Eötvös Loránd Tudományegyetem

Természettudományi Kar

Schefler Barna

Centrális egyszerű algebrák

BSc Matematikus Szakdolgozat

Témavezető:

Zábrádi Gergely

Algebra és Számelmélet Tanszék

Budapest, 2020

Köszönetnyilvánítás

Köszönettel tartozom Zábrádi Gergely tanár úrnak, aki 4 féléven keresztül tanított nekem algebrát olyan lendülettel, hogy az egyből a kedvenc tárgyammá vált. Sokat számított nekem, hogy az órán nem csak a tantervben szereplő anyagot adta le, hanem amint befejeztük a kötelező részeket, egyből rátértünk az érdekességekre. Ennek lenyomata határozottan fellelhető ezen dolgozatban is, hiszen minden fejezetben valami olyan témát járok körül, amiből már kaptunk ízelítőt az algebra kurzusok folyamán. Köszönettel tartozok azért is, mert elvállalta, hogy vele írjam a dolgozatot, és óriási lelkiismerettel küldözgette a javított változatokat, tartotta a konzultációkat.

Köszönettel tartozom továbbá az összes egyetemi tanáromnak. Hiszem, hogy az olyan befogadó, tiszteletteljes, megértő közeg, amilyen a Matematika Intézetben van, a lehető legjobban segíti a hallgatók tanulmányait.

Ezen felül meg kell említenem édesanyámat, Schefler Enikőt, és iskolai matematikatanáromat Polcz Zitát, akik elindítottak az úton, valamint testvéremet Gergőt, aki viszi előttem a fáklyát. Köszönet a családom többi részének: Imolának, Tamásnak és Ervinnek, akik megteremtik a szükséges háttért, valamint köszönet a Pásztornak a gondviselésért.

Köszönet a Márton Áron Szakkollégiumnak, hogy támogatta a dolgozat létrejöttét.

Tartalomjegyzék

1. fejezet

Előszó

Ezen dolgozat fő mozgatórugója - mint ahogy a cím is mutatja - a centrális egyszerű algebrák elméletének a tanulmányozása. Elméleti szakirányon, Algebra 4 kurzus folyamán a Galois-elmélet körében találkoztunk először ezzel a témakörrel, mely később a szakdolgozati témám lett.

1.1. Kvaternióalgebrák

A második fejezet - mely a kvaternióalgebrák elméletének megértéséről szól - bevezetőként szolgál a fő téma előtt, valamint kitérünk a témakör egyik legfontosabb tételére is (2.4.3 - Witt tétele). A fejezet forrása a Philippe Gille - Tamás Szamuely Central Simple Algebras and Galois Cohomology című könyvének 1. fejezete. Felépítését tekintve előbb a bevezető fogalmakkal ismerkedünk (2.1 alfejezet), majd bizonyítunk néhány alapvető tételt, melyre szükségünk lesz a továbbiakban (2.2 alfejezet). A (2.3) alfejezetben egy új megközelítéssel élünk: a korábban bevezetett (a, b) kvaternióalgebrához (2.1.5 definíció) hozzárendeljük a projektív sík egy kúpszeletét (2.3.1 definíció), és levonjuk a következtetéseket. A (2.4) alfejezetben tárgyaljuk a fejezet legfontosabb tételét, Witt tételét, mely az előző részben bizonyítottakra épít.

A kvaterniók megértéséhez segítségünkre lehet az alábbi gondolatmenet:

Tekintsük a következő jólismert másodfokú egyenletet: $x^2 - 1 = 0$
Két gyöke könnyen megtalálható például a másodfokú egyenlet megoldóképletének használatával:

$$x_{1,2} = \frac{-0 \pm \sqrt{0-4(-1)}}{2} = \pm 1$$

Mi történik azonban, ha a következő egyenletünk van: $x^2 + 1 = 0$?
A megoldóképletben a gyökjel alatt negatív mennyiség jelenik meg, így ahhoz, hogy az egyenletet megoldhassuk, be kell vezessük a komplex számokat. -1 négyzetgyökét i szimbólummal jelölve a komplex számok $z = a + bi$ alakban írhatóak, ahol $a, b \in \mathbb{R}$. A komplex számok $\mathbb{C}$ halmaza testet alkot a (persze értelmes módon definiált komplex) összeadásra és szorzásra nézve. Ez a test a valós számok testének másodfokú bővítése.

A komplex számok a matematika számos ágában nagy sikerrel alkalmazhatóak. Ezek közé tartozik többek között a síkon való ábrázolás is: egy komplex számot könnyen meg lehet feleltetni a sík egy pontjának. Ennek mintájára William Rowan Hamilton ír matematikus olyan testet keresett, mely elemeivel a háromdimenziós teret lehet leírni. Hosszas gondolkozás után azonban rájött, hogy erre nincs esélye, viszont 4 dimenzióban több sikerrel járhat. Így jöttek létre a kvaterniók, amelyek képzéséhez szükségünk lesz i, j, k képzetes elemekre, mégpedig a következő módon:

$$i^2 = -1, j^2 = -1, ij = -ji = k.$$

A precízebb definíciót későbbre hagyjuk, azonban megjegyezzük, hogy Hamilton túlteljesítette a kitűzött célt: a kvaternióknak sok érdekes tulajdonságuk van, amellyel megéri önmagában is foglalkozni. A három dimenziós tér leírására pedig alkalmasak a tisztán képzetes kvaterniók (olyan kvaterniók, amelyeket csupán i, j, k generálják). További észrevétel, hogy a kvaterniók nem alkotnak testet, ugyanis a kommutativitás már a báziselemekre sem teljesül. Az viszont igaz, hogy ferdetestet alkotnak.

1.2. Centrális egyszerű algebrák

A fő témával, a centrális egyszerű algebrákkal a harmadik fejezetben foglalkozunk, itt forrásként használtam az órai jegyzeteimet, Zábrádi Gergely Centrális egyszerű algebrák osztályozása című jegyzetét, valamint Philippe Gille - Tamás Szamuely Central Simple Algebras and Galois Cohomology című könyvének a 2.1 valamint 2.2 fejezeteit. A (3.1) alfejezet Wedderburn tételének (3.1.1) felvázolásáról és bizonyításáról szól, a (3.2) pedig a centrális egyszerű algebrák és speciális mátrixgyűrűk izomorfiáját tárgyalja.

Évariste Galois fiatal francia matematikus 1811 október 25.-én született, rövid élete 1932 május 31.-én egy halálos kimenetelű párbajjal fejeződött be. A párbaj előtti éjszakát jegyzeteléssel töltötte, ekkor rakta le a testelmélet azóta Galois-elméletnek elnevezett fejezetének alapjait. Galois észrevette, hogy egy L/k testbővítés esetén a

$$Hom_k(L, L) = \{\varphi : L \to L : \varphi|_k = id\}$$

alakú homomorfizmusok csoportot alkotnak. Ezáltal kapcsolatot létesített a csoportelmélet és a testelmélet között, melynek eredménye többek között az a híres állítás is, hogy az ötödfokú egyenletre nincs megoldóképlet.

A Galois-elméletnek számos alkalmazása van a modern matematikában is, ide tartozik a centrális egyszerű algebrák vizsgálata. Egy A k-algebra centrális, ha centruma megegyezik az alaptestettel, azaz

$$Z(A) = \{x \in A : \forall y \in A xy = yx\} = k,$$

és egyszerű, ha nincs nemtriviális kétoldali ideálja (pontos definíció a harmadik fejezetben). Az egyik legegyszerűbb példa centrális egyszerű algebrára a mátrixgyűrű, melyről a 3.2.2 példában meg is állapítjuk, hogy valóban centrális egyszerű.

A harmadik fejezet gyakorlatilag épp erről szól: azt vizsgáljuk, hogy milyen körülmények között tekinthetünk egy centrális egyszerű algebrát izomorfnak valamely test felett értelmezett mátrixgyűrűvel. Ezt többnyire a tenzorszorzat, és egy fontos fogalom, a hasadás (3.2.3 definíció) segítségével fogjuk vizsgálni (A centrális egyszerű algebrát felhasítja az L/k bővítés, ha $A \otimes_k L \cong M_n(L)$ alkalmas $n \in \mathbb{N} - re$).

1.3. Algebrai geometriai összefoglaló

A korábbi fejezetek erősen támaszkodtak algebrai geometriai eszközök használatára, így született a negyedik fejezet, melyben rendszerezzük az algebrai geometriai ismereteket. E fejezet forrása Robin Hartshorne Algebraic Geometry című könyvének I.1, I.2, I.3, I.4, valamint II.6 alfejezetei.

Két fő célunk van: a 2.4.4 következmény belátása (vagyis hogy két sima projektív görbe pontosan akkor izomorf, ha a görbe fölötti testjeik izomorfak); valamint hogy megalapozzuk a 2.4.3 tétel bizonyítása során használt fogalmakat, és bizonyítsuk az 2.4.6 állítást (melyet szintén a 2.4.3 tétel bizonyítása során jelentettünk ki). Ennek érdekében mélyebben belemegyünk az algebrai geometriába: a (4.1) alfejezetben az affin varietásokat, a (4.3)-ban pedig a projektív varietásokat tekintjük át. Továbbá bizonyítjuk az algebrai geometria egyik fő kiinduló tételét, Hillbert nullhelytételét (4.2 alfejezet). A (4.4) alfejezetben definiáljuk a varietások közötti morfizmusokat, hogy végül a (4.5)-ben bizonyíthassuk a fentebb kijelentett ekvivalenciát. Végül, a (4.6) alfejezet teljesen eltér az azt megelőzőektől: a divizorokról szól, és belátjuk a 2.4.6 állítást az egzakt sorokról.

2. fejezet

Kvaternióalgebrák

2.1. Bevezető fogalmak

A pontos definíciójuk után értelmezzük a normát és konjugáltat, mely elengedhetetlen az alapvető számolásokhoz, és a legegyszerűbb tulajdonságok belátásához. Ezután még tovább általánosítunk, és eljutunk az általánosított kvaterniókig.
Kezdjük tehát a következő definícióval:

2.1.1. Definíció. *k-algebra*
Legyen k egy test, és tekintsünk egy k feletti vektorteret. Ha e vektortér elemei között bevezetünk egy k-lineáris asszociatív, de nem feltétlenül kommutatív szorzást, akkor egy k-algebrát kapunk. Végig fel fogjuk tenni, hogy a k-algebra egységelemes.
k feletti ferdetestnek fogjuk hívni azon k-algebrákat, amelyben minden elemnek van kétoldali inverze az előbb bevezetett szorzásra nézve

2.1.2. Megjegyzés. *Az egyszerűség kedvéért, ha innentől kezdve k-algebráról van szó, akkor automatikusan feltesszük, hogy char $k \neq 2$.*

2.1.3. Definíció. *Kvaterniók*
$\mathbb{R}$ feletti 4 dimenziós algebra, melynek bázisa: $1, i, j, k$, úgy hogy a következők teljesülnek:

$$i^2 = -1, j^2 = -1, ij = -ji = k.$$

Egy kvaternió alakja $x, y, z, w \in \mathbb{R}$ esetén:

$$q = x + yi + zj + wk$$

A kvaterniók nem alkotnak testet, hiszen a kommutativitásról már definiáló relációkból látszik, hogy nem teljesül. Igaz azonban a következő állítás:

2.1.4. Állítás. *A kvaterniók egy $\mathbb{R}$ feletti ferdetestet alkotnak, azaz egy olyan algebrát, amelyben minden elemnek van kétoldali inverze.*

Bizonyítás. Előbb vezessük be egy, a fenti alakú kvaternió konjugáltját:

$$\overline{q} = x - yi - zj - wk$$

Ennek segítségével értelmezhetjük a kvaternió normáját a következőképpen:

$$N(q) = x^2 + y^2 + z^2 + w^2$$

Így egy $q \neq 0$ inverze $\overline{q}/N(q)$ lesz. □

2.1.5. Definíció. *Kvaternióalgebra*
$\forall a, b \in k^\times$ esetén az $1, i, j, k$ bázissal rendelkező 4 dimenziós k-algebrát kvaternióalgebrának nevezzük, ha a következő relációkkal van definiálva:

$$i^2 = a, j^2 = b, ij = -ji$$

2.1.6. Megjegyzés. *(a, b) izomorfiaosztálya csak a és b $k^\times/(k^\times)^2$-beli osztályától függ, ugyanis $\forall u, v \in k^\times$ esetén $i \to ui, j \to uj$ helyettesítéssel $(a, b) \cong (u^2a, v^2b)$*
Sőt, az is igaz, hogy $(a, b) \cong (b, a)$, hiszen $u = v = ab$ alkalmazásával kapjuk, hogy:

$$(a, b) \cong (a^2b^3, a^3b^2) \cong (b, a)$$

2.1.7. Definíció. *általánosított kvaternió konjugáltja és normája*
Egy általánosított kvaternió konjugáltját ugyanúgy definiáljuk, mint a fenti esetben, míg normája:

$$N(q) = q\overline{q} = x^2 - ay^2 - bz^2 + abw^2 \in k, \text{ továbbá:}$$

$$N(q_1q_2) = q_1q_2\overline{q_2q_1} = q_1N(q_2)\overline{q_1} = N(q_1)N(q_2)$$

2.1.8. Megjegyzés. *Egy $q_0 \in (a, b)$ elemet tisztán képzetes kvaterniónak nevezünk, ha ${q_0}^2 \in k$, de $q_0 \notin k$.*
Tekintsük a $q_0 = yi + zj + wij$ alakú kvaterniókat. Ezekre teljesül, hogy $\overline{q_0} = -q_0$, így ${q_0}^2 = -N(q_0) \in k$, vagyis tisztán képzetesek. Ha pedig $x \neq 0$ és $q_0 \neq 0$, akkor $q^2 = x^2 - N(q_0) + 2xq_0 \notin k$, mert $2xq_0 \notin k$, így pontosan a fenti alakúak lesznek a tisztán

képzetesek.
Vagyis q egyértelműen írható $x + q_0$ alakba, ahol x k-beli, q_0 pedig tisztán képzetes, sőt ilyenkor ${q_0}^2 = -N(q_0)$ is teljesül. Számolással ellenőrizhetjük, hogy a felbontásra $N(q) = N(x) + N(q_0) = x^2 - {q_0}^2$ is igaz, innen pedig látszik, hogy a norma nem függ a bázis választásától.

2.1.9. Példa. *$M_2(k)$ mátrixalgebra*
Legyenek a következő megfeleltetések:

$$i \to I := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ j \to J := \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \text{ így } IJ = \begin{pmatrix} 0 & b \\ -1 & 0 \end{pmatrix}$$

amit kiegészítve az egységmátrix-szal: $Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $M_2(k)$ egy bázisát kapjuk.

Ehhez vegyük észre, hogy $I+Id; Id-I; J+IJ; J-IJ$ négy olyan mátrix, melyekre mindben különböző helyen egy nemnulla k-beli elem, az összes többi helyen pedig 0 áll. Így e négy elem generálja az eredeti báziselemeket.
A fenti megfeleltetéssel pedig azt is beláttuk, hogy $M_2(k) \cong (1, b)$

Ez a példa a későbbiekben lesz fontos, mikor a testek hasadását fogjuk vizsgálni, vagyis azt, hogy milyen körülmények között egyeznek meg bizonyos mátrixalgebrákkal. A példa azt mutatja, hogy minden kvaternióalgebra, melyben az egyik tag 1 izomorf $M_2(k)$-val, vagyis hasad k fölött. Ebben az irányban megyünk tovább a következő alfejezetben.

2.2. Kvaternióalgebrák hasadása

2.2.1. Definíció. *Hasadás*
Egy (a, b) kvaternióalgebra hasad, ha izomorf $M_2(k)$-vel.

A hasadás fogalmának megértéséhez előbb tekintsük az alábbi állítást, mely épp azért lesz fontos továbbiakban, mert 3 ekvivalens jellemzést is ad:

2.2.2. Állítás. *(a, b) kvaternióalgebrára ekvivalensek a következők:*

1. *(a, b) hasad*

2. *(a, b) nem egy k feletti ferdetest*

3. Az $N:(a,b)\to k$ normának, mint leképezésnek létezik nemtriviális nulleleme

4. $b\in k$ egy $k(\sqrt{a})|k$ bővítésben levő elem normája

Bizonyítás. $1\Rightarrow 2$: Az $M_2(k)$ nyilvánvalóan nem k feletti ferdetest (mert egyik 0 determinánsú elemnek sincs inverze, ráadásul létezik ilyen a nullmátrixon kívül is: például egy 1-es tetszőleges helyen és három 0-ás), így az $1\Rightarrow 2$ egyszerű.

$2\Rightarrow 3$: Feltételezzük, hogy nincs nemtriviális nullelem. Ekkor viszont láttuk már a 2.1.7 megjegyzésnél, hogy egy nemnulla kvaterniónak van konjugáltja, amit megfelelően lenormálva eljutunk az inverzhez. Ez pedig ellentmondás.

A $3\Rightarrow 4$-hez feltehetjük, hogy a nem egy k-beli négyzet, különben b triviálisan a k-beli $b\cdot 1$ normája. Legyen $0\neq q=x+yi+zj+wk$, hogy $N(q)=0$. Ekkor a norma definíciója szerint:

$$x^2-ay^2=(z^2-aw^2)b\ (1)$$

Mivel annyi maradt, hogy a nem egy négyzet, így

$$0\neq x^2-ay^2=(z^2-aw^2)b=(z+\sqrt{a}w)(z-\sqrt{a}w)b.$$

Alkalmazva a $k(\sqrt{a})|k$-beli normát az (1) egyenlőségre, kapjuk hogy

$$N_{k(\sqrt{a})|k}(x+\sqrt{a}y)=N_{k(\sqrt{a})|k}(z+\sqrt{a}w)b,$$

és felhasználva a norma multiplikativitását amit a 2.1.7-ben láttunk:

$$b=N_{k(\sqrt{a})|k}(x+\sqrt{a}y)(z+\sqrt{a}w)^{-1}$$

Végül, a $4\Rightarrow 1$-hez elég megmutassuk, hogy $(a,b)\cong(1,4a^2)$, ez utóbbi ugyanis a 2.1.6 megjegyzés szerint izomorf $(1,1)$-el, azaz $M_2(k)$-vel, ami épp a hasadás definíciója. Ismét feltehetjük, hogy a nem négyzet, ekkor ugyanis a 2.1.9 miatt $(1,b)\cong M_2(k)$. Ha b egy megfelelő norma, akkor b^{-1} is az, így $\exists r,s\in k$, hogy $b^{-1}=r^2-as^2$. $u=rj+sij$ helyettesítéssel $u^2=br^2-abs^2=1$. Továbbá

$$ui=(rj+sij)i=-i(rj+sij)=-iu,$$

ahonnan $v=(1+a)i+(1-a)ui$-re igaz, hogy:
$uv=(1+a)ui+(1-a)u^2i=-(1+a)iu-(1-a)uiu=-((1+a)i+(1-a)iu)u=-vu.$
$v^2=(1+a)^2a+(1-a^2)iui+(1-a^2)ui^2-(1-a)^2a=0+(1+2a+a^2-1+2a-a^2)2a=4a^2.$
Ekkor $(1,u,v,uv)$ bázisra áttérve kapjuk, hogy $(a,b)\cong(1,4a^2)$. □

2.2.3. Definíció. *Centrális algebra*
Legyen A egy k-algebra. Ekkor A centrumán (melyet $Z(A)$-val jelölünk) a következő halmazt értjük: $Z(A) = \{x \in A\colon \forall y \in A\text{-ra } xy = yx\}$. Nyilvánvalóan $k \subset Z(A)$.
Egy A k-algebrát centrálisnak mondunk, ha $Z(A) = k$.

