártját.*
(1) *A v diszkrét értékelés kiterjeszthető K_s-re.*
(2) *A Γ_K abszolút Galois-csoport tranzitívan hat a v kiterjesztettjein. Ha w egy kiterjesztett, akkor jelöljük Dec_w-vel a w stabilizátorát a Γ_K hatására nézve.*
(3) *Legyen w egy kiterjesztése v-nek K_s-re és jelöljük $K_{s,w}$-vel a K_s teljes burkát w-re nézve. A $K_s \cdot K_v \subseteq K_{s,w}$ kompozítum lesz a K_v szeparábilis lezártja $K_{s,w}$-ben. A $\Gamma_{K_v} = Gal(K_s \cdot K_v|K_v)$ abszolút Galois-csoport izomorf lesz Dec_w-vel.*
(4) *Ha K teljes v-re nézve, akkor v egyértelműen terjeszthető ki K_s-re v_s diszkrét értékeléssé. Ebben az esetben $k(v_s)$ a $k(v)$ algebrai lezártja lesz.*

A továbbiakban feltesszük, hogy a $k(v_s)|k(v)$ bővítés szeparábilis (vagyis $k(v_s)$ a $k(v)$ szeparábilis lezártja). Ha $g \in Gal(K_s|K) = \Gamma_K$, akkor $v_s \circ g$ is egy v-t kiterjesztő diszkrét értékelése lesz K_s-nek. Mivel v_s egyértelmű, ezért $v_s \circ g = v_s$ minden $g \in \Gamma_K$-ra. Speciálisan, minden $g \in \Gamma_K$ az R_{v_s} értékelésgyűrűt és a $\mathfrak{p}_{v_s}$ ideált is önmagába képezi, sőt $\mathfrak{p}_{v_s} \cap R_v = \mathfrak{p}_v$, ezért létezik a következő leképezés

$$Gal(K_s|K) \to Gal(k(v_s)|k(v))$$

az abszolút Galois-csoportok között. Ennek a leképezésnek a magját inercia csoportnak nevezzük és I-vel jelöljük. A következő állításban összefoglaljuk a számunkra fontos tulajdonságait.

2.5.10. Állítás. *Az előző jelöléseket jelöléseket megtartva igazak a következők:*
(1) *Létezik $1 \to I_w \to I \to I_t \to 1$ egzakt sorozat.*
(2) *Az I_w részcsoport triviális, ha $char(k(v)) = 0$ vagy egyenlő az I egyetlen pro-p-Sylow-részcsoportjával, ha $char(k(v)) = p$.*
(3) *Legyen μ_l a $k(v_s)$-beli l-edik egységgyökök csoportja. Ekkor $I_t \cong \varprojlim \mu_l$, ahol $char(k(v)) \nmid l$.*
(4) *$cd_l(I) = 1$, ahol $l \neq char(k(v))$ prím.*
(5) *Az $1 \to I \to \Gamma_K \to \Gamma_k(v) \to 1$ rövid egzakt sorozat felhasad.*

6. Reziduum leképezés lokális testekre

A 2.4. pontban megismert reziduum leképezést szeretnénk definiálni egy értékelt test Galois kohomológia-csoportjain. Látni fogjuk, hogy a konstrukció feltételei teljesülnek, sőt ebben a speciális esetben a 2.4.3. Állításbeli hosszú egzakt sorozat is felhasad rövid egzakt sorozatokra.

Legyen K test, amin adott v diszkrét értékelés. Jelöljük $k(v)$-vel a maradéktestet, Γ_K-val illetve $\Gamma_{k(v)}$-vel az abszolút Galois-csoportokat.

Tegyük fel, hogy K *teljes* v-re nézve. Legyen C olyan véges $\Gamma_{k(v)}$-modulus, melynek rendje relatív prím $char(k(v))$-hez. A már ismert $\Gamma_K \to \Gamma_{k(v)}$ leképezésen keresztül C egy Γ_K-modulus lesz, amin az I inercia-csoport triviálisan hat. A 2.4.2. Megjegyzés feltételei teljesülnek, ezért minden $n \geq 1$-re létezik

$$r_n : H^n(K, C) \to H^{n-1}(k(v), H^1(I, C))$$

reziduum leképezés. Mivel I triviálisan hat C-n, ezért $H^n(I, C) = Hom_{cont}(I, C)$. Mivel C rendje relatív prím $char(k(v))$-hez, ezért $Hom_{cont}(I, C) = Hom_{cont}(I_t, C)$. Legyen l olyan pozitív egész, hogy $lC = 0$, ekkor $Hom_{cont}(I_t, C) = Hom(\mu_l, C)$ (belátható, hogy ez független az l választásától). A $Hom(\mu_l, C)$ $\Gamma_{k(v)}$-modulust a továbbiakban $C(-1)$-gyel fogjuk jelölni (ha $\phi \in Hom(\mu_l, C)$, akkor $g \in \Gamma_{k(v)}$ elem $g(\phi)(\varepsilon) = g(\phi(g^{-1}(\varepsilon)))$ hatással hat ϕ-n).

2.6.1. Állítás. *Az előbbiekben tárgyalt esetben a 2.4.3. Állításbeli hosszú egzakt sorozat felhasad.*

Bizonyítás. Speciális esetben lásd [**7**] Corollary 6.8.8., az általános esetben pedig [**6**] II. 6. és 7. részét. □

Az alábbi következményben foglaljuk össze az eddigi eredményeket.

2.6.2. Következmény. *Legyen (K, v) teljes test, jelölje $k(v)$ a maradéktestet. Ha C olyan véges $\Gamma_{k(v)}$-modulus, mely rendje relatív prím $char(k(v))$-hez, akkor létezik a következő rövid egzakt sorozat*

$$0 \to H^n(k(v), C) \xrightarrow{Inf} H^n(K, C) \xrightarrow{r_n} H^{n-1}(k(v), C(-1)) \to 0.$$

Ha nem tesszük fel, hogy K teljes v-re nézve, akkor a következőt mondhatjuk. Legyen w a v egy kiterjesztése K_s-re és legyen Dec_w a a w stabilizátora. Láttuk, hogy Dec_w izomorf a K_v abszolút Galois-csoportjával. A C véges Γ_K-modulusról tegyük fel, hogy a rendjét nem osztja a $k(v)$ karakterisztikája és, hogy a Dec_w inercia csoportja triviálisan hat rajta. Ha adott $\alpha \in H^n(K, C)$ elem, akkor jelöljük a képét α_v-vel $H^n(K_v, C)$-ben (a kohomológiák közötti leképezést a $K \hookrightarrow K_v$ beágyazás indukálja). Mivel K_v teljes test, ezért az előző eset alkalmazható rá, így az alábbi diagramhoz jutottunk

$$\begin{array}{ccccccccc} & & & & H^n(K, C) & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & H^n(k(v), C) & \xrightarrow{Inf} & H^n(K_v, C) & \xrightarrow{r_n} & H^{n-1}(k(v), C(-1)) & \longrightarrow & 0 \end{array}$$

Összefoglalva a következőt kapjuk.

2.6.3. Következmény. *Legyen K test v diszkrét értékeléssel, jelölje $k(v)$ a maradéktestet. Ha C olyan véges $\Gamma_{k(v)}$-modulus, ami teljesíti az előző* *feltételeket, akkor léteznek a következő leképezések*

$$r_v : H^n(K,C) \to H^{n-1}(k(v), C(-1))$$
$$ker(r_v) \to H^n(k(v), C).$$

Egy $\alpha \in H^n(K,C)$ elem képét r_v-nél az α v-nél vett reziduumának nevezzük. Ha $r_v(\alpha) \neq 0$, akkor α-t elágazónak nevezzük v-nél, egyébként nemelágazónak. Ez utóbbi esetben α_v azonosítható a $H^n(k,C)$ egy elemével, ezt nevezzük az α v-nél vett értékének.
Láttuk, hogy ha K teljes test, akkor az első leképezés szürjektív és a második leképezés pedig izomorfizmus.

7. Fagyejev egzakt sorozata

Tekintsük a $\mathbf{P}^1$ projektív egyenest a k test felett, a függvényteste $K = k(x)$ lesz. Minden egyes zárt pontja meghatároz egy olyan diszkrét értékelést K-n, ami triviális lesz k-n. Legyen V az ilyen értékelések halmaza és $v \in V$ egy értékelés, ekkor K_v-vel fogjuk jelölni a K teljes burkát v-re nézve, $k(v)$ pedig a maradéktestét. Vegyük észre, hogy a $\mathbf{P}^1$ végtelen távoli pontja olyan diszkrét értékelést indukál, amihez tartozó maradéktest k lesz.

2.7.1. Tétel. *Legyen k test, $\mathbf{P}^1$ a k feletti projektív egyenes és legyen $K = k(x)$ a projektív egyenes függvényteste. Ha m invertálható k-ban és C olyan véges $Gal(k_s|k)$-modulus, melynek rendjét nem osztja a k karakterisztikája, akkor minden $n > 0$-ra létezik a következő egzakt sorozat:*

$$0 \to H^n(k,C) \to H^n(K,C) \xrightarrow{\oplus r_v} \bigoplus_{v\in V} H^{n-1}(k(v), C(-1)) \xrightarrow{c} H^{n-1}(k, C(-1)) \to 0,$$

ahol c a $Cor : H^{n-1}(k(v), C(-1)) \to H^{n-1}(k, C(-1))$ komegszorítási leképezések direkt összege.

Bizonyítás. Lásd [**6**] Theorem 9.2. vagy [**7**] Theorem 6.9.1. □

2.7.2. Következmény. *Az előző tétel jelöléseit megtartva létezik a következő rövid egzakt sorozat*

$$0 \to H^n(k,C) \to H^n(K,C) \to \bigoplus_{v\in V\setminus\{v_\infty\}} H^{n-1}(k(v), C(-1)) \to 0.$$

Bizonyítás. A végtelen távoli ponthoz tartozó komegszorítási leképezés $k(v_\infty) = k$ miatt az identitás lesz, így az utolsó két tagból elhagyható $H^{n-1}(k, C(-1))$. □

2.7.3. Tétel. *Legyen $n \geq 1$ és $K = k(x_1, \ldots, x_m)$, ahol x_i-k független határozatlanok. Ha C véges $Gal(k_s|k)$-modulus és a rendjét nem osztja a k test karakterisztikája, akkor a*

$$H^n(k,C) \xrightarrow{Inf} H^n(K,C)$$

leképezés injektív.
Továbbá, ha $\alpha \in H^n(K,C)$ olyan, hogy a reziduuma 0 a K minden olyan diszkrét értékelésénél, amely az $\mathbf{A}^m$ n dimenziós affin tér irreducibilis hiperfelületeiből származik, akkor α konstans, azaz $H^n(k,C)$-ből jön.

Bizonyítás. [**6**] Theorem 10.1. □

8. Nem-Abel együtthatós kohomológia és torzorok

Ebben a részben G provéges csoport lesz. Célunk az előzőekben definiált H^0 és H^1 kohomológia-csoportok általánosítása nem-Abel együttható-csoportokra.

2.8.1. Definíció. *Legyen E diszkrét topologikus tér (azaz E halmaz). Azt mondjuk, hogy E (bal oldali) G-halmaz, ha G folytonosan hat E-n. Már tudjuk, hogy ez azzal ekvivalens, hogy minden $e \in E$ pont stabilizátora nyílt részcsoportja G-nek. Ha E_1 és E_2 két G-halmaz, akkor az $f : E_1 \to E_2$ leképezés G-morfizmus, ha $f(g(e)) = g(f(e))$ minden $g \in G, e \in E_1$-re. A (bal oldali) G-csoport, ha A (diszkrét) csoport, amin G az A-beli szorzást megtartva hat, azaz $g(a_1a_2) = g(a_1)g(a_2)$.*

Ha A Abel-csoport, akkor A, mint G-csoport nem más, mint egy G-modulus. A következő definíció az előző részek alapján kézenfekvő:

2.8.2. Definíció. *Ha E G-halmaz, akkor legyen $H^0(G, E) = E^G = \{e \in E : g(e) = e$ minden $g \in G$-re $\}$. Ez a G nulladik A együtthatós kohomológia-halmaza.*

A későbbiekben fontos lesz az az észrevétel, hogy ha A egy G-csoport, akkor $H^0(G, A)$ pontozott halmaz (sőt csoport) lesz, a bázispont az 1_A lesz. Halmazok közötti leképezéseknél természetesen értelmezett a leképezés képe, azonban pontozott halmazok körében már leképezések magja is értelmezhető, mint a bázispont ősképe.

2.8.3. Definíció. *Legyen A G-csoport. Egy $G \to A : g \mapsto a_g$ folytonos leképezést 1-kociklusnak nevezünk, ha $a_{gh} = a_g g(a_h)$ minden $g, h \in G$-re. Az 1-kociklusok halmazát $Z^1(G, A)$-val jelöljük. Ha a és a' két 1-kociklus, akkor azt mondjuk, hogy a és a' kohomológok, ha létezik olyan $b \in A$, hogy $a'_g = b^{-1}a_g g(b)$. Könnyen ellenőrizhető, hogy ez egy ekvivalencia-relációt definiál $Z^1(G, A)$-n, az ekvivalencia-osztályok halmazát $H^1(G, A)$-val jelöljük és azt mondjuk, hogy ez a G A együtthatós első kohomológia-halmaza.*

2.8.4. Megjegyzés.

(1) Ha k test és az előző definícióban $G = \Gamma_k$, akkor $H^1(k, A)$-val fogjuk jelölni az első kohomológia-halmazt. Ezt nevezzük a k első nem-Abel együtthatós Galois kohomológia-halmazának.
(2) Érdemes megjegyezni hogy, ha G triviálisan hat A-n, akkor $H^1(G, A)$ nem más, mint a $G \to A$ leképezések halmaza

Az első kohomológia-halmazok is pontozottak, a bázispont annak az 1-kociklusnak az ekvivalenciaosztálya lesz, ami mindenhez az együtthatócsoport egységelemét rendeli. Fontos azonban megjegyezni, hogy általában nem értelmezhető csoportstruktúra az első kohomológia-halmazon. Kommutatív együttható-csoport esetén a korábbiakban és a most definiált H^0 és H^1 megegyeznek (és H^1-en definiálható csoportstruktúra).

A következőkben egy másfajta megközelítését mutatjuk meg az első kohomológia-halmaznak. A kulcsfogalom a következő lesz:

2.8.5. DEFINÍCIÓ. *Legyen A G-csoport és E G-halmaz. Azt mondjuk, hogy az A G-kompatibilisen hat (balról) E-n, ha adott E-n egy A-hatás és $g(ae) = g(a)g(e)$ minden $g \in G, a \in A$ és $e \in E$-re (azaz az $A \times E \to E$ leképezés G-morfizmus).*
Azt mondjuk, hogy P nemüres G-halmaz (jobb oldali) A-torzor (G felett), ha A (jobbról) hat P-n és minden $x, y \in P$-re egyértelműen létezik $a \in A$, hogy $xa = y$.

Ha P_1 és P_2 két A-torzor, akkor azt mondjuk, hogy ők izomorfak, ha létezik közöttük olyan bijekció, amely invariáns a G és az A hatására nézve is.

2.8.6. ÁLLÍTÁS. *Legyen A G-csoport, P G-halmaz, amin A jobbról hat. Ekkor a következők ekvivalensek:*

(1) *P A-torzor.*
(2) *A $P \times A \to P \times P : (p, a) \mapsto (pa, p)$ leképezés G-izomorfizmus.*

BIZONYÍTÁS. Mindkét irány triviális. □

Természetes kérdés, hogy tudjuk-e klasszifikálni a G feletti A-torzorokat. Jelöljük $Torsor_G(A)$-val az A-torzorok izomorfiaosztályainak halmazát. A következő tétel köti össze a torzorokat és az első kohomológia-halmazt.

Legyen P A-torzor és válasszunk ki egy $x \in P$ pontot. Minden $g \in G$-re $g(x) \in P$, így egyértelműen létezik olyan $a_g \in A$, hogy $xa_g = g(x)$. Ekkor a $g \mapsto a_g$ leképezés 1-kociklust definiál: könnyen láthatóan folytonos és

$$(gh)(x) = g(h(x)) = g(xa_h) = g(x)g(a_h) = xa_g g(a_h).$$

Ha megváltoztatjuk az $x \in P$ pontot az $y \in P$ pontra, akkor kohomológ kociklust kapunk, mivel létezik olyan $b \in A$, hogy $xb = y$, így

$$g(y) = g(xb) = g(x)g(b) = xa_g g(b) = yb^{-1}a_g g(b).$$

Jelöljük ezt a leképezést λ-val.

2.8.7. TÉTEL. *Legyen A G-csoport. Ekkor $Torsor_G(A)$ és $H^1(G, A)$ pontozott halmazok között a λ leképezés bijekció lesz.*

BIZONYÍTÁS. A fordított irányú leképezést a következőképpen definiáljuk: legyen a_g kociklus és jelöljük P_a-val az A csoportot, de a következőképpen definiált G-hatással: $g * a = a_g g(a)$. Ha az $a \in A$ elem P_a-n jobb oldali eltolásként hat, akkor P_a A-torzor lesz. Két kohomológ kociklushoz izomorf torzorok tartoznak: ha $a'_g = b^{-1}a_g g(b)$, akkor

$$\begin{aligned} \phi : P_{a'} &\to P_a \\ a &\mapsto ba \end{aligned}$$

leképezés lesz az izomorfizmus. Mivel ϕ a balról b-vel szorzás, ezért A-ekvivariáns lesz a leképezés. Nézzük a G-ekvivarianciát:

$$\phi(g * a') = \phi(a'_g g(a)) = ba'_g g(a) = a_g g(b)g(a),$$

másrészt

$$g * \phi(a) = a_g g(ba) = a_g g(b)g(a).$$

Ezzel definiáltuk a $H^1(G, A) \to Torsor_G(A)$ leképezést, a továbbiakban ezt μ-vel jelöljük.

Legyen a_g 1-kociklus és készítsük el hozzá a P_a torzort. Legyen $x \in P_a$ rögzített és nézzük $g \in G$-re $g * x$-t:

$$g * x = a_g g(x) = xx^{-1}a_g g(x),$$

tehát a P_a-hoz tartozó kociklus $x^{-1}a_g g(x)$ lesz, ami kohomológ a_g-vel. Azaz $\lambda \circ \mu$ az identitás lesz.
Most legyen P A-torzor és készítsük el a hozzá tartozó a_g 1-kociklust ($x \in P$-re $g(x) = xa_g$), majd pedig a P_a torzort. Legyen

$$\begin{aligned} \phi : P &\to P_a \\ y &\mapsto a, \end{aligned}$$

ahol $y = xa$. Ez a ϕ A-ekvivariáns, mert $\phi(ya') = \phi(xaa') = aa' = \phi(y)a'$. Nézzük a G-ekvivarianciát:

$$g * \phi(y) = g * a = a_g g(a) = \phi g(x) g(a) = \phi(g(xa)) = \phi(g(y)).$$

Továbbá ez a ϕ leképezés bijekció lesz, mert tetszőleges $a \in P_a$-hoz létezik $y \in P$, hogy $\phi(y) = a$, ugyanis $y = xa$ jó lesz. Másrészt $y \neq y'$ P-beli elemekhez különböző A-beli elemek tartoznak, melyekre $y = xa$. Tehát $\mu \circ \lambda$ is az identitás lesz. $\square$

Korábban már említettük, hogy pontozott halmazok közötti leképezéseknek is értelmezhető a magja, így definiálható pontozott halmazok egzakt sorozata is. A továbbiakban azt vizsgáljuk, hogy a kohomologikus hosszú egzakt sorozathoz hasonló egzakt sorozat milyen feltételek mellett létezik.

Legyen B G-halmaz és tegyük fel, hogy A G-részcsoportja B-nek, azaz részcsoport és a G-beli elemekkel való hatás sem vezet ki A-ból. A célunk egy kohomológikus egzakt sorozat létezésének bizonyítása lesz. Jelöljük B/A-val az A bal oldali mellékosztályait, ez természetes módon G-halmaz lesz, így $H^0(G, B/A)$ értelmezett, sőt ez pontozott halmaz lesz, a bázispont az egységelemhez tartozó mellékosztály lesz.

2.8.8. Állítás. *Legyen B G-csoport és az A G-részcsoportja. Ekkor a következő sorozat pontozott halmazok egzakt sorozata lesz:*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B).$$

Bizonyítás. A δ leképezés kivételével az összes leképezés definíciója világos. Legyen $bA \in (B/A)^G$. Ekkor a bA mellékosztály A-torzor lesz: a G illetve A elemei a természetes módon hatnak és a mellékosztály bármely két eleméhez egyértelműen tartozik egy A-beli elem, amivel való jobbról szorzás az egyik elemet a másikba viszi. Ehhez a torzorhoz tartozó $H^1(G, A)$-beli ekvivalenciaosztályt fogjuk $\delta(bA)$-val jelölni.
Egzaktság $H^0(G, A)$-nál: triviális, mert A részcsoportja G-nek.
Egzaktság $H^0(G, B)$-nél: egy $b \in B^G$ elem akkor és csak akkor képződik az 1-hez tartozó A szerinti mellékosztályba, ha b eleme A-nak.
Egzaktság $H^0(G, B/A)$-nál: könnyű felírni egy $bA \in (B/A)^G$-hez tartozó $\delta(bA)$ 1-kociklust. Rögzítsük bA halmazban b-t, ekkor $g(b) = ba_g$ egyenletet kell megoldanunk, vagyis $a_g = b^{-1}g(b)$ lesz. Ha bA egy $H^0(G, B)$-beli elem képe, akkor $g(b) = b$ miatt a_g a triviális kociklus lesz. Másrészt,

ha $a_g = b^{-1}g(b)$ kociklus A-ban kohomológ a triviális kociklussal, akkor $b^{-1}g(b) = a^{-1}g(a)$, vagyis $g(ba^{-1}) = ba^{-1}$ és ezzel készen vagyunk.
Egzaktság $H^1(G, A)$-nál: tudjuk, hogy a $bA \in (B/A)^G$-hez tartozó $\delta(bA)$ 1-kociklus $a_g = b^{-1}g(b)$ lesz, amiről rögtön látjuk, hogy nullkohomológ $H^1(G, B)$-ben. Továbbá, ha a_g olyan 1-kociklus $H^1(G, A)$-ban, ami nullkohomológ $H^1(G, B)$-ben, akkor $a_g = b^{-1}g(b)$ valamilyen $b \in B$-re. Mivel $a_g \in A$, ezért $g(b) \in bA$, azaz $bA \in (B/A)^G$ és ez kellett nekünk. □

A későbbiekben szükségünk lesz az alábbi következményre:

2.8.9. KÖVETKEZMÉNY. *A $H^1(G, A) \to H^1(G, B)$ leképezés magja azonosítható $(B/A)^G$ halmaz B^G hatása szerinti orbitjainak a halmazával.*

BIZONYÍTÁS. B^G a balról szorzással hat a mellékosztályokon. Az előző állítás miatt elég a következőt belátnunk: $bA, b'A \in (B/A)^G$ mellékosztályokra $\delta(bA) = \delta(b'A)$ akkor és csak akkor teljesül, ha létezik olyan $c \in B^G$, hogy $b'A = cbA$. A $\delta(bA) = \delta(b'A)$ egyenlőséget átírva kociklusokra a kívánt eredmény azonnal adódik. □

9. Speiser-lemma és Hilbert 90-es tétele

2.9.1. ÁLLÍTÁS (Speiser-lemma). *Legyen K/k véges Galois-bővítés $G = Gal(K/k)$ Galois-csoporttal. Ha adott V véges dimenziós K-vektortér szemilineáris G-hatással (azaz igaz lesz $g(\lambda v) = g(\lambda)g(v)$ minden $g \in G$, $\lambda \in K$ és $v \in V$-re), akkor a*

$$\phi : V^G \otimes_k K \to V$$

természetes leképezés izomorfizmus lesz.

BIZONYÍTÁS. Ez a speciális esete a 1.1.9. Állításnak. □

2.9.2. DEFINÍCIÓ. *Legyen k test, V vektortér k felett. A V-n értelmezett racionális függvények testét $k(V)$-vel jelöljük. Ha G csoport és adott G-nek leképezése $GL(V)$-be (azaz G egy reprezentációja), akkor G természetes módon fog hatni a $k(V)$ testen is.*

Nézzük egy következményét a Speiser-lemmának.

2.9.3. KÖVETKEZMÉNY.

(1) *Legyen $K|k$ véges Galois-bővítés és G a Galois-csoport. Ha V véges dimenziós vektortér K felett úgy, hogy G szemilineárisan hat rajta, akkor*

$$K(V)^G|k = k(V^G)|k$$

tiszta transzcendens bővítés lesz.

(2) *Ha H véges csoport és adott H-nak két véges dimenziós hűséges V ill. W reprezentációja a k test felett, akkor $k(V)^H$ és $k(W)^H$ stabilan racionálisak, azaz léteznek $x_1, \ldots, x_n$ és $y_1, \ldots, y_m$ határozatlanok úgy, hogy*

$$k(V)^H(x_1, \ldots, x_n) \cong k(W)^H(y_1, \ldots, y_m)$$

BIZONYÍTÁS. [**5**] Theorem 3.3. és Lemma 3.5. □

A Speiser-lemma segítségével belátható a *Hilbert 90-es tétel* általánosítása (bővebben lásd [**7**] 2.3)

2.9.4. TÉTEL. *Legyen K/k véges Galois-bővítés G Galois-csoporttal. Ekkor a G csoport természetes módon hat a $GL_n(K)$ csoporton és erre a hatásra nézve $H^1(G, GL_n(K)) = 1$.*

BIZONYÍTÁS. Ha $a_g \in H^1(G, GL_n(K))$ 1-kociklus, akkor $V = K^n$-en értelmezhető az a_g szerint csavart hatás: $g * v = a_g(g(v))$. Jelöljük ${}_aV$-vel a csavart hatással ellátott V vektorteret. Speiser-lemma miatt $({}_aV)^G$ olyan k-vektortér, ami K felett V-vel izomorf, ezért $({}_aV)^G = k^n$, amiből már következik az állítás. □

10. Kummer-elmélet

Az előző rész egyik következményeként adódik a Hilbert 90-es tétel folytonos változata.

2.10.1. ÁLLÍTÁS. *Ha k test és k_s egy fixált szeparábilis lezártja k-nak, akkor $H^1(k, k_s^\times)$ triviális lesz.*

BIZONYÍTÁS. A Galois-kohomológia definíciója miatt

$$H^1(k, k_s^\times) = \varinjlim H^1(K, K^\times),$$

ahol K végigfut a k véges Galois-bővítésein. Láttuk, hogy a $H^1(K, K^\times)$ csoportok mind triviálisak, ezért $H^1(k, k_s^\times)$ is triviális lesz. □

2.10.2. TÉTEL. *Legyen k test és $m > 0$ egész szám, amely relatív prím a test karakterisztikájához. Legyen k_s a k egy fixált szeparábilis lezártja és jelöljük μ_m-mel a k_s-beli m-edik egységgyökök csoportját. A $\Gamma_k = Gal(k_s/k)$ csoport természetes módon hat μ_m-en és ekkor létezik egy természetes izomorfizmus*

$$k^\times/k^{\times m} \xrightarrow{\cong} H^1(k, \mu_m)$$
$$[a] \mapsto a_g = g(\alpha)\alpha^{-1}$$

ahol α az a egy m-edik gyöke.

BIZONYÍTÁS. Nézzük az alábbi Γ_k-modulusok rövid egzakt sorozatát

$$1 \to \mu_m \to k_s^\times \xrightarrow{m} k_s^\times \to 1,$$

ahol a harmadik leképezés az m-edik hatványra emelés. Mivel m relatív prím $char(k)$-hoz, ezért $x^m - a$ szeparábilis polinom lesz minden $a \in k_s$-re, így valóban szürjektív lesz ez a leképezés. Nézzük az ehhez a rövid egzakt sorozathoz tartozó hosszú egzakt sorozat következő részét

$$\cdots \to H^0(k, k_s^\times) \xrightarrow{m} H^0(k, k_s^\times) \to H^1(k, \mu_m) \to H^1(k, k_s^\times) \to \ldots$$

Az első és második csoport $k^\times$-val izomorf és a köztük menő leképezés pedig az m-edik hatványra emelés lesz. Az előző állítás miatt az utolsó csoport triviális, így az egzaktság miatt kapjuk az állítást. □

11. Brauer-csoportok

A most következők részletes tárgyalása megtalálható a [**7**] könyv 1., 2. és 4. fejezetében.

2.11.1. DEFINÍCIÓ. *Legyen k test és A véges dimenziós k-algebra (ebben a részben minden algebráról feltesszük, hogy véges dimenziós).*

(1) *Azt mondjuk, hogy A egyszerű, ha nincs nem-triviális valódi ideálja.*
(2) *Azt mondjuk, hogy A centrális, ha az A centruma k-val egyenlő.*

A következő tétel az egyszerű algebrák struktúráját írja le.

2.11.2. Tétel (Wedderburn tétele). *Legyen k test és A véges dimenziós egyszerű k-algebra. Ekkor létezik olyan D ferdetest k felett és egy olyan n pozitív egész, hogy A izomorf lesz $M_n(D)$-vel. Sőt, a D ferdetest és az n szám egyértelműen meghatározott.*

Az előző tétel motiválja a következő definíciót.

2.11.3. Definíció. *Legyenek A_1 és A_2 centrális egyszerű k-algebrák. Az előző tétel miatt léteznek olyan D_1 és D_2 ferdetestek, hogy $A_1 \cong M_{n_1}(D_1)$ és $A_2 \cong M_{n_2}(D_2)$. Azt mondjuk, hogy A_1 és A_2 hasonlóak, ha D_1 és D_2 izomorfak egymással.*

Triviális, hogy a hasonlóság ekvivalenciareláció lesz a k feletti centrális egyszerű algebrák izomorfia-osztályainak a halmazán. Az ekvivalenciaosztályok halamazát $Br(k)$-val fogjuk jelölni.

2.11.4. Állítás.

(1) *Legyenek A_1 és A_2 centrális egyszerű k-algebrák. Ekkor $A_1 \otimes_k A_2$ is centrális egyszerű algebra lesz.*
(2) *Ha A n dimenziós centrális egyszerű k-algebra és A^{opp} az oppozitalgebrája, akkor A^{opp} is centrális egyszerű k-algebra lesz és $A \otimes_k A^{opp} \cong M_n(k)$.*

2.11.5. Következmény. *A $Br(k)$ halmaz elemein a tenzorszorzás Abel-csoport struktúrát definiál. Az egységelem a k osztálya lesz és az $[A]$ osztály inverze az $[A^{opp}]$ osztály lesz. A $Br(k)$ csoportot Brauer-csoportnak nevezzük.*

A Brauer-csoportnak szoros kapcsolata van a Galois-kohomológiával, mint azt a következő tétel is mutatja.

2.11.6. Tétel. *Legyen k test és fixáljuk egy k_s szeparábilis lezártját. Ekkor létezik természetes izomorfizmus*

$$Br(k) \cong H^2(k, k_s^\times).$$

Emiatt a $Br(k)$ minden eleme véges rendű lesz. Sőt, ha m olyan pozitív egész, mely relatív prím a k test karakterisztikájához, akkor létezik természetes izomorfizmus

$${}_mBr(k) \cong H^2(k, \mu_m),$$

ahol ${}_mBr(k)$ a Brauer-csoport m-torzió-részcsoportja és μ_m a k_s-beli m-edik egység-gyökök csoportja.

Bizonyítás. [**7**] Theorem 4.4.7 és Corollary 4.4.9 □

Lássunk néhány példát centrális egyszerű algebrára.

2.11.7. Példa.

(1) Legyen D ferdetest k felett és tekintsük a D feletti $n \times n$-es mátrixok $M_n(D)$ gyűrűjét. Jól ismert, hogy $M_n(D)$ egyszerű algebra (speciálisan D maga is egyszerű) és a centruma izomorf D centrumával. Tehát, ha $Z(D) = k$, akkor $M_n(D)$ is centrális egyszerű algebra lesz.
(2) Legyen k test, $char(k) \neq 2$. Vegyünk két nem-nulla elemet k-ból: $a, b \in k^\times$. Ekkor elkészíthető a következő, (a, b)-vel jelölt 4 dimenziós k-algebra, melynek bázisa $\{1, i, j, ij\}$ lesz és amiben a szorzást a következő összefüggések határozzák meg
$$i^2 = a, j^2 = b, ij = -ji$$
Az (a, b) algebrát (általánosított) kvaternió-algebrának nevezzük. Erről is belátható, hogy centrális, egyszerű algebra lesz.
(3) Az előző pontbeli konstrukciót még tovább lehet általánosítani bizonyos feltételek mellett. Legyen m pozitív egész. Tegyük fel, hogy a k test olyan, hogy m invertálható k-ban és k tartalmaz egy ω primitív m-edik egységgyököt. Ha $a, b \in k^\times$, akkor definiáljuk az $(a, b)_\omega$ ciklikus k-algebrát a következőképpen
$$(a, b)_\omega = \langle x, y : x^m = a, y^m = b, xy = \omega yx\rangle.$$
Ha $m = 2$ és $\omega = -1$, akkor a kvaternió-algebrákat kapjuk vissza. Bizonyítható, hogy az $(a, b)_\omega$ ciklikus algebrák is centrálisak és egyszerűek.

Érdekes kérdés, hogy ciklikus algebrának melyik elem fog megfelelni $H^2(k, k_s^\times)$ csoportban. Legyen m pozitív egész, k olyan test, melyben invertálható az m és amely tartalmaz egy ω primitív m-edik egységgyököt. Legyenek $a, b \in k^\times$ nem-nulla elemek. Igazolható, hogy $(a, b)_\omega$ osztályának a rendje $Br(k)$-ban osztja az m-et. A Kummer-elméletből következik, hogy a és b meghatároznak egy-egy elemet $H^1(k, \mu_m)$-ben. Mielőtt továbbmennénk, értsük meg először μ_m struktúráját.

2.11.8. Állítás. *A fenti feltételek mellett μ_m egy m rendű ciklikus csoport lesz. Továbbá $\mu_m \otimes_{\mathbb{Z}} \mu_m \cong \mathbb{Z}/m\mathbb{Z}$, mint csoportok. Speciálisan, ha $\mu_m \subseteq k$ (azaz Γ_k triviálisan hat μ_m-en), akkor az izomorfizmus Γ_k-ekvivariáns.*

Bizonyítás. A μ_m csoport elemei az $x^m - 1$ polinom gyökei lesznek. Mivel m relatív prím a test karakterisztikájához, ezért a polinom összes gyöke k_s-ben lesz, ezért μ_m rendje nagyobb lesz, mint m. Másrészt egy test feletti m-edfokú polinomnak legfeljebb m gyöke van, így μ_m rendje pontosan m. Tudjuk, hogy egy test multiplikatív csoportjának véges részcsoportja ciklikus, ezzel készen vagyunk. A Γ_k csoport hatását a $\mu_m \otimes_{\mathbb{Z}} \mu_m$ csoporton $g(a \otimes b) = g(a) \otimes g(b)$ adja meg és az állítás második fele könnyen ellenőrizhető. $\square$

A cup-szorzás segítségével definiálhatjuk a következő leképezést
$$H^1(k, \mu_m) \times H^1(k, \mu_m) \xrightarrow{\cup} H^2(k, \mu_m^{\otimes 2})$$
Rögzítsük azt a $\mu_m \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$ izomorfizmust, ami az ω-t a ciklikus csoport generátorába viszi. Tekintsük az alábbi leképezéseket
$$H^2(k, \mu_m^{\otimes 2}) \xrightarrow{\cong} H^2(k, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\cong} H^2(k, \mu_m) \xrightarrow{\cong} {}_mBr(k),$$

ahol a harmadik leképezést a rögzített izomorfizmusunk indukálja.

2.11.9. ÁLLÍTÁS. *Legyen m pozitív egész, k olyan test, melyben invertálható az m és amely tartalmaz egy ω primitív m-edik egységgyököt. Legyenek $a, b \in k^\times$ nem-nulla elemek. Ekkor a*

$$k^\times/k^{\times m} \times k^\times/k^{\times m} \xrightarrow{\cong} H^1(k, \mu_m) \times H^1(k, \mu_m) \xrightarrow{\cup} H^2(k, \mu_m^{\otimes 2}) \xrightarrow{\cong}$$
$$\xrightarrow{\cong} H^2(k, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\cong} H^2(k, \mu_m) \xrightarrow{\cong} {}_mBr(k)$$

kompozíciónál az $(a, b) \in k^\times/k^{\times m} \times k^\times/k^{\times m}$ elem képe az $(a, b)_\omega$ ciklikus algebra lesz.

