10. Primér ideálok, Lasker-Noether tétel

R ebben a fejezetben kivétel nélkül egységelemes kommutatív gyűrűt jelöl.

10.1 Primér ideál, irreducibilis ideál

10.1.1 Definíció: $Q \trianglelefteq R$ ideál primér, ha $ab \in Q \Rightarrow (a \in Q$ vagy $\exists n \in \mathbb{N}: b^n \in Q)$, másképp megfogalmazva $ab \in Q \Rightarrow (a \in Q$ vagy $b \in \sqrt{Q})$. Nyilván minden prímideál primér ideál. Q P-primér, ha primér és radikálja P.

10.1.2 Állítás: Q primér $\Leftrightarrow$ R/Q-ban minden nullosztó nilpotens. (Egyszerűen kiszámolható.)

10.1.3 Állítás: ha Q primér, akkor $P=\sqrt{Q})$ prímideál.

Bizonyítás: $ab \in P \Rightarrow \exists k \in \mathbb{N}: (ab)^k \in Q$, azaz $a^k b^k \in Q$. Ekkor vagy $a^k \in Q$, vagy valamely $m \in \mathbb{N}$-re $(b^k)^m \in Q$. Az első esetben $a \in P$, a másodikban $b \in P$.

Példák:

– $R=\mathbb{Z}$ esetén (n) primér $\Leftrightarrow$ $(n=0$ vagy $n=p^s$, p prím, $s \in \mathbb{Z}^+)$.
– legyen $R=K[x,y]$, $Q=(x,y^2)$. Ez primér, mert $R/Q \simeq K[y]/(y^2)$, amiben a nullosztók $\bar{y}$ többszörösei és ezek $\bar{y}^2=0$ miatt nilpotensek. Viszont Q nem áll elő semmilyen prímideál hatványaként. (Ezt csak úgy tehetné, ha a radikáljának hatványa lenne, de $\sqrt{Q}=(x,y)$. Ennek első hatványa bővebb Q-nál, minden további hatványa pedig szűkebb nála.)
– legyen $R=K[x,y,z]/(xy-z^2)$. Jelölje $\bar{x},\bar{y},\bar{z}$ az x,y,z polinomok képét a természetes homomorfimusnál. Legyen $P=(\bar{x},\bar{z})$. Ez prímideál, mert $R/P \simeq K[x,y,z]/(x,z) \simeq K[y]$ nullosztómentes. $\bar{x}\cdot\bar{y}=\bar{z}^2 \in P^2$ de $\bar{x} \notin P^2$ (ez némi számolással kijön…) és $\bar{y} \notin \sqrt{P^2}=P$. Ezek szerint P^2 nem primér ideál, hiába áll elő prímideál hatványaként.

10.1.4 Állítás: ha $\sqrt{A}=M$ maximális ideál R-ben, akkor A M-primér.

Bizonyítás: R/A-ban M képe, $M/A=M^*$ is maximális. A faktorgyűrű nilradikálja $N(R/A)=\{x+A \mid \exists n: x^n+A=A\}=\sqrt{A}/A=M^*$. Ez tehát a prímideálok metszete, azaz minden prímideál tartalmazza M^*-ot. Mivel maximális, ez az egyetlen prímideál, tehát az egyetlen maximális ideál (egységelemes kommutatív gyűrűben minden maximális ideál prímideál, R/A pedig ilyen). Tehát R/A lokális gyűrű, azaz minden nem-egység M^*-ban van. Speciálisan minden nullosztó eleme a nilradik álnak, azaz nilpotens; ez volt bizonyítandó.

10.1.5 Definíció: $A,B \triangleleft R$-re A és B hányadosideálja $(A:B)=\{r \in R \mid rB \subseteq A\}$. Nyilvánvaló, hogy ez is ideál, $A \subseteq (A:B)$, $(\bigcap A_i : B)=\bigcap (A_i : B)$. Az $(A:x)$ jelölés alatt a $(A:(x))$ hányadosideált értjük.

Megjegyzés: nyilván $A \triangleleft R$, $B \subseteq R$ esetén $\{r \in R \mid rB \subseteq A\}=(A:(B))$, speciálisan $(A:x)=\{r \in R \mid rx \in A\}$. A $B \triangleleft R$ feltétel tehát nem túl fontos.

10.1.6 Definíció: $B \triangleleft R$ annulátor-ideálja $Ann(B)=(0:B)$.

10.1.7 Lemma: ha Q P-primér, $x \in R$, akkor

(1) $x \in Q \Rightarrow (Q:x)=(1)$,
(2) $x \notin Q \Rightarrow \sqrt{(Q:x)}=P$ és $(Q:x)$ P-primér
(3) $x \notin P \Rightarrow (Q:x)=Q$.

Bizonyítás: **(1)**: ha $x \in Q$, akkor $\forall r \in R$: $r\cdot(x) \subseteq Q$, tehát $(Q:x)=R=(1)$.

(2): $y \in (Q:x) \Leftrightarrow xy \in Q$. Mivel $x \notin Q$, ebből $y \in P$. Tehát $Q \subseteq (Q:x) \subseteq (P)$. Véve az egyenlet radikálját $P \subseteq \sqrt{(Q:x)} \subseteq P$. Ezek szerint ha Q primér, akkor P-primér. Legyen $yz \in (Q:x)$ és lássuk be, hogy $z \in P$ vagy $y \in (Q:x)$, akkor kész vagyunk. Ha nem, akkor $x\cdot yx \in Q$ -ból következik $xy \in Q$, azaz $y \in (Q:x)$.

(3): $(Q:x) \supseteq Q$ mindig teljesül. Ha $x \notin P$ de $xy \in Q$, akkor $y \in Q$, amiből $(Q:x) \subseteq Q$.

10.1.8 Állítás: ha Q_i minden $i \in \mathbf{I}$-re P-primér, akkor $Q=\bigcap_{i \in \mathbf{I}} Q_i$ is P-primér.

Bizonyítás: $\sqrt{Q}=\sqrt{\bigcap Q_i}=\bigcap\sqrt{Q_i}=P$, tehát ha Q primér, akkor P-primér. Ha $xy\in Q$ de $x\notin Q$, akkor $\exists i\colon x\notin Q_i \Rightarrow y\in\sqrt{Q_i}=P=\sqrt{Q}$.

10.1.9 Definíció: $I\lhd R$ irreducibilis ideál, ha az ideálhálóban metszetirreducibilis.

10.1.10 Tétel: ha R noether, akkor minden ideál előáll véges sok irreducibilis ideál metszeteként.

Bizonyítás: R pontosan akkor noether, ha az $I(R)$ ideálhálóra teljesül a maximumfeltétel. Ideálháló moduláris, tehát alkalmazhatjuk **9.9.8**-at és kész vagyunk.

10.1.11 Tétel: ha R noether, akkor minden irreducibilis ideálja primér.

Bizonyítás: először azt látjuk be, hogy ha (0) irreducibilis ideál, akkor primér, tehát R minden nullosztója nilpotens.

Legyen $xy=0$. Azt állítjuk, hogy ha $x\neq 0$, akkor alkalmas n kitevőre $y^n=0$. Ha valamely $r\in R, k\in\mathbb{Z}^+$-ra $ry^k=0$, akkor $ry^{k+1}=y\cdot 0=0$, így $Ann(y^k)\subseteq Ann(y^{k+1})$. Tekintsük az $Ann(y)\subseteq Ann(y^2)\subseteq Ann(y^3)\subseteq\ldots$ végtelen ideálsorozatot. R noether, tehát ez idővel stabilizálódik: $Ann(y^n)=Ann(y^{n+1})$.

$(0)\subseteq(x)\cap(y^n)$ és $(x)\neq(0)$. Ha $(y^n)=(0)$, akkor kész vagyunk. $\dagger$ $(y^n)\neq(0)$. Ekkor $(0)\neq(x)\cap(y^n)$, hiszen (0) irreducibilis, azaz választhatunk egy $a\neq 0$ elemet $(x)\cap(y^n)$-ból. $a\in(x)$ miatt $ay=0$. $a\in(y^n)$ miatt $\exists b\in R\colon a=by^n$. Ekkor $by^{n+1}=ay=0$, azaz $b\in Ann(y^{n+1})=Ann(y^n)$, $by^n=0$. Eszerint $a=by^n=0$, $\lightning$.

Legyen $A\lhd R$ tetszőleges. Vegyük észre, hogy $I(R)$-ben A pontosan akkor metszetirreducibilis, ha az $[A,R]$ intervallumban metszetirreducibilis.

Könnyen látható, hogy $\varphi\colon I\mapsto I/A$ bijekció R I-t tartalmazó ideáljai és R/A ideáljai közt. Az is triviális, hogy az $I,J\supseteq A$ ideálokra $I\subseteq J \Leftrightarrow \left(I/A\subseteq J/A\right)$. Így φ egy oda-vissza rendezéstartó bijekció, ismertebb nevén hálóizomorfizmus az $I(R)$ háló $[A,R]$ részhálójából $I\left(R/A\right)$-ba. Tehát A pontosan akkor metszetirreducibilis $[A,R]$-ben, ha $A\varphi=(0)$ metszetirreducibilis R/A-ben. A maximumfeltétel öröklődik az $[A,R]$ részhálóra, azaz R/A is noether. A tétel már belátott első része szerint ekkor R/A-ban minden nullosztó nilpotens, tehát A primér R-ben. Ezzel az állítást beláttuk.

10.2 Primér és irredundáns felbontás, Lasker-Noether tétel

10.2.1 Definíció: primér felbontás alatt egy A ideál felírását értjük véges sok primér ideál metszeteként.

10.2.2 Definíció: legyen R noether, $A\lhd R$. Az $A=\bigcap_{i=1}^n Q_i$ primér felbontás irredundáns, ha a Q_i-k között nincs felesleges ($(\bigcap_{j\neq i}Q_j)\nsubseteq Q_i$) és ha $i\neq j$, akkor $\sqrt{Q_i}\neq\sqrt{Q_j}$ (ha Q_i és Q_j egyaránt P-primér, akkor a metszetük is az, tehát e két tényező triviális módon helyettesíthető eggyel – ezt nem akarjuk irredundánsnak nevezni). Az előző két tétel szerint minden A-nak van primér felbontása és ez nyilván lerövidíthető irredundánssá, azaz minden $A\lhd R$-nek van irredundáns felbontása.

10.2.3 Lemma: ha P prímideál R-ben és az $A_1,A_2,\ldots,A_n$ ideálokra $\bigcap_{k=1}^n A_k\subseteq P$, akkor valamely k-ra $A_k\subseteq P$.

Bizonyítás: $\dagger$ $\forall k\in\{1,\ldots,n\}\exists x_k\in A_k\setminus P$. Ekkor $(\prod_{k=1}^n x_k)\in\prod A_k\subseteq\bigcap A_k\subseteq P$. Mivel P prímideál, valamelyik tényező benne kellene legyen, hogy a szorzat benne lehessen, $\lightning$.

10.2.4 Következmény: minden prímideál irreducibilis.

10.2.5 Lasker-Noether tétel: legyen $A\lhd R$. Ekkor n értéke bármely $A=\bigcap_{k=1}^n Q_k$ irredundáns felírásnál azonos, sőt $P_k=\sqrt{Q_k}$ jelöléssel $\{P_k \mid 1\leq k\leq n\}$ is mindig ugyanaz (amennyiben létezik primér felbontás, azaz pl. ha R noether).

Bizonyítás: nyilván elég $\{P_k \mid 1\leq k\leq n\}$ állandóságát belátni. Azt állítjuk, hogy $\{P_k\}$ pontosan az olyan prímideálok halmaza, melyek előállnak $\sqrt{(A:x)}$ alakban.

(1) Ha $P=\sqrt{(A:x)}$ prímideál, akkor szerepel $\{P_k\}$-ban.

$P=\sqrt{(A:x)}=\sqrt{((\bigcap Q_k):x)}=\sqrt{\bigcap(Q_k:x)}=\bigcap\sqrt{(Q_k:x)}$. **10.1.7.1** szerint $x\in Q_k$ esetén $\sqrt{(Q_k:x)}=\sqrt{R}=R$. Ha $x\notin Q_k$, akkor **10.1.7.2** alapján $(Q_k:x)$ P_k-primér, azaz $\sqrt{(Q_k:x)}=P_k$. Tehát $P=\bigcap_k(P_k \text{ vagy } R)$. **10.2.3** szerint P_k megegyezik a metszet valamely tagjával, ez pedig nem lehet R, hiszen azt nem nevezzük prímideálnak. Tehát alkalmas k-ra $P=P_k$, ahogy azt szerettük volna.

(2) P_i előáll $\sqrt{(A:x)}$ alakban.

Legyen $x\in(\bigcap_{k\neq i}Q_k)\setminus Q_i$ (irredundáns felírásnál ez a halmaz nem üres, tehát választható ilyen x). Ekkor a fenti számolással $\sqrt{(A:x)}=\sqrt{(Q_i:x)}\cap\left(\bigcap_{k\neq i}\sqrt{(Q_k:x)}\right)=P_i\cap\left(\bigcap_{k\neq i}R\right)=P_i$.

10.2.6 Definíció: legyen A olyan ideál R-ben, amelynek van primér felbontása. Ekkor létezik $A=\bigcap_k Q_k$ irredundáns felírás is. Az A-hoz tartozó prímideálok alatt a $P_k=\sqrt{Q_k}$ prímideálok halmazát értjük. A Lasker-Noether tétel következtében ez a definíció értelmes. Nyilván $A\subseteq P_k$, hiszen $A\subseteq Q_k\subseteq P_k$.

10.2.7 Definíció: az $A\triangleleft R$ ideálhoz tartozó minimális avagy izolált prímideálok az A-hoz tartozó prímideálok halmazának minimális elemei.

10.2.8 Állítás: ha $A\triangleleft R$ és a P prímideálra $A\subseteq P$, akkor valamely P_k A-hoz tartozó minimális prímideálra $P_k\subseteq P$. Tehát az A-hoz tartozó minimális prímideálok a minimális A-t tartalmazó prímideálok.

Bizonyítás: $P=\sqrt{P}\supseteq\sqrt{A}=\bigcap_k\sqrt{Q_k}=\bigcap_k P_k$. **10.2.3** szerint P tartalmazza valamelyik P_k-t, amely tartalmaz A-hoz tartozó izolált prímideált.

10.2.9 Következmény: ha R noether, akkor az A-t tartalmazó prímideálok között véges sok minimális van.

Megjegyzés: Q primér $\Leftrightarrow$ Q-hoz pontosan egy prímideál tartozik.

10.2.10 Tétel: ha A-nak van primér felbontása és P A-hoz tartozó izolált prímideál, akkor az A irredundáns felbontásában szereplő P-primér ideál egyértelmű. Ha P beágyazott prímideál (A-hoz tartozó prímideál, de nem minimális), akkor a hozzá tartozó Q nem feltétlenül egyértelmű. (Ezt nem bizonyítjuk.)

Példa: legyen $n\in\mathbb{Z}$, $n>1$, $A=(n)\triangleleft\mathbb{Z}$. Írjuk fel n-t prímhatványok szorzataként: $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$. Ekkor $(n)=\bigcap_{k=1}^{s}(p_k^{\alpha_k})$ irredundáns felbontás, az (n)-hez tartozó prímideálok $\{(p_k)\,|\,1\leq k\leq s\}$. A Lasker-Noether tétel szerint ezeket n egyértelműen meghatározza. Mivel mindegyik izolált, az iménti tétel szerint a kitevők is egyértelműek. Ezzel ismét beláttuk az egyértelmű prímfelbontás létezését.

10.3 A tétel geometriai jelentése

Legyen K test. Vegyük egyrészt a K^n affin teret, másrészt az $R=K[x_1,\ldots,x_n]$ polinomgyűrűt. Tetszőleges $X\subseteq R$ részhalmazra legyen $V(X)=\{(v_1,v_2,\ldots,v_n)\in K^n\,|\,\forall f\in X\colon f(v_1,\ldots,v_n)=0\}$. Az ilyen halmazokat affin algebrai halmaznak nevezzük.

$V(X)\cup V(Y)=V(X\cdot Y)$, hiszen akár a jobb, akár a bal oldalnak pontosan akkor nem eleme $v\in K^n$, ha X-nek és Y-nak is van olyan eleme, ami nem tűnik el (nem ad 0 behelyettesítési értéket) v-ben. $V(X)\cap V(Y)=V(X\cup Y)$, mert bármelyik oldalnak pontosan akkor eleme a, ha X és Y minden eleme eltűnik V-ben. Ha $X\subseteq Y$, akkor $V(Y)\subseteq V(X)$. Ha X minden eleme eltűnik az $a=(a_1,\ldots,a_n)$ pontban, akkor nyilván (X) minden eleme is eltűnik, azaz $V(X)=V\big((X)\big)$. Így szorítkozhatunk a $V(A)\ :\ A\triangleleft R$ halmazokra.

Hilbert bázistétele szerint R noether, tehát A végesen generált: előáll $(f_1,f_2,\ldots,f_m)$ alakban, azaz $V(A)=V(f_1,f_2,\ldots,f_m)=\bigcap_{i=1}^{m}V(f_i)$. Tehát $V(A)$ megadható véges sok polinom nullhelyeinek metszeteként.

R noether, így A-nak a Lasker-Noether tétel értelmében van irredundáns primér felbontása, $A=\bigcap_{k=1}^{n}Q_k$, amiből $V(A)=\bigcup_{k=1}^{n}V(Q_k)$, azaz $V(A)$ előáll véges sok, primér ideálhoz tartozó affin algebrai halmaz uniójaként. Ez utóbbiakat algebrai sokaság avagy algebrai varietás névvel illetjük.

Vegyük észre, hogy $f\in R$ pontosan akkor tűnik el a-ban, ha f^n eltűnik, hiszen $f^n(v)=(f(v))^n$, ami pontosan akkor 0, ha $f(v)=0$ (K test $\Rightarrow$ nullosztómentes). Tehát $V(Q)=V(\sqrt{Q})$.

Azaz $V(A)$ éppen az A-hoz tartozó prímideálokhoz tartozó algebrai sokaságok uniója. A beágyazott ideálok érdektelenek, mivel $P\subseteq P'$ esetén $V(P')\subseteq V(P)$.

Összefoglalva: $V(X)=\bigcup V(P)$, ahol P befutja az X által generált ideálhoz tartozó minimális prímideálokat, melyek véges sokan vannak.

Példák:

– legyen $K=\mathbb{R}$, $n=2$. Az egységkör felírása $V(\{x^2+y^2-1\})$. Ha elmetsszük az $x=y$ egyenessel, akkor $V(\{x^2+y^2-1, x-y\})=V(\{2x^2-1, x-y\})$-t kapjuk, ez valóban $\{(\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2}),(-\frac{\sqrt{2}}{2},-\frac{\sqrt{2}}{2})\}$. Ha viszont uniózzuk az egyenessel, akkor $V(\{(x^2+y^2-1)\cdot(x-y)\})$ lesz a felírás.

– $K[x,y]$-ban $A=(x^2,xy)=(x)\cap(x,y)^2=(x)\cap(x^2,y)$ két irredundáns felírás. A megfelelő prímideálok (x) és (x,y); (x) izolált, (x,y) beágyazott. Így $V(A)=V(x)$ – ezt szoktuk függőleges egyenesnek vagy y tengelynek hívni.