2.2.4. Állítás. *Egy k felett 4-dimenziós D centrális k feletti ferdetest izomorf egy kvaternióalgebrával.*

Előbb a következő lemmát bizonyítjuk:

2.2.5. Lemma. *Ha D tartalmaz egy kommutatív k-részalgebrát, amely izomorf $k(\sqrt{a})|k$ nemtriviális bővítéssel, akkor D izomorf egy (a, b) kvaternióalgebrával megfelelő $b \in k^\times$-re*

Bizonyítás. Legyen q a részalgebra egy olyan eleme, melyre $q^2 = a \in k$, és $q \notin Z(D) = k$. Ekkor az $x \to q^{-1}xq$ belső automorfizmus négyzete: $x \to q^{-2}xq^2 = a^{-1}xa = x$ az identitás, így az eredeti automorfizmus rendje maximum 2. Mivel $q \notin Z(D) = k$, így $q \neq q^{-1}xq$, következik, hogy a fenti rend pontosan 2. Így a fenti automorfizmus karakterisztikus polinomja $X^2 - 1$, vagyis -1 egy sajátérték, tehát $\exists r \in D$, hogy $qr = -rq$.
Indirekt bizonyítjuk, hogy $1, q, r, qr$ lineárisan függetlenek, ehhez feltételezzük tehát, hogy lineárisan összefüggők. Ekkor:

$$\lambda_1 + \lambda_2 q = (\lambda_4 q + \lambda_3)r \Rightarrow r = (\lambda_1 + \lambda_2 q)(\lambda_4 q + \lambda_3)^{-1},$$

vagyis feltehetjük, hogy $\lambda_3 = 0$. Így $qr \in \langle 1, q\rangle$, vagyis qr kommutál q-val. Ez viszont ellentmondás, ugyanis: $q(qr) = -q(rq) = -(qr)q$. Így tehát $1, q, r, qr$ lineárisan függetlenek.

$$\begin{aligned} r^{-2}qr^2 &= (-1)^2 qr^{-2}r^2 = q \\ r^{-2}(qr)r^2 &= (-1)^2 qr^{-2}r^3 = qr, \end{aligned}$$

így az $x \to r^{-2}xr^2$ automorfizmus az összes báziselemet fixen hagyja, vagyis $r^2 \in Z(D) = k$. $b = r^2 \in k^\times$ választással készen vagyunk. □

2.2.4 állítás bizonyítása. Legyen $d \in D \setminus k$. D végesdimenziós k felett, így $\{1, d, d^2, ...\}$ lineárisan összefüggők, azaz $\exists f \in k[x]$ polinom, hogy $f(d) = 0$. D egy k feletti ferdetest, így nincsenek zérusosztói, tehát feltehetjük, hogy f irreducibilis. Vagyis $\exists k[x]/(f) \to D$ k-algebra homomorfizmus, ahol $k(d)$ a D k-részalgebrája. $[k(d) : k]$ fok D fokának osztói közül kerül ki, így lehet 1,2, vagy 4. Azonban 1 nem lehet, mert $d \notin k$, továbbá nem lehet 4, mert ekkor $k(d) = D$ lenne, de az előbbi kommutatív, míg az utóbbi centrális a kezdeti feltétel szerint, azaz nem kommutatív. Így $[k(d) : k] = 2$, ekkor alkalmazhatjuk a lemmát és készen vagyunk. □

A centrális algebrákra is visszatérünk még ezen dolgozat folyamán, azonban most a másodfokú bővítések mentén megyünk tovább. Ezek jelentőségét szintén a későbbiekben fogjuk látni de jegyezzük meg az alábbi ekvivalens állítások közül a másodikat, vagyis azt, hogy bizonyos körülmények között találunk az A kvaternióalgebrához egy olyan testet, amely fölött már hasad.

2.2.6. Állítás. *Legyen A egy k feletti kvaternióalgebra, továbbá $a \in k^\times \setminus k^{\times 2}$. A következők ekvivalensek:*

1. *A izomorf (a, b) kvaternióalgebrával egy megfelelő $b \in k$-ra*

2. *$A \otimes_k k(\sqrt{a})$, mint $k(\sqrt{a})$-algebra, hasad*

3. *A tartalmaz egy $k(\sqrt{a})$-vel izomorf kommutatív k-részalgebrát.*

Bizonyítás. (1) $\Rightarrow$ (2): Előbb vegyük észre, hogy $(a, b) \otimes_k k(\sqrt{a})$ nem más, mint a $k(\sqrt{a})$ fölött definiált (a,b) kvaternióalgebra. a egy négyzet $k(\sqrt{a})$-ben, így a 2.1.6 megjegyzés szerint fennáll az első, míg a 2.1.9 példa alapján a második izomorfia: $(a, b) \cong (1, b) \cong M_2(k(\sqrt{a})$. Így (a, b) hasad $k(\sqrt{a})$ felett, ami az első megállapítás szerint azt jelenti, hogy $(a, b) \otimes_k k(\sqrt{a})$ hasad. Ha tehát az (1) szerint A izomorf (a, b) kvaternióalgebrával, akkor $A \otimes_k k(\sqrt{a})$ hasad, így ezt az irányt beláttuk.

(3) $\Rightarrow$ (1): Két esetet különböztetünk meg. Ha A hasad, akkor az előző érvelések most is helytállóak, így $A \cong M_2(k(\sqrt{a}) \cong (1, b) \cong (a, b)$, vagyis ebben az esetben az (1) mindig teljesül. Ha pedig A nem hasad, akkor alkalmazhatjuk a 2.2.5 lemmát.

(2) $\Rightarrow$ (3): Szintén a két előbbi esetre bontunk. Ha $A \cong M_2(k)$, akkor a 2.1.9 példa szerint választunk egy a-t, melyre $M_2(k) \cong (1, a)$, és a $k(J)$ résztest megfelelő lesz, ahol $J^2 = a$. Ha pedig A nem hasad, Alkalmazzuk a 2.2.2 állítás harmadik állítását $A \otimes_k k(\sqrt{a})$-re így kapunk $q_0, q_1 \in A$-et (nem egyszerre 0-ák), úgy hogy $N(q_0 + \sqrt{a}q_1) = 0$. Legyen

$$B : A \otimes_k k(\sqrt{a}) \times A \otimes_k k(\sqrt{a}) \to k(\sqrt{a})$$
$$B(x, y) = (N(x + y) - N(x) - N(y))/2.$$

Ekkor $B(x, x) = (4N(x) - 2N(x))/2 = N(x)$. Így

$$0 = B(q_0 + \sqrt{a}q_1, q_0 + \sqrt{a}q_1) = N(q_0) + aN(q_1) + 2\sqrt{a}B(q_0, q_1).$$

Mivel $q_0, q_1 \in A$, következik, hogy $N(q_0) + aN(q_1), B(q_0, q_1) \in k$. Tehát mindkettő 0 kell legyen, azaz $N(q_0) = -aN(q_1)$, valamint $2B(q_0, q_1) = q_0\overline{q_1} + q_1\overline{q_0} = 0$. q_0, q_1 nem egyszerre 0-ák, legyen például $q_0 \neq 0$. Feltételezzük továbbá, hogy $N(q_0) = 0$. Ugyancsak a 2.2.2 miatt következne, hogy A hasad, ami ellentmondás, így $N(q_0), N(q_1) \neq 0$. Legyen $q_2 = q_0\overline{q_1} \in A$. Ekkor

$$q_2^2 = q_0\overline{q_1}q_0\overline{q_1} = q_0\overline{q_0}q_1\overline{q_1} = -N(q_0)N(q_1) = aN(q_1)^2.$$

Ekkor $q := q_2N(q_1)^{-1}$ négyzete épp a, tehát ha $\sqrt{a}$-t q-ba küldjük, akkor ez a hozzárendelés $k(\sqrt{a})$-t beágyazza A-ba. □

2.3. Hozzárendelt kúpszelet

A továbbiakban a kvaternióalgebrák hasadását algebrai geometriai szemmel vizsgáljuk. A fő cél Witt tételének a bizonyítása, ehhez azonban szükségünk van némi előismeretre. Ebben a fejezetben a kvaternióalgábrához rendelt projektív kúpszelettel ismerkedünk meg. Bevezetjük a k-racionális pont fogalmát, mely nagyon egyszerű, de mégis nagy jelentőséggel bír majd. Néhány helyen a bizonyítás hiányos, ezek mind megtalálhatóak az Algebrai geometriai összefoglalóban (3. fejezet).

2.3.1. Definíció. *Hozzárendelt kúpszelet*
Legyen (a,b) kvaternióalgebra. Ekkor az ehhez hozzárendelt kúpszelet a $\boldsymbol{P^2}$ *projektív sík*

$$ax^2 + by^2 = z^2$$

homogén koordinátákkal leírt kúpszelete. A hozzárendelt kúpszelet jele $C(a, b)$

2.3.2. Megjegyzés. *A fenti kúpszelet csak a kvaternióalgebrától, és nem annak a bázisválasztásától függ. Először is,* $C(a, b)$ *izomorf az*

$$ax^2 + by^2 = abz^2$$

egyenlettel leírt kúpszelettel, ugyanis alkalmazható a következő helyettesítés:

$$x \to by, y \to ax, z \to abz$$

Így $a(by)^2 + b(ax)^2 = (abz)^2$*, majd ab-vel osztva* $by^2 + ax^2 = abz^2$*.*

$$ax^2 + by^2 - abz^2 = (xi + yj + zij)^2,$$

azaz a $xi+yj+zij$ *tisztán képzetes kvaternió négyzete, ami a normája ellentettjével egyezik meg, ez pedig nem függ a bázisválasztástól a 2.1.8 megjegyzés alapján.*
Innen látszik, hogyha $(a, b) \cong (c, d)$*, akkor a hozzárendelt kúpszeletek is izomorfak lesznek, mivel* (a, b) *és* (c, d) *izomorfiája épp azt jelenti, hogy* (a, b)*-t egy új bázisban felírva* (c, d)*-t kapjuk.*

2.3.3. Definíció. *k-racionális pont*
$x_0, y_0, z_0 \in k$ (nem mind 0) a $C(a,b)$ k-racionális pontja, ha kielégítik az $ax^2 + by^2 = z^2$ egyenletet.

2.3.4. Megjegyzés. *Az alábbiakban látni fogjuk, hogy a k-racionális pont létezéséből sok mindenre lehet következtetni, így egy fontos fogalom. Most egy olyan görbére is példát mutatunk, amelynek nincs k-racionális pontja: $k = \mathbb{R}^2$ felett az $x^2 + y^2 = -1$ egyenletű görbe. (Nincs olyan valós számpár, amire az egyenlet teljesülne).*

2.3.5. Állítás. *(a,b) kvaternióalgebra pontosan akkor hasad, ha $C(a,b)$ kúpszeletnek van k-racionális pontja.*

Bizonyítás. Legyen (x_0, y_0, z_0) az (a,b) egy k-racionális pontja. $y_0 \neq 0$ esetben $b = (z_0/y_0)^2 - a(x_0/y_0)^2$ kielégíti a 2.2.2 állítás 4. részét, ha pedig $y_0 = 0$, akkor $x_0 \neq 0$, és az előző feltétel a-ra teljesül.
Fordítva, mivel b egy $k(\sqrt{a})|k$ bővítésben levő elem normája, felírható $b = r^2 - as^2$; $r, s \in k$ alakban. Ekkor $(s, 1, r)$ k-racionális pont lesz. □

2.3.6. Állítás. *Legyen (a,b) k feletti kvaternióalgebra. Ekkor (a,b) pontosan akkor hasad k felett, ha $(a,b) \otimes_k k(t)$ hasad $k(t)$ felett. (Ahol $k(t)$-vel jelöljük a k feletti racionális törtfüggvények testét.)*

Bizonyítás. Ha (a,b) hasad, akkor nyílvánvalóan $(a,b) \otimes_k k(t)$ is.
A másik irányban, mivel $(a,b) \otimes_k k(t)$ hasad, az ehhez hozzárendelt kúpszeletnek van egy $k(t)$-racionális pontja, tehát legyen $a{x_t}^2 + b{y_t}^2 = {z_t}^2$. Ez az egyenlet homogén koordinátákkal van leírva, ezért a nevezőkkel beszorozva $k[t]$-beli elemeket kapunk, így feltehetjük, hogy $x_t, y_t, z_t \in k[t]$. $t = 0$ helyettesítéssel megkapjuk a k feletti $C(a,b)$ kúpszelet egy k-racionális pontját: $(x_t(0), y_t(0), z_t(0))$ □

2.3.7. Állítás. *$a \in k^\times$ esetén a $k(t)$ feletti (a,t) algebra pontosan akkor hasad, ha a egy négyzet k-ban.*

Bizonyítás. Ha a egy négyzet k-ban, akkor a 2.1.6 megjegyzés, és 2.1.9 példából egyből következik, hogy (a,t) hasad.
Fordítva pedig, legyen ismét egy (x_t, y_t, z_t) $k(t)$-racionális pont, úgy hogy x_t, y_t, z_t $k[t]$-beli. Ha x_t és z_t osztható t-vel, akkor y_t is, így t^2-tel addig oszthatjuk az $a{x_t}^2 + t{y_t}^2 = {z_t}^2$ egyenletet, míg x_t és z_t nem lesz osztható t-vel. Ekkor $t = 0$ helyettesítéssel $ax_t(0)^2 = z_t(0)^2$, ahonnan $a = x_t(0)^{-2} z_t(0)^2$ □

2.4. Witt tétele

Ebben az alfejezetben összegezzük az eddig tanultakat, és erősen támaszkodva az algebrai geometriai összefoglalóra bizonyítjuk Witt tételét, mely a legelegánsabb állítása a fejezetnek, hiszen az eddig ismertetett anyagok közül szinte mindegyikre épít.
Ehhez először szükségünk lesz a C algebrai görbe $k(C)$-vel jelölt racionális függvénytestére, amit ebben az esetben az alábbi faktorgyűrű hányadostesteként kaphatunk meg:

$$k[x,y]/(ax^2+by^2-1)$$

A pontos definíciót az algebrai geometriai összefoglalóban, a 4.4.10 pontban tárgyaljuk.

2.4.1. Megjegyzés. *$(a,b)\otimes_k k(C(a,b))$ mindig hasad $k(C(a,b))$ felett, ugyanis $(x,y,1)$ minden esetben a $C(a,b)$ pontja ez pedig a 2.3.6 miatt igazolja a megjegyzést.*

2.4.2. Lemma. *Ha (a,b) egy kvaternióalgebra, és $c\in k^\times$ egy $k(\sqrt{a})|k$ bővítésben levő elem normája, akkor $(a,b)\cong(a,bc)$*

Bizonyítás. A feltevés miatt $c=x^2-ay^2$ alakban írható $(x,y\in k)$, azaz $q=x+yi$ normája. $J=qj$ tisztán képzetes kvaternió, továbbá $iJ+Ji=0$, $J^2=-N(J)=-N(q)N(j)=bc$, ahonnan $1,i,J,iJ$ is az (a,b) bázisa (hasonlóan a 2.2.5 lemma bizonyításához) $\square$

2.4.3. Tétel. *Witt tétele*
Legyenek $Q_i=(a_i,b_i)$ kvaternióalgebrák, és $C_i=(a_i,b_i)$ a hozzárendelt kúpszeletek, ahol (i=1,2). Q_1 és Q_2 izomorfak k felett pontosan akkor, ha $k(C_1)$ és $k(C_2)$ izomorfak k felett.

2.4.4. Megjegyzés. *A 4.5.8 következmény alapján algebrai geometriából tudjuk, hogy két sima projektív görbe pontosan akkor izomorf, ha a fentiekben felvázolt görbe fölötti testjeik izomorfak.*
Így Witt tétele azt állítja, hogy két kvaternióalgebra pontosan akkor izomorf, ha a hozzárendelt kúpszeletek izomorfak, mint algebrai görbék.

A bizonyítás megkezdése előtt érdemes felsorolni az eddig ismertetett ekvivaleniciákat:

2.4.5. Állítás. *Ekvivalensek:*

1. *(a,b) kvaternióalgebra hasad k felett*
2. *$C(a,b)$ kúpszeletnek van k-racionális pontja*

3. $C(a,b)$ kúpszelet izomorf a projektív egyenessel

4. $C(a,b)$ kúpszelet racionális függvényeinek teste megegyezik $k(t)$-vel.

5. $(a,b) \otimes_k k(t)$ hasad $k(t)$ felett.

Bizonyítás. Az $1 \Leftrightarrow 2$ (2.3.5); $1 \Leftrightarrow 5$ (2.3.6) részben tárgyaltuk.

$3 \Leftrightarrow 4$: vegyük észre, hogy a 4.5.8 szerint csak annyit kell ellenőrizni, hogy a projektív egyenes racionális függvényeinek teste megegyezik $k(t)$-vel. Ez pedig teljesül, hiszen a projektív egyenes homogén koordinátás egyenlete: $ax + by = c$, és $k[x,y]/(ax + by - 1) \cong k[t]$, mivel $y = (1 - ax)/b$ helyettesítéssel minden . $k[t]$ hányadosteste pedig $k(t)$.

$2 \Leftrightarrow 3$: Ha nincs k-racionális pont, akkor az üres halmaz persze nem izomorf a projektív egyenessel, így $3 \Rightarrow 2$ egyből adódik. Ha pedig van k-racionális pont, akkor a 4.5.8-ből következik a fordított állítás: a C feletti racionális függvények teste $k[x,y]/(ax^2 + by^2 = 1)$ alakú, így $y^2 := \frac{1-ax^2}{b}$ segítségével a racionális függvénytestbeli polinomoknak kölcsönösen egyértelműen megfelelnek egy egyváltozós polinomok. A fentiek alapján tehát készen vagyunk. $\square$

Bizonyítás. Witt tételének bizonyítása.

A 2.3.2 megjegyzés szerint $Q_1 \cong Q_2 \Rightarrow C_1 \cong C_2$, továbbá a 2.4.4 megjegyzés alapján $C_1 \cong C_2 \iff k(C_1) \cong k(C_2)$, vagyis a $Q_1 \cong Q_2 \Rightarrow k(C_1) \cong k(C_2)$ iránnyal készen vagyunk.

A másik irányhoz vegyük észre, hogy ha Q_1 és Q_2 is hasad, akkor készen vagyunk. Ezért tegyük fel, hogy egyikük, például Q_1 nem hasad. A 2.4.1 megjegyzés szerint $Q_1 \otimes_k k(C_1)$ hasad, tehát a feltételezett $k(C_1) \cong k(C_2)$ miatt $Q_1 \otimes_k k(C_2)$ is hasad. Ha Q_2 hasadna, akkor $k(C_2)$ az 2.4.5 állítás negyedik része alapján megegyezne $k(t)$-vel, így a 2.3.6 állítás szerint Q_1 is hasadna, ami lehetetlen.
Vagyis feltehetjük, hogy sem Q_1, sem Q_2 nem hasad. Ekkor viszont a_1 nem négyzet k-ban ugyanis akkor $(1,b)$-re tudnánk egyszerűsíteni, ami hasad. $L = k(\sqrt{a_1})$-ben már a_1 négyzet, így az előző észrevételt használva $Q_1 \otimes_k L$ hasad L felett.
A továbbiakban C_1 helyett C rövidítést írunk. $L(C) = L \otimes_k k(C)$ a C_L görbe feletti teste. $Q_1 \otimes_k L$ hasad L felett, így a meghatározott C_L kúpszeletnek van egy L-racionális pontja, ami egyenértékű azzal, hogy C_L izomorf az L feletti P^1 projektív egyenessel. Innen kapjuk hogy $L(C)$ izomorf $L(t)$-vel. (Itt gyakorlatilag a 2.4.5 állítás szinte minden irányát használjuk, épp ezért volt érdemes összegezni őket). Így $Q_2 \otimes_k L(C)$ is hasad $L(C)$ felett, tehát

az 2.3.6 állítás következményeként kapjuk, hogy $Q_2 \otimes_k L$ hasad L felett. Ekkor az 2.2.6 állítás szerint $Q_2 \cong (a_1, c)$ megfelelő $c \in k^\times$-ra. $Q_2 \otimes_k k(C)$ hasad $k(C)$ felett (feltevés és 2.4.1 miatt), így a 2.2.2 értelmében $c = N_{L(C)/k(C)}(f)$ valamilyen $f \in L(C)^\times$-re.
Azonosítani szeretnénk f-et, hogy megkaphassuk c-t. Ehhez jelenleg bizonyítás nélkül kijelentjük az alábbi állítást, melyre építeni fogunk a továbbiakban. Ezen állítás bizonyításával az Algebrai geometriai összefoglalóban foglalkozunk.

2.4.6. Állítás. *A következő sor egzakt:*

$$0 \to L(C)^\times / L^\times \xrightarrow{div} Div(C_L) \xrightarrow{deg} \mathbb{Z} \to 0$$

Gal(L|K)= $\{1, \sigma\}$ Galois csoport a következő módon hat a fenti soron: $L(C)$-n az L hatásán keresztül. $Div(C_L)$ esetében egy zárt P pontot a $\sigma(P)$ konjugáltjába küldi, $\mathbb{Z}$-n pedig triviálisan hat.
Tekintsük most a $(1+\sigma) : Div(C_L) \to Div(C_L)$ leképezést. A div leképezés additivitása miatt

$$(1+\sigma)div(f) = div(f\sigma(f)) = div(N_{L(C)/k(C)}(f)) = div(c) = 0$$

így c konstans. Másrészt, σ rendje 2, tehát a következőt kapjuk:

$$Div(C_L) = (\bigoplus_{P=\sigma(P)} \mathbb{Z}P) \oplus (\bigoplus_{P \neq \sigma(P)} \mathbb{Z}P)$$

σ triviálisan hat az első összeadandón, és megcseréli P-t $\sigma(P)$-vel a másodikban. Ezek szerint $div(f) = E_1 + E_2$ írható, ahonnan

$$0 = (1+\sigma)div(f) = (1+\sigma)(E_1 + E_2) = 2E_1 + (1+\sigma)E_2$$

Következik tehát, hogy $E_1 = 0$, továbbá $E_2 = \sum(m_i P_i - m_i \sigma(P))$, ahol $P_1, ...P_r$ zárt pontok és $m_i \neq 0$. Legyen $D = \sum m_i P_i$, vagyis $div(f) = (1-\sigma)D$. Jelöljük d-vel D fokát. $P_0 := (1 : 0 : \sqrt{a_1})$ a C_L egy L-racionális pontja. A fenti sor egzaktsága miatt $\exists g \in L(C)^\times$, hogy $D - dP_0 = div(g)$
Következik, hogy

$$div(f) = (1-\sigma)D = (1-\sigma)(div(g) + dP_0) = (g\sigma(g)^{-1}) + d(1-\sigma)P_0$$

ahonnan $div(f\sigma(g)g^{-1}) = d(1-\sigma)P_0$
Láttuk, hogy a norma művelettartó, így

$$N_{L(C)/k(C)}(f\sigma(g)g^{-1}) = N(f)N(\sigma(g))N(g^{-1}) = c \cdot N(g)N(g^{-1}) = c \cdot N(gg^{-1}) = c$$

Tehát lecserélhetjük f-et $f' = f\sigma(g)g^{-1}$-re, és kapjuk, hogy $div(f') = d(1-\sigma)P_0$
Mostmár konstans erejéig meghatározható f. Ehhez előbb belátjuk a következőt:
$h := (z - \sqrt{a_1}x)y^{-1} \in L(C)^\times$ kielégíti az alábbiakat:

$$div(h) = (1:0:\sqrt{a_1}) - (1:0:-\sqrt{a_1}) = (1-\sigma)P_0$$

Legyen tehát $P = (x_0 : y_0 : z_0)$ a h pólusa (egy algebrai lezárt, $\overline{k}$ felett). Mivel ez egy pólus, $y_0 = 0$, vagyis $P = (1:0:\pm\sqrt{a_1})$, és P egy L-racionális pont. C egyenletéből

$$a_1x^2 + b_1y^2 = z^2 \Rightarrow b_1y^2 = (z - \sqrt{a_1}x)(z + \sqrt{a_1}x),$$

ahonnan $h = b_1y(z + \sqrt{a_1}x)^{-1}$, tehát $(1:0:\sqrt{a_1})$ a h nullhelye, így az egyetlen pólus $(1:0:-\sqrt{a_1})$ (és $(1:0:\sqrt{a_1})$ az egyetlen nullhely). Innen kapjuk, hogy valóban teljesül a $div(h) = (1-\sigma)P_0$ alak.
Az előbbit összehasonlítva a fent kapott $div(f') = d(1-\sigma)P_0$-vel, és kihasználva a fenti sor egzaktságát (div-nél, azaz div injektív), kapjuk hogy $div(f' - c_0h^d) = 0$, vagyis $f' = c_0h^d$ valamely $c_0 \in L^\times$ konstansra.

$$c = N_{L(C)/k(C)}(f') = N_{L|k}(c_0)N_{L(C)/k(C)}(h)^d = N_{L|k}(c_0)(\tfrac{z^2 - a_1x^2}{y^2})^d = N_{L|k}(c_0)b_1^d$$

Alkalmazva a 2.4.2 lemmát, kapjuk, hogy $Q_2 \cong (a_1, c) \cong (a_1, b_1^d)$
Mivel azt feltételeztük, hogy Q_2 nem hasad, következik hogy d páratlan, és $Q_2 \cong (a_1, b_1)$, amit akartunk. □

3. fejezet

Centrális egyszerű algebrák

3.1. Wedderburn tétele

Legyen k egy test, A egy véges dimenziós k-algebra. Ezt egyszerűnek nevezzük, ha nincs nemtriviális kétoldali ideálja.

Innentől kezdve ebben az alfejezetben az alábbi, Wedderburn tételének bizonyítására, és annak következményeire koncentrálunk. Ez azért lesz fontos, továbbra is azt vizsgáljuk, hogy mikor írható fel egy A k-algebra valamilyen mátrixalgebraként. Nos, Wedderburn tétele épp ezt tárgyalja, ha A egyszerű, és végesdimenziós:

3.1.1. Tétel. *Wedderburn tétele*
Legyen A egy egyszerű végesdimenziós k-algebra. Ekkor létezik egy k feletti végesdimenziós D ferdetest, és egy $n > 0$ egész, hogy $A \cong M_n(D)$.

A jobb átláthatóság érdekében a tétel bizonyítását kisebb lépésekre bontjuk, és úgy haladunk. Figyeljük meg tehát először is az alábbi állítást:

3.1.2. Állítás. *$M_n(D)$ egyszerű.*

Bizonyítás. Ehhez tekintsük azon E_{ij} mátrixot, mely i. sorának j. eleme 1, az összes többi helyen pedig 0 van. Az ilyen alakú mátrixokra fennáll:

$$E_{ij}E_{kl} = \begin{cases} 0, \; j \neq k \\ E_{il}, \; j = k \end{cases}$$

Indirekt bizonyítunk. Feltételezzük, hogy létezik $0 \neq I \lhd M_n(D)$ nemtriviális kétoldali ideál. Legyen $B \in I$, ahol B egy olyan mátrix, melynek i. sorának j. eleme nem 0, sőt, az is feltehető, hogy éppen 1-el egyenlő, mivel a D ferdetestben mindenkinek van inverze. Ekkor az ideál definícióját kihasználva $E_{1i}BE_{j1} = E_{1,1} \in I$, majd minden $1 \leq k, l \leq n$-re $E_{k1}E_{1,1}E_{1l} = E_{kl} \in I$. Azonban E_{kl}-ek D-beli együtthatós lineáris kombinációjaként az összes $M_n(D)$-beli elem előáll, azaz $I = M_n(D)$, mely ellentmondás igazolja, hogy $M_n(D)$ valóban egyszerű. □

A bizonyítást a következő lemmával folytatjuk:

3.1.3. Lemma. *Schur lemma*
Legyen R tetszőleges egységelemes gyűrű, M egyszerű (bal) modulus R felett. Ekkor

$$End_R(M) = \{f : M \to M|\ R\text{-modulus homomorfizmus } \}\ \text{ferdetest.}$$

Bizonyítás. Legyen $f, g : M \to M$ R-modulus homomorfizmus, ekkor adódik, hogy $f + g$ is az. $End_R(M)$-ben a szorzás művelet a kompozíció lesz. Ellenőrizni kell, hogy teljesíti-e az előírt tulajdonságokat.

$$f \circ (g + h) = f \circ g + f \circ h;\ (g + h) \circ f = g \circ f + h \circ f$$

ahol az első azonosság az f additivitásából, a második pedig a kompozíció definíciójából jön ki. Kapjuk tehát, hogy $End_R(M)$ egy gyűrű.

$$\text{egységelem: } id_M : M \to M, \text{ nullelem: azonosan 0 homomorfizmus}$$

Legyen $f : M \to M$ nem azonosan 0. Ekkor $Kerf < M$, és mivel M egyszerű, $Kerf = \{0\}$. Hasonlóan, $0 \neq Imf \leq M \Rightarrow Imf = M \Rightarrow f$ bijekció, vagyis f-nek van inverze: f^{-1}. Kérdés, hogy f^{-1} is R-modulus homomorfizmus-e.

$$m_1 + m_2 = f(f^{-1}(m_1 + m_2))$$
$$m_1 + m_2 = f(f^{-1}(m_1)) + f(f^{-1}(m_2)) = f(f^{-1}(m_1) + f^{-1}(m_2))$$

Mindkét oldalra alkalmazva f^{-1}-et kapjuk, hogy

$$f^{-1}(m_1 + m_2) = f^{-1}(m_1) + f^{-1}(m_2),$$

ahonnan már következik f^{-1} additivitása. Az r-el való szorzás bizonyítása hasonló. □

A Schur lemmája nyomán kaptunk egy ferdetestet, most pedig azt ellenőrizzük, hogy a k-beli elemekkel való szorzás is benne van az endomorfizmusok ferdetestében.

3.1.4. Állítás. *Legyen M egy egyszerű A modulus (Ilyen biztosan létezik, például A maximális balideálja szerint vett faktormodulus). Ekkor $k \leq End_A(M)$*

Bizonyítás. Könnyen ellenőrizhetjük, hogy a k-beli elemekkel való szorzás valóban endomorfizmus:

$$k \ni \lambda : M \to M;\, m \mapsto \lambda m$$
$$\lambda(m_1 + m_2) = \lambda m_1 + \lambda m_2$$
$$\lambda(rm) = (\lambda r)m = (r\lambda)m = r(\lambda m)$$

ahol az $r \in A$-val való szorzás bizonyítása során felhasználtuk (az elején és a végén), hogy tetszőlegesen csoportosíthatunk, és hogy $\lambda \in k \leq Z(A)$ (középen). □

3.1.5. Állítás. *Legyen* $D := End_A(M)$*. Ekkor* $dim_k End_D(M) < \infty$.

Bizonyítás. $dim_k A < \infty$ a feltételek szerint. M egy A modulus, így $dim_k M < \infty$. $k \subset A$, így ami A endomorfizmus az egyben k endomorfizmus is, tehát:

$$dim_k D = dim_k End_A(M) \leq dim_k End_k(M) \leq (dim_k M)^2 < \infty$$

Ebből pedig már következik, hogy $dim_k End_D(M) < \infty$. □

Továbbá, $\varphi \in D, r \in A, m \in M$ esetén $\varphi(rm) = r\varphi(m)$, mert φ A modulus homomorfizmus, így az r-rel való szorzás D lineáris vagyis

$$s_r : M \to M \;\, m \mapsto rm \text{ esetén } s_r \in End_D(M)$$

Legyen tehát $dim_D(M) = n$, ekkor tekintsük a következő leképezést:

$$\Phi : A \to End_D(M);\, r \mapsto s_r$$

Mivel A egyszerű, $1 \notin Ker\Phi \lhd A \Rightarrow Ker\Phi = \{0\} \Rightarrow \Phi$ injektív.

A fent definiált D már majdnem jó jelölt lenne a Wedderburn tételében szereplő ferdetestnek, azonban mint ahogy később látni fogjuk, az elemek fordított sorrendben szorzódnak. Ezt azonban könnyen orvosolhatjuk, ha az oppozit gyűrűre térünk.

3.1.6. Definíció. *Oppozit gyűrű*
Legyen $(R, +, \cdot)$ *egy gyűrű. Ekkor* R *oppozit gyűrűjét így értelmezzük: az* R^{op} *alaphalmaz megegyezik* R*-rel, az összeadás művelet ugyanaz, mint* R *esetében, így ugyanazt az Abel csoportot kapjuk. A szorzás:* $a, b \in R^{op} = R$ *esetén* $a_{op} \cdot b_{op} = b \cdot a$

3.1.7. Állítás. $End_D(M) \cong Mn(D^{op})$

Bizonyítás. Legyen $e_1, e_2, ...e_n \in M$ bázis D felett, továbbá

$$End_D(M) \ni s_r \mapsto ((\varphi_{ij}))_{ij} \in D^{n\times n} \text{ és } t \in A\text{-ra } s_t \mapsto ((\psi_{ij}))_{ij} \in D^{n\times n}$$

Ekkor $re_j = s_r(e_j) = \sum_i \varphi_{ij} e_j$, ahonnan

$$tre_j = t(\sum_i \varphi_{ij} e_j) = \sum_i \varphi_{ij}(te_i) = \sum_i \varphi_{ij} \sum_k \psi_{ki} e_k = \sum_{i,k} (\varphi_{ij} \circ \psi_{ki}) e_k$$

Innen már következik az eredmény. □

Jelenleg tehát A-ból van egy Φ injektív leképezésünk $End_D(M)$-be, ami viszont izomorf $M_n(D^{op})$-nel. Szeretnénk tehát, hogy Φ bijektív legyen. Viszont tudjuk, hogy A és $End_D(M)$ is végesdimenziós k felett, így Φ szürjektivitását kellene vizsgálni. Ehhez nézzük a következő lemmát:

3.1.8. Lemma. *Jacobson sűrűségi lemmája*
R tetszőleges egységelemes gyűrű, M egyszerű modulus, $D := End_R(M)$ ferdetest. Ekkor $R \to End_D(M)$ képe sűrű, azaz: ha $x_1, ..., x_k \in M$ lineárisan független D felett, és $y_1, ..., y_k \in M$ tetszőleges, akkor $\exists r \in R$, hogy $rx_i = y_i$ $i = 1, ..., k$

3.1.9. Definíció. *kompakt-nyílt topológia*
Legyen M topologikus tér a diszkrét topológiával, és tekintsük a $C(M, M)$, M-ből M-be képező folytonos függvényeket. Ezen értelmezhetjük a kompakt-nyílt topológiát: vegyük az összes M-beli (K, U) párt, ahol K kompakt, U nyílt, a bázisnyíltak a következők lesznek:

$$\{f \in C(M, M) : f[K] \subset U\}$$

3.1.10. Megjegyzés. *A fent említett sűrűségre vonatkozó értelmezés az alábbiakból ered: mivel $End_D(M)$ elemei egyben folytonos $M \to M$ leképezések, vehetjük a kompakt-nyílt topológiát $End_D(M)$-en. M-en diszkrét topológia van, így nyílt lesz bármely részhalmaz, és kompakt bármely véges részhalmaz. Erre vonatkoztatva lesz sűrű R képe, mely azt jelenti, hogy $Im \cap U \neq \emptyset$, ahol Im az R képe, U tetszőleges nyílt halmaz. $f \in End_D(M)$ környezetbázisa:*

$$V(x_1, ..., x_k, f) = \{g \in End_D(M) : g(x_i) = f(x_i);\ i = 1, ..., k\},$$

így a sűrűség azt jelenti, hogy $\exists r \in R$, hogy az r-rel való szorzásra (azaz $s_r \in End_D(M)$) teljesül: $s_r(x_i) = rx_i = f(x_i) = y_i$; $i = 1, ..., k$, ez pedig a lemmában megfogalmazott állítás, ugyanis elég csak a báziselemekre ellenőrizni.

Bizonyítás. (3.1.8 lemma bizonyítása). k szerinti indukciót alkalmazunk.
$k = 1$-re $0 \neq x_1 \in M$, $\langle x_1 \rangle_R = M$. Világos, hogy $\forall y_1 \in M$ $\exists r \in R$, hogy $rx_1 = y_1$
Feltételezzük, hogy k-ra már készen vagyunk. Ez azt jelenti, hogy $\exists r' \in R$, hogy $r'x_j = y_j$, $j = 1...k-1$. Keresnünk kell tehát egy olyan s-et, amelyre $sx_j = 0$, $j = 1...k-1$, és $sx_k = y_k - r'x_k$. Ekkor $r = s + r'$ jó választás lesz. Vagyis $s \in Ann_R(x_1, ...x_{k-1}) := L_{k-1} \lhd R$
A következő segédállítást használjuk:

3.1.11. Állítás. $L_{k-1}x_k \neq \{0\}$

Bizonyítás. Indirekt bizonyítunk. Feltételezzük, hogy $L_{k-1}x_k = \{0\}$.
Az indukciós feltevés miatt $(x_1, ..., x_{k-1})$ generálja M^{k-1}-et, azaz tetszőleges $(z_1, ..., z_{k-1}) \in M^{k-1}$-re $\exists t \in R$, hogy $t(x_1, ..., x_{k-1}) = (z_1, ..., z_{k-1})$. Ezek szerint $R(x_1, ..., x_{k-1}) = M^{k-1}$.
Tekintsük most a

$$\Phi : M^{k-1} \to M;\ t(x_1, ..., x_{k-1}) \mapsto tx_k$$

leképezést. Ez jóldefiniált, ugyanis $t(x_1, ..., x_{k-1}) = t'(x_1, ..., x_{k-1})$ esetén $tx_k = t'x_k$ is teljesül, ugyanis $L_{k-1}x_k = \{0\}$.

$$\Phi \in Hom_K(M^{k-1}, M) = \oplus_j Hom_K(M, M) = \oplus_j End_R(M) = D^{k-1}$$

Ezek szerint $\Phi \sim (\varphi_1, ..., \varphi_{k-1}) \in D^{k-1}$. Legyen $t = 1$, ekkor $\Phi(x_1, ..., x_{k-1}) = x_k$, Így:

$$\varphi_1 x_1 + \varphi_2 x_2 + ... + \varphi_{k-1} x_{k-1} = x_k,$$

ez pedig ellentmondás, ugyanis $(x_1, x_2..., x_k)$ lineárisan függetlenek. Az ellentmondás igazolja, hogy $L_{k-1}x_k \neq \{0\}$ □

A lemma bizonyításához már csak arra van szükségünk, hogy mivel M egyszerű modulus, és $L_{k-1}x_k \neq \{0\}$, következik, hogy $L_{k-1}x_k = M$. Végül, $y_k - r'x_k \in M$, így tehát $\exists s \in L_{k-1}$, hogy $sx_k = y_k - r'x_k$ □

Mostmár minden adott, hogy teljessé tegyük Wedderburn tételének bizonyítását:

Bizonyítás. (3.1.1 tétel bizonyítása). Tekintsük a fent definiált

$$\Phi : A \to End_D(M);\ r \mapsto s_r$$

injektív leképezést. A 3.1.5 állítás miatt $End_D(M)$ véges dimenziós k felett, továbbá 3.1.7 állítás miatt $End_D(M) \cong M_n(D^{op})$. Végül, Jacobson sűrűségi lemmája miatt Φ szürjektív. Ekkor tehát a fentiek alapján bijektív is, vagyis: $A \cong Mn(D^{op})$, amit bizonyítani akartunk.
□

3.1.12. Következmény. *$M_n(D)$ felett izomorfia erejéig egyetlen egyszerű (bal-) modulus van.*

Bizonyítás. Előbb belátjuk, hogy D^n egyszerű (bal-)modulus (D^n i-edik példánya az olyan $M_n(D)$-beli mátrix, melynek az i.-edik oszlopán kivűl mindegyik eleme 0). Ehhez vegyünk egy D^n-beli nemnulla mátrixot, ekkor feltehetjük, hogy az k.-adik sor i.-edik eleme 1. Ezt az (fejezet elején használt jelöléssel) E_{jk}-val (balról) szorozva ($j = 1, ..., n$) E_{ji}-t kapjuk. Ezek pedig már generálják D^n-et, ami így valóban egyszerű.
Legyen most M egy tetszőleges egyszerű (bal-)modulus. Ekkor előáll $M_n(D)$ faktormodulusaként, vagyis

$$\Phi : Mn(D) = \oplus_i D^n \twoheadrightarrow M$$

szürjektív. Mivel Φ nem azonosan 0, van olyan i, hogy D^n i-edik példányára vonatkozó megszorítás nem azonosan 0. Mivel M egyszerű, $ker\Phi_i \neq \{0\}$ eset nem állhat fenn, mert akkor lenne nemtriviális részmodulus. Így $ker\Phi_i = \{0\}$, Φ_i injektív és szürjektív, és véges dimenzió miatt bijektív. Vagyis minden M egyszerű (bal-)modulus izomorf D^n-nel. □

3.1.13. Következmény. *$M_n(D) \cong M_m(D') \Rightarrow n = m; D \cong D'$ (és így a Wedderburn tételéből kapott mátrixgyűrű izomorfia erejéig egyértelmű).*

Bizonyítás. Legyen M a 3.1.12 következményben belátott izomorfia erejéig egyértelmű egyszerű (bal-)modulus $M_n(D) \cong M_m(D') := A$ felett. Wedderburn tételének bizonyítása során felhasználtak szerint: $D^{op} \cong End_A(M) \cong D'^{op}$, és $m = dim_{D^{op}} M = n$. □

3.2. Hasító testek

Egy A végesdimenziós k-algebrát centrálisnak nevezzük, ha a centruma megegyezik k-val (a pontosabb definíció 2.2.3-ben). A centrális algebra egyszerű, ha nincs nemtriviális kétoldali ideálja.
Az alábbi állítás jól mutatja, hogy az egyik legegyszerűbb példa a centrális egyszerű algebrákra a mátrixalgebra.

3.2.1. Állítás. *$M_n(k)$ mátrixalgebra centrális.*

Bizonyítás. Most is az E_{ij} mátrixokat nézzük. Legyen tehát $A \in Z(M_n(k))$, ekkor $AE_{ij} = E_{ij}A$. Az elsőnek minden eleme 0, a j.-edik oszlop kivételével: ide írjuk be A i.-edik oszlopát. A másodiknak is minden eleme 0, kivéve az i.-edik sora: ide az A j.-edik sora kerül. Mivel e kettő megegyezik, következik, hogy a szorzatmátrixoknak csak i.-edik sorának j.-edik eleme nem kell 0 legyen. Ez az elem egyrészt a_{ii}, másrészt a_{jj}-vel egyenlő, vagyis $a_{ii} = a_{jj}$, továbbá $a_{ij} = 0$, ha $i \neq j$. Ezt minden (i, j) párra elvégezve kapjuk, hogy $Z(M_n(k))$ elemei pontosan azok a diagonális mátrixok, amelyeknek minden főátlóbeli eleme megegyezik, azaz $Z(M_n(k)) \cong k$, és ezt akartuk. □

3.2.2. Példa. *$M_n(k)$ mátrixalgebra*
A 3.1.2 állításban már megvizsgáltuk, hogy $M_n(k)$ egyszerű, az előbb bizonyított, 3.2.1 állításban pedig beláttuk, hogy $M_n(k)$ centrális. Ezen fejezet során látni fogjuk, hogy ez milyen fontos példa: minden végesdimenziós centrális egyszerű algebra valamilyen módon kötődni fog egy mátrixalgebrához.

3.2.3. Definíció. *Hasadás.*
A centrális egyszerű k-algebra, L/k bővítés. Azt mondjuk, hogy L felhasítja A-t (A hasad L fölött), ha $A \otimes_k L \cong M_n(L)$ alkalmas $n \in \mathbb{N} - re$.

3.2.4. Állítás. *Algebrailag zárt test felett minden centrális egyszerű algebra hasad.*

Bizonyítás. Legyen K a zárt test. Wedderburn tétele (3.1.1) szerint $A \cong M_n(D)$, valamilyen n-re és D-re. Legyen $\alpha \in D$, ennek minimálpolinomja $m_\alpha(x) \in K[x]$ irreducibilis, így K zártsága miatt $m_\alpha(x)$ foka 1. Ennek következtében $D = K$, vagyis $A \cong M_n(K)$, amit igazolni akartunk. □

A célunk továbbra az lesz, hogy megvizsgáljuk, hogy egy adott k-algebra mikor hasad bizonyos testek felett, azaz hogy elég bő testet találjunk, amely fölött már hasad. Ahhoz, hogy egy k-algebra tulajdonságait egy bővebb test felett vizsgáljuk, tenzorszorzást fogunk használni. Emiatt ismételjük át röviden a tenzorszorzás következő tulajdonságait:

3.2.5. Állítás. *$M_n(k) \otimes_k M_m(k) \cong M_{mn}(k)$*

Bizonyítás. Legyen $S \in M_n(k)$, és $T \in M_m(k)$, ezeket felfoghatjuk, mint $k^n \to k^n$, valamint $k^m \to k^m$ leképezések. Vigye S a k^n $e_1, ..., e_n$ bázisát $u_1, ..., u_n$-be, T pedig a k^m $b_1, ..., b_m$ bázisát $v_1, ..., v_m$-be. Ezt megtehetjük, hiszen a lineáris leképezés előírható a bázison. Ekkor

$$S \otimes_k T : k^n \otimes_k k^m \to k^n \otimes_k k^m.$$

$k^n \otimes_k k^m$ k feletti $n \cdot m$ dimenziós vektortér, így azonosíthatjuk k^{nm}-mel.
Feleljen meg $S \otimes_k T$-nak az a $r_{ST} : k^{nm} \to k^{nm}$ leképezés, amely az $in+j$.-edik báziselemet $u_i v_j$-be viszi. Ez a megfeleltetés injektív, mivel $u_i v_j = 0$ $\forall i \in \{1, ..., n\}$, és $\forall j \in \{1, ..., m\}$ csak akkor teljesülhet, ha $u_i = 0$ $\forall i \in \{1, ..., n\}$, vagy $v_j = 0$ $\forall j \in \{1, ..., m\}$ (ha egyik sem teljesülne, azaz lenne i_0, j_0, melyre $u_{i_0} \neq 0, v_{j_0} \neq 0$, akkor $u_{i_0} v_{j_0} \neq 0$). Ekkor viszont S vagy T 0 mátrix, így $S \otimes_k T = 0$.
Továbbá az $S \otimes_k T \to r_{ST}$ megfeleltetés homomorfizmus is, így kapunk egy $M_n(k) \otimes_k M_m(k) \to M_{mn}(k)$ homomorfizmust, mely azonos dimenziós k fölötti vektorterek között injektív, szürjektív, vagyis bijektív. □

3.2.6. Állítás. *Legyen A egy k-algebra, ekkor $M_n(k) \otimes_k A \cong M_n(A)$.*

Bizonyítás. Tekintsük a már korábban is használt $E_{i,j} \in M_n(k)$ mátrixokat, mint $M_n(k)$ bázisát. Azt is láttuk, hogy az $Z(M_n(A)) = \{aI |\ a \in A\}$, így $E_{i,j}(aI) = (aI)E_{i,j}$, és $E_{i,j} \in M_n(A)$ az $M_n(A)$-nak is egy A feletti bázisát adják. Ekkor $M_n(A)$ elemei egyértelműen írhatóak $\sum_l a_l E_l$ alakba, ($a_l \in A$, $E_l \in E_{i,j}$ $i, j \in \{1, ..., n\}$). Vegyük most a

$$\Phi : M_n(A) \to M_n(k) \otimes_k A$$
$$\textstyle\sum_l a_l E_l \mapsto \sum_l E_l \otimes a_l$$

leképezést, melyet ezután lineárisan kiterjeszthetünk. Kihasználva az előbb mutatott felcserélhetőséget:

$$\Phi(aE_a \cdot bE_b) = \Phi(abE_aE_b) = ab \otimes_k E_aE_b = (a \otimes_k E_a)(b \otimes_k E_b) = \Phi(aE_a)\Phi(bE_b)$$
$$\forall a, b \in Z(M_n(A)),\ E_a, E_b \in E_{i,j}\ i, j \in \{1, ..., n\}$$

Ezt szintén kiterjesztve kapjuk, hogy Φ homomorfizmus.
Φ nyílvánvalóan szürjektív. Az injektivitáshoz belátjuk, hogy minden $M_n(k) \otimes_k A$-beli elem egyértelműen írható $\sum_l a_l \otimes_k E_l$ alakba, ($a_l \in A$, $E_l \in E_{i,j}$ $i, j \in \{1, ..., n\}$). Ehhez:

$$M_n(k) \otimes_k A \cong (\oplus_l kE_l) \otimes_k A \cong \oplus_l (kE_l \otimes_k A).$$

Vagyis ha $\sum_l E_l \otimes a_l = 0$, akkor $E_l \otimes a_l = 0$ minden l-re. $kE_l \otimes_k A \cong k \otimes_k B \cong B$, így $E_l \otimes a_l = 0 \Leftrightarrow a_l = 0$, így $\sum_l E_l a_l = 0$, ahonnan kapjuk az injektivitást is. Vagyis Φ bijektív. □

Most pedig rátérhetünk az alábbi nagy jelentőségű tételre:

3.2.7. Állítás. *Legyen A centrális egyszerű algebra k fölött, és L/k egy algebrai bővítés. Ekkor A pontosan akkor centrális egyszerű k fölött, ha $A \otimes_k L$ centrális egyszerű L fölött.*

Bizonyítás. $2 \Rightarrow 1$. Legyen $A \otimes_k L$ centrális egyszerű, így $Z(A \otimes_k L) = L$. Mivel L test, minden eleme felcserélhető bármely másikkal, így $Z(A) \otimes_k L \subseteq Z(A \otimes_k L) = L$.

$$1 = dim_L Z(A \otimes_k L) = dim_k Z(A) \Rightarrow Z(A) = k, \ A \text{ centrális.}$$

Az egyszerűséget indirekt bizonyítjuk: feltételezzük, hogy létezik egy I valódi ideál A-ban. Be akarjuk látni, hogy ekkor $I \otimes_k L$ is ideál $A \otimes_k L$-ben. Mivel a tenzorszorzat k-lineáris, az összeadásra való zártság automatikusan adódik. Az elemi tenzorok generálják az egész tenzorszorzatot, így elég azokra ellenőrizni. Legyen tehát $a \in I$ $c \in A$; $m, n \in L$, ekkor $ac \in I$; $mn \in L$ tehát:

$$(a \otimes m) \cdot (c \otimes n) = (ac \otimes mn) \in I \otimes_k L$$

Innen látszik, hogy $I \otimes_k L \lhd A \otimes_k L$, és ekkor

$$dim_L I \otimes_k L = dim_k I < dim_k A = dim_L A \otimes_k L$$

miatt $I \otimes_k L$ egy valódi ideál $A \otimes_k L$-ban, mely ellentmondás igazolja az A egyszerűségét.

$1 \Rightarrow 2$. Wedderburn tételéből (3.1.1) tudjuk: $A \cong M_n(D)$ valamely n-re és D-re. Ekkor

$$A \otimes_k L \cong M_n(D) \otimes_k L \cong (M_n(k) \otimes_k D) \otimes_k L \cong M_n(k) \otimes_k (D \otimes_k L) \cong M_n(D \otimes_k L)$$

Mivel ha A centrális egyszerű, akkor $M_n(A)$ is az, így elég $D = A$ esetet vizsgálni. Ehhez legyen $dim_k L = l$, és $u_1, u_2, ..., u_l$ az L egy k feletti bázisa. Ekkor $D \otimes_k L$ bármely $d \otimes \lambda$ eleme egyértelműen írható $\sum_{i=1}^{l} d_i \otimes u_i$ alakba ($d \in D$ és $\lambda = \sum_{i=1}^{l} \lambda_i u_i \in L$):

$$d \otimes \lambda = d \otimes \sum \lambda_i u_i = \sum d\lambda_i \otimes u_i.$$

$\sum d_i \otimes u_i \in Z(D \otimes_k L) \Rightarrow \sum d_i \otimes u_i \in L$, azaz $D \otimes_k L$ centrális, ugyanis:

$$(d \otimes 1)(\sum d_i \otimes u_i) = (\sum d_i \otimes u_i)(d \otimes 1) \Leftrightarrow \sum dd_i \otimes u_i = \sum d_i d \otimes u_i$$

ahonnan az egyértelműség miatt:

$$dd_i = d_i d \ \forall d \in D \Rightarrow d_i \in Z(D) = k \Rightarrow \sum d_i \otimes u_i \in k \otimes_k L = L.$$

Az egyszerűséghez a következő eljárást használjuk: feltételezzük, hogy van egy kétoldali ideál, és bizonyítjuk, hogy ez csak $D \otimes_k L$ lehet. Legyen $J \lhd D \otimes_k L$ $z_1, ..., z_r \in J$ D feletti bázissal. Tehát $z_1, ..., z_r$ függetlenek D fölött, sőt azt is feltehetjük, hogy ugyanazt az alteret feszítik ki $D \otimes_k L$-ben, mint $1 \otimes u_1, ..., 1 \otimes u_r$. Így $z_1, ..., z_r, 1 \otimes u_{r+1}, ..., 1 \otimes u_l$ is egy D fölötti bázis lesz $D \otimes_k L$-ben.

Ekkor $D \otimes_k L = J \oplus (\oplus_{j=r+1}^{l} D \otimes u_i)$, vagyis $i \in \{1, ..., r\}$ esetén $1 \otimes u_i = y_i + \sum_{j=r+1}^{l} \alpha_{ij} \otimes u_j$, ahol $y_i \in J$ és $\alpha_{ij} \in D$. Sőt, ez a felírás egyértelmű a direktösszeg miatt, továbbá az y_i-k függetlenek D fölött:

$$\sum_{i=1}^{r} \lambda_i y_i = \sum_{i=1}^{r} \lambda_i (1 \otimes u_i) + \sum_{i=1}^{r} \lambda_i (\sum_{j=r+1}^{l} \alpha_{ij} \otimes u_j),$$

ahonnan $1 \otimes u_n$, $n \in \{1, ..., l\}$ függetlensége miatt $\lambda_i = 0$, $i \in \{1, ..., r\}$, amit akartunk. Mivel $(d^{-1} \otimes 1)(1 \otimes u_i)(d \otimes 1) = 1 \otimes u_i$, kapjuk, hogy:

$$1 \otimes u_i = (d^{-1} \otimes 1) y_i (d \otimes 1) + \sum_{j=r+1}^{l} (d^{-1} \alpha_{ij} d) \otimes u_i$$

J kétoldali ideál, vagyis $(d^{-1} \otimes 1) y_i (d \otimes 1) \in J$, így a felírás egyértelműsége miatt: $(d^{-1} \otimes 1) y_i (d \otimes 1) = y_i$, és $d^{-1} \alpha_{ij} d = \alpha_{ij}$, azaz $\alpha_{ij} \in Z(D) = k$. Tehát:

$$y_i = 1 \otimes u_i - \sum_{j=r+1}^{l} \alpha_{ij} \otimes u_j \in k \otimes_k L = L \ i \in \{1, ..., r\}\text{-re.}$$

Azaz J-nek van $J \cap L$-beli generátorrendszere (itt használjuk az $u_i \mapsto 1 \otimes u_i$ azonosítást), így $J \cap L$ ideál L-ben, de mivel ez test, így $J \cap L = L$, vagyis $L \subseteq J$. Innen pedig az ideál szorzásra vonatkozó tulajdonsága alapján $D \otimes_k L = J$, vagyis amit bizonyítani akartunk, azaz $D \otimes_k L$ egyszerű.

Hátramaradt azt megvizsgálni, hogy mi történik akkor, ha L/k algebrai bővítés nem véges. A $2 \Rightarrow 1$ esetben és a $1 \Rightarrow 2$ esetben a centrális tulajdonság bizonyítása során nem használtuk ki, hogy véges lenne az L/k bővítés.

Az $1 \Rightarrow 2$ esetben az egyszerűség bizonyításához legyen $L = \cup_{i \in I} L_i$, ahol $I = \{L$ test: L/k véges bővítés$\}$. Legyen ismét J a feltételezett ideál. $dim_L D \otimes_k L = dim_k D < \infty$, így $dim_L J < \infty$ azaz tekinthetjük J $x_1, ..., x_k$ bázisát. Mivel ez véges, van olyan i, hogy $x_1, ..., x_k \in D \otimes_k L_i$. Ekkor az $x_1, ..., x_k$ által generált altér nemtriviális ideál $D \otimes_k L_i$-ben, amiből a véges bővítésekre már bizonyított változat szerint $J = D \otimes_k L_i$. Ekkor L_i egy véges L_j bővítésére elismételve az előzőket: $D \otimes_k L_i = J = D \otimes_k L_j$, ami ellentmondás. Tehát tetszőleges algebrai bővítésre igaz az állítás. □

3.2.8. Következmény. *A centrális egyszerű k fölött $\Rightarrow dim_k A = n^2$ alkalmas $n \in \mathbb{N}$-re.*

Bizonyítás. A 3.2.7 tétel szerint $A \otimes_k \overline{k}$ centrális egyszerű $\overline{k}$ fölött. A 3.2.4 állítás szerint $A \otimes_k \overline{k} \cong M_n(\overline{k})$, ahonnan $dim_k A = dim_{\overline{k}} A \otimes_k \overline{k} = n^2$ ($\overline{k}$ a k algebrai lezártja). □

3.2.9. Definíció. *Centrális egyszerű algebra foka*

Az előző következmény szerint egy centrális egyszerű algebra n^2 dimenziós k felett. Ekkor ennek foka: $\sqrt{dim_k A} = n$

Az előző állítások után pedig meg tudjuk mutatni, hogy valamilyen értelemben az egyetlen példa a centrális egyszerű algebrákra a mátrixalgebra.

3.2.10. Állítás. *A végesdimenziós algebra k fölött. A centrális egyszerű pontosan akkor, ha van L/k véges bővítés, hogy $A \otimes_k L \cong M_n(L)$.*

Bizonyítás. A $2 \Rightarrow 1$ irány közvetlenül következik a 3.2.7 tételből, hiszen a 3.2.2 példában ellenőriztük, hogy a mátrixalgebra centrális egyszerű.

A $1 \Rightarrow 2$ irányhoz vegyük előbb a 3.2.4 állítást, mely szerint $A \otimes_k \overline{k} \cong M_n(\overline{k})$. Ennek egy $\overline{k}$ fölötti bázisát adja az $E_{ij}, i, j \in \{1, ..., n\}$ rendszer. Ez véges, így van olyan L/k véges bővítés, hogy $E_{ij} \in A \otimes_k L$. E_{ij}-k függetlenek $\overline{k}$ fölött, így L fölött is, így ezek egy L fölötti n^2 dimenziós alteret generálnak $A \otimes_k L$-ben. De $A \otimes_k L$ maga is n^2 dimenziós L fölött, így izomorf az E_{ij}-k által generált $M_n(L)$-el. □

A következőkben még megemlítjük a fenti állítás néhány következményét:

3.2.11. Következmény. *Ha A és B centrális egyszerű, akkor $A \otimes_k B$ is az.*

Bizonyítás. Az előző, 3.2.10 állítás szerint találunk olyan L-et, hogy A és B is hasad L fölött. Ekkor $A \otimes_k L \cong M_n(L)$, és $B \otimes_k L \cong M_m(L)$, ahonnan:

$$(A \otimes_k B) \otimes_k L \cong A \otimes_k (B \otimes_k L) \cong A \otimes_k (L \otimes_L B \otimes_k L) \cong (A \otimes_k L) \otimes_L (B \otimes_k L) \cong$$
$$M_n(L) \otimes_L M_m(L) \cong M_{mn}(L)$$

□

3.2.12. Állítás. $A \otimes_k A^{op} \cong M_{n^2}(k)$

Bizonyítás. Legyen $\Phi : A \otimes_k A^{op} \to End_k(A) \cong M_{n^2}(k)$, ahol:

$$a \otimes b \mapsto [A \to A \text{ leképezés, melyre } x \mapsto axb]$$

A Φ egy k-lineáris leképezés, ugyanis a tenzorszorzás k-lineáris. Sőt a szorzattartás is teljesül (elég csak az elemi tenzorokra ellenőrizni hiszen ezek generálják az egész tenzorszorzatot):

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2 \otimes b_2 b_1) \mapsto [x \mapsto a_1(a_2 x b_2) b_1]$$

Kell még, hogy Φ bijektív. Mivel $\Phi(1 \otimes 1) = id_A$, kapjuk, hogy $\Phi \neq 0$, így tekinthetjük a $Ker\Phi \lhd A \otimes_k A^{op}$ ideált, de a 3.2.11 következmény miatt $A \otimes_k A^{op}$ egyszerű, így $Ker\Phi = 0$, vagyis Φ injektív. $A \otimes_k A^{op}$ és $M_{n^2}(k)$ is n^4 dimenziós k felett, így az injektív egyben bijektív is, és ezzel beláttuk. □

3.2.13. Állítás. *A egy k feletti n-edfokú centrális egyszerű algebra, és $L \leq A$ a k egy n-edfokú bővítése. Ekkor A hasad L fölött.*

Bizonyítás. L kommutativitása miatt $A \otimes_k L \subset A \otimes_k A^{op} \cong End_k A$ (épp az utóbbit igazoltuk az 3.2.12 állításnál). A L-vektortér a jobbszorzással, így $A \otimes_k L$ elemei az előző bizonyításban használt Φ képénél L-lineárisak:

$$\Phi(a \otimes \lambda)(x\mu) = ax\mu\lambda = \Phi(a \otimes \lambda)(x)\mu \;\; \mu, \lambda \in L;\; a, x \in A \text{ esetén}$$

$\Phi(a \otimes \lambda)$ L-lineáris, így $\Phi(A \otimes_k L) \subseteq End_L A \subset End_k A$, ugyanis ami L lineáris, az k lineáris is egyben. $dim_k A = n^2, dim_k L = n$, így $dim_L A = n$, ahonnan $dim_L End_L(A) = n^2$, továbbá $dim_L A \otimes_k L = dim_k A = n^2$. Vagyis Φ azonos dimenziós algebrák közötti injekív homomorfizmus, ami így bijektív is. □

Végezetül pedig megnézünk egy állítást, mely megmutatja, hogy minden (végtelen test feletti) centrális ferdetestnek van alkalmas részteste amely fölött hasad.

3.2.14. Állítás. *D n-edfokú centrális ferdetest k végtelen test fölött. Ekkor létezik D-ben $L \leq D$ résztest, úgy, hogy $|L : k| = n$-edfokú szeparábilis bővítés, és $D \otimes_k L \cong M_n(L)$*

Az állítás bizonyításához szükségünk lesz néhány lineáris algebrában tanult állításra, melyeket a rend kedvéért az alábbiakban bizonyítás nélkül felsorolunk, továbbá egy lemmára, melynek bizonyítását is tárgyaljuk.

3.2.15. Állítás. *Lineáris leképezés minimálpolinomja megegyezik tetszőleges bázisban felírt mátrixának minimálpolinomjával.*

3.2.16. Állítás (Cayley-Hamilton tétel)**.** *Lineáris leképezés karakterisztikus polinomjába beírva a leképezés mátrixát nullmátrixot kapunk. (Speciálisan egy $n \times n$-es mátrix minimálpolinomjának foka legfeljebb n).*

3.2.17. Definíció. *Rezultáns*
Legyenek $f, g \in k[x]$ polinomok:

$$f(x) = a_n x^n + ...a_1 x + a_0 \text{ és } g(x) = b_m x^m + ...b_1 x + b_0$$

Ezek rezultánsán a következő $(n+m)\times(n+m)$-es mátrix determinánsát értjük:

$$R(f,g) = det\begin{pmatrix} a_n & a_{n-1} & ... & a_0 & 0 & ... & & 0 \\ 0 & a_n & ... & a_1 & a_0 & 0 & ... & 0 \\ ... & & & & & & & \\ 0 & 0 & ... & & a_n & ... & & a_0 \\ b_m & b_{m-1} & ... & b_0 & 0 & ... & 0 & 0 \\ ... & & & & & & & \\ 0 & 0 & ... & & b_m & ... & & b_0 \end{pmatrix}$$

3.2.18. Állítás. *$f,g\in k[x]$ polinomoknak pontosan akkor van közös gyöke, ha $R(f,g)=0$. (Speciálisan, egy polinomnak pontosan akkor van többszörös gyöke, ha $R(f,f')=0$)*

3.2.19. Lemma. *$\beta\in D$ elemnek $m_\beta(x)\in k(x)$ a minimálpolinomja. Ekkor $\beta\otimes 1\in A\otimes_k\overline{k}\cong M_n(\overline{k})$-nak szintén $m_\beta(x)$ a minimálpolinomja, így $m_\beta(x)$ maximum n-edfokú.*

Bizonyítás. A tenzorszorzás tulajdonságai alapján:

$$m_\beta(\beta\otimes 1) = m_\beta(\beta)\otimes 1 = 0\otimes 1 = 0.$$

Be szeretnénk látni, hogy nincs ennél kisebb fokú polinom, melynek $\beta\otimes 1$ gyöke lenne. Tekintsük a

$$s_\beta : D\to D;\ x\mapsto \beta x$$

k-lineáris leképezést. Nyílvánvalóan $p(x)\in k(x)$ polinomra $p(s_\beta)$ épp a $p(\beta)$-val, azaz egy elemmel való szorzással egyezik meg. Ez pontosan akkor lesz a 0 operátor, ha azonosan 0-val szorzunk, vagyis β a p gyöke. A legkisebb fokú ilyen p egyben β minimálpolinomja is, így az s_β lineáris leképezés minimálpolinomja is $m_\beta(x)$.
A 3.2.15 állítást alkalmazva a fenti lineáris leképezés $M\in M_{n^2}(k)$ mátrixának minimálpolinomja is $m_\beta(x)$. Ez viszont ugyanaz marad, ha M-et $\overline{k}$-beli együtthatós mátrixnak tekintjük, ami pedig éppen a $(\beta\otimes 1)$-el való szorzás, azaz $s_{\beta\otimes 1} : A\otimes_k\overline{k}\to A\otimes_k\overline{k}$ lineáris leképezés. A fent leírtakhoz hasonlóan $\beta\otimes 1\in M_n(\overline{k})$, és $s_{\beta\otimes 1}$ minimálpolinomjai ugyanazok, és ezek is $m_\beta(x)\in k(x)$-val egyeznek meg. Végül, a Cayley-Hamilton tétel szerint e minimálpolinom foka legfeljebb n. □

Bizonyítás. (a 3.2.14 állítás bizonyítása) A fenti, 3.2.19 lemma szerint a minimálpolinom foka legfeljebb n. Keresünk egy olyan $\alpha\in D$ elemet, melynek minimálpolinomja pontosan n-edfokú és nincs többszörös gyöke. Ekkor $m_\alpha(x)$ irreducibilis D nullosztómentessége miatt, tehát $L := k(\alpha)$ meg fog felelni.

Legyen $e_1, ..., e_{n^2}$ a D k fölötti bázisa, továbbá keressük α-t $\alpha = \sum_{j=1}^{n^2} y_j e_j$ $(y_j \in k)$ alakban. Így $\alpha \otimes 1 = \sum_{j=1}^{n^2} y_j(e_j \otimes 1)$ elemnek megfelel az $M_\alpha = \sum_{j=1}^{n^2} y_j M_j \in M_n(\overline{k})$ mátrix (ahol $e_j \otimes 1$-nek $M_j \in M_n(\overline{k})$ felel meg a $A \otimes_k \overline{k} \cong M_n(\overline{k})$ azonosításnál $j = 1, ..., n^2$-re). Ha az y_j-ket meg tudjuk úgy választani, hogy M_α karakterisztikus polinomjának ne legyen többszörös gyöke, akkor ez egyben a minimálpolinom is (mivel az összes sajátérték a minimálpolinom gyöke kell legyen). Nézzük a következő polinomot.

$$F(x, z_1, ..., z_{n^2}) := det(xI - \textstyle\sum_{j=1}^{n^2} z_j M_j) \in \overline{k}[x, z_1, ..., z_{n^2}]$$

A keresett rezultáns ez esetben egy

$$R(F, \tfrac{\partial F}{\partial x}) =: H(z_1, ..., z_{n^2}) \in \overline{k}[x, z_1, ..., z_{n^2}]$$

polinom. Mivel k végtelen test, van olyan polinom, melynek minden gyöke különböző. Azaz van egy olyan k-beli $z_j \mapsto y_j$ behelyettesítés, hogy $H(y_1, ..., y_{n^2}) \neq 0$, így a 3.2.18 állítás szerint a $F = det(xI - M_\alpha)$ karakterisztikus polinomnak nincs többszörös gyöke, és épp az ilyen α-t kerestük. $\square$

4. fejezet

Algebrai geometriai összefoglaló

4.1. Affin varietások

Ebben az alfejezetben az affin téren értelmezett függvények alapvető tulajdonságait vizsgáljuk, ezzel bepillantást nyerve az algebrai geometriai szemléletbe. Gyakorlatilag az alapokat helyezzük le: olyan állításokat bizonyítunk, és definíciókat tekintünk melyre az egész elmélet épül.

Legyen k egy algebrailag zárt test. A k-beli elemekből álló szám n-esek halmazát n dimenziós affin térnek nevezzük. Ennek jele: $\boldsymbol{A^n}$, elemei pedig (később még látni fogjuk a jelölés jelentőségét): $(a_1, ..., a_n)$
Legyen továbbá $A = k[x_1, ..., x_n]$ az n változós polinomgyűrű. Egy $f \in A$ polinom gyökei:

$$Z(f) = \{P \in \boldsymbol{A^n} | f(P) = 0\}.$$

4.1.1. Definíció. *Algebrai halmaz*
$Y \subset \boldsymbol{A^n}$ algebrai halmaz, ha létezik $T \subset A$ úgy, hogy:

$$Y = Z(T) = \{P \in \boldsymbol{A^n} | f(P) = 0 \ \forall f \in T\}.$$

Ha I egy olyan ideál A-ban, amit egy T részhalmaz generál, akkor $Z(T) = Z(I)$, hiszen az ideálban lévő polinomok nullhelyei megegyeznek a generáló polinomok nullhelyeivel. Emlékezzünk vissza, hogy noether gyűrűnek neveztük az olyan gyűrűket, amelynek minden ideálja végesen generált. Mivel a polinomgyűrű noether, kapjuk, hogy bármely T-re $Z(T)$ kifejezhető, mint véges sok $f_1, ...f_r$ polinom közös nullhelye.

4.1.2. Állítás. *Két algebrai halmaz uniója is algebrai halmaz, továbbá algebrai halmazok tetszőleges családjának metszete is az. Végül az üres halmaz, és az egész tér is algebrai halmaz.*

Bizonyítás. Legyen $T_1T_2 = \{f_1f_2 |\ f_1 \in T_1;\ f_2 \in T_2\}$. Belátjuk, hogy:

$$\text{ha } Y_1 = Z(T_1), \text{ és } Y_2 = Z(T_2), \text{ akkor } Y_1 \cup Y_2 = Z(T_1T_2).$$

$P \in Y_1 \cup Y_2 \Rightarrow P \in Y_1$ vagy $P \in Y_2$, vagyis minden $f_1 \in T_1$-re $f_1(P) = 0$, vagy minden $f_2 \in T_2$-re $f_2(P) = 0$ (esetleg egyszerre is teljesülhetnek). Mindegyikből következik, hogy $(f_1f_2)(P) = 0\ \forall f_1 \in T_1$ és $\forall f_2 \in T_2$-re, azaz P minden T_1T_2-beli polinom gyöke. Fordítva pedig, legyen $P \in Z(T_1T_2)$, de $P \notin Y_1 \Rightarrow \exists f_1 \in T_1$, hogy $f_1(P) \neq 0$. Ekkor bármely $f_2 \in T_2$-re $(f_1f_2)(P) = 0$, ahonnan $f_2(P) = 0 \Rightarrow P \in Y_2$. (Ha $P \notin Y_2$, akkor felcserélve az indexeket hasonló következtetésre jutunk).

Ha metszetről van szó, és $Y_\gamma = Z(T_\gamma)$ egy $\gamma \in \Gamma$ indexhalmazra, akkor a $\cap Y_\gamma = Z(\cup T_\gamma)$ egyenlőséghez jutunk, ugyanis: $P \in \cap Y_\gamma \Leftrightarrow P \in Y_\gamma$ minden $\gamma \in \Gamma$-ra, ez pedig egyenértékű azzal, hogy $f(P) = 0$ minden $f \in T_\gamma$ és $\gamma \in \Gamma$-ra, vagyis $f \in \cup T_\gamma$-ra.
Végezetül $\emptyset = Z(1)$ és $\boldsymbol{A^n} = Z(0)$. □

Vegyük észre, hogy az előző állítáasban épp azt ellenőriztük, hogy az algebrai halmazok teljesítik egy topológia definiálása során a zárt halmazokra vonatkozó tulajdonságot. Ennek megfelelően definiálhatjuk a következő topológiát.

4.1.3. Definíció. *Zariski topológia*
$\boldsymbol{A^n}$-en azon topológia, amelyben a zárt halmazok az algebrai halmazok. (Vagyis a nyíltak ezek komplementerei).

4.1.4. Definíció. *Irreducibilis részhalmaz*
Legyen X topologikus tér. $Y \subset X$ irreducibilis, ha nem írható fel $Y = Y_1 \cup Y_2$ alakban, ahol Y nemüres, Y_1, Y_2 pedig az Y valódi zárt részhalmazai. (Az üres halmaz definíció nem irreducibilis).

4.1.5. Megjegyzés. *$\boldsymbol{A^1}$ irreducibilis, mivel minden valódi zárt részhalmaza véges (hiszen néhány polinom nullhelye), az egész $\boldsymbol{A^1}$ pedig végtelen k zártsága miatt.*

4.1.6. Definíció. *Affin varietás*
$\boldsymbol{A^n}$ egy zárt irreducibilis részhalmazát affin varietásnak nevezzük. Egy affin varietás nyílt részhalmazának neve: kvázi-affin varietás.

4.1.7. Definíció. *Affin koordinátagyűrű*
$Y \subseteq \boldsymbol{A^n}$ *affin algebrai halmaz* $A(Y)$ *koordinátagyűrűje* $A/I(Y)$*, ahol*

$$I(Y) = \{f \in A | f(P) = 0 \ \forall P \in Y\}$$

4.2. Hilbert nullhelytétele

Ebben az alfejezetben a algebrai geometria egyik alapvető tételét, Hilbert nullhelytételét bizonyítjuk. Ehhez először szükségünk van néhány lemmára és bevezető állításra, melyek közül lesz olyan, amit bizonyítás nélkül közlünk.

4.2.1. Tétel. *Krull tétele*
Legyen R *egy egységelemes gyűrű, és* $I \lhd R$ *egy valódi ideál. Ekkor létezik egy* M *maximális ideál, hogy* $I \subseteq M \lhd R$

4.2.2. Definíció. *algebrai egész*
Legyenek R, S *integritási tartományok,* $R \leq S$. $\alpha \in S$ *algebrai szám* R *fölött, ha létezik* $f \in R[x]$ *polinom, hogy* $f(\alpha) = 0$*. Ha ez nem teljesül, akkor* α *transzcendens.*
α *algebrai egész, ha létezik 1 főegyütthatós* $f \in R[x]$ *polinom, hogy* $f(\alpha) = 0$.

4.2.3. Definíció. *egészre való zártság*
Legyen egy R *integritási tartomány* K *hányadostesttel.* R *egészre zárt, ha* $\forall \alpha \in K$ *egész* R *fölött* $\Rightarrow \alpha \in R$.

4.2.4. Állítás. R *UFD* $\Rightarrow$ *egészre zárt.*

4.2.5. Állítás. *Minden algebrai szám előáll egy algebrai egész, és egy racionális egész (így nevezzük ebben a környezetben a* $\mathbb{Z}$ *elemeit) hányadosaként.*

4.2.6. Lemma. *Legyen* K *egy tetszőleges test.* $K \leq L$ *végesen generált testbővítésre* $dim_K L < \infty$.

Bizonyítás. $L = K[\beta_1, ..., \beta_n]$. n szerinti indukcióval igazoljuk, hogy $\beta_1, ..., \beta_n$ algebrai K fölött. $n = 0$-ra triviális.
$n = 1$-re $L = K[\beta_1]$, és tegyük fel, hogy β_1 transzcendens. Ekkor $K[\beta_1] \cong K[x]$, ami nem test, így ellentmondás, vagyis β_1 algebrai.
$n > 2$-re is feltételezzük, hogy β_1 transzcendens, így $R = K[\beta_1] \cong K[x]$, de $K[\beta_1] \leq L$ test, tehát $F = K(\beta_1) \leq L$, ahol $K(\beta_1) \cong K(x)$ a racionális törtfüggvények teste. Azaz

$L = F[\beta_2, ..., \beta_n]$, ahonnan az indukció miatt $\beta_2, ..., \beta_n$ mind algebrai F fölött. $R \cong K[x]$, és R UFD, így léteznek $f_2, ..., f_n \in R \setminus \{0\}$, hogy $f_i\beta_i$ algebrai egész R fölött.
Legyenek $f = f_2...f_n$, és $\alpha \in L = F[\beta_2, ..., \beta_n]$ és $H \in R[x_2, ..., x_n]$.

$$\alpha = H(\beta_2, ..., \beta_n) = \sum_i a_i\beta_2^{i_2}...\beta_n^{i_n},\ i = (i_2, ..., i_n).$$

Legyen $N = max_i(i_2 + ... + i_n)$, ekkor $f^N\alpha$ egész R fölött. Válasszuk most $\alpha = \frac{1}{1+\beta_1 f} \in L$, ekkor $(1 + \beta_1 f, f^N)$= 1. Mivel $\frac{f^N}{1+\beta_1 f} \in F$ egész R fölött, és R egészre zárt, $\frac{f^N}{1+\beta_1 f} \in R$, mely ellentmond annak, hogy β_1 transzcendens. Ezzel az állítást igazoltuk. □

Most visszatérünk az algebrai geometriához, és belátjuk, hogy az n változós polinomgyűrű minden maximális ideáljának megfelel az affin tér egy pontja. A bizonyítást épp az előző véges dimenzióról szóló 4.2.6 lemma teszi lehetővé.

4.2.7. Lemma. *$A = k[x_1, ..., x_n]$ minden maximális ideálja felírható az alábbi formában:*

$$\{f \in A|\ f(P) = 0 \text{ valamely } P \in \boldsymbol{A^n}\text{-re } \}$$

Bizonyítás. Legyen $M \lhd A$ maximális ideál, ekkor $k \leq A/M$ egy testbővítés. A/M-t $\{\beta_i = x_i + M|i = 1, ..., n\}$ generálja, mint gyűrűbővítést, így a 4.2.6 lemma szerint $dim_k L < \infty$, azonban ne felejtsük el, hogy ebben az esetben k algebrailag zárt, így $K = L$. Ekkor $\exists z_i \in k$, hogy $x_i + M = z_i + M$, $i = 1, ..., n$-re, vagyis $x_i - z_i \in M$, ahonnan $(x_1 - z_1, ..., x_n - z_n) = M$, vagyis M megegyezik a $(z_1, ..., z_n) = P \in \boldsymbol{A^n}$-ben eltűnő polinomok ideáljával. □

4.2.8. Definíció. *Ideál radikálja*
Legyen $I \lhd R$ egy ideál a kommutatív, egységelemes R gyűrűben. I ideál radikálja:

$$\sqrt{I} = \{f \in R|\ \exists n \in \mathbb{Z}, \text{ hogy } f^n \in I\}$$

4.2.9. Megjegyzés. *$\sqrt{I} \lhd R$.*
Legyenek az $f, g \in \sqrt{I}$-hez a megfelelő kitevők n és m. Ekkor

$$(f + g)^{n+k-1} = \sum \binom{n+k-1}{i} f^i \cdot g^{n+k-1-i}$$

esetén $i > n$ és $n+k-1-i > m$ közül legalább az egyik $\forall i$-re teljesül $(i = 1, ..., n+m-1)$, így az ideálokra vonatkozó szorzási tulajdonság miatt minden tag, s ezért ezek összege is benne lesz az I ideálban.
Az elemmel való szorzás: $(rf)^n \in I\ \forall r \in R$ szintén teljesül, így $\sqrt{I} \lhd R$

4.2.10. Tétel. *Hilbert nullhelytétele*
Bármely I ideálra $I(Z(I)) = \sqrt{I}$

Bizonyítás. Legyen $f \in \sqrt{I}$. Ekkor $\exists n$, hogy $f^n \in I$, azaz $f^n(P) = 0$ $\forall P \in Z(I)$-re $\Rightarrow f(P) = 0$ így a $\sqrt{I} \subseteq I(Z(I))$ irány megvan.
Legyen most $f \in I(V(I))$. Láttuk, hogy $I = (f_1, ..., f_r)$ véges sok polinom közös nullhelye. Ekkor J szintén ideál lesz:

$$J = (f_1, ..., f_r, 1 - yf) \lhd k[x_1, ..., x_n, y]$$

4.2.11. Állítás. $J = k[x_1, ..., x_n, y]$

Bizonyítás. Feltételezzük az ellenkezőjét. Krull tétele szerint $\exists M$ maximális ideál, hogy $J \subseteq M \lhd k[x_1, ..., x_n, y]$, ahonnan a 4.2.7 lemma miatt létezik $(z_1, ..., z_n, w) \in \boldsymbol{A^{n+1}}$, hogy $f_i(z_1, ..., z_n) = 0$ $i = 1, ..., k$ és $1 - wf(z_1, ..., z_n) = 0$
$(z_1, ..., z_n) \in Z(I)$ és $f \in I(V(I))$, így $f(z_1, ..., z_n) = 0$, de ekkor a $1 - wf(z_1, ..., z_n) = 0$-be visszahelyettestve $1 = 0$ ellentmondást kapunk, vagyis valóban $J = k[x_1, ..., x_n, y]$. □

Folytatva a nullhelytétel bizonyítását, kapjuk, hogy $1 \in J$. Ekkor

$$1 = g_1 f_1 + ... + g_k f_k + g(1 - fy)$$

valamely $g_1, ..., g_k, g \in k[x_1, ..., x_n, y]$-re. Helyettesítsünk most $y = 1/f$-et, majd válasszuk úgy N-et, hogy $N \geq deg_y(g_i)$ $i = 1, ..., k$. Ekkor f^N-nel szorozva:

$$f^N = f^N \cdot g_1(x_1, ..., x_n, 1/f) \cdot f_1(x_1, ..., x_n) + ... + f^N \cdot g_k(x_1, ..., x_n, 1/f) \cdot f_k(x_1, ..., x_n)$$

N választása miatt a nevezőkben nem fog szerepelni f. A jobb oldalon ekkor f_i-t szorozzuk $x_1, ..., x_n$ egy függvényével (vagyis azzal, ami g_i-ből marad) és f valamely hatványával.Így az ideáltulajdonság miatt a bal oldal, és így $f^N \in I$, azaz $f \in \sqrt{I}$, amit igazolni akartunk. □

4.2.12. Következmény. *$\boldsymbol{A^n}$ algebrai halmazai és A radikálideáljai (olyan ideál, mely megegyezik a radikáljával) között létezik egy tartalmazásfordító bijekció: $Y \mapsto I(Y)$, és $I \mapsto Z(I)$. Sőt, egy algebrai halmaz irreducibilis pontosan akkor, ha prímideál.*

Bizonyítás. Csak az utóbbit bizonyítjuk, hiszen az előbbi a nullhelytételből közvetlenül kijön. Az Y irreducibilis, akkor $I(Y)$ prímideál irányhoz legyen $fg \in I(Y)$. Következik, hogy $Y \subseteq Z(fg) = Z(f) \cup Z(g)$. Így

$$Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$$

két Y-beli zárt uniója. Y irreducibilitása miatt $Y = Y \cap Z(f) \Rightarrow Y \subseteq Z(f)$ vagy $Y \subseteq Z(g)$, azaz $f \in I(Y)$ vagy $g \in I(Y)$, amit bizonyítani akartunk.
Fordítva, legyen I egy prímideál, és $Z(I) = Y_1 \cup Y_2$. Ekkor $I = I(Y_1) \cap I(Y_2)$, ahonnan $I = I(Y_1)$, vagy $I = I(Y_2)$, innen pedig $Z(I) = Y_1$, vagy $Z(I) = Y_2$, és így irreducibilis. $\square$

4.2.13. Következmény. *Az előző következmény miatt $\boldsymbol{A^n}$ irreducibilis, mivel a nullideálhoz tartozik, az pedig prímideál.*

Az alábbi állítás szintén kulcsfontosságú lesz a következőkben:

4.2.14. Állítás. *Legyen $\boldsymbol{A^n}$ a Zariski topológiával. Ekkor minden nyílt részhalmaz sűrű.*

Bizonyítás. Legyen U egy tetszőleges nyílt halmaz. Megmutatjuk, hogy akárhogy válasszunk egy U' nyíltat $\boldsymbol{A^n}$-ben $U \cap U' \neq \emptyset$, így U valóban sűrű.
Feltételezzük, hogy $U \cap U' = \emptyset$, ekkor $V \cup V' = \boldsymbol{A^n}$, ahol V és V' az U és U' komlementerei így zártak. Azonban $\boldsymbol{A^n}$ irreducibilis, így ez lehetetlen. $\square$

4.3. Projektív varietások

Ebben az alfejezetben az Affin varietások című alfejezet mintájára átvesszük az alapvető állításokat és definíciókat a projektív tér esetében is. A projektív varietások definiálása előtt felevenítjük a projektív térről tanultakat.
Legyen k ismét egy algebrailag zárt test, és tekintsük $\boldsymbol{A^{n+1}}$ elemein a következő ekvivalenciarelációt: $(a_0, ..., a_n) \sim (\lambda a_0, ..., \lambda a_n)$ $\forall \lambda \in k$-ra. Az n dimenziós $\boldsymbol{P^n}$ projektív tér pontjai az előbbi ekvivalenciaosztályok lesznek. A könnyebb megkülönböztethetőség érdekében a projektív tér pontjait így jelöljük: $(a_0 : ... : a_n)$

Az affin esethez hasonlóan itt is definiálni szeretnénk a polinomgyűrűt, azonban némi nehézséget okoz, hogy ezúttal homogén koordinátás elemeink vannak. Tekintsük tehát a következő definíciót:

4.3.1. Definíció. *Fokszámozott gyűrű*
Egy S gyűrű fokszámozott, ha rendelkezik az alábbi 2 tulajdonsággal: $S = \oplus_{d \geq 0} S^{(d)}$ és bármely $d, e \geq 0$-ra $S^{(d)} \cdot S^{(e)} \subseteq S^{(d+e)}$.
$S^{(d)}$ elemeit az S homogén d-edfokú elemeinek nevezzük.

4.3.2. Megjegyzés. *Vegyük észre, hogy a $k[x_1, ..., x_n]$ polinomgyűrű fokszámozott, hiszen bármely polinomot felbonthatjuk polinomok összegére úgy, hogy minden ilyen polinomban a monomok összesített foka megegyezik. Ilyenkor természetesen az is igaz, hogy egy d-ed-, és egy e-edfokú monomokból álló polinom szorzata $e + d$-edfokú monomokból áll.*

4.3.3. Definíció. *Homogén polinomok*
Legyen k egy algebrailag zárt test. Legyen $S^{(d)} \subset k[x_0, ..., x_n]$ azon $x_0, ...x_n$-ből származó monomok lineáris kombinációinak összessége, ahol minden monom összesített foka pontosan d. $S^{(d)}$ elemeit homogén d-edfokú polinomoknak nevezzük.

4.3.4. Definíció. *$I \subseteq S$ egy homogén ideál, ha $I = \oplus_{d \geq 0}(I \cap S^{(d)})$*

Egy d-edfokú homogén polinom esetében $f(\lambda a_0, ..., \lambda a_n) = \lambda^d f(a_0, ..., a_n)$, így az, hogy f egy adott $(a_0, ..., a_n)$ szám $n+1$-esen 0 vesz fel, csak az ekvivalenciaosztálytól függ. Ezek szerint értelmes a következő definíció:

4.3.5. Definíció. *Homogén polinom gyöke*
Az n-dimenziós $\boldsymbol{P^n}$ projektív sík egy $(a_0 : ... : a_n)$ pontja gyöke az $n + 1$ változós S-beli homogén polinomnak, ha $f(a_0, ..., a_n) = 0$. Ezt így is felírhatjuk:

$$Z(f) = \{P \in \boldsymbol{P^n} | f(P) = 0\}.$$

4.3.6. Definíció. *Algebrai halmaz*
$Y \subset \boldsymbol{P^n}$ egy algebrai halmaz, ha létezik homogén polinomok egy olyan T halmaza, hogy

$$Y = Z(T) = \{P \in \boldsymbol{P^n} | f(P) = 0; \forall f \in T\}.$$

4.3.7. Állítás. *Két algebrai halmaz uniója is algebrai halmaz, továbbá algebrai halmazok tetszőleges családjának metszete is az.*

Bizonyítás. Ugyanúgy, mint affin esetben. □

Az affin esethez hasonlóan, az előző állításból kiindulva most is a Zariski topológiát fogjuk használni.

4.3.8. Definíció. *Projektív varietás*
$\boldsymbol{P^n}$ egy irreducibilis algebrai halmazát projektív varietásnak nevezzük. A projektív varietás nyílt részhalmazának neve: kvázi-projektív varietás.

4.3.9. Definíció. *Homogén koordinátagyűrű*
$Y \in \boldsymbol{P^n}$ algebrai halmaz $S(Y)$ homogén koordinátagyűrűje $S/I(Y)$, ahol

$I(Y)$ *az* $\{f \in S | f$ *homogén és* $f(P) = 0\ \forall P \in Y\}$ *által generált homogén ideál*

A továbbiakban arra törekszünk, hogy kapcsolatot találjuk az affin, és a projektív tér között. Ehhez legyen egy H_i azon $\boldsymbol{P^n}$-beli pontok összessége, melyek i-edik koordinátája 0, továbbá legyenek $U_i = \boldsymbol{P^n} \setminus H_i\ i = 0, ..., n$ nyílt halmazok. Ekkor az U_i-k a $\boldsymbol{P^n}$ egy fedését adják, hiszen $P = (a_0 : ... : a_n)$ esetén $\exists i$, hogy $a_i \neq 0 \Rightarrow P \in U_i$. Legyen tehát

$$\varphi_i : U_i \to \boldsymbol{A^n};\ \varphi_i(a_0, ..., a_n) = (a_0/a_i, ..., a_n/a_i), \text{ ahol az } a_i/a_i\text{-t kihagytuk.}$$

φ_i jóldefiniált, ugyanis a fent megjelenő arányok függetlenek a homogén koordináták megválasztásától.

A következő állítás kijelentése előtt emlékezzünk vissza egy egyszerű topológiai megfigyelésre, melyet mindjárt használni is fogunk. A bizonyítás a zártság fogalmának egyszerű átgondolása így arra nem térünk ki külön.

4.3.10. Állítás. *Legyen* X *topologikus tér,* U *egy részhalmaza az altértopológiával,* Y *pedig az* U *részhalmaza. Ekkor* $\overline{Y}^X \cap U = \overline{Y}^U$.

4.3.11. Állítás. φ_i *egy homeomorfizmus* U_i *(az örökölt topológiával) és* $\boldsymbol{A^n}$ *(a Zariski topológiával) között.*

Bizonyítás. A meghatározásból látszik, hogy φ_i bijektív, hiszen egy homogén koordinátákkal leírt szám $(n+1)$-eshez rendel egy affin koordinátákkal leírt szám n-est. Tehát a homeomorfizmushoz a mindkét irányban való folytonosság kell, amit úgy fogunk igazolni, hogy φ_i és φ_i^{-1}-nél is zárt képe zárt (vagyis hogy U_i és $\boldsymbol{A^n}$ zárt részhalmazai egymásba képződnek). Ehhez előbb az általánosság megszorítása nélkül feltehetjük, hogy $i = 0$, sőt, a továbbiakban U, és φ-t használunk az $i = 0$-val indexelt változat helyett. Legyen S^h az S homogén elemeinek halmaza és tekintsük az alábbi leképezéseket:

$$\alpha : S^h \to A;\ f \mapsto f(1, y_1, ..., y_n) \text{ valamint}$$
$$\beta : A \to S^h;\ g \mapsto x_0^e \cdot g(x_1/x_0, ..., x_n/x_0), \text{ ahol } g \in A \text{ összesített foka } e$$

Legyen $Y \in U$ egy zárt részhalmaz, aminek a $\boldsymbol{P^n}$-beli lezártja $\overline{Y}^{\boldsymbol{P^n}}$. Ekkor $\overline{Y}^{\boldsymbol{P^n}}$ zárt, így egy algebrai halmaz $\boldsymbol{P^n}$-ben, tehát $\overline{Y}^{\boldsymbol{P^n}} = Z(T)$ valamely $T \subseteq S^h$-ra. Topológiából tudjuk, hogy $\overline{Y}^{\boldsymbol{P^n}} \cap U = \overline{Y}^U = Y$ (az utóbbi egyenlőség igaz, mert Y zárt U-ban), így $\varphi(Y) = \varphi(\overline{Y}^{\boldsymbol{P^n}} \cap U)$. Legyen $P \in Y$ azaz $P = (a_0 : ... : a_n) \in \overline{Y}^{\boldsymbol{P^n}}$; $a_0 \neq 0$. Ekkor $\overline{Y}^{\boldsymbol{P^n}} = Z(T)$ szerint

$$\forall f \in T\text{-re } 0 = f(a_0, ..., a_n) = f(1, a_1/a_0, ..., a_n/a_0),$$

vagyis $\varphi(a_0, ..., a_n) = (a_1/a_0, ..., a_n/a_0)$-re $\varphi(P)$ gyöke $\alpha(f)$-nek, és mivel ez a másik irányba is ugyanígy megy, így $\varphi(Y) = Z(\alpha(T))$. Ekkor Y képe zárt.

Fordítva, legyen W az $\boldsymbol{A^n}$ zárt részhalmaza, így $W = Z(T')$ valamilyen $T' \subset A$-ra. Legyen $R = (b_1, ...b_n) \in W$, melyre

$$\forall g \in T'\text{-re } 0 = g(b_1, ...b_n) = 1^e g(b_1, ...b_n).$$

Ekkor $\varphi^{-1}(b_1, ..., b_n) = (1 : b_1 : ... : b_n) \in Z(\beta(T')) \cap U$, vagyis $\varphi^{-1}(W) = Z(\beta(T')) \cap U$. Azaz W képe is zárt φ^{-1}-nél.
Tehát φ_i, és φ_i^{-1} zárt leképezések, ahonnan következik a homeomorfizmus. □

4.3.12. Következmény. *Y projektív, vagy kvázi-projektív varietás, akkor az $Y \cap U_i$-k egy nyílt fedését adják az Y-nak, ráadásul az $Y \cap U_i$-ik homeomorfak valamilyen affin vagy kvázi-affin varietásokkal a fenti φ_i szerint.*

4.4. Morfizmusok

Az alábbiakban a varietások közötti leképezéseket fogjuk vizsgálni.

4.4.1. Definíció. *Reguláris függvények*
Legyen $Y \subset \boldsymbol{A^n}$ egy kvázi-affin varietás. $f : Y \to k$ reguláris $P \in Y$-ban, ha létezik egy U nyílt környezet, hogy $P \in U \subseteq Y$ és $g, h \in A = k[x_1, ..., x_n]$ úgy, hogy $h \neq 0$ az U-n, és $f = g/h$ az U-n. f reguláris Y-n, ha minden pontjában az.
Kvázi-projektív varietás esetében a definíció annyiban módosul, hogy $g, h \in S$ azonos fokú homogén koordinátás polinomok.

A következő lemma kijelentése előtt ismét egy topológiai állítás felevenítése következik. Bizonyítása egyszerű, az egyik irány triviális, a másikban pedig a komplementerre áttérve kihasználjuk a nyíltak uniójára vonatkozó tulajdonságot.

4.4.2. Állítás. *Egy Y topologikus tér Z részhalmaza pontosan akkor zárt, ha Y lefedhető olyan U nyíltakkal, hogy $Z \cap U$ zárt U-ban minden U-ra.*

4.4.3. Lemma. *Affin esetben k-t $\boldsymbol{A^1}$-gyel azonosítva kapjuk, hogy egy reguláris függvény folytonos.*

Bizonyítás. A folytonossághoz elég belátni, hogy zárt őse zárt. A 4.1.5 megjegyzésben láttuk, hogy $\boldsymbol{A^1}$ zárt részhalmazai pontok véges halmaza, így elég annyi, hogy $\forall a \in k$ $f^{-1}(a) = \{P \in Y | f(P) = a\}$ zárt, mivel véges sok zárt uniója zárt marad. A zártságot a 4.4.2 állítás felhasználásával bizonyítjuk. Legyen tehát U nyílt, és itt $f = g/h$ alakú a 4.4.1 definíció szerint.

$$f^{-1}(a) \cap U = \{P \in U | g(P)/h(P) = a\},$$
$$\text{de } g(P)/h(P) = a \Leftrightarrow (g - ah)(P) = 0 \Rightarrow f^{-1}(a) \cap U = Z(g - ah) \cap U$$

ami zárt, így $f^{-1}(a)$ is zárt Y-ban. □

4.4.4. Megjegyzés. *Az előző lemma igaz a projektív esetben is hasonló bizonyítással.*

4.4.5. Következmény. *Ha egy nemüres $U \subseteq X$ nyílt részhalmazon f, g reguláris függvények megegyeznek, akkor $f - g = 0$ zárt és sűrű, vagyis $f = g$ az egész X-en.*

4.4.6. Definíció. *Morfizmus*
Legyen X, Y két (affin, kvázi-affin, projektív, vagy kvázi-projektív) varietás. $\varphi : X \to Y$ egy morfizmus, ha olyan folytonos leképezés, hogy bármely $V \in Y$ nyílt halmazra, és minden $f : V \to k$ reguláris függvényre $f \circ \varphi : \varphi^{-1}(V) \to k$ reguláris.
$\varphi : X \to Y$ izomorfizmus, ha létezik $\varphi^{-1} : Y \to X$, hogy $\varphi^{-1} \circ \varphi = id_X$ és $\varphi \circ \varphi^{-1} = id_Y$

4.4.7. Megjegyzés. *Két morfizmus kompozíciója nyílvánvalóan morfizmus:*

$$f \circ (\varphi \circ \psi) = (f \circ \varphi) \circ \psi \text{ reguláris.}$$

4.4.8. Definíció. *Egy Y varietás fölötti reguláris függvények gyűrűjét $\mathcal{O}(Y)$-nal jelöljük. $P \in Y$ esetén $\mathcal{O}_P$-vel jelöljük azt a gyűrűt, melynek elemei olyan $\langle U, f\rangle$ párok ekvivalencia-osztályai, ahol $\emptyset \neq U \subset Y$ nyílt, $P \in U$, f pedig reguláris U-n. $\langle U, f\rangle \sim \langle V, g\rangle$, ha $f = g$ $U \cap V$-n.*

4.4.9. Megjegyzés. *Emlékezzünk vissza, hogy egy olyan gyűrűt, melynek egyetlen maximális ideálja van, lokális gyűrűnek nevezzük. A fent definiált $\mathcal{O}_P$ is ilyen, hiszen az egyetlen maximális ideál elemei azon reguláris függvények, melyek eltűnnek P-ben. Ugyanis, ha egy f függvény nem tűnik el P-ben és benne lenne az ideálban, akkor a folytonosság miatt van P-nek olyan környezete, hogy ott sem tűnik el, így itt $1/f$ reguláris, vagyis az ideáltulajdonság miatt 1, és így minden reguláris függvény az ideálban lenne.*

Most elértünk oda, hogy definiálhassuk a varietás fölötti racionális függvények testét.

4.4.10. Definíció. *Varietás fölötti racionális függvények*
Egy Y varietás fölötti függvények $K(Y)$ testének elemei olyan $\langle U, f\rangle$ párok ekvivalencia-osztályai, ahol $\emptyset \neq U \subset Y$ nyílt, f pedig reguláris U-n. $\langle U, f\rangle \sim \langle V, g\rangle$, ha $f = g$ $U \cap V$-n. $K(Y)$ elemeinek neve: Y fölötti racionális függvények.

4.4.11. Megjegyzés. *$K(Y)$ valóban test. Mivel Y irreducibilis, bármely két nemüres nyíltnak metszete nemüres, így az összeadás és szorzás értelmezhető, vagyis $K(Y)$ gyűrű. Ha pedig $\langle U, f\rangle \in K(Y)$, hogy f nem azonosan 0, akkor legyen $V = U \setminus (U \cap Z(f))$, így $\langle V, 1/f\rangle$ lesz $\langle U, f\rangle$ inverze.*

4.4.12. Megjegyzés. *Vegyük észre, hogy $\mathcal{O}(Y) \subseteq \mathcal{O}_P \subseteq K(Y)$.*
Legyen ugyanis $f \neq g \in \mathcal{O}(Y)$, ekkor ezeknek $\mathcal{O}_P$-ben különböző ekvivalenciaosztály felel meg: ha nem így lenne, akkor $f = g$ valamely $U \cap V$ nyílt környezeten, de ekkor a 4.4.5 következmény miatt $f = g$ az egész Y-on, ami ellentmondás. A $\mathcal{O}_P \subseteq K(Y)$ pedig szintén teljesül, hiszen $K(Y)$ definíciója során kevesebb megszorítás van a nyílt halmazokra, mint $\mathcal{O}_P$ esetében.

4.4.13. Definíció. *Lokalizálás*
Legyen R egy gyűrű, melynek I egy prímideálja. Ekkor a $T = R \setminus I$ multiplikatív rendszer segítségével elkészített $T^{-1}R$ hányadosgyűrűt az R gyűrű I ideáljánál vett lokalizált gyűrűjének hívjuk és R_I-vel jelöljük.

A következő állítás segítségével pontra tehetjük az eddig definiált $\mathcal{O}(Y)$; $\mathcal{O}_P$; $K(Y)$ gyűrűket, ugyanis mindről kiderül, hogy rendre izomorfak az n változós polinomgyűrűből különböző módon származtatott gyűrűkkel.

4.4.14. Állítás. *$Y \subseteq \boldsymbol{A^n}$ affin varietás $A(Y)$ affin koordinátagyűrűvel. Ekkor:*

1. *$\mathcal{O}(Y) \cong A(Y)$.*
2. *$\forall P \in Y$ $m_P \subseteq A(Y)$ a P-ben eltűnő függvények ideálja. Ekkor $P \mapsto m_P$ egy bijektív megfeleltetés Y pontjai és $A(Y)$ maximális ideáljai között.*
3. *$\forall P$-re $\mathcal{O}_P \cong A(Y)_{m_P}$.*
4. *$K(Y)$ izomorf $A(Y)$ hányadostestével.*

Bizonyítás. Előbb definiálunk egy $\alpha : A(Y) \to \mathcal{O}(Y)$ leképezést. Minden $f \in A = k[x_1, ..., x_n]$ polinom egy reguláris függvény is egyben $\boldsymbol{A^n}$-en, így Y-on is. Innen kapunk egy $A \to \mathcal{O}(Y)$ homomorfizmust, melynek magja $I(Y) = \{f \in A | f(P) = 0 \ \forall P \in Y\}$, ahonnan α injektív homomorfizmus (hiszen $A(Y) = A/I(Y)$).

A 4.2.12 következmény alapján tudjuk, hogy Y pontjai (azaz Y minimális algebrai részhalmazai) és az A gyűrű $I(Y)$-t tartalmazó maximális ideáljai között bijekció van. $I(Y)$-vel faktorizálva ezek $A(Y)$ maximális ideáljai lesznek. Továbbá, $A(Y)$ elemeinek megfelel egy-egy $\mathcal{O}(Y)$-beli elem az α szerint. Ekkor a $P \in Y$-nek megfelelő maximális ideál: $m_P = \{f \in A(Y) | f(P) = 0\}$, így a 2.-vel készen vagyunk.

Az $A(Y)_{m_P}$ gyűrű elemei a lokalizálás definíciója szerint g/h alakban írhatóak, ahol $h, g \in A(Y)$, és $h(P) \neq 0$. Ezek éppen a reguláris függvények P környezetében. A 4.4.5 megjegyzés szerint pedig $A(Y)_{m_P}$ különböző elemeihez különböző ekvivalenciaosztály tartozik. Így a $\mathcal{O}_P \to A(Y)_{m_P}$ leképezés injektív. Fordítva, a reguláris függvények definíciója miatt a fenti leképezés szürjektív is (hiszen $A(Y)_{m_P}$-ben felsoroljuk az összes g/h; $h(P) \neq 0$ alakú függvényt). Így $\mathcal{O}_P \cong A(Y)_{m_P}$.

A 4.-hoz tekintsük a 3.-ban szereplő gyűrűk hányadostesteit: $A(Y)_{m_P}$ hányadostestének elemei $\frac{g_1/h_1}{g_2/h_2} = \frac{g_1 \cdot h_2}{g_2 \cdot h_1}$ alakban írhatóak, $g_i, h_i \in A(Y)$; $h_i(P) \neq 0$; $i = 1, 2$ feltételekkel. Ez pedig éppen megegyezik $A(Y)$ hányadostestével. Következik, hogy $A(Y)$ hányadosteste izomorf $\mathcal{O}_P$ hányadostestével minden P-re, ez viszont megegyezik $K(Y)$-nal, mivel minden racionális függvény benne van valamely $\mathcal{O}_P$-ben. Vagyis a 4.-el is készen vagyunk.

Az 1. bizonyításához vegyük észre, hogy a 4.4.12 következmény szerint $\mathcal{O}(Y) \subseteq \cap_{P \in Y} \mathcal{O}_P$. A 2. alapján azonban $\cap_{P \in Y} \mathcal{O}_P = \cap_m A(Y)_m$, és α injektivitása miatt kapjuk, hogy $A(Y) \subseteq \mathcal{O}(Y) \subseteq \cap_m A(Y)_m$, ahol m végigfut $A(Y)$ maximális ideáljain. Innen pedig az alábbi lemma szerint következik az egyenlőség, vagyis az 1.-sel is készen vagyunk. $\square$

4.4.15. Lemma. *Legyen R egy integritási tartomány, melynek hányadosteste K. Tekintsük m-et, mint K részgyűrűjét, és legyen R_m az m maximális ideálnál vett lokalizált. Ekkor $R = \cap_m R_m$, ahol m végigfut R maximális ideáljain.*

Bizonyítás. Az egyik irány nyílvánvaló, a másikhoz feltételezzük, hogy $z \in \cap_m R_m$, de $z \notin R$. Vegyük az $I = \{x \in R | \ xz \in R\}$ valódi ideált ($1 \notin I$). Krull tétele szerint létezik egy M maximális ideál, hogy $I \subseteq M$. Ekkor $z \notin R_M$, különben létezne egy $s \notin M$, hogy $sz \in R$, ahonnan $s \in I$, mely ellentmondana $I \subseteq M$-nek. Vagyis $z \notin R_M \Rightarrow z \notin \cap_m R_m$, mely ellentmondás igazolja az állítást. $\square$

Az affin térben bizonyítottak mintájára a projektív esetben is azonosítani szeretnénk a definiált gyűrűket. Ehhez először a következő lemmát tekintjük:

4.4.16. Állítás. *Legyen $U_i \subset \boldsymbol{P^n}$ az a nyílt halmaz, amit $x_i \neq 0$ határoz meg. Ekkor a 4.3.11 állításban használt $\varphi_i : U_i \to \boldsymbol{A^n}$ egy varietások közötti izomorfizmus.*

Bizonyítás. A 4.3.11 állításban már láttuk, hogy φ egy homeomorfizmus, kell még, hogy a reguláris függvények megegyeznek a nyílt halmazokon. U_i reguláris függvényei az $x_0, ...x_n$-ből ($x_0 \neq 0$) képzett homogén- , míg $\boldsymbol{A^n}$ reguláris függvényei az $y_1, ..., y_n$-ből képzett -polinomok hányadosa. Ezek pedig a 4.3.11 állításban definiált α és β leképezések segítségével bijekcióban állnak. □

Mielőtt továbbhaladnánk, tisztázzuk a következő fogalmat: tekintsük a homogén koordinátás S polinomgyűrű I homogén prímideáljánál vett lokalizált gyűrűjét. Ebben a nullfokú tagok részgyűrűje adja a S_{I_0} gyűrűt melyre szükség lesz a későbbiekben.

Most pedig nézzük mi történik a projektív esetben.

4.4.17. Állítás. *$Y \subseteq \boldsymbol{P^n}$ egy projektív varietás $S(Y)$ homogén koordinátagyűrűvel.*

1. *$\mathcal{O}(Y) = k$*
2. *bármely $P \in Y$-ra legyen $m_P \subseteq S(Y)$ az az ideál, amelyet $f \in S(Y)$; $f(P) = 0$ homogén függvények generálnak. Ekkor $\mathcal{O}_P = S(Y)^{(0)}_{m_P}$*
3. *$K(Y) \cong S(Y)^{(0)}_{(0)}$*

Bizonyítás. A bizonyítást a könnyebb átláthatóság érdekében kisebb állításokra bontjuk. Kezdetnek legyen U_i a 4.4.16 állításban megfogalmazottak szerint, továbbá $Y_i = Y \cap U_i$. Ugyancsak a 4.4.16 szerint $U_i \cong \boldsymbol{A^n}$ azaz Y_i-t tekinthetjük affin varietásnak.

4.4.18. Állítás. *Létezik egy φ_i^* természetes izomorfizmus az $A(Y_i)$ és $S(Y)[x_i^{-1}]^{(0)}$ között.*

Bizonyítás. Először tisztázzuk a jelölést: itt $[x_i^{-1}]^{(0)}$ azt jelenti, hogy a nevezőben x_i, vagy annak hatványai lehetnek, és csak a 0-adfokú tagokat figyeljük.
Rátérve a bizonyításra, előbb hozzuk létre a következő izomorfizmust a 4.3.11 állításban definiáltak mintájára:

$$\varphi_i : k[y_1, ..., y_n] \to k[x_0, ...x_n][x_i^{-1}]$$
$$f(y_1, ..., y_n) \mapsto f(x_0/x_i, ...x_n/x_i) \text{ } (x_i/x_i\text{-t kihagyjuk})$$

Láthatjuk, hogy egy $f \in k[y_1,...,y_n]$ φ_i-nél vett képében x_i van a nevezőben, sőt a fok is 0. Megmutatjuk, hogy ennél az izomorfizmusnál $I(Y_i)$ képe $I(Y)S[x_i^{-1}]^{(0)}$.
Ehhez vegyük észre, hogy $f(y_1,...,y_n)$ pontosan akkor van benne az $I(Y_i)$-ben, amikor $f(x_0/x_i,...,x_n/x_i)$ eltűnik Y_i-n. Viszont elég nagy l-re $f(x_0/x_i,...,x_n/x_i)x_i^l$ eltűnik az egész Y-on, mert Y_i-n az első szorzó nulláz ki, míg ennek komplementere, $Y \cap H_i \subseteq H_i$, így itt x_i nulláz (emlékezzünk vissza, hogy U_i komplementere, $H_i \subset \boldsymbol{P^n}$ azon részhalmaza, melyben az i-edik koordináta 0). Ez pedig épp azt jelenti, hogy $f(x_0/x_i,...,x_n/x_i)x_i^l$ benne van $I(Y)$-ben, így pedig $f(x_0/x_i,...,x_n/x_i)$ benne van $I(Y)S[x_i^{-1}]$-ben. Mivel láttuk, hogy $f(x_0/x_i,...,x_n/x_i)$ 0 fokú, $f(x_0/x_i,...,x_n/x_i) \in S(Y)[x_i^{-1}]^{(0)}$ is teljesül.
Visszafelé, ha $g \in S[x_i^{-1}]$ benne van $I(Y)S[x_i^{-1}]^{(0)}$-ben, akkor $g(x_0,...,x_n)x_i^{-deg(g)}$ alakú, ahol $g \in I(Y)$, azaz g eltűnik Y-on. Így $g(x_0,...,x_n)x_i^{-deg(g)}$ eltűnik Y_i-n, azaz $g \in I(Y_i)$. Vagyis az adott izomorfizmusnál $I(Y_i)$ képe $I(Y)S[x_i^{-1}]^{(0)}$, ahonnan faktorizálással kapjuk, hogy $\varphi_i^* : A(Y_i) \to S(Y)[x_i^{-1}]^{(0)}$ izomorfizmus. □

Visszatérve a 4.4.17 állítás 2. részének bizonyításához, legyen $P \in Y$ és legyen i úgy, hogy $P \in Y_i$. A 4.4.14 alapján $\mathcal{O}_P \cong A(Y_i)_{m'_P}$, ahol m'_P az $A(Y_i)$-nek a P-hez tartozó maximális ideálja.
A 4.4.18 állítás bizonyításában látottak mintájára $\varphi_i^*(m'_P) = m_P \cdot S(Y)[x_i^{-1}]^{(0)}$. Ugyancsak a 4.4.18 állítás eredménye, hogy $A(Y_i)$ izomorf $S(Y)[x_i^{-1}]^{(0)}$-vel, így $A(Y_i)$-nek az m'_P szerinti lokalizáltja izomorf $S(Y)[x_i^{-1}]^{(0)}$ gyűrű $m_P \cdot S(Y)[x_i^{-1}]^{(0)}$-nél vett lokalizáltjával. Ez utóbbi nyílvánvalóan izomorf $S(Y)_{m_P}^{(0)}$-vel, így igazoltuk 2.-t, hiszen:

$$\mathcal{O}_P \cong A(Y_i)_{m'_P} \cong S(Y)_{m_P}^{(0)},$$

4.4.19. Állítás. $K(Y) = K(Y_i)$

Bizonyítás. Legyen $\langle f, U\rangle \in K(Y)$. Mivel Y_i nyílt Y-ban, $\langle f, U \cap Y_i\rangle$ is értelmes, sőt ez ugyanazt az ekvivalenciaosztályt határozza meg, mint $\langle f, U\rangle$. Így $K(Y)$ eleme a $K(Y_i)$ eleme is. Fordítva, $\langle f, U_i\rangle \in K(Y_i)$ esetén Y_i nyílt Y-ban, így U_i nyílt Y-ban is, így $\langle f, U_i\rangle \in K(Y)$, azaz $K(Y_i)$ eleme a $K(Y)$ eleme is.
Van tehát egy $K(Y_i) \to K(Y) \to K(Y_i)$ leképezéssorozat, aminek a kompozíciója az identitás. Ezek testek, így kénytelen mindegyik izomorfizmus lenni (a leképezések nyilván műveletartók) □

Ismét visszatérve a 4.4.17 állítás 3. részének bizonyításához, az előző, 4.4.19 állítás szerint pedig $K(Y) = K(Y_i)$. A 4.4.14 állítás alapján pedig kapjuk, hogy $K(Y_i)$ az $A(Y_i)$ hányadosteste. Végül, $A(Y_i)$ hányodosteste $S(Y)_{(0)}^{(0)}$-vel izomorf φ_i^* szerint. Ezeket egybevetve

$K(Y) \cong S(Y)_{(0)}^{(0)}$, így a 3. is kész.

Az 1.-hez legyen $f \in \mathcal{O}(Y)$ egy globálisan reguláris függvény. Ez reguláris lesz minden Y_i-re, vagyis a 4.4.14 állítás alapján $f \in A(Y_i)$. Bizonyítottuk már, hogy $A(Y_i) \cong S(Y)[x_i^{-1}]$, vagyis $f = g_i/x_i^{N_i}$ alakba írható, ahol $g_i \in S(Y)$ N_i fokú homogén.
Ha $\mathcal{O}(Y)$, $K(Y)$, $S(Y)$-t az $S(Y)$ hányadostestének a részgyűrűiként tekintjük, akkor $x_i^{N_i} f \in S(Y)^{(N_i)}$ (ez az N_i fokú homogén polinomok gyűrűje) minden i-re.
Legyen $N \geq \sum N_i$, ekkor $S(Y)^{(N)}$ egy k-vektortér, amit olyan N-fokú $x_0, ..., x_n$-ből álló monomok feszítenek ki, amelyekben legalább az egyik x_i foka $\geq N_i$. Így előbb $x_i^{N_i} f \in S(Y)^{(N_i)}$, majd a megmaradt tagok foka $N - N_i$, és ezt alkalmazva az előzőre kapjuk, hogy $S(Y)^{(N)} \cdot f \subseteq S(Y)^{(N)}$. Ezt folytatva oda jutunk, hogy $S(Y)^{(N)} \cdot f^q \subseteq S(Y)^{(N)}$ minden $q > 0$-ra. $x_0^N \in S(Y)^{(N)}$-et választva $x_0^N f^q \in S(Y)$ minden $q > 0$-ra.
Eszerint $S(Y)[f] \subset x_0^{-N} S(Y)$ ami egy végesen generált $S(Y)$ modulus. $S(Y)$ noether, így $S(Y)[f]$ végesen generált $S(Y)$ modulus ahonnan következik, hogy f egész $S(Y)$ felett. Ez épp azt jelenti, hogy vannak olyan $a_1, ..., a_m \in S(Y)$, függvények, hogy

$$f^m + a_1 f^{m-1} + ... + a_m = 0.$$

Mivel f 0 fokú, elég az egész azonosság nullafokú tagjait tekinteni, így az a_i-k helyére beírhatjuk a 0 fokú homogén komponenseiket és még így is igaz marad az állítás. Az $S(Y)$ gyűrű 0 fokú tagjai a konstans polinomok, így $S(Y)_0 = k$, vagyis minden a_i 0 fokú része szintén k-beli, tehát f algebrai k felett. k algebrailag zárt, így $f \in k$ ahonnan készen vagyunk. □

Ezen alfejezet hátramaradt utolsó célja, hogy belássuk azt, hogy X és Y affin varietások pontosan akkor izomorfak, ha $A(X)$ és $A(Y)$ izomorfak, mint k-algebrák. Ehhez azonban további előkészületekre van szükség:

4.4.20. Lemma. *X egy akármilyen- , $Y \subseteq \boldsymbol{A^n}$ egy affin varietás. $\psi : X \to Y$ leképezés pontosan akkor morfizmus, ha $x_i \circ \psi$ reguláris függvény x-en minden i-re $(x_1, ..., x_n)$ az $\boldsymbol{A^n}$ koordinátafüggvényei).*

Bizonyítás. A morfizmusok definíciója miatt $x_i \circ \psi$ reguláris.
Fordítva, legyen $x_i \circ \psi$ reguláris, és be szeretnénk látni, hogy ψ is az. Ehhez kell, hogy ψ folytonos, valamint $f \circ \psi$ reguláris, ha f az. Mivel $x_i \circ \psi$ reguláris minden i-re, $f \circ \psi$ is

reguláris X-n minden $f = f(x_1, ..., x_n)$ polinomra. Vegyük Y egy tetszőleges zárt részhalmazát, azaz néhány $f_1, ..., f_r$ polinom közös nullhelyét. Ennek ψ szerinti őse megegyezik a 0 $f_i \circ \psi$ szerinti őseinek metszetével ($i = 1, ..., r$). A reguláris függvények folytonosak, így minden $f_i \circ \psi$ szerinti ős zárt, vagyis ezek metszete is az, ahonnan ψ folytonos. Y nyílt részhalmazain a reguláris függvények lokálisan polinomok hányadosai, és mivel $f \circ \psi$ reguláris minden polinomra, így $g \circ \psi$ reguláris minden g reguláris függvényre, ahonnan ψ valóban morfizmus. □

A lemma segítségével már hozzáfoghatunk az alábbi tételhez, melynek már egyszerű következménye lesz a fent felvázolt eredmény.

4.4.21. Állítás. *Legyen X egy akármilyen- , Y pedig egy affin varietás. Ekkor van egy*

$$\alpha : Hom(X, Y) \xrightarrow{\sim} Hom(A(Y), \mathcal{O}(X))$$

természetes izomorfizmus, ahol a baloldalon varietások, a jobbon pedig k-algebrák közötti homomorfizmusokat tekintünk.

Bizonyítás. Egy $\varphi : X \to Y$ morfizmus reguláris függvényeket reguláris függvényekbe visz, így indukál egy leképezést $\mathcal{O}(Y)$ és $\mathcal{O}(X)$ között, ami nyílvánvalóan k-algebra homomorfizmus. A 4.4.14 állítás során beláttuk, hogy $\mathcal{O}(Y) \cong A(Y)$, vagyis φ valóban egy $A(Y) \to \mathcal{O}(X)$ homomorfizmust indukál, így az egyik iránnyal készen vagyunk.
Fordítva, legyen $h : A(Y) \to \mathcal{O}(X)$ egy adott k-algebra homomorfizmus. Ha Y az $\boldsymbol{A^n}$ egy zárt részhalmaza, akkor $A(Y) = k[x_1, ..., x_n]/I(Y)$ a megfelelő koordinátagyűrű. Legyen x_i $A(Y)$-beli megfelelője $\overline{x_i}$, és tekintsük a $\xi_i = h(\overline{x_i}) \in \mathcal{O}(X)$ függvényeket. Ezek globális függvények X-en, így definiálhatjuk az alábbi leképezést:

$$\psi : X \to \boldsymbol{A^n};\ \psi(P) = (\xi_1(P), ..., \xi_n(P))\ \forall P \in X$$

Belátjuk, hogy ψ képe Y-ban van. Mivel $Y = Z(I(Y))$, így elég az, hogy $\forall P \in X$ és $\forall f \in I(Y)$-ra $f(\psi(P)) = 0$. f polinom, h k-algebra homomorfizmus, így

$$f(\psi(P)) = f(\xi_1(P), ..., \xi_n(P)) = h(f(\overline{x_i}, ...\overline{x_n}))(P) = 0$$

hiszen $f \in I(Y)$. Tehát ψ indukálja az adott h homomorfizmust. A lemmával pedig készen vagyunk. □

4.4.22. Következmény. *X és Y affin varietások pontosan akkor izomorfak, ha $A(X)$ és $A(Y)$ izomorfak, mint k-algebrák.*

4.5. Racionális leképezések

4.5.1. Definíció. *Segre beágyazás*
A $\psi : \boldsymbol{P^r} \times \boldsymbol{P^s} \to \boldsymbol{P^N}$, $N = rs + r + s$ leképezésnél $(a_0 : ... : a_r) \times (b_0 : ... : b_s)$ képe legyen $(... : a_i b_j : ...)$, ahol megtartjuk a lexikografikus sorrendet. ψ jóldefiniált, injektív, és ψ képe a $\boldsymbol{P^N}$ részvarietása.

4.5.2. Lemma. *X és Y két varietás, φ és ψ X-ből Y-ba menő morfizmusok, úgy, hogy létezik egy nemüres nyílt $U \subseteq X$ részhalmaz, hogy azon φ és ψ megegyezik. Ekkor $\varphi = \psi$.*

Bizonyítás. Feltételezhetjük, hogy $Y \subseteq \boldsymbol{P^n}$ valamely n-re (projektív varietás esetében ez semmitmondó, affin varietás esetében láttunk megfelelő izomorfizmust). Ekkor az $Y \to \boldsymbol{P^n}$ beágyazó morfizmussal komponálva arra az esetre jutunk, amikor $Y = \boldsymbol{P^n}$.
Tekintsünk a $\boldsymbol{P^n} \times \boldsymbol{P^n}$ szorzatra, mint egy projektív varietásra, ezt megtehetjük a Segre-beágyazás szerint. Ekkor kapunk egy $\varphi \times \psi : X \to \boldsymbol{P^n} \times \boldsymbol{P^n}$ leképezést, mely valójában egy morfizmus. Legyen

$$\Delta = \{(P, P)|\ P \in \boldsymbol{P^n}|\ x_i y_j = x_j y_i;\ i, j = 0, ..., n\}$$

Ezt úgy is fel lehet írni, mint $x_i y_j - x_j y_i$ alakú polinomok közös nullhelye, így Δ zárt. φ és ψ megegyezik U-n, így

$$\varphi \times \psi(U) \subseteq \Delta \Rightarrow U \subseteq (\varphi \times \psi)^{-1}(\Delta).$$

De U nyílt, így sűrű X-ben, $(\varphi \times \psi)^{-1}(\Delta)$ pedis zárt Δ zártsága, és $\varphi \times \psi$ folytonossága miatt, így $\varphi = \psi$, hiszen:

$$(\varphi \times \psi)^{-1}(\Delta) = X \Rightarrow \varphi \times \psi(X) \subseteq \Delta$$

□

A 4.5.2 lemma lehetővé teszi, hogy a következő definíció értelmes legyen, ugyanis valóban egy ekvivalenciarelációt írunk fel (ehhez kell a lemma).

4.5.3. Definíció. *Racionális leképezés*
Legyenek X, Y varietások. Egy $\varphi : X \to Y$ leképezés racionális, ha olyan $\langle U, \varphi_U \rangle$ párok ekvivalenciaosztályai, ahol U nemüres, és $U \subseteq X$, φ pedig egy morfizmus U-ból Y-ba. $\langle U, \varphi_U \rangle \sim \langle V, \varphi_V \rangle$, ha φ_U és φ_V megegyeznek $U \cap V$-n. A racionális leképezés domináns, ha néhány (és így mindegyik) $\langle U, \varphi_U \rangle$ párra φ_U képe sűrű Y-ban.

4.5.4. Definíció. *Biracionális leképezés*
Egy $\varphi : X \to Y$ racionális leképezés biracionális, ha van $\psi : Y \to X$ inverze, hogy $\psi \circ \varphi = id_X$ és $\varphi \circ \psi = id_Y$. Ha X és Y között létezik biracionális leképezés, akkor azt mondjuk, hogy X és Y biracionálisan ekvivalens.

Most, hogy eljutottunk a biracionális ekvivalencia fogalmához, megfogalmazhatjuk ezen alfejezet célját, mely egyben az egész algebrai geometriai összefoglaló egyik fő eredménye: be szeretnénk látni, hogy két tetszőleges varietás pontosan akkor biracionálisan ekvivalens, ha a racionális függvénytestjeik izomorfak, mint k-algebrák. Néhány alapozó lemma után rá is térünk a tétel tárgyalására.

4.5.5. Lemma. *Legyen $Y \subset \boldsymbol{A^n}$ az $f(x_1, ..., x_n) = 0$ által meghatározott hiperfelület. Ekkor $\boldsymbol{A^n} - Y$ izomorf $H \subset \boldsymbol{A^{n+1}}$-val, ahol H az $x_{n+1}f = 1$ egyenletű hipersík. $\boldsymbol{A^n} - Y$ affin, és affin koordinátagyűrűje $k[x_1, ..., x_n][f^{-1}]$.*

Bizonyítás. $P = (a_1, ..., a_{n+1}) \in H$ esetén $\varphi(P) = (a_1, ..., a_n)$. φ egy morfizmus H-ból $\boldsymbol{A^n}$-ba, mely megfelel az $A \to A[f^{-1}]$ gyűrűhomomorfizmusnak. Továbbá φ bijektív H és a képe között, mely $\boldsymbol{A^n} - Y$. Tehát elég megmutatni, hogy φ^{-1} morfizmus, ami pedig következik a 4.4.20 lemmából, hiszen $\varphi^{-1}(a_1, ..., a_n) = (a_1, ..., a_n, 1/f(a_1, ..., a_n))$ □

4.5.6. Állítás. *Bármely Y varietáson a nyílt affin részhalmazok az Y-on levő topológia egy bázisát adják.*

Bizonyítás. Bármely $P \in Y$-ra és $U \ni P$ nyílt halmazra kell mutassunk egy V nyílt affin halmazt, hogy $P \in V \subseteq U$. Mivel U szintén egy varietás, így feltehetjük, hogy $U = Y$. A 4.3.12 következmény értelmében minden varietásnak létezik kvázi-affin varietásokkal való fedése így azt is feltehetjük, hogy Y kvázi-affin $\boldsymbol{A^n}$-ben. Tehát Y kvázi-affin, így nyílt, ezért a komplementere zárt vagyis $Z = \overline{Y} - Y = \overline{Y} \cap Y^C$ is zárt $\boldsymbol{A^n}$-ben (Y^C a komplementert jelenti).
Legyen tehát $I \subseteq A$ a Z ideálja. Mivel Z zárt, $P \in U = Y \Rightarrow P \notin Z = \overline{Y} \cap Y^C$, így van olyan $f \in I$, hogy $f(P) \neq 0$. Legyen H ezen f-re az $f = 0$ által meghatározott hiperfelület $\boldsymbol{A^n}$-ben, ami így H zárt lesz. Ekkor $Z \subseteq H$, de $P \notin H$. Azaz $P \in Y \setminus (Y \cap H)$, ami egy nyílt részhalmaza Y-nak (ugyanis $Y \cap H$ zárt az altértopológiában, így komplementere nyílt). De $Y \setminus (Y \cap H)$ az altértopológia szerint nyílt részhalmaza $\boldsymbol{A^n} - H$-nak, ami az előző, 4.5.5 lemma szerint affin, így $Y \setminus (Y \cap H)$ affin, és ez lesz a P keresett affin környezete. □

Legyen $\varphi : X \to Y$ egy domináns leképezés melyet $\langle U, \varphi_U \rangle$ ír le, $f \in K(Y)$ pedig egy racionális függvény, amit $\langle V, f \rangle$ ír le ($V \subset Y$ nyílt, f pedig reguláris V-n). $\varphi_U(U)$ sűrű

Y-ban, mert φ domináns, $\varphi_U^{-1}(V)$ nemüres nyílt X-ben, így $f \circ \varphi_U$ reguláris $\varphi_U^{-1}(V)$-n. Ez egy racionális függvényt ad X-en, így pedig meghatároztunk egy homomorfizmust $K(Y)$ és $K(X)$ között.

4.5.7. Tétel. *X és Y két varietás esetén a fenti konstrukció egy bijekciót ad a következők között:*

- *X-ből Y-ba menő domináns racionális leképezések halmaza*
- *$K(Y)$-ból $K(X)$-be menő k-algebra homomorfizmusok*

Bizonyítás. A fenti leképezés inverzét fogjuk felépíteni. Legyen $\theta : K(Y) \to K(X)$ k-algebra homomorfizmus. A 4.5.6 állítás alapján Y-hoz létezik egy affin varietásokból álló fedés, így feltehetjük, hogy Y affin $A(Y)$ affin koordinátagyűrűvel. Legyenek $y_1, ..., y_n$ az $A(Y)$ generátorai, így $\theta(y_1), ..., \theta(y_n)$ racionális függvények X-en. Találunk olyan $U \subseteq X$ nyílt halmazt, hogy $\theta(y_i)$ mind reguláris U-n. Ekkor θ egy injektív homomorfizmust határoz meg: $A(Y) \to \mathcal{O}(U)$. Az 4.4.21 állítás szerint ennek megfelel egy $\varphi : U \to Y$ morfizmus, ami egy X és Y közti domináns leképezést ad. Ezzel megkaptuk a kért leképezés inverzét. □

4.5.8. Következmény. *Bármely X, Y varietásra ekvivalensek a következők:*

1. *X és Y biracionálisan ekvivalens*
2. *léteznek $U \subseteq X$, $V \subseteq Y$ nemüres, nyílt részhalmazok, hogy U és V izomorfak*
3. *$K(X) \cong K(Y)$, mint k-algebrák*

Bizonyítás. $1 \Rightarrow 2$: Legyen $\varphi : X \to Y$, és $\psi : Y \to X$ racionális leképezések egymás inverzei, melyeket $\langle U, \varphi \rangle$ és $\langle V, \psi \rangle$ reprezentálnak. Ekkor $\psi \circ \varphi$-t $\langle \varphi^{-1}(V), \psi \circ \varphi \rangle$ reprezentálja, és $\psi \circ \varphi = id_X$, vagyis $\psi \circ \varphi$ identitás $\varphi^{-1}(V)$-n. Hasonlóan $\varphi \circ \psi$ identitás $\psi^{-1}(U)$-n. Válasszuk most a 2.-ben megadott nyílt részhalmazoknak $\varphi^{-1}(\psi^{-1}(U)) \subset X$-t és $\psi^{-1}(\varphi^{-1}(V)) \subset Y$-t. Ekkor az izomorfizmus definíciójából látszik, hogy az előbb kiválasztott nyílt részhalmazok izomorfak ψ és φ-n keresztül.
$2 \Rightarrow 3$: Legyen $\langle f, U \rangle \in K(X)$. Kihasználva az U és V között felírható izomorfiát, ezt azonosíthatjuk $\langle f, V \rangle \in K(Y)$-vel. Így kapunk egy $K(X) \to K(Y)$ homomorfizmust. Visszafelé ugyanezt megtehetjük, és ezek egymás inverzei lesznek, hiszen $K(X)$, $K(Y)$ testek.
$3 \Rightarrow 1$: Következik a 4.5.7 tételből. □

4.6. Divizorok

Az eddig megszokottakkal ellentétben ebben az alfejezetben olyan k test feletti X varietásokat fogunk tekinteni, mely nem feltétlenül algebrailag zárt.
Célunk, hogy a Witt tételének (2.4.3) bizonyítása során használt fogalmakat megalapozzuk, valamint hogy bizonyítsuk az 2.4.6 állítást, amelyet ugyancsak Witt tételének bizonyítása során jelentettünk ki.

4.6.1. Definíció. *Divizorok csoportja*
$Div(X)$ az X zárt, irreducibilis, 1-kodimenziós részvarietásain definiált szabad Abel-csoport.

A továbbiakban csak egy egyszerű esettel fogunk foglalkozni, mégpedig X a $\boldsymbol{P^2}$ projektív sík egy kúpszelete lesz, így az 1-kodimenziós részvarietások a kúpszelet pontjai. Vagyis a $Div(X)$ egy elem ebben az esetben $D = \sum m_P P$, ahol $m_P \in \mathbb{Z}$, és $P \in X$.

4.6.2. Definíció. *div leképezés*
A fenti egyszerűsített esetben a következőképpen definiáljuk a div leképezést:

$$div : k(X)^\times \to Div(X)$$
$$f \mapsto \sum m_P P - \sum m_Q Q,$$

ahol P végigfut f nullhelyein, Q pedig a pólusain, míg m_P és m_Q az adott nullhely, vagy pólus multiplicitását jelöli.

4.6.3. Definíció. *Maradéktest*
Legyen $P \in X \subseteq \boldsymbol{A^n}$ egy affin varietás pontja. Láttuk, hogy ebben az esetben létezik egy $m_P \subseteq A(X)$ maximális ideál. A P-hez tartozó maradéktest az $A[P^{-1}] = A(X)[m_P^{-1}]$ lokális gyűrű faktora a maximális ideállal: $A[P^{-1}]/m_P \cdot A[P^{-1}]$

4.6.4. Megjegyzés. *Projektív varietás esetében a 4.4.16 állítás szerint minden pontnak van lokálisan affinnal izomorf környezete, így a definíció ott is működik.*

A maradéktest valóban egy test, hiszen egy lokális gyűrűt a maximális ideállal faktorizálva testet kapunk.

4.6.5. Definíció. *deg leképezés*
A fenti egyszerűsített esetben a következőképpen definiáljuk a deg leképezést:

$$deg : Div(X) \to \mathbb{Z}$$
$$\sum m_i P_i \mapsto \sum m_i [\kappa(P_i) : k],$$

ahol $[\kappa(P_i) : k]$ a P_i-hez tartozó maradéktest k feletti foka.

4.6.6. Definíció. *Egzakt sorozat*
A, B, C modulusok esetén

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

sorozat rövid egzakt, ha f injektív, g szürjektív, és $Im\ f = Ker\ g$.

Most pedig végre rátérhetünk a Witt tételében említett sorozat egzaktságának bizonyítására. Ehhez azonban tisztáznunk kell, hogy mi történik abban az esetben, ha nem algebrailag zárt test felett figyeljük a varietásokat.
Először azt figyeljük meg, hogy ebben az esetben mik a pontok, vagyis a 0-dimenziós részvarietások. Ezek a (homogén) koordinátagyűrű maximális (homogén) ideáljai lesznek. A jobb megértés érdekében vegyük a $\mathbb{Q}$ fölötti affin egyenest, ennek koordinátagyűrűje $\mathbb{Q}[x]$ egyváltozós polinomgyűrű lesz. Vagyis egy pontja például az $(x^3 - 2)$ által generált ideál. A maradéktest ebben az esetben $\mathbb{Q}(\sqrt[3]{2})$, ami 3-adfokú bővítése $\mathbb{Q}$-nak, tehát a *div* leképezés ezt a pontot majd 3-szor fogja számolni, ezért ugyanúgy, ahogy az algebrailag zárt esetben *div* képében minden elem foka 0 lesz (a $+$-osok itt is f fokát adják).

4.6.7. Állítás. *A következő sorozat rövid egzakt:*

$$0 \to L(t)^\times / L^\times \xrightarrow{div} Div(C_L) \xrightarrow{deg} \mathbb{Z} \to 0$$

Bizonyítás. *div* injektivitása: azon függvények kerülnek itt a 0-ba, akiknek nincs sem gyökük, sem pólusuk, de mivel csak konstansszorzó erejéig tekintjük őket, ez épp az azonosan 1 függvény. Vagyis csak az egységelem megy a 0-ba, így ez a rész megvan.

deg szürjektivitása: egy k-racionális pont esetén a maradéktest megegyezik az alaptesttel, így a *deg* függvényt meghatározó formulában a k-racionális pont esetében a fok 1. Vagyis egy k-racionális pont mellé tetszőleges együtthatót választva kapjuk a szürjektivitást.

$Im\ div = Ker\ deg$: Mivel projektív esetben vagyunk, homogén koordinátákkal dolgozunk. Így $L(t)^\times / L^\times$ elemei azon f/g polinomok, ahol f, g homogén, ugyanakkora a fokuk, és főegyütthatójuk 1. Egy ilyen elem képe *div*-nél a gyököknek és pólusoknak megfelelő pontok kombinációja, úgy hogy az előbbieket "$+$", míg utóbbiakat "-" előjellel írjuk, nem feledve a multiplicitást. Mivel f és g foka megegyezik, a pólusok és gyökök száma multiplicitással számolva szintén egyenlő, amire alkalmazva a deg függvényt épp 0-t kapunk. Vagyis $Ker\ deg \supset Im\ div$.

A másik irányhoz vegyük észre, hogy alkalmazva a deg függvényt pontosan azok a $Div(C_L)$-beli elemek kerülnek 0-ba, ahol multiplicitással számolva ugyanannyi pont van "$+$" előjellel, mint ahány "-"-szal. Viszont pontosan az ilyen alakúak adják $Im\ div$-et is, ahonnan $Ker\ deg \subset Im\ div$. Ezzel pedig már teljes a bizonyítás. $\square$

Irodalomjegyzék

[1] PHILIPPE GILLE - TAMÁS SZAMUELY, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006, felhasznált oldalak: 1-24

[2] ROBIN HARTSHORNE, *Algebraic Geometry*, Springer, 1997 - nyolcadik kiadás, felhasznált oldalak: 1-26; 129-132

[3] ZÁBRÁDI GERGELY, *Centrális egyszerű algebrák osztályozása*, 2019, (https://zabradi.web.elte.hu/Jegyzetek/csa.pdf), felhasznált oldalak: 1-9