BIZONYÍTÁS. [**7**] Proposition 4.7.1 □

2.11.10. MEGJEGYZÉS. A Brauer-csoport kohomologikus jellemzésének és az előző tételnek egy következménye, hogy az $(a) \cup (b)$ kohomológia-osztály akkor és csak akkor lesz triviális, ha az (a, b) k feletti kvaternió-algebra izomorf $M_2(k)$-val. Belátható, hogy ez utóbbi akkor és csak akkor teljesül, ha létezik olyan $(x, y, z) \in k^3 \backslash \{(0, 0, 0)\}$, hogy $ax^2 + by^2 = z^2$. (lásd [**7**] Proposition 1.3.2)

3. FEJEZET

Sémák, csoportsémák és torzorok

Mint már említettük, a második fejezetben megismert fogalmakat tovább lehet általánosítani algebrai geometria keretek között. A fejezet elején villámgyorsan bevezetjük a sémák fogalmát és a legfontosabb konstrukciókat (részletekért az olvasó a [**9**] könyvhöz fordulhat). Habár a szakdolgozat további részeihez elégséges lenne az affin sémák ismerete (azaz maradhatnánk a kommutatív algebra berkein belül), azonban a geometriai megfogalmazás természetessége miatt érdemes általánosan dolgozni. Látni fogjuk, hogy a kommutatív gyűrűk Galois-bővítése vagy a generikus Galois-bővítés hogyan fogalmazható meg a sémák és torzorok segítségével, továbbá összekapcsoljuk adott k test (nem-Abel) Galois-kohomológiáját a k test feletti torzorok izomorfiaosztályainak halmazával. Ennek a kapcsolatnak kulcsszerepe lesz az utolsó fejezetben.

1. Alapfogalmak

Legyen A egységelemes, kommutatív gyűrű.

3.1.1. Definíció. *Az A gyűrű $Spec(A)$ spektruma az a topologikus tér, melynek alaphalmaza az A prímideáljainak halmaza és amelynek nyílt halmazainak bázisa a következő halmazokból áll: $D_a = \{P : P \text{ prímideál}, a \notin P\}$. Ezt a topológiát Zariski-topológiának nevezzük.*

Könnyű belátni, hogy a D_a halmazok zártak a véges metszet képzésre, így valóban egy topológia bázisát alkotják.

3.1.2. Definíció. *Legyen X topologikus tér. Azt mondjuk, hogy $(X, \mathcal{F})$ gyűrűzött tér, ha adott X-en gyűrűk $\mathcal{F}$ kévéje. Ha $(Y, \mathcal{G})$ egy másik gyűrűzött tér, akkor a $(\phi, \phi^{\#})$ párt gyűrűzött terek morfizmusának nevezzük, ha $\phi : X \to Y$ folytonos leképezés és $\phi^{\#} : \mathcal{G} \to \phi_*\mathcal{F}$ kévemorfizmus.*

3.1.3. Állítás. *Legyen $X = Spec(A)$, ahol A gyűrű. Ekkor egyértelműen létezik $\mathcal{O}_X$ gyűrűk kévéje X-en, hogy $\mathcal{O}_X(D(a)) = A_a$ minden $0 \neq a \in A$-ra, ahol A_a az A lokalizáltja az $\{1, a, a^2, \dots\}$ multiplikatívan zárt halmaz szerint.*

Sőt, az is belátható, hogy minden $P \in Spec(A)$ prímideálra a $\mathcal{O}_X$ kéve P pontbeli $\mathcal{O}_{X,P}$ kocsánya lokális gyűrű lesz, nevezetesen A_P. Ez motiválja a következő definíciót.

3.1.4. Definíció. *Az $(X, \mathcal{F})$ gyűrűzött teret lokálisan gyűrűzött térnek nevezzük, ha X minden x pontjában az $\mathcal{F}$ kéve $\mathcal{F}_x$ kocsánya lokális gyűrű. Az x pontbeli lokális gyűrű maradéktestét $\kappa(x)$-szel jelöljük. Legyen $(Y, \mathcal{G})$ szintén lokálisan gyűrűzött tér és $(\phi, \phi^{\#})$ gyűrűzött terek morfizmusa $(X, \mathcal{F})$-ből $(Y, \mathcal{G})$-be. A $\phi^{\#}$ kévemorfizmus minden $x \in X$-re indukál $\phi_x : \mathcal{G}_{\phi(x)} \to \mathcal{F}_x$*

gyűrűhomomorfizmust. Azt mondjuk, hogy $(\phi, \phi^{\#})$ lokálisan gyűrűzött terek morfizmusa, ha minden $x \in X$-re ϕ_x lokális homomorfizmus, azaz az $\mathcal{F}_x$ lokális gyűrű maximális ideáljának őse képe ϕ_x-nél a $\mathcal{G}_{\phi(x)}$ lokális gyűrű maximális ideálja.

Az előzőek szerint minden A gyűrűre $X = Spec(A)$ a fenti $\mathcal{O}_X$ kévével lokálisan gyűrűzött tér lesz. Ha adott $f : A \to B$ gyűrű-homomorfizmus, akkor természetes módon definiálható $Spec(f) : Spec(B) \to Spec(A)$ lokálisan gyűrűzött terek morfizmusa.

3.1.5. DEFINÍCIÓ. *A $(Spec(A), \mathcal{O}_{Spec(A)})$ lokálisan gyűrűzött teret affin sémának nevezzük. Az $(X, \mathcal{O}_X)$ lokálisan gyűrűzött teret sémának nevezzük, ha létezik olyan $\{U_i\}$ $(i \in I)$ nyílt fedése, hogy minden i-re $(U_i, \mathcal{O}_X|_{U_i})$ izomorf egy affin sémával. Két séma közötti morfizmuson lokálisan gyűrűzött terek közötti morfizmust értünk. A sémák kategóriáját Sch-val fogjuk jelölni.*

3.1.6. DEFINÍCIÓ. *Azt mondjuk, hogy az X séma redukált, ha minden $U \subseteq X$- nxílt részhalmazra az $\mathcal{O}_X(U)$ gyűrűben nincsenek nilpotens elemek.*
Azt mondjuk, hogy az X séma integrális, ha minden $U \subseteq X$ nyílt részhalmazra az $\mathcal{O}_X(U)$ gyűrű nullosztómentes.

3.1.7. ÁLLÍTÁS. *Ha X integrális séma, akkor egyértelműen létezik olyan pont X-ben, aminek a lezártja az egész X lesz. Ezt a pontot nevezzük az X séma generikus pontjának.*

3.1.8. DEFINÍCIÓ. *Legyen S rögzített séma. Azt mondjuk, hogy az (X, ϕ) S-séma, ha X séma és $\phi : X \to S$ sémamorfizmus. Ha a ϕ morfizmus ismert, akkor a rövidség kedvéért azt mondjuk, hogy X S-séma. Ha (X, ϕ) és (Y, ψ) S-sémák, akkor $f : (X, \phi) \to (Y, \psi)$ S-morfizmus, ha $f : X \to Y$ sémamorfizmus és a*

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\phi}\downarrow & & {\scriptstyle\psi}\downarrow \\ S & = & S \end{array}$$

diagram kommutatív. Az S-sémák kategóriáját Sch_S-sel jelöljük.

3.1.9. DEFINÍCIÓ. *Legyen k test. Azt mondjuk, hogy az X $Spec(k)$ feletti séma (röviden k-séma) véges típusú, ha X kompakt és létezik olyan affin nyílt fedése X-nek $Spec(A_i)$ affin sémákkal, hogy A_i-k végesen generált k-algebrák.*

3.1.10. DEFINÍCIÓ. *Legyen S séma, (X, ϕ) és (Y, ψ) S-sémák. Az X és Y sémák S feletti fibrált szorzata az a $(X \times_S Y, p, q)$ hármas, ahol $X \times_S Y$ S-séma, $p : X \times_S Y \to X$ és $q : X \times_S Y \to Y$ S-morfizmus, úgy, hogy minden olyan Z S-sémára, amire adottak $f : Z \to X$ és $g : Z \to Y$ S-morfizmusok, melyekre a*

$$\begin{array}{ccc} Z & \xrightarrow{g} & Y \\ {\scriptstyle f}\downarrow & & \downarrow \\ X & \longrightarrow & S \end{array}$$

diagram kommutatív, akkor létezik $u = f \times g : Z \to X \times_S Y$ S-morfizmus úgy, hogy $f = p \circ u$ és $g = q \circ u$.

3.1.11. Állítás. *A fibrált szorzat létezik és izomorfizmus erejéig egyértelmű. Ha $S = Spec(C)$, $X = Spec(A)$ és $Y = Spec(B)$, akkor $X \times_S Y = Spec(A \otimes_C B)$.*

3.1.12. Megjegyzés.

(1) Belátható, hogy minden X S-sémára $S \times_S X$ kanonikusan izomorf X-szel.
(2) Az $X \times_S Y$ természetesen izomorf $Y \times_S X$-szel.
(3) Az $X \times_S Y$ fibrált szorzat X (ill. Y) feletti sémának tekinthető a p (ill. q) morfizmuson keresztül.
(4) $(X \times_S Y) \times_{S'} Z$ természetesen izomorf lesz $X \times_S (Y \times_{S'} Z)$-vel.
(5) A $(X \times_S Y, p, q)$ fibrált szorzat rendelkezik a következő tulajdonsággal: minden T S-sémára a következő
$$Hom_S(T, X \times_S Y) \to Hom_S(T, X) \times Hom_S(T, Y)$$
$$w \mapsto (p \circ w, q \circ w)$$
leképezés bijekció lesz.

Legyen most $Y \to X$ sémamorfizmus. Szeretnénk értelmezni a morfizmus egy adott $x \in X$ pont feletti fibrumát. Legyen $U = Spec(A)$ olyan affin nyílt részhalmaza X-nek, amire $x \in U$. Ekkor x azonosítható az A gyűrű egy P prímideáljával és így értelmezhető az $A \to A_P \to A_P/PA_P = \kappa(x)$ kompozíció. Ennek segítségével pedig definiálható
$$Spec\,\kappa(x) \to U = Spec(A) \to X$$
morfizmus (és így $Spec\,\kappa(x)$ X feletti séma lesz).

3.1.13. Definíció. *Legyen $\phi : Y \to X$ sémamorfizmus és tegyük fel, hogy $x \in X$ egy pont. Ekkor a ϕ morfizmus x feletti fibrumát az $Y \times_X Spec\,\kappa(x)$ fibrált szorzatként definiáljuk. Belátható, hogy a fibrum független az U választásától.*

Ha X integrális séma, akkor a generikus pont feletti fibrumot generikus fibrumnak nevezzük.

3.1.14. Definíció. *Legyen k test. Azt mondjuk, hogy a X $Spec(k)$ feletti séma affin (projektív) k-varietás, ha redukált és véges típusú affin (projektív) séma.*

3.1.15. Példa. Legyen k test. A $k[x_1, \ldots, x_n]$ polinomgyűrűhöz tartozó $\mathbf{A}^n$ affin sémát a k feletti n dimenziós affin térnek nevezzük. Ragasztással vagy a $Proj$-konstrukcióval definiálható a k feletti $\mathbf{P}^n$ n dimenziós projektív tér.

2. Csoportsémák

3.2.1. Definíció. *Legyen X séma. Ekkor az X egy $Hom(-, X) : Sch \to Set$ funktort határoz meg a sémák kategóriájából a halmazok kategóriájába. A $Hom(Y, X)$ halmazt $X(Y)$-nal fogjuk jelölni és azt mondjuk, hogy ez az X Y értékű pontjainak a halmaza. Ha X S-séma, akkor hasonlóan létezik $X(-) : Sch_S \to Set$ funktor.*

Legyen S rögzített séma és tegyük fel, hogy G egy S-séma.

3.2.2. DEFINÍCIÓ. *Azt mondjuk, hogy G S feletti csoportséma, ha a $Hom_S(-,G) : Sch_S \to Set$ funktornak létezik faktorizációja a $Grp \to Set$ felejtő funktoron keresztül.*

Másképpen azt is mondhatjuk, hogy minden X S-sémára a $G(X) = Hom_S(X,G)$ halmazon adott egy csoportstruktúra és minden $X \to Y$ S-morfizmusra adott $G(Y) \to G(X)$ csoport-homomorfizmus.

3.2.3. ÁLLÍTÁS (Yoneda-lemma). *Legyen $\mathcal{C}$ kategória, $A \in Ob(\mathcal{C})$ objektum és $F : \mathcal{C} \to Set$ kontravariáns funktor. Jelöljük h_A-val a $Hom_{\mathcal{C}}(-,A)$ kontravariáns funktort és $Nat(h_A,F)$-fel a $h_A \Rightarrow F$ természetes transzformációk halmazát. Ekkor a*

$$Nat(h_A,F) \to F(A)$$
$$\mu \mapsto \mu_A(id_A)$$

leképezés bijekció lesz, sőt funktoriális A-ban. Speciálisan, ha B egy másik objektum, akkor a $Nat(h_A,h_B)$ és $Hom_{\mathcal{C}}(A,B)$ halmazok között létezik bijekció.

BIZONYÍTÁS. Lásd [**10**] III.2. □

A Yoneda-lemma következményeként adódik, hogy a reprezentáló G séma izomorfizmus erejéig egyértelmű. Egy másik következénye az alábbi állítás.

3.2.4. ÁLLÍTÁS. *Legyen S séma és G S-séma. Ekkor a következő állítások ekvivalensek:*

(1) *G S-csoportséma*
(2) *Léteznek $m : G \times_S G \to G$, $i : G \to G$ és $e : S \to G$ S-morfizmusok úgy, hogy a következő diagramok kommutatívak:*

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{m \times id_G} & G \times_S G \\ {\scriptstyle id_G \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G \times_S S & = & G \\ {\scriptstyle id_G \times e}\downarrow & & \downarrow{\scriptstyle id_G} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{id_G \times i} & G \times_S G \\ \downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow{e} & G \end{array}$$

BIZONYÍTÁS. Ha teljesül a (2) feltétel, akkor adott X S-sémára alkalmazva a $Hom_S(X,-)$ funktort az m, i és e leképezésekre ill. a kommutatív diagramokra, továbbá felhasználva a fibrált szorzat 3.1.12. Megjegyzés (5) pontjának tulajdonságát, azonnal látjuk, hogy $Hom_S(X,G)$ csoport lesz (és ez triviálisan funktoriális az első változójában). Ha G csoportséma, akkor $G(X) = Hom_S(X,G)$ csoport lesz minden X-re, így létezik

$$m_X : Hom_S(X,G) \times Hom_S(X,G) \to Hom_S(X,G)$$

szorzás leképezés. A fibrált szorzat fent említett tulajdonsága miatt ekkor ez egy $m_X : Hom_S(X, G \times_S G) \to Hom_S(X, G)$ leképezés lesz, ami funktoriális az első változójában (vagyis m egy természetes tarnszformáció $Hom_S(-, G \times_S G)$-ből $Hom_S(-, G)$-be). Ekkor a Yoneda-lemma miatt létezik $m : G \times_S G \to G$ leképezés. Hasonlóan lehet megkonstruálni az e ill. az i leképezést. A fenti diagramok kommutativitása szintén ezzel a módszerrel látható be a csoportművelet asszociativitását, stb. felhasználva. □

3.2.5. Megjegyzés.

(1) Az előző állítás (2) pontját úgy is megfogalmazhatjuk, hogy G csoportobjektum az S feletti sémák Sch_S kategóriájában.
(2) Legyen $S \to S'$ sémamorfizmus, ekkor $G \times_S S'$ S'-csoportséma lesz és minden X S'-sémára $(G \times_S S')_{S'}(X) = G_S(X)$ (X az $S \to S'$ morfizmuson keresztül S-séma lesz).

Számos példát lehetne adni csoportsémára, azonban most csak a két számunkra legfontosabbat tárgyaljuk.

3.2.6. Példa.

(1) Legyen G (véges) csoport és jelöljük $\underline{G}_S$-sel azt az S-csoportsémát, ami minden X S-sémához hozzárendeli a $\underline{G}_S(X) = \{f : X \to G$ lokálisan konstans leképezés$\}$ halmazt. Másképpen, legyen $\underline{G}_S = \coprod_{g \in G} S$, ekkor $Hom_S(X, \underline{G}_S)$ a fenti halmaz lesz.
(2) Legyen $S = Spec(C)$. Ekkor definiáljuk a GL_n általános lineáris csoportsémát a következőképpen:
$$GL_n = Spec(C[x_{11}, \ldots, x_{nn}, y]/(y \cdot det((x_{ij})) - 1)).$$
Ha $X = Spec(A)$ S-séma, akkor könnyen látható, hogy $GL_n(X)$ az $n \times n$-es invertálható A feletti mátrixok $GL_n(A)$ csoportja lesz.

3.2.7. Definíció. *Legyen most k test. Azt mondjuk, hogy a G $Spec(k)$ feletti csoportséma affin algebrai csoportséma, ha $G = Spec(A)$, ahol A végesen generált k-algebra.*

3.2.8. Állítás. *Ha k test, akkor minden $G = Spec(A)$ affin algebrai csoportséma izomorf a GL_n k-csoportséma zárt részcsoportjával, azaz létezik olyan*
$$G \to GL_n$$
természetes transzformáció, hogy az indukált
$$k[x_{11}, \ldots, x_{nn}, y]/(y \cdot det((x_{ij})) - 1) \to A$$
gyűrű-homomorfizmus szürjektív.

Bizonyítás. Lásd [**18**] 3.4. Theorem. □

3.2.9. Definíció. *Legyen S séma, G S-csoportséma és X S-séma. Azt mondjuk, hogy G hat az X-en, ha adott $a : G \times_S X \to X$ S-morfizmus úgy, hogy minden T S-sémára az $a(T) : G(T) \times X(T) \to X(T)$ leképezés az $X(T)$ halmazon a $G(T)$ csoport hatását definiálja.*

A Yoneda-lemma segítségével bizonyítható (a fentihez hasonló módszerrel) a következő állítás.

3.2.10. Állítás. *Ha G S-csoportséma és X S-séma és $a : G \times_S X \to X$ S-morfizmus, akkor a következők ekvivalensek:*

(1) *Az a leképezés a G hatását definiálja X-en*
(2) *A következő diagramok kommutatívak lesznek*

$$\begin{array}{ccc} G \times_S G \times_S X & \xrightarrow{id_G \times a} & G \times_S X \\ {\scriptstyle m \times id_X}\downarrow & & \downarrow{\scriptstyle a} \\ G \times_S X & \xrightarrow{a} & X \end{array}$$

$$\begin{array}{ccc} S \times_S X & \xrightarrow{e \times id_X} & G \times_S X \\ \Vert & & \downarrow{\scriptstyle a} \\ X & \xrightarrow{id_X} & X \end{array}$$

3. Torzorok

A 2.8. részben megismert torzorok fogalmának létezik algebrai geometriai megfelelője, ezeket fogjuk most vizsgálni. Láttuk, hogy adott G provéges csoportra és A G-csoportra a $Torsor_G(A)$ halmaz és a $H^1(G, A)$ kohomológia-halmaz között létezik bijekció. Ha az S alapsémának $Spec(k)$-t választjuk, ahol k test, akkor az előzőhöz hasonló állítás mondható ebben az algebrai geometriai esetben is.

3.3.1. Definíció. *Legyen S séma, G S-csoportséma és X S-séma. Tegyük fel, hogy adott G hatása X-en. Azt mondjuk, hogy X G-torzor S felett, ha az*

$$a \times id_X : G \times_S X \to X \times_S X$$
$$(g, x) \mapsto (gx, x)$$

S-morfizmus izomorfizmus lesz.
G-torzorok morfizmusán olyan S-morfizmust értünk, ami kommutál a G hatásával (G-ekvivariáns morfizmus).

Könnyen ellenőrizhető a Yoneda-lemma segítségével és felhasználva a 2.8.6. Állítást, hogy ez a definíció ekvivalens azzal, hogy minden T S-sémára $G(T)$ egyszeresen tranzitívan hat az $X(T)$ halmazon.

3.3.2. Példa.

(1) Ha G S-csoportséma, akkor G a balról szorzással hat önmagán és ezzel a hatással a G egy G-torzor lesz. Ezt nevezzük a triviális G-torzornak.
(2) Legyen $S = Spec(k)$, ahol k test. Tegyük fel, hogy $K|k$ véges Galois-bővítés és legyen $G = Gal(K|k)$. Legyen $\underline{G}_k$ a G-hez tartozó konstans csoportséma k felett. Ekkor $Spec(K)$ egy k feletti $\underline{G}_k$-torzor lesz. Ez az állítás a Galois-elméletből ismert

$$K \otimes_k K \xrightarrow{\cong} \prod_{g \in G} K$$

(G-ekvivariáns) izomorfizmusból következik.

(3) Hasonlóan az előző példához, a 2. fejezetbeli eredményeket felhasználva belátható, hogy ha $B|A$ kommutatív gyűrűk Galois-bővítése G csoporttal, akkor $Spec(B)$ egy $Spec(A)$ feletti $\underline{G}_A$-torzor lesz.

3.3.3. Állítás. *Ha G S-csoportséma, akkor a triviális G-torzor G-ekvivariáns S-automorfizmusainak $Aut_S(G)$ csoportja izomorf lesz a $G(S)$ csoporttal.*

Bizonyítás. Legyen $\psi : G \to G$ egy G-ekvivariáns automorfizmus, ekkor az $e : S \to G$ egység-morfizmussal komponálva ψ-t egy $S \to G$ morfizmust kapunk. Különböző automorfizmusokhoz különböző $S \to G$ morfizmus tartozik, mivel a következő diagram az egység definíciója és a G-ekvivariáns tulajdonság miatt kommutatív lesz

$$\begin{tikzcd} G \times_S S \arrow[r, "id_G \times e"] \arrow[d, equal] & G \times_S G \arrow[r, "id_g \times \psi"] \arrow[d, "m"'] & G \times_S G \arrow[d, "m"'] \\ G \arrow[r, equal] & G \arrow[r, "\psi"] & G \end{tikzcd}$$

Ha adott $\phi : S \to G$ morfizmus, akkor legyen a ψ automorfizmus a következő kompozíció

$$G = G \times_S S \xrightarrow{id_G \times \phi} G \times_S G \xrightarrow{m} G.$$

Könnyen ellenőrizhető, hogy ez valóban G-ekvivariáns morfizmus lesz és így már következik az állítás is. $\square$

3.3.4. Megjegyzés. Vegyük észre, hogy ha X G-torzor, akkor a

$$G \times_S X \to X \times_S X$$

S-izomorfizmus X-izomorfizmus lesz a második koordinátára való projekción keresztül. Ennek felhasználásával belátható, hogy ha Y S-sémára $X(Y) \neq \varnothing$, azaz létezik $Y \to X$ S-morfizmus, akkor $G \times_S Y \to X \times_S Y$ is izomorfizmus lesz. Egyszerűen a $G \times_S X \to X \times_S X$ izomorfizmusra alkalmazzuk az $Y \to X$ morfizmusra vonatkozó báziscserét és használjuk fel a fibrált szorzat tulajdonságait.

3.3.5. Állítás. *Legyen S séma, G S-csoportséma és X G-torzor S felett. X akkor és csak akkor izomorf a triviális G-torzorral, ha $X(S) \neq \varnothing$.*

Bizonyítás. Az előző megjegyzést használva triviális az állítás. Ha X izomorf G-vel, akkor $X(S) = G(S)$ és ez utóbbi nem üres, eleme lesz például az $e : S \to G$ egység.
Ha $X(S)$ nem üres, akkor a megjegyzés miatt $G \cong G \times_S S \cong X \times_S S \cong X$. $\square$

Legyen k test és G sima affin algebrai csoportséma k felett. Jelöljük $Torsor_k(G)$-vel a k feletti G-torzorok izomorfia-osztályainak halmazát. Ha X G-torzor, akkor ebben az esetben belátható, hogy X is affin és sima lesz.

3.3.6. Állítás. *Legyen k test és rögzítsük a k egy k_s szeparábilis lezártját. Tegyül fel, hogy G sima affin algebrai csoportséma k felett és X olyan k-séma, amin adott a G hatása. Ebben az esetben X akkor és csak akkor lesz*

G-torzor, ha $X \times_k Spec(k_s)$ izomorf lesz a triviális $G \times_k Spec(k_s)$-torzorral $Spec(k_s)$ felett.

Bizonyítás. Ha X G-torzor, akkor $X \times_k Spec(k_s)$ $G \times_k Spec(k_s)$-torzor lesz. A G simasága miatt $X \times_k Spec(k_s)$-nek van k_s értékű pontja és ekkor az előző állításból következik a szükségesség. Az elégségesség leszállás segítségével bizonyítható, azonban ez meghaladja a dolgozat kereteit, így ezt nem közöljük.

□

Az előző állítás azt mondja ki, hogy a k feletti G-torzorok nem mások, mint a triviális G-torzor $k_s|k$-formái. Vegyük észre, hogy a $Gal(k_s|k)$ abszolút Galois-csoportnak adott egy hatása az $Aut_{k_s}(G \times_k Spec(k_s))$ csoporton. A továbbiakban jelöljük az X k-sémára $X \times_k Spec(k_s)$-t X_{k_s}-sel. Ha X G-torzor, akkor az $X_{k_s} \to G_{k_s}$ $Spec(k_s)$-izomorfizmusok $P(X, G)$ halmaza $Aut_{k_s}(G_{k_s})$-torzor lesz a $Gal(k_s|k)$ csoport felett. A 3.3.3. Állítás miatt tudjuk, hogy $Aut_{k_s}(G_{k_s}) = G(k_s)$. A 2.8.7. Tételhez hasonlóan létezik $\lambda : Torsor_k(G) \to H^1(k, G(k_s))$ leképezés: ha $x \in P(X, G)$, akkor minden $g \in \Gamma_k$-ra létezik $a_g \in G(k_s)$, hogy $gx = xa_g$. Ez a leképezés is jóldefiniált és a következő igaz rá.

3.3.7. Tétel. *Legyen k test, G sima affin algebrai csoportséma k felett. Ekkor az előbb definiált λ leképezés bijekció lesz a k feletti G-torzorok izomorfiaosztályainak $Torsor_k(G)$ halmaza és a $H^1(k, G(k_s))$ nem-Abel Galois kohomológia-halmaz között.*

Bizonyítás. A λ leképezés azért lesz bijektív, mert G kvázi-projektív, a részletekért lásd [**14**] III.1.3. Proposition 5. □

3.3.8. Megjegyzés. Legyen $K|k$ véges Galois-testbővítés $G = Gal(K|k)$ Galois-csoporttal. Feltehető, hogy K benne van a k egy k_s szeparábilis lezártjában. Vegyük észre, hogy a Galois-elmélet alaptétele szerint létezik $\Gamma_k \to G$ szürjektív homomorfizmus, aminek a magja Γ_K. A $Spec(K)$ $Spec(k)$ feletti $\underline{G}_k$-torzorhoz tartozó elemet szeretnénk meghatározni $H^1(k, \underline{G}_k(k_s))$-ben. Mivel $\underline{G}_k$ konstans csoportséma, ezért Γ_k triviálisan fog hatni rajta, így $H^1(k, \underline{G}_k(k_s)) = H^1(k, G) = Hom(\Gamma_k, G)$. Felhasználva az előző tételbeli és a 2.8.7. Tételbeli expliciten megadott leképezéseket, kiszámolható, hogy ehhez a torzorhoz a fenti $\Gamma_k \to G$ homomorfizmus fog tartozni $H^1(k, G)$-ben.

4. Klasszifikáló és verzális torzorok

3.4.1. Definíció. *Legyen k_0 test és G sima affin algebrai csoportséma k_0 felett. Tegyük fel, hogy X sima, irreducibilis varietás k_0 felett K függvénytesttel, ahol K végesen generált k_0 felett. Legyen Q G-torzor X felett. Azt mondjuk, hogy $Q \to X$ klasszifikáló G-torzor, ha minden $k|k_0$ testbővítésre, ahol k végtelen, minden $T \to Spec(k)$ G-torzorra és minden $U \subseteq X$ nem-üres nyílt részvarietásra létezik olyan $x \in U(k)$, hogy a Q x feletti Q_x fibruma izomorf lesz T-vel.*

3.4.2. Definíció. *Legyen k_0 test, G sima affin algebrai csoportséma k_0 felett és $Q \to X$ klasszifikáló G-torzor. A Q klasszifikáló torzor generikus pont* *feletti P fibrumát verzális torzornak nevezzük. A P verzális torzor K feletti G-torzor lesz.*

3.4.3. Megjegyzés. Legyen X séma és $x, x' \in X$ két pont. Azt mondjuk, hogy x' specializáltja x-nek, ha x' benne van az $\{x\}$ egyelemű halmaz lezártjában. Speciálisan, ha X-nek létezik generikus pontja, akkor az X minden pontja a generikus pont specializáltja. Ebben az értelemben mondhatjuk tehát, hogy a verzális torzor specializáltjaként megkapható minden k feletti G-torzor minden $k|k_0$ testbővítésre.

A következő két példa mutatja, hogy léteznek verzális torzorok.

3.4.4. Példa.

(1) A fenti jelöléseket használjuk. Tudjuk, hogy G beágyazható zárt részcsoportként GL_n-be. Válasszuk X-nek a GL_n/G homogén teret és legyen $Q = GL_n$. Ekkor $Q \to X$ klasszifikáló G-torzor lesz, speciálisan a generikus pont feletti fibruma pedig verzális torzor lesz. Legyen k végtelen test k_0 felett és $T \to Spec(k)$ G-torzor. Ha ebben a szituációban alkalmazzuk a 2.8.8. Állításbeli egzakt sorzatot, akkor a következőt kapjuk

$$1 \to H^0(k, G(k_s)) \to H^0(k, GL_n(k_s)) \to H^0(k, GL_n(k_s)/G(k_s)) \to$$
$$\to H^1(k, G(k_s)) \to H^1(k, GL_n(k_s))$$

A Hilbert 90-es tétel miatt tudjuk, hogy minden GL_n-torzor triviális, ezért minden k feletti G-torzor megfeleltethető a $GL_n(k_s)/G(k_s)$ egy Γ_k-invariáns elemének, azaz egy $x \in X(k) = GL_n(k)/G(k)$ ponthoz jutottunk. Felhasználva a 2.8.9. Következményt, azt kapjuk, hogy létezik olyan $x \in X(k)$, hogy $Q_x \cong T$ és minden ilyen x egyértelműen meghatározott a $GL_n(k)$ $X(k)$-n való hatásának erejéig. Mivel k végtelen, ezért belátható, hogy az x orbitja is sűrű lesz X-ben és ezzel készen vagyunk.

(2) A klasszifikáló torzorok fogalma általánosítása a 1.3.1. Definícióban megismert generikus Galois-bővítésnek. Legyen adott a k_0 alaptest és tegyük fel, hogy adott a $B|A$ generikus Galois-bővítés k_0-ra és G-re. Nézzük a G-hez tartozó k_0 feletti konstans $\underline{G}_{k_0}$ csoportsémát. Ekkor $X = Spec(A)$ egy k_0 feletti irreducibilis varietás lesz, melynek a függvényteste végesen generált bővítése lesz k_0-nak a 1.3.1. Definíció (1) pontja miatt. Láttuk, hogy $Q = Spec(B)$ egy $\underline{G}_{k_0}$-torzor lesz $X = Spec(A)$ felett. Ha k egy k_0-t tartalmazó test, akkor a $Spec(C)$ alakú, $Spec(k)$ feletti $\underline{G}_{k_0}$-torzorok nem lesznek mások, mint a $C|k$ Galois-bővítések G csoporttal. A 1.3.1. Definíció (2) pontja pontosan azt mondja ki, hogy X-nek létezik olyan k értékű pontja (azaz egy $A \to k$ homomorfizmus), hogy az efölötti fibrum izomorf lesz a $Spec(C)$-vel (azaz a $B \otimes_A k$ "fibrum" izomorf lesz C-vel).

3.4.5. Megjegyzés. Legyen most G véges csoport és tegyük fel, hogy adott a G hűséges, lineáris hatása a V n dimenzós k_0 feletti vektortéren. Legyen

$U = V \setminus \cup_{1 \neq g} ker(g-1)$. Ekkor $Spec(k[U]) \to Spec(k[U]^G)$ klasszifikáló G-torzor lesz. A generikus ponthoz tartozó fibrum, tehát a verzális torzor ebben az esetben $Spec(k(V)) \to Spec(k(V)^G)$ lesz. Az állítás általánosabban is igaz, bizonyításért lásd [**6**] Example 5.4.

4. FEJEZET

Noether-probléma és kohomologikus invariánsok

A fejezet fő eredménye az, hogy ha G olyan csoport, amelynek 2-Sylow-részcsoportja 2^m $(m \geq 3)$ rendű ciklikus csoport, akkor G nem rendelkezik a Noether-tulajdonsággal $\mathbb{Q}$ felett. Mivel a Noether-tulajdonság nehezen vizsgálható, ezért először definiálunk egy új fogalmat csoportokra és testekre, mely gyengébb lesz, mint a Noether-tulajdonság, azonban jól kezelhető kohomologikus módszerekkel. Ez a tárgyalás, a fő eredményünkkel együtt a 3. részben található. Célunk felé haladva szükségünk lesz két nehéz és fontos tételre, ezek tárgyalását a fejezet utolsó két részére halasztottuk.

1. Noether-probléma

A továbbiakban G véges csoportot fog jelölni. A következő kérdéssel már találkoztunk a bevezetésben.

4.1.1. Definíció. *Legyen k_0 test. Azt mondjuk, hogy a G csoport rendelkezik a Noether-tulajdonsággal (k_0 felett), ha létezik olyan $\rho : G \to GL_n(k_0)$ beágyazás, hogy K_ρ racionális (tiszta transzcendens) bővítése k_0-nak, ahol $K_\rho = k_0(x_1, \ldots, x_n)^G$.*

Noether-problémának nevezzük azt a kérdést, hogy adott G csoportra és k_0 testre G rendelkezik-e a Noether-tulajdonsággal k_0 felett.

A Noether-problémához szorosan kapcsolódik a következő kérdés. Saltman 1.3.2. Tétele szerint, ha k_0 végtelen test és K_ρ a k_0 racionális bővítése, akkor létezik generikus Galois-bővítés k_0-ra és G-re nézve. Láttuk, hogy a generikus Galois-bővítés fogalmát általánosítja a verzális torzor fogalma, ezért természetes a következő definíció.

4.1.2. Definíció. *Legyen k_0 test, G véges csoport. Azt mondjuk, hogy G racionális k_0 felett, ha létezik $K|k_0$ testbővítés és T G-torzor K felett úgy, hogy $K|k_0$ racionális bővítés és T verzális torzor.*

4.1.3. Állítás. *Legyen k_0 test. Ha G rendelkezik a Noether-tulajdonsággal k_0 felett, akkor racionális k_0 felett.*

Bizonyítás. A $G \hookrightarrow GL_n(k_0)$ beágyazás a 3.4.4. Példa (2) pontjához hasonlóan verzális torzort definiál a fixtest felett és ez a fixtest a Noether-tulajdonság miatt racionális. □

Látjuk tehát, hogy a G csoport k_0 feletti racionalitása gyengébb tulajdonság, mint a Noether-tulajdonság eldöntése G-re és k_0-ra, azonban a torzorok miatt az előbbi vizsgálható lesz kohomologikus keretek között, ami végeredményben egy szükséges feltételt fog adni nekünk a G racionalitásának eldöntéséhez.

2. Kohomologikus invariánsok

Legyen $K|k_0$ testbővítés és C diszkrét Γ_{k_0}-modulus. Tudjuk, hogy ekkor létezik $\Gamma_K \to \Gamma_{k_0}$ folytonos homomorfizmus, így értelmezhetőek a $H^i(K,C)$ kohomológia-csoportok (és ezek izomorfia erejéig függetlenek az abszolút Galois-csoportok közötti leképezés megválasztásától). Jelöljük a $\oplus_i H^i(K,C)$ direkt összeget $H(K,C)$-vel.

Legyen G sima affin algebrai csoportséma k_0 felett. Nézzük a $Torsor_G(K)$-t, vagyis a K feletti G-torzorok izomorfiaosztályainak halmazát. Láttuk, hogy a K feletti G-torzorokat az első nem-Abel kohomológia-halmaz, $H^1(K, G(K_s))$ klasszifikálja, a továbbiakban így lesz célszerű tekinteni $Torsor_G(K)$-ra.

Szeretnénk minden $K|k_0$ testbővítéshez és minden T K feletti G-torzorhoz hozzárendelni egy $a_K(T)$ kohomológia osztályt $H(K,C)$-ben úgy, hogy a következő kompatibilitási feltétel teljesüljön: ha $K|k_0$ és $K'|k_0$ két testbővítés és $\phi : K \to K'$ egy k_0-homomorfizmus, akkor jelöljük ϕ_*-gal a ϕ által indukált leképezést $H^1(K,G)$ és $H^1(K',G)$ (ill. $H(K,C)$ és $H(K',C)$) között. Ekkor azt szeretnénk, ha a következő diagram kommutatív lenne

$$\begin{array}{ccc} H^1(K,G) & \xrightarrow{\phi_*} & H^1(K',G) \\ {\scriptstyle a_K}\big\downarrow & & {\scriptstyle a_{K'}}\big\downarrow \\ H(K,C) & \xrightarrow{\phi_*} & H(K',C), \end{array}$$

vagyis $\phi_*(a_k(T)) = a_{K'}(\phi_*(T_{K'}))$, ahol $T_{K'}$ a T torzorból $Spec(K') \to Spec(K)$ bázisbővítéssel kapott K' feletti G-torzor.

Ezt a következőképpen lehet formalizálni. Vegyük észre, hogy $H^1(-,G)$ ill. $H(-,C)$ funktorok a k_0 testbővítéseinek $Fields_{k_0}$ kategóriájából a halmazok Set ill. az Abel-csoportok Ab kategóriájába. Ekkor az a hozzárendelés nem lesz más, mint egy $H^1(-,G) \Rightarrow H(-,C)$ természetes transzformáció (ahol $H(-,C)$ az $Ab \to Set$ felejtő funktorral komponálva képez Set-be).

4.2.1. DEFINÍCIÓ. *Az $a : H^1(-,G) \Rightarrow H(-,C)$ természetes transzformációt másképpen kohomologikus invariánsnak nevezzük. A kohomologikus invariánsok halmazát $Inv(G,C)$-vel jelöljük.*

4.2.2. PÉLDA.

(1) Létezik $H(k_0,C) \to Inv(G,C)$ természetes beágyazás. Ha $h \in H(k_0,C)$, akkor minden $K|k_0$ testbővítésre nézzük h képét $H(K,C)$-ban és minden $H^1(K,G)$-beli elemhez rendeljük hozzá ezt az elemet. Könnyen látható, hogy ez az a_h leképezés kohomologikus invariáns lesz. Az ilyen alakú invariánsokat *konstans invariánsok*nak nevezzük.

(2) A $H^1(K,G)$ halmaz pontozott halmaz, a bázispont a triviális torzorhoz tartozó kohomológia osztály. Ha $K \to K'$ egy k_0-homomorfizmus, akkor a bázispont képe bázispont lesz a leképezés által indukált $H^1(K,G) \to H^1(K',G)$ leképezésnél. Legyen $a \in$

$Inv(G, C)$ kohomologikus invariáns. Azt mondjuk, hogy *a normalizált*, ha minden bázisponton eltűnik (0-ba képezi le). Minden invariáns egyértelműen írható fel egy konstans és egy normalizált invariáns összegeként.

3. Kohomologikus invariánsok egyenlősége és verzális torzorok

Legyen G sima affin algebrai csoportséma k_0 felett és A olyan véges Γ_{k_0}-modulus, amely rendje nem osztható a k_0 test karakterisztikájával. Tegyük fel, hogy adott egy P verzális G-torzor. Tudjuk, hogy minden $k|k_0$ testbővítésre és minden T k feletti G-torzorra T előáll, mint a P specializációja. Emiatt azt sejthetjük, hogy egy kohomologikus invariánst a P-n felvett értéke már meghatározza.

4.3.1. DEFINÍCIÓ. *Legyen R kommutatív, Noether lokális gyűrű, jelöljük $\mathfrak{m}$-mel a maximális ideálját. Azt mondjuk, hogy R reguláris lokális gyűrű, ha az $\mathfrak{m}$ maximális ideál minimális elemszámú generátorrendszerének elemszáma megegyezik az R gyűrű Krull-dimenziójával.*

4.3.2. TÉTEL. *Tegyük fel, hogy k_0 végtelen test. Legyen $P \in H^1(K, G)$ verzális torzor (lásd 3.4.1. Definíció) és legyenek $a, b \in Inv_{k_0}(G, C)$ kohomologikus invariánsok. Ha $a(P) = b(P)$ $H(K, C)$-ben, akkor $a = b$.*

BIZONYÍTÁS. Feltehető, hogy $b = 0$, mert a-t lecserélhetjük $a - b$-re. Azt kell megmutatnunk, hogy ha $k|k_0$ testbővítés és T k feletti G-torzor, akkor $a(T) = 0$. Mivel P verzális torzor, ezért létezik olyan $x \in X(k)$, hogy T és Q_x izomorfak. Legyen R az $X_{/k}$ x-beli lokális gyűrűje, K_x az $X_{/k}$ hányadosteste, ez az $X_{/k}$ függvényteste. Az x maradékteste k lesz. Mivel X sima, ezért R reguláris lokális gyűrű lesz. Jelöljük Q_R-rel a Q visszahúzottját a $Spec(R) \to X$ leképezésre nézve.

$$\begin{array}{ccc} Q_R & \longrightarrow & Q \\ \big\downarrow & & \big\downarrow \\ Spec(R) & \longrightarrow & X \end{array}$$

A Q_R x-beli fibruma T lesz, míg a továbbiakban P_x-szel jelölt generikus fibrumát pedig P-ből kapjuk a $K \to K_x$ báziscserével, ezért $a(P_x)$ 0 lesz.

Az R dimenziója szerinti indukcióval folytatjuk a bizonyítást. Legyen $dim(R) = 1$, ekkor R diszkrét értékelésgyűrű lesz, legyen v a hozzá tartozó értékelés. Ha R nem teljes, akkor tegyük teljessé, a v diszkrét értékelés kiterjed a teljes burokra, a hányadostest pedig $k((t))$ lesz. A P_x torzor a $K_x \to k((t))$ leképezéssel kiterjeszthető P' torzorrá. Mivel $a(P_x) = 0$, ezért $a(P')$ is 0 lesz. Jelölje i a $k \to k((t))$ által indukált $H^1(k, G) \to H^1(k((t)), G)$ leképezést. Belátható, hogy az i-nél a T képe pont a P' torzor lesz. A következő diagram kommutativitása ill. az alsó sor egzaktsága miatt

$$\begin{array}{ccccccccc} & & H^1(k,G) & \xrightarrow{i} & H^1(k((t)),G) & & & & \\ & & {\scriptstyle a_k}\big\downarrow & & {\scriptstyle a_{k((t))}}\big\downarrow & & & & \\ 0 & \longrightarrow & H(k,C) & \xrightarrow{Inf} & H(k((t)),C) & \xrightarrow{r_v} & H(k,C(-1)) & \longrightarrow & 0, \end{array}$$

az $a(P')$ értéke v-nél $a(T)$ (az $a(P')$-nek azért van értéke v-nél, mert a diagramról az is leolvasható, hogy a reziduuma v-nél 0). De $a(P') = 0$, ezért $a(T) = 0$ és ez kellett nekünk.

Most tegyük fel, hogy R dimenziója s és legyenek az $\mathfrak{m}$ generátorai $t_1, \ldots, t_s$. Az R/t_1R reguláris gyűrű dimenziója $s-1$ lesz, legyen K' a hányadosteste. Az 1 dimenziós eset miatt $a(T_{K'}) = 0$ lesz.Az R' gyűrűre és K' testre alkalmazva az indukciós feltételt kapjuk, hogy $a(T_k) = 0$. □

4. Alkalmazás a racionalitási problémára

Ebben a részben párhuzamosan két dolgot fogunk kidolgozni: egyrészt adott G csoport k_0 feletti racionalitásának látjuk majd egy szükséges feltételét és a $\mathbb{Z}/2^m\mathbb{Z}$ egy konkrét kohomologikus invariánsára alkalmazzuk ezt a szükséges feltételt. A szükséges feltétel azt mondja ki, hogy ha G racionális k_0 felett, akkor egy megfelelő tulajdonságokkal rendelkező kohomologikus invariánsnak 0-nak kell lennie. A példánk esetén pedig azt fogjuk látni, hogy van olyan - a megfelelő tulajdonságokkal rendelkező - kohomologikus invariánsa $\mathbb{Z}/2^m\mathbb{Z}$ csoportnak, ami felvesz nem-0 értéket.

A továbbiakban a k_0 alaptestről feltesszük, hogy nem 2 karakterisztikájú, G véges csoport, C véges Γ_{k_0}-modulus és legyen $K|k_0$ végesen generált bővítés.

A példánkban szereplő G csoport a $\mathbb{Z}/2^m\mathbb{Z}$ ($m \geq 3$) ciklikus csoport lesz, C-nek pedig válasszuk a $\mathbb{Z}/2\mathbb{Z}$ ciklikus csoportot. Először lássunk példát $\mathbb{Z}/2^m\mathbb{Z}$ egy kohomologikus invariánsára.

4.4.1. Konstrukció. Legyen $K|k_0$ testbővítés. A $\mathbb{Z}/2^m\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ leképezés indukál $H^1(K, \mathbb{Z}/2^m\mathbb{Z}) \xrightarrow{d} H^1(K, \mathbb{Z}/2\mathbb{Z})$ leképezést ("mod 2 redukció"). Jelöljük (2)-vel a $2 \in K$ elem képét a Kummer-izomorfizmusnál (miután azonosítottuk $H^1(K, \mu_2)$-t $H^1(K, \mathbb{Z}/2\mathbb{Z})$-vel). Nézzük a következő b kohomologikus invariánst:

$$\begin{aligned} b_K : H^1(K, \mathbb{Z}/2^m\mathbb{Z}) &\to H(K, \mathbb{Z}/2\mathbb{Z}) \\ x &\mapsto (2) \cup d(x) \end{aligned}$$

A redukció-leképezés és a cup-szorzat természetessége miatt ez valóban kohomologikus invariáns lesz. Fontos megjegyezni, hogy b normalizált kohomologikus invariáns, mivel d is az. Vegyük még észre továbbá azt is, hogy minden $x \in H^1(K, \mathbb{Z}/2^m\mathbb{Z})$-re $b(x)$ a $H^2(K, \mathbb{Z}/2\mathbb{Z})$ eleme lesz, vagyis a Brauer-csoport 2-torzió-részcsoportjának egy elemét határozza meg.

A reziduum leképezés segítségével definiáljuk $H(K, C)$ egy részcsoportját és belátjuk, hogy ha $K|k_0$ racionális bővítés, akkor ez a bizonyos részcsoport csak konstans, azaz $H(k_0, C)$-ből származó kohomológia osztályokból áll.

Emlékeztetünk a korábban definiált reziduum leképezésre: ha v diszkrét értékelés K-n, akkor létezik a következő leképezés

$$r_v : H^n(K, C) \to H^{n-1}(k(v), C(-1)).$$

A következő fogalom definícióját a Fagyejev egzakt sorozat és a 2.7.3. Tétel motiválja.

4.4.2. DEFINÍCIÓ. *Azt mondjuk, hogy $\alpha \in H(K, C)$ kohomológia osztály nemelágazó k_0 felett, ha K minden olyan v diszkrét értékelésére, ami triviális k_0-n, az α v-nél vett reziduuma 0. A $H^n(K, C)$ kohomológia-csoport k_0 felett nemelágazó elemeinek részcsoportját $H^n_{nr}(K|k_0, C)$-vel fogjuk jelölni.*

Vizsgáljuk meg először az előző fogalmat az $n = 1$ esetben a konkrét példánkban. Ebben az esetben a reziduuma leképezés az alábbi

$$r_v : H^1(K, \mathbb{Z}/2\mathbb{Z}) \to \mathbb{Z}/2\mathbb{Z}$$
$$(\alpha) \mapsto v(\alpha)\ mod\ 2$$

leképezés lesz, ahol (α) az $\alpha \in K^\times$ elem Kummer-izomorfizmusnál vett képe lesz.

Ha most $K = k_0(x_1, \dots, x_n)$ racionális bővítés, akkor vizsgáljuk meg a $H^1_{nr}(K|k_0, \mathbb{Z}/2\mathbb{Z})$ csoportot. Egyrészt, ha $\alpha \in k_0^\times$, akkor $r_v(\alpha) = 0$ minden v diszkrét értékelésre, mert v triviális k_0-n. Másrészt, tegyük fel, hogy $\alpha \in K^\times$ eleme $H^1_{nr}(K|k_0, \mathbb{Z}/2\mathbb{Z})$-nek. Egy megfelelő négyzettel felszorozva feltehető, hogy $\alpha \in K[x_1, \dots, x_n]$. Tudjuk, hogy $K[x_1, \dots, x_n]$ egyértelmű faktorizációs tartomány, bontsuk fel α-t irreducibilis elemek szorzatára, legyen π egy faktora. A π elemhez tartozik egy v_π diszkrét értékelés K-n és ez triviális lesz k_0-n. A feltétel miatt $r_{v_\pi}(\alpha) = v_\pi(\alpha) = 0$ (mod 2), vagyis π^2 is osztja α-t, így azt kapjuk, hogy $\alpha = c\beta^2$, ahol $c \in k_0^\times$ és $\beta \in K^\times$. De akkor $(\alpha) \in H^1(K, \mathbb{Z}/2\mathbb{Z})$ osztály egyenlő lesz (c)-vel, vagyis (α) konstans kohomológia osztály. Azt kaptuk tehát, hogy $H^1_{nr}(K|k_0, \mathbb{Z}/2\mathbb{Z}) = H^1(k_0, \mathbb{Z}/2\mathbb{Z})$, ha $K|k_0$ racionális bővítés.

Ennek nagymértékű általánosítása a következő állítás.

4.4.3. ÁLLÍTÁS. *Ha $K|k_0$ racionális bővítés, akkor a $H(K, C)$ minden nemelágazó kohomológia osztálya konstans, azaz $H(k_0, C)$-ből származik. Megfordítva, minden konstans kohomológia osztály nemelágazó, tehát $H_{nr}(K|k_0, C) = H(k_0, C)$.*

BIZONYÍTÁS. Az állítás a 2.7.3. Tételből következik, mivel az irreducibilis hiperfelületekhez tartozó értékelések triviálisak k_0-n. □

4.4.4. DEFINÍCIÓ. *Legyen $a \in Inv(G, C)$ kohomologikus invariáns. Azt mondjuk, hogy az a nemelágazó, ha minden $K|k_0$ végesen generált testbővítésre és minden T G-torzorra K felett, az $a(T) \in H(K, C)$ kohomológia osztály nemelágazó k_0 felett.*

Nem meglepő módon a példánkban szereplő invariáns rendelkezik ezzel a tulajdonsággal.

4.4.5. ÁLLÍTÁS. *A fent definiált $b \in Inv(\mathbb{Z}/2^m\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ kohomologikus invariáns nemelágazó.*

BIZONYÍTÁS. Legyen k olyan testbővítése k_0-nak, ami teljes egy olyan v diszkrét értékelésre nézve, ami k_0-n triviális. Tudjuk, hogy ekkor létezik a következő rövid egzakt sorozat, ahol I az inercia csoport

$$1 \to I \to \Gamma_k \to \Gamma_{k_0} \to 1.$$

Legyen $x \in H^1(k, G) = Hom(\Gamma_k, G)$ és jelöljük az x-hez tartozó $\Gamma_k \to G$ homomorfizmust ϕ_x-szel. Ha $\phi_x(I) \neq G$, akkor az $d(x)$ reziduuma 0 lesz, mivel ebben az esetben a reziduum leképezés nem más, mint a megszorítási leképezés és az $I \xrightarrow{\phi_x} G \to C$ kompozíció 0 lesz a feltétel miatt. Emiatt $b(x)$ nemelágazó lesz. Ha $\phi_x(I) = G$, akkor a maradéktest tartalmazni fogja a 2^m-edik egységgyököket, $m \geq 3$ miatt pedig 2 négyzet lesz a maradéktestben, így 2 lesz k-ban is, tehát $b(x) = 0$, vagyis ebben az esetben is nemelágazó. □

Térjünk vissza az általános eset vizsgálatára. Tegyük fel, hogy a G csoport racionális k_0 felett, ekkor létezik $K|k_0$ racionális bővítés és P K feletti verzális G-torzor. Mivel $K|k_0$ racionális, ezért $H_{nr}(K, C)$ minden eleme konstans. Ha $a \in Inv(G, C)$ nemelágazó kohomologikus invariáns, akkor a verzális torzorhoz tartozó $a(P)$ kohomológia osztály is konstans lesz. Mivel minden $k|k_0$ testbővítésre a T k feletti G-torzorok megkaphatóak a P specializáltjaiként, ezért azt várjuk, hogy az a invariánst meghatározza a P-n felvett értéke. A következő tétel szerint, ha az $a(T)$ osztály konstans, akkor már az a kohomologikus invariáns is konstans lesz.

4.4.6. ÁLLÍTÁS. *Ha G racionális k_0 felett és $a \in Inv(G, C)$ nemelágazó kohomologikus invariáns, akkor a konstans.*

BIZONYÍTÁS. Láttuk, hogy az $a(P) \in H(K, C)$ osztály konstans, azaz $a_0 \in H(k_0, C)$ osztályból jön, vagyis $a(T) = a_0(T)$. Ekkor az 4.3.2. Tétel miatt a konstans. □

4.4.7. KÖVETKEZMÉNY. *Ha G racionális k_0 felett és $a \in Inv(G, C)$ normalizált nemelágazó kohomologikus invariáns, akkor $a = 0$.*

Ezt a következmény alapvető fontosságú: adott G csoportra és k_0 alaptestre, ha tudunk olyan nemelágazó, normalizált kohomologikus invariánst konstruálni, ami nem azonosan 0, akkor G nem rendelkezhet a racionalitási tulajdonsággal k_0 felett, így a Noether-tulajdonsággal sem.

Most térjünk vissza a $\mathbb{Z}/2^m\mathbb{Z}$ csoporthoz és b kohomologikus invariánshoz. Mivel bizonyítottuk, hogy b normalizált és nemelágazó, ezért az előző következmény szerint, elég belátni, hogy b nem a konstans 0 kohomologikus invariáns $\mathbb{Q}$ felett.

4.4.8. ÁLLÍTÁS. *Ha $k_0 = \mathbb{Q}$, akkor a b invariáns nem lesz 0.*

BIZONYÍTÁS. Ha $k_0 = \mathbb{Q}$, akkor legyen $k = (Q)_2$ és k' legyen a $\mathbb{Q}_2$ 2^m fokú, nemelágazó bővítése, ennek a Galois-csoportja pont $\mathbb{Z}/2^m\mathbb{Z}$ lesz. Belátható (lásd [**8**] Proposition 5.5.11), hogy $k' = k(\epsilon)$, ahol ϵ egy primitív $2^{2^m} - 1$-edik egységgyök. Mivel $m \geq 3$, ezért $5 | 2^{2^m} - 1$, így $\sqrt{5} \in k'$ és $\mathbb{Q}_2(\sqrt{5})|\mathbb{Q}_2$ részbővítése lesz $k'|\mathbb{Q}_2$-nek.
Legyen $x \in H^1(k, \mathbb{Z}/2^m\mathbb{Z})$ a k' által meghatározott torzorhoz tartozó kohomológia osztály. Láttuk, hogy $H^1(k, \mathbb{Z}/2^m\mathbb{Z}) = Hom(\Gamma_k, \mathbb{Z}/2^m\mathbb{Z})$-ben az x-hez a természetes $\Gamma_k \to \mathbb{Z}/2^m\mathbb{Z}$ homomorfizmus fog tartozni. Ha ezt komponáljuk a $\mathbb{Z}/2^m\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ redukcióval, akkor a kapott homomorfizmus

pont a $\mathbb{Q}_2(\sqrt{5})|\mathbb{Q}_2$ bővítés által meghatározott torzorhoz tartozó homomorfizmus lesz. A Kummer-izomorfizmus miatt pedig azt látjuk, hogy ez utóbbi megegyezik az $(5) \in k^\times/k^{\times 2} \cong H^1(k, \mathbb{Z}/2\mathbb{Z})$ kohomológia osztállyal.
Összefoglalva, $b(x) \in H^2(k, \mathbb{Z}/2^m\mathbb{Z})$ a $(2) \cup (5)$ cup-szorzat lesz. Mivel $\mathbb{Q}_2$-ben nincsenek olyan x, y és z számok, hogy $2x^2 + 5y^2 = z^2$, ezért a $b(x)$ osztály a 2.11.10. Megjegyzés miatt nem lesz triviális, így a b invariáns sem triviális. $\square$

4.4.9. KÖVETKEZMÉNY. *A $\mathbb{Z}/2^m\mathbb{Z}$ csoport a $\mathbb{Q}$ test felett nem rendelkezik a Noether-tulajdonsággal.*

Többet is lehet még mondani.

4.4.10. ÁLLÍTÁS. *Legyen G olyan csoport, melynek 2-Sylow-részcsoportja ≥ 8-adrendű ciklikus csoport. Ekkor G nem racionális $\mathbb{Q}$ felett, így nem rendelkezik a Noether-tulajdonsággal sem.*

BIZONYÍTÁS. Legyen S a G csoport 2-Sylow-részcsoportja. Mivel S ciklikus, ezért Burnside normális komplementum-tételének egy következménye miatt (lásd [**13**] 6.2.11.), S-nek létezik normális komplementuma, ezt N-nel fogjuk jelölni. A $G \xrightarrow{\pi} S$ természetes projekció a kohomológiákban szürjektív leképezést indukál, mivel az

$$S \hookrightarrow G \xrightarrow{\pi} S$$

kompozíció az S identitása lesz, így áttérve a kohomológiákra

$$H^1(K, S) \to H^1(K, G) \xrightarrow{\pi_*} H^1(K, S)$$

a kompozíció itt is az identitás lesz, így a második leképezés valóban szürjektív. Sőt, az előző állításbeli b kohomologikus invariáns is meghatároz egy G-hez tartozó a invariánst. Mivel b normalizált és nemelágazó, ezért a is rendelkezik ezekkel a tulajdonságokkal. Legyen k a $\mathbb{Q}$ olyan bővítése, amire létezik olyan $t \in H^1(k, S)$, hogy $b(t) \neq 0$. A $H^1(k, G) \to H^1(k, S)$ leképezés szürjektivitása miatt ekkor $a(t)$ sem lesz nulla. $\square$

Irodalomjegyzék

[1] M. F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969

[2] G. Berhuy, *An Introduction to Galois Cohomology and its Applications*, London Mathematical Society Lecture Note Series, vol. 377, Cambridge University Press, 2010

[3] J. W. S. Cassels, A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967

[4] S.U. Chase, D.K. Harrison, A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. , 52 (1965), Amer. Math. Soc., 1-19.

[5] J.-L. Colliot-Thélène, J.-J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups (with special regards to the rationality problem)*, Proceedings of the International Colloquium on Algebraic groups and Homogeneous Spaces (Mumbai 2004), ed. V. Mehta, TIFR Mumbai, Narosa Publishing House (2007), 113-186.

[6] S. Garibaldi, A. Merkurjev, J.-P. Serre, *Cohomological Invariants in Galois Cohomology*, University Lecture Series, vol. 28, A.M.S., Providence, RI, 2003

[7] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge studies in advanced mathematics, vol. 101, Cambridge University Press, 2006

[8] F. Q. Gouvea, *p-adic Numbers: an Introduction*, 2nd edition, Universitext, Springer-Verlag, Berlin, Heidelberg, 1997

[9] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, Berlin, New York, 1977

[10] S. Mac Lane, *Categories for the Working Mathematician*, 2nd edition, Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998

[11] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2000

[12] D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math., 43 (1982), 250-283.

[13] W. R. Scott, *Group theory*, Dover Publications Inc., New York, 1987

[14] J.-P. Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Corrected Second Printing of the First English Edition of 1997, Springer-Verlag, Berlin-Heidelberg-New York, 2002

[15] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd edition, Braunschweig, Germany: Vieweg, 1997.

[16] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979

[17] R. G. Swan, *Noether's problem in Galois theory*, in *Emmy Noether in Bryn Mawr: Proceedings of a Symposium in Honor of Emmy Noether's 100th Birthday*, B. Srinivasan, J. D. Sally (eds.) Spinger-Verlag, New York-Berlin-Heidelberg-Tokyo, 1983

[18] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979