AZ IDEÁLELMÉLET FŐTÉTELÉRŐL

FUCHS LÁSZLÓ

I. Ideálok a matematikában először a véges algebrai számtestek egész számainak oszthatósági vizsgálatai során léptek fel. Az első lépést *E. Kummer* tette meg, mikor a körosztási testek egészeinek kanonikus felbontását az általa bevezetett „ideális számok" segítségével valósította meg. A mai értelemben vett ideál fogalmát *R. Dedekind* vezette be, hogy a véges algebrai számtestek egészeire bebizonyítsa az elemi számelmélet alaptételével analóg tételt: minden ideál egyértelműen felbontható prímideálok szorzatára. Az algebrai számelmélettel párhuzamosan az algebrai geometriában is felmerül az ideál fogalmának szükségessége s hamarosan megvetik a polinomideálok elméletét (*E. Lasker, F. S. Macaulay*). Az ideálok elméletének ezt a két, addig egymástól teljesen elszigetelten álló ágát egyesíti *Emmy Noether* egy magasabb fokon: az absztrakt ideálelméletben. *Noether*nek ez az alapvető munkája[1] messze túlnő a kommutatív gyűrűk ideálelméletén, hiszen e munkával indulnak meg intenzív módon az addig komoly jelentőséggel nemigen bíró gyűrűelméleti kutatások, amelyeknek nagy influáló hatása az egész modern algebrára közismert. Ezen munkájából kiindulva axiomatizálta *Noether* azokat az R kommutatív gyűrűket, amelyekben érvényes az ideálelmélet főtétele, vagyis a nem-triviális ideálok felbontása egyértelműen meghatározott maximális (prím-) ideálok szorzatára.[2] A *Noether* által adott szükséges és elégséges feltételek a következők:

1. *Nullosztómentesség;*[3] más szóval: az R gyűrű integritási tartomány.
2. *Egységelem létezése* (az egységelemet e-vel fogjuk jelölni).
3. *Maximum-feltétel:* R ideáljainak tetszőleges nem-üres halmaza tartalmaz legalább egy maximális ideált, vagyis oly ideált, mely nem valódi részideálja egyetlen, a szóbanforgó halmazhoz tartozó ideálnak sem. (Ez a feltétel ekvivalens azzal, hogy R minden ideáljának véges bázisa van.)

[1] *Noether* [9]. — A szögletes zárójelbe foglalt számok a dolgozat végén található irodalomjegyzékre utalnak.

[2] *Noether* [10]. — Az egyes fogalmakra vonatkozóan utalunk a jelen dolgozat II alatti részére.

[3] A nullosztómentesség szükségességének igazolására *Noether* a primideálok szorzatára való egyértelmű felbonthatóságon kívül azt is megkövetelte, hogy $P^{\nu} = P^{\nu+1}$ ne lehessen (itt P maximális ideál). E nélkül u. i. nem következik a nullosztómentesség, amint ezt a következő példa illusztrálja: Legyen R a racionális egészek gyűrűjének modulo 8 vett maradékosztálygyűrűje. Itt az összes ideálok: (1), (2), (4), (0), s mivel itt (2) primideál, érvényes a nem-triviális ideáloknak egyértelmű felbontása; de itt $(2)^3 = (2)^4$.

4. *Minimum-feltétel modulo tetszőleges nem-zérus A ideál:* egy fix $A \neq 0$ ideált tartalmazó ideálok tetszőleges nem-üres halmaza tartalmaz legalább egy minimális ideált (tehát ennek valódi részideálja már nem tartozhatik a szóbanforgó halmazhoz).

5. *A gyűrű integrálisan zárt kvocienstestében:* ha R kvocienstestének valamely x eleme kielégít egy $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ $(a_i \in R)$ alakú egyenletet (vagyis x egész elem R-re vonatkozóan), akkor x már R-hez tartozik.

Noether e munkájának előfutárja *M. Sono* vizsgálatai;[4] *Sono* az ideálelmélet főtételét szintén bizonyos axiómák felvétele után bizonyította be. Ő 3. és 4. helyett azt követeli meg, hogy minden $A \neq 0$ ideálra az R/A maradékosztálygyűrűnek legyen Jordan-féle kompoziciós-lánca; ez a feltétel — miként ezt *Noether* megmutatta — ekvivalens 3. és 4. együttes teljesülésével. *Sono*nál 5. helyett az a követelmény áll, hogy semilyen P primideálra se essék P és P^2 közé ezektől különböző ideál.

Noether eredményeit kétféle irányban sikerült élesíteni.

Az egyik irány az axiómák csökkentése. Az egységelem létezését megkövetelő axióma feleslegessé válik, ha az 5. axiómában szereplő egyenlet helyett (a bizonyos okokból indokoltabb) $x^n + (a_1 x^{n-1} + \nu_1 x^{n-1}) + \cdots + (a_{n-1} x + \nu_{n-1} x) + a_n = 0$ egyenletet vesszük alapul ($a_\varkappa \in R$, $\nu_\varkappa$ racionális egészek); ekkor u. i. a kvocienstest e egységeleme kielégíti az $x^2 - x = 0$ egyenletet, s így R-hez kell tartoznia. Továbbá *Y. Akizuki*[5] (nem-kommutatív esetben pedig *Ch. Hopkins*[6]) kimutatta, hogy egységelemes gyűrűkben a minimum-feltételből, s így a gyengébb 4. axiómából is, már következik a maximum-feltétel. Ezek szerint már az 1., 4. és 5. axiómák is elégségesek.

Az élesítés másik iránya a feltételek szükségességével kapcsolatos; e vizsgálatoknál előre fel szokás tenni a gyűrű nullosztómentességét. *Noether,* axiómáinak szükségességét bizonyítva, a felbontásban szereplő primideáloktól megkövetelte, hogy azok maximális ideálok legyenek. *K. Kubo* megmutatta,[7] hogy ezt felesleges külön kikötni. *K. Matusita*[8] továbbmenőleg azt is bebizonyította, hogy még az egyértelműség követelménye is elhagyható: elegendő csupán a primideálszorzatra való felbonthatóságot feltenni az összes nemtriviális ideálokra vonatkozóan, már abból is következnek az axiómák.[9]

Túl messze vezetne, ha itt a *Noether* említett vizsgálataihoz kapcsolódó nagyszámú eredményt bővebben ismertetni akarnók.[10] Legyen szabad mind-

[4] *Sono* [11].

[5] *Akizuki* [1], egyszerűbb bizonyítás: *Cohen* [2]. *Akizuki* többet bizonyít, mint amit fent említettünk, t. i. nála nincs feltéve egységelem létezése, hanem csupán olyan elemé, mely nem nullosztó.

[6] *Hopkins* [4]. (Eredménye fontos szerepet játszik a Wedderburn—Artin-féle struktúratételeknél.)

[7] *Kubo* [7].

[8] *Matusita* [8].

[9] Ezekre egyszerű bizonyítást *Cohen* adott [2].

[10] *Krull* munkájában [6] bő irodalomjegyzék található.

össze annak említésére szorítkoznunk, hogy gyakran a 4. axióma helyett annak azt a következményét veszik fel axiómának, hogy R-ben minden primideál ($\neq R, 0$) maximális. Így jár el pl. *B. L. van der Waerden* is ismert könyvében. Ebben az esetben azonban a maximum-követelmény nem hagyható el az axiómák közül.

A jelen közleményben szintén a primideálok szorzatára való egyértelmű felbonthatóságot vizsgáljuk, de ezt nem a gyűrűnek *összes* nem-triviális ideáljaira, hanem a gyűrűnek csak *egyetlen* kiszemelt A ideáljára tesszük. Vizsgálatainkban ezen A ideálra vonatkozóan nem elég csak azt a tulajdonságot megkövetelni, hogy A egyértelműen meghatározott primideálok szorzatára legyen bontható, hanem még azt is kell — ami automatikusan teljesül, ha a felbonthatóság minden nem-triviális ideálra teljesül, — hogy A tetszésszerinti B osztójának ($A \subset B$)[11] felbontása A felbontásának része legyen. Viszont A felbontásának egyértelműségét csak a felbontásban szereplő primideálhatványokra vonatkozóan fogjuk megkövetelni. Ez más szóval azt jelenti, hogy megengedjük azt a lehetőséget is, hogy $P^{\varkappa} = P^{\lambda}$ teljesüljön különböző $\varkappa$ és λ mellett, vagyis hogy a P primideál hatványai között a $P \supset P^2 \supset \cdots \supset P^{\lambda} = P^{\lambda+1} = \cdots$ ($\lambda \geqq 1$) reláció álljon fenn (ezek szerint pl. a [2] lábjegyzetben említett gyűrűt nem zárjuk ki vizsgálatainkból). Ekkor A felbontásában a primideálok hatványainak kitevői csak az esetben lesznek egyértelműen meghatározva, ha tőlük *minimalitást* is megkövetelünk.[12] Pontosabban szólva:

azt fogjuk mondani, hogy az R gyűrű A ideáljára teljesül az ideálelmélet főtétele, ha

$$A = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_{\nu}^{\alpha_{\nu}}$$

egyértelműen meghatározott $P_{\varkappa}$ primideálokkal és egyértelműen meghatározott minimális természetes egész $\alpha_{\varkappa}$ kitevőkkel; továbbá $A \subseteq B \subset R$ esetén B ilyen alakú:

$$B = P_1^{\beta_1} P_2^{\beta_2} \cdots P_{\nu}^{\beta_{\nu}},$$

ahol $0 \leqq \beta_{\varkappa} \leqq \alpha_{\varkappa}$.

E dolgozatban annak szükséges és elégséges feltételét fogjuk megadni, hogy az A ideálra teljesüljön az ideálelmélet főtétele. Az R gyűrű tetszőleges kommutatív gyűrű lehet (nullosztókkal vagy azok nélkül), csupán *egységelem létezését kötjük ki.* Egyik korábbi dolgozatomban [3] már adtam erre egy elégséges feltételt, de az nem okvetlenül szükséges feltétel, s azonfelül a gyűrű összes ideáljaira ki volt kötve a maximum-feltétel, ami az általánosság jelentős megszorítását jelenti. Most semmi olyan kikötés nem fog szerepelni, ami a

[11] A $\subseteq$-jel tartalmazást, a $\subset$-jel valódi tartalmazást jelöl.

[12] A fentebb mondottakból kitűnik, hogy ha a gyűrű nullosztómentes és ha az összes ideálra vonatkozóan vizsgálnók az ideálelmélet főtételének teljesülését, akkor a minimalitási megszorítás elveszti értelmét, hiszen ekkor a felbonthatóságból már következik az egyértelműség a kitevőkre vonatkozóan is.

gyűrű összes ideálját érintené, hanem csupán olyanok, amelyek A-ra és annak osztóira vonatkoznak.

Mielőtt a részletes diszkusszióba bocsátkoznánk, megjegyezzük, hogy az ismeretes eredményekből nem következik közvetlenül problémánk megoldása. Igaz ugyan, hogy lényegileg az R/A maradékosztálygyűrű ideáljait fogjuk vizsgálni, de ezekre nem alkalmazható a *Noether* és követői által kidolgozott elmélet, minthogy e maradékosztálygyűrűben általában bőven vannak nullosztó ideálok is.[13] Sőt, az R/A maradékosztálygyűrű nullideáljának (A/A-nak) primideálhatványok szorzataként való előállításából egyáltalán nem következik a megfelelő előállítás érvényessége A-ra, hanem csak A valamely részideáljára. Ennélfogva az R/A maradékosztálygyűrű ideálelméletéből nem tudnánk visszafelé következtetni teljes mértékben az A-t tartalmazó R-beli ideálok elméletére. — Az az út, amelyen problémánk megoldásához eljutunk, nagyrészt ismert módszerekből tevődik össze, de nem támaszkodik ismeretes eredményekre. Mivel arra törekedtünk, hogy az olvasótól minél kevesebb tárgyi előismeretet kívánjunk meg, a használandó módszereket részletesen kifejtjük, csupán a legalapvetőbb fogalmak (ideál, műveletek ideálokkal) ismeretét tételezzük fel.[14] Tárgyalásmódunk elemi lesz abból a szempontból is, hogy transzfinit módszerek használatára nem lesz szükségünk.

II. A továbbiakban jelentsen R tetszőleges egységelemes kommutatív gyűrűt. R elemeit latin kis betűkkel, ideáljait latin nagy betűkkel jelöljük, míg a görög betűket racionális egészek számára tartjuk fenn.

*Primideál*nak nevezünk olyan P ideált, melyre $ab \in P$-ből $a \in P$ vagy $b \in P$ következik. Célszerűnek mutatkozik a továbbiakban az egész gyűrűt nem tekinteni primideálnak. Könnyen belátható, hogy P primideálra $AB \subseteq P$-ből $A \subseteq P$ vagy $B \subseteq P$ következik. Valóban, ha $AB \subset P$ és sem A, sem B nem tartoznék P-hez, akkor lenne olyan $a \in A$ és $b \in B$, melyre $a \notin P, b \notin P$. De ekkor P prim-tulajdonsága folytán $ab \notin P$ következnék, ellentétben az $AB \subset P$ feltétellel.

*Maximális ideál*on olyan M ideált értünk, melyre $M \subset R$, de nincs olyan N ideál, mely kielégíti az $M \subset N \subset R$ feltételt. Jól ismert tény, hogy egységelemes gyűrűben minden maximális ideál prim, megfordítva azonban általában nem.

Az A, B ideálok (A, B) legnagyobb közös osztójára és $A \cap B$ legkisebb közös többesére teljesül a számelméletből jólismert formula analogonja: $(A, B) = R = (e)$ esetén $A \cap B = AB$. Valóban: az $AB \subseteq A \cap B$ tartalmazási reláció a definíciók triviális következménye, az ellenkező irányú pedig a követ-

[13] *Kubo* vizsgálatai [7] bizonyos fajtájú, nem szükségképpen nullosztómentes gyűrűkre is érvényesek, de ezek a jelen problémára csak akkor lennének alkalmazhatók, ha A maga primideálhatvány lenne.

[14] Az egészen alapvető fogalmak értelmezését lásd pl. *van der Waerden* könyvében [12].

kezőképpen látható be:

$$A \cap B = (A, B)(A \cap B) = (A(A \cap B), B(A \cap B)) \subseteq (AB, BA) = AB.$$

Az A, B ideálokra $A : B$ jelöli R azon x elemeinek halmazát, melyekre $xB \subseteq A$. A definícióból tüstént folyik, hogy $A : B$ ismét ideál lesz, mely A-t tartalmazza és rá nézve teljesül:

$$(A:B):C = A:BC = (A:C):B; \quad A:B = A:(A, B).$$

Az A ideálnak legyen P primosztója, $A \subseteq P$. A-nak P-hez tartozó $A(P)$ *főkomponensén*[15] értjük mindazon x gyűrűelemekből álló halmazt, amelyekhez található oly $c \notin P$ elem, hogy $cx \in A$. $A(P)$ ismét ideál lesz, mert ha $x \in A(P)$ és $c \notin P$-re teljesül $cx \in A$, akkor tetszőleges $r \in R$-re $c(rx) = r(cx) \in A$, vagyis $rx \in A(P)$; továbbá, ha $y \in A(P)$ és $d \notin P$-re $dy \in A$, akkor $cd(x \pm y) \in A$ és $cd \notin P$ miatt $x \pm y \in A(P)$. Az $A(P)$ főkomponensre nyilván fennáll: $A \subseteq A(P)$. Hogy $A \subseteq P$ esetén $A(P) \subseteq P$ is áll, azt a következő okoskodás mutatja: ha $x \in A(P)$, van $c \notin P$, hogy $cx \in A$, így annál inkább $cx \in P$, ahonnan $c \notin P$ miatt valóban $x \in P$ adódik. Az is könnyen látható, hogy $A(P) \subseteq B(P)$, feltéve, hogy $A \subseteq B$. Csakugyan: ha $x \in A(P), c \notin P$ és $cx \in A$, akkor $cx \in B$ is, tehát $x \in B(P)$.

III. Az a tétel, amit be kívánunk bizonyítani, a következő.

Tétel. *Az R kommutatív egységelemes gyűrű A ideáljára akkor és csak akkor teljesül az ideálelmélet főtétele, ha*

(i) *érvényes a minimum-feltétel modulo A, és*

(ii) *A minden olyan P primosztójára, melyre az $A(P)$ főkomponens P-nek valódi többszöröse, igaz az, hogy R-ben nem létezik a $P^2 \subset M \subset P$ tulajdonságú M ideál (vagyis P^2 közvetlen többszöröse P-nek).*

Az (i) és (ii) feltételek *szükségessége* könnyen adódik. Ha az $A = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_\nu^{\alpha_\nu}$ ideálra érvényes az ideálelmélet főtétele, akkor A-nak csak véges-sok különböző osztója van, tehát modulo A okvetlenül érvényes a minimum-feltétel (sőt, a maximum-feltétel is). Ekkor pedig az alább bizonyítandó 1. lemmából következik, hogy a $P_\varkappa$ ($\varkappa = 1, 2, \ldots, \nu$) primideálok maximálisak R-ben. Továbbá $A(P_\varkappa) = P_\varkappa^{\alpha_\varkappa}$ kell, hogy fennálljon. U. i.: hogy $P_\varkappa^{\alpha_\varkappa} \subseteq A(P_\varkappa)$, az onnan folyik, hogy $P_1^{\alpha_1} \cdots P_{\varkappa-1}^{\alpha_{\varkappa-1}} P_{\varkappa+1}^{\alpha_{\varkappa+1}} \cdots P_\nu^{\alpha_\nu}$ tartalmaz P_λ maximalitásánál fogva $P_\varkappa$-hoz nem tartozó elemet is, és ennek $P_\varkappa^{\alpha_\varkappa}$ tetszőleges elemével vett szorzata A-ba tartozik. Viszont a $P_\varkappa^{\alpha_\varkappa} \subseteq A(P_\varkappa)$ tartalmazás nem lehet valódi, mert ellenkező esetben $A(P_\varkappa)$-ban lenne oly x elem, mely $P_\varkappa^{\alpha_\varkappa - 1}$-hez hozzátartozik, de $P_\varkappa^{\alpha_\varkappa}$-hoz nem.[16] Ha $c \notin P_\varkappa$ és $cx \in A \subseteq P_\varkappa^{\alpha_\varkappa}$, akkor $P_\varkappa x \subseteq P_\varkappa^{\alpha_\varkappa}$ tekintetbe vételével: $x \in Rx = (P_\varkappa, c)x = (P_\varkappa x, cx) \subseteq P_\varkappa^{\alpha_\varkappa}$, ellentmondás. — Ha mármost $A(P_\varkappa) = P_\varkappa^{\alpha_\varkappa} \subset P_\varkappa$, akkor $\alpha_\varkappa \geqq 2$. P^2 és P közé nem eshetik tőlük különböző ideál, mert ez A-nak olyan osztója lenne, mely nem állítható elő primideál-

[15] A főkomponens fogalmát *Krull* vezette be [5].

[16] Itt $\alpha_\varkappa$-ról feltételeztük, hogy minimálisnak van választva.

hatványok szorzataként. Ennélfogva (ii) is teljesül, s így a szükségesség igazolva van.

Megjegyzés. A bizonyításból látható, hogy a szükségesség igazolásánál nem használtuk ki a felbontás egyértelműségét.

IV. A feltételek *elégségességének* kimutatásához szükségünk van néhány lemmára. Előbb ezeket fogjuk bizonyítani.

1. *lemma.* Ha modulo A érvényes a minimum-feltétel, akkor A-nak minden P primosztója maximális ideál R-ben.

Legyen $a \notin P$; ekkor a prim-tulajdonság miatt egyszersmind $a^\nu \notin P$ $(\nu = 1, 2, \ldots)$. Kimutatjuk, hogy $(P, a) = R$, amiből már következik P maximális volta. A minimum-követelmény miatt az A-t tartalmazó

$$(P, a) \supseteq (P, a^2) \supseteq \cdots \supseteq (P, a^\nu) \supseteq \cdots$$

ideálok között van minimális, tehát valamilyen természetes egész ν-re $(P, a^\nu) = (P, a^{\nu+1})$. Így $a^\nu \in (P, a^{\nu+1})$, vagyis $a^\nu = p + ra^{\nu+1}$ $(p \in P, r \in R)$, ahonnan $a^\nu(e - ra) = p \in P$. Minthogy P primideál és $a^\nu \notin P$, ezért $e - ra \in P$, tehát $e \in (P, a)$. Más szóval: $(P, a) = R$, q. e. d.

2. *lemma.*[17] Ha teljesül a minimum-követelmény modulo A és $A \subseteq B \subset R$, akkor van oly P primideál, $B \subseteq P \subset R$, melyre $B : P \supset B$.

Azon C $(C \supset B)$ ideálok halmaza, melyekre $B : C \neq R$, nem-üres, mert pl. R e halmazhoz tartozik. Legyen C_0 e halmaz egy minimális ideálja. Ekkor $P = B : C_0$ primideál, mert ha $a \notin P, b \notin P, ab \in P$ lenne, akkor $P \subset P : a$ (hiszen $b \in P : a$), viszont $P : a \subset R$ tekintettel arra, hogy $Ra = (a) \subseteq P$ nem lehet. Ennélfogva $P : a = (B : C_0) : a = B : (aC_0) = B : (aC_0, B)$ tekintetbe vételével $B : C_0 \subset B : (aC_0, B) \subset R$, ami ellentmond C_0 minimalitásának. Így P prim és mivel $B : P \supseteq C_0$, ezért $B : P = B$ nem lehet s állításunk igazolva van.

3. *lemma.* Ha modulo A érvényes a minimum-feltétel, akkor A-nak véges-sok primosztója van. (Megjegyezzük: az, hogy egyáltalán van primosztója A-nak ($A \neq R$ esetén), a 2. lemmából következik.)

Ha $P_1, P_2, \ldots$ A-nak összes különböző primosztói, akkor a minimum-feltétel következtében a

$$P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \cdots \supseteq P_1 \cap P_2 \cap \cdots \cap P_\nu \supseteq \cdots$$

láncban valamely ν-re

$$P_1 \cap P_2 \cap \cdots \cap P_\nu = P_1 \cap P_2 \cap \cdots \cap P_\nu \cap P_{\nu+1}$$

teljesül, innen pedig

$$P_1 P_2 \cdots P_\nu \subseteq P_1 \cap P_2 \cap \cdots \cap P_\nu \subseteq P_{\nu+1},$$

ill. $P_{\nu+1}$ prim volta miatt: $P_\varkappa \subseteq P_{\nu+1}$ valamely $\varkappa = 1, 2, \ldots, \nu$-re. Ez pedig különböző primideálokra lehetetlen, mert ezek az 1. lemma miatt maximális ideálok R-ben.

[17] E lemma (bizonyításával együtt) *Cohen*től való [2].

4. *lemma.* Ha érvényes a minimum-feltétel modulo A, továbbá $A \subset P$ és $A(P)$ az A-nak P-hez tartozó főkomponense, akkor van oly λ kitevő, hogy $P^\lambda \subseteq A(P)$.

Mivel $A(P) \subseteq P$ folytán e főkomponens különbözik R-től, a 2. lemma alapján arra következtethetünk, hogy létezik oly P^* primideál, hogy $A(P):P^* \supset A(P)$. Itt $P^* \neq P$ nem lehet, mert ha $x \in A(P):P^*$, akkor $xP^* \subseteq A(P)$ és oly c-t véve, hogy $c \in P^*, c \notin P$, adódik: $cx \in A(P)$. A főkomponens definíciója folytán van oly $d \notin P$, melyre $cdx \in A$. Innen $cd \notin P$ miatt $x \in A(P)$, tehát $A(P):P^* = A(P)$ lenne. Kaptuk tehát, hogy $A(P):P \supset A(P)$.

Ha $A(P):P^\mu$ még különbözik R-től, akkor legyen neki P^* oly primosztója, hogy $A(P):P^\mu \subset (A(P):P^\mu):P^* = (A(P):P^*):P^\mu$. Innen $A(P) \subset A(P):P^*$, tehát a megelőző bekezdés értelmében $P^* = P$, s így $A(P):P^\mu \subset A(P):P^{\mu+1}$. Mármost ha az

$$(A(P),P) \supseteq (A(P),P^2) \supseteq \cdots$$

csökkenő ideálláncban $(A(P),P^\lambda)$ minimális ideál, akkor

$$(A(P),P^\lambda) = (A(P),P^{\lambda+1})$$

miatt

$$A(P):P^\lambda = A(P):(A(P),P^\lambda) = A(P):(A(P),P^{\lambda+1}) = A(P):P^{\lambda+1},$$

s így az imént mondottak alapján csak $A(P):P^\lambda = R$ lehet, ami éppen azt fejezi ki, hogy $P^\lambda \subseteq A(P)$.

5. *lemma.* Ha az A-t tartalmazó ideálok eleget tesznek a minimum-követelménynek, akkor A előállítható (véges-sok) főkomponensének szorzataként.

A-nak összes primosztói legyenek: $P_1, P_2, \ldots, P_\nu$. Mindenekelőtt kimutatjuk az

$$A = A(P_1) \cap A(P_2) \cap \cdots \cap A(P_\nu)$$

előállítás helyességét. Minthogy $A(P_\varkappa) \supseteq A$ s így A benne van főkomponensei közös részében, elegendő azt verifikálni, hogy ha $x \in A(P_1) \cap \cdots \cap A(P_\nu)$, akkor $x \in A$ is. Tekintsük az $A:x$ ideált. Ez nem lehet benne egyik $P_\varkappa$-ban sem ($\varkappa = 1, \ldots, \nu$), mert $x \in A(P_\varkappa)$-hoz található oly $c_\varkappa \notin P_\varkappa$, hogy $c_\varkappa x \in A$, azaz $c_\varkappa \in A:x$. Ennélfogva $A:x$ nem lehet osztható A-nak egyetlen primosztójával sem, ami $A \subseteq A:x$ és a 2. lemma tekintetbe vételével csak úgy lehet, ha $A:x = R$, azaz $x \in A$.

Hogy a szorzatelőállítást is kimutassuk, vegyük figyelembe, hogy

$$(A(P_1) \cdots A(P_{\varkappa-1}), A(P_\varkappa)) = R \qquad (\varkappa = 2, \ldots, \nu)$$

teljesül, hiszen a baloldalon álló ideálnak nem lehet egyetlen P primosztója sem, mert ebből a 4. lemma miatt $P_1^{\lambda_1} \cdots P_{\varkappa-1}^{\lambda_{\varkappa-1}} \subseteq A(P_1) \cdots A(P_{\varkappa-1}) \subseteq P$ és $P_\varkappa^{\lambda_\varkappa} \subseteq P$, innen pedig $P_\mu \subseteq P$ és $P_\varkappa \subseteq P$ következnék valamilyen $\mu = 1, 2, \ldots, \varkappa - 1$-re, ami az 1. lemmával ellenkezésben van. Minthogy pedig $(A, B) = R$ esetén $A \cap B = AB$, ezért rendre kapjuk:

$$A(P_1) \cap A(P_2) = A(P_1) \cdot A(P_2), \quad A(P_1)A(P_2) \cap A(P_3) = A(P_1)A(P_2)A(P_3) \text{ stb.}$$

Így tehát valóban: $A = A(P_1)A(P_2) \cdots A(P_\nu)$.

6. *lemma.* Ha P maximális ideál, továbbá P és P^2 közé nem esik ezektől különböző ideál, akkor minden B ideál, melyre $P^\lambda \subseteq B \subseteq P$, P-nek valamilyen hatványa.

Ha P és P^2 $(\subset P)$ közé nem esik újabb ideál és c a $c \in P$, $c \notin P^2$ követelményeknek eleget tevő tetszőleges elem, akkor $(c, P^2) = P$. Teljes indukcióval következik, hogy ekkor minden természetes egész μ-re:

$$P^\mu = (c^\mu, P^{\mu+1}). \tag{1}$$

Valóban, ha ez μ-re igaz, akkor

$$P^{\mu+1} = (c^\mu P, P^{\mu+2}) = (c^\mu (c, P^2), P^{\mu+2}) = (c^{\mu+1}, c^\mu P^2, P^{\mu+2}) = (c^{\mu+1}, P^{\mu+2}).$$

Legyen mármost B egy a feltételt kielégítő ideál és legyen μ az a legnagyobb, ill. $\varkappa$ az a legkisebb kitevő, melyre[18]

$$P^\varkappa \subseteq B \subset P^\mu.$$

Ha $\varkappa = \mu$, készen vagyunk. Kimutatjuk, hogy $\varkappa > \mu$ ellentmondásra vezet. Legyen $b \in B$, de $b \notin P^{\mu+1}$. Ez esetben $b \in P^\mu$ és (1) miatt létezik olyan $r \in R$, hogy $b \equiv rc^\mu \pmod{P^{\mu+1}}$. Itt $r \notin P$, ellenkező esetben u. i. $rc^\mu \in P^{\mu+1}$, $b \notin P^{\mu+1}$ ellentmondás lenne. Az utóbbi kongruenciából

$$rc^\mu \equiv 0 \pmod{(B, P^{\mu+1})},$$

ahonnan $Pc^\mu \subseteq P^{\mu+1}$ miatt $c^\mu \in Rc^\mu = (P, r)c^\mu = (Pc^\mu, rc^\mu) \subseteq (B, P^{\mu+1})$. Innen azt kapjuk, hogy

$$c^{\varkappa-1} = c^\mu c^{\varkappa-\mu-1} \in (B, P^{\mu+1}) P^{\varkappa-\mu-1} \subseteq (B, P^\varkappa) = B,$$

s így (1) miatt

$$P^{\varkappa-1} = (c^{\varkappa-1}, P^\varkappa) \subseteq B.$$

ellentétben $\varkappa$ minimalitásával.

V. Ezek után rátérhetünk a tételben foglalt feltételek elégségességének igazolására. Tegyük fel, hogy az (i) és (ii) feltételek teljesülnek; bebizonyítjuk, hogy ekkor A-ra érvényes az ideálelmélet főtétele.

Az 5. lemmából következik, hogy A előállítható (véges-sok) főkomponensének szorzataként. Ki kell mutatnunk, hogy mindegyik főkomponens primideálhatvány. Nyilván csak azt az esetet kell tekintenünk, mikor $A(P_\varkappa) \neq P_\varkappa$. Ekkor a 4. lemma szerint $P_\varkappa^\lambda \subseteq A(P_\varkappa) \subset P_\varkappa$, és így a 6. lemma felhasználásával arra az eredményre jutunk, hogy $A(P_\varkappa)$ a $P_\varkappa$ primideálnak valamely hatványa:

$$A = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_\nu^{\alpha_\nu}.$$

Vegyük most tekintetbe, hogy A-nak más primosztója, mint $P_1, P_2, \ldots, P_\nu$, nem lehet, továbbá, hogy $A(P_\varkappa) = P_\varkappa^{\alpha_\varkappa}$ egyértelműen meg van határozva P által. Ha még az $\alpha_\varkappa$ kitevőt a lehető legkisebbnek választjuk (amennyiben

[18] Az az eset, midőn a kívánt tulajdonságú μ nem létezik, triviális, t. i. ekkor B megegyezik P-nek (tovább már nem esökkenő) hatványával. Így $\varkappa \geqq \mu$.

egyáltalán mód van választásra), akkor világos, hogy A-nak ez az előállítása egyértelmű.

Hátra van még az A osztóira vonatkozó állítás igazolása. Legyen $A \subseteq B \subset R$. Mindenekelőtt világos, hogy a minimum-feltétel modulo B is érvényes; ennélfogva B szintén főkomponenseinek szorzatával egyenlő (5. lemma). Továbbá tekintettel arra, hogy $P_\varkappa^{\alpha_\varkappa} = A(P_\varkappa) \subseteq B(P_\varkappa)$ teljesül minden $\varkappa$-ra, ezért a 6. lemma szerint $B(P_\varkappa)$ csak R-rel vagy $P_\varkappa^{\beta_\varkappa}$-val lehet egyenlő $(0 < \beta_\varkappa \leqq \alpha_\varkappa)$.

Ezzel tételünk bizonyítását befejeztük.

Végezetül megjegyezzük, hogy ha az $\alpha_\varkappa$ kitevők egyértelműségét is biztosítani akarnók, akkor az (i) és (ii) feltételekhez még hozzá kellene venni a következőt is:

(iii) $A(P).P$ *különbözik* P-*től.*

Ezen állításunk bizonyítása egészen kézenfekvő.

IRODALOM

[1] *Yasuo Akizuki,* Teilerkettensatz und Vielfachenkettensatz, *Proceedings of the Phys. Math. Soc. of Japan, 17* (1935), 337—345.

[2] *I. S. Cohen,* Commutative rings with restricted minimum condition, *Duke Math. Journal, 17* (1950), 27—41.

[3] *L. Fuchs,* A note on the idealizer of a subring, *Publicationes Math. Debrecen, 1* (1950), 160—161.

[4] *Charles Hopkins,* Rings with minimum condition for left ideals, *Annals of Math., 40* (1939), 712—730.

[5] *W. Krull,* Idealtheorie in Ringen ohne Endlichkeitsbedingung, *Math. Annalen, 101* (1929), 729—744.

[6] *W. Krull, Idealtheorie,* Ergebnisse d. Math. u. Grenzgeb., *4,* (Berlin, 1935).

[7] *Keizi Kubo,* Über die Noetherschen fünf Axiome in kommutativen Ringen, *Journal of Sci. Hiroshima Univ., 10* (1940), 77—84.

[8] *Kameo Matusita,* Über ein bewertungstheoretisches Axiomensystem für die Dedekind—Noethersche Idealtheorie, *Japanese Journal of Math., 19* (1944), 97—110.

[9] *Emmy Noether,* Idealtheorie in Ringbereichen, *Math. Annalen, 83* (1921), 24—66.

[10] *Emmy Noether,* Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, *Math. Annalen, 96* (1927), 26—61.

[11] *M. Sono,* On congruences, I—IV, *Mem. Coll. Sci. Kyoto, 2* (1917), 203—226; *3* (1918), 113—149, 189—197 és 229—308.

[12] *B. L. van der Waerden, Moderne Algebra.* II (Berlin, 1940).