A normagráfos algebrai geometriai tétel igazolása

Tétel. Legyen F egy tetszőleges test, $a_{11},\ldots,a_{tt}\in F$ elemek, melyekre $a_{ij}\neq a_{kj}$, ha $i,j,k\in\{1,\ldots,t\}$ és $i\neq k$. (azaz az (a_{ij}) mátrix minden oszlopában t különböző elem van.) Ekkor tetszőleges $b_1,\ldots,b_t\in F$-re a

$$\begin{array}{ccccc}(x_1-a_{11}) & \cdots & (x_t-a_{1t}) & = & b_1\\ & & & \vdots & \\ (x_t-a_{t1}) & \cdots & (x_t-a_{tt}) & = & b_t\end{array}$$

egyenletrenszernek legfeljebb $t!$ megoldása van.

Hozzávalók

Kínai Maradéktétel

Tétel. Legyen R egy kommutatív egységelemes gyűrű, $J_1,\ldots,J_n$ páronként relatív prím ideálok R-ben (azaz $i\neq k$-ra $J_i+J_k=R$). Ekkor a $\phi: x\mapsto(x+J_1,\ldots,x+J_k)$ leképezés izomorfizmust indukál az $R/\cap_{i=1}^n J_i$ maradékosztálygyűrű és a $\bigoplus_{i=1}^k R/J_i$ gyűrű között.
Biz.: Legyen $I=\cap_{i=1}^n J_i$. Világos, hogy (az R gyűrűn értelmezett) ϕ homomorfizmus és magja éppen I. Legyenek $i\neq k$-ra $f_{ik}\in J_i$, $e_{ik}\in J_k$ olyan elemek, melyekre $1=e_{ik}+f_{ik}$. Minden egyes i-re legyen $e_i=\prod_{k\neq i}e_{ik}$. Ekkor $e_i\in\cap_{k\neq i}J_k$ és $1-e_i\in J_i$. (Ez utóbbi onnan látszik, hogy $1-e_i=\prod_{k\neq i}(e_{ik}+f_{ik})-\prod_{k\neq i}e_{ik}$, és ezt kifejtve csupa olyan monom marad, amelyben van legalább egy J_i beli f_{ik} tényező.) Más szóval $e_i\cong 1 \mod J_i$ és $e_i\cong 0 \mod J_k$, ha $k\neq j$. Könnyen ellenőrizhető, hogy a (eredendően R^n-en értelmezett) $\psi:(x_1,\ldots,x_n)\mapsto x_1e_1+\ldots+x_ne_n$ leképezés egy gyűrű homomorfizmust ad $\bigoplus_{i=1}^k R/J_i$-ből R/I-be, és ϕ inverze éppen ψ lesz.

Nakayama-lemma

Tétel. Legyen R egy tetszőleges kommutatív egységelemes gyűrű, I egy ideál R-ben, M egy végesen generált R-modulus. Tegyük fel, hogy $(1+a)M\neq 0$ tetszőleges $a\in I$ esetén. Ekkor $IM\neq M$.
Biz.: Tegyük fel indirekte, hogy $IM=M$. Legyen $u_1,\ldots,u_r$ M egy generátorrendszere. Az $IM=M$ úgy fogalmazható meg, hogy minden i-re $u_i=\sum_{j=1}^r a_{ij}u_j$ alakba írható (nem feltétlenül egyértelműen, de sebaj), ahol $a_{ij}\in I$. Rögzítsünk ilyen a_{ij} elemeket $(i,j=1,\ldots,n)$. Legyen $b_{ij}=a_{ij}-\delta_{ij}$. Így $\sum_{j=1}^l b_{ij}u_j=0$ minden $i=1,\ldots r$-re. Legyen b'_{ij} a $(b_{kl})_{k,l=1}^r$ mátrix adjungáltjának ij-edik eleme. Ekkor tetszőleges $i,j=1,\ldots r$-re a Cramer-szabály szerint $\sum_l b'_{il}b_{lj}=\delta_{ij}d$, ahol $d=\det(b_{kl})_{k,l=1}^r$. A determináns kifejtéséből látható, hogy $d\in 1+I$. A fenti képletet alkalmazva kapjuk, hogy tetszőleges $i=1,\ldots r$-re $\sum_{l,j=1}^r b'_{il}b_{lj}u_j=du_i$. Ugyanakkor tudjuk már, hogy $\sum_{j=1}^r b_{lj}u_j=0$ minden l-re, ezért az előbbi összeg is 0. Kaptuk, hogy $du_i=0$ minden i-re, azaz $dM=0$. Ez ellentmond a feltevésnek, hiszen $d=1+a$ alakú, ahol $a\in I$.

Következmény (a "szokásos" Nakayama-lemma). Legyen $1\in R$ egy lokális gyűrű, I maximális ideállal, $0\neq M$ egy végesen generált R-modulus. Ekkor $IM\neq M$. (Mert: $a\in I$-re $1+a\in R\setminus I$ egység R-ben.)

Egészség

Ld. J. S. Milne, Algebraic Number Theory (University of Michigan Math 676) course notes, Section 2: Rings of Integers (pp 19-24).
(http://www.jmilne.org/math/CourseNotes/math676.ps.gz,
vagy http://www.jmilne.org/math/CourseNotes/math676.pdf)

$K[x_1,\ldots,x_n]$ miért egész-zárt: ld. Lee Lady, Unique Factorization Domains
(http://www.math.hawaii.edu/ lee/algebra/gauss.pdf) a szerző algebra kurzusanyagai
(http://www.math.hawaii.edu/ lee/algebra/) között.

Lemma. Legyen $1\in R$ egy K test részgyűrűje. Tegyük fel, hogy $z\in K$ nem egész R felett. Legyenek $p_1(x),\ldots,p_r(x)\in R[x]$ tetszőleges 1 főegyütthatós polinomok és $b_1=1/p_1(z),\ldots,b_r=1/p_r(z)$. Ekkor létezik egy K-ban egész-zárt $R'\supseteq R[b_1,\ldots,b_r]$ részgyűrű K-ban, melyre az R'-ben a $b_1,\ldots,b_r$ elemek által generált ideál valódi.
Biz.: Legyen $R''=R[b_1,\ldots,b_r]$ és J R''-nek a $b_1,\ldots,b_r$ elemek által generált ideálja. Először belátjuk, hogy $J\neq R$. Tegyük fel, hogy nem valódi, azaz léteznek $u_1(x_1,\ldots,x_r),\ldots,u_r(x_1,\ldots,x_r)\in R[x_1,\ldots,x_r]$ polinomok, hogy $1=u_1(b_1,\ldots,b_r)b_1+\ldots+u_r(b_1,\ldots,b_r)b_r$. Legyen $d_i=\max\{\deg_{x_i}u_j|j=1,\ldots,r\}$. Felszorozva a fenti egyenletet $\prod p_i^{d_i+1}(z)$-vel és kivonva a két oldalt egymásból z-re egy $\sum(d_i+1)\deg p_i$-edfokú, egy főegyüthatós R feletti polinomegyenlet kapunk. Ez azt jelenti, hogy z egész R felett, ami ellentmond a feltevésnek.

Tehát $J<R''$. Legyen R' az R'' egész-lezártja K-ban. Tegyük fel, hogy $R'J=R'$. Ekkor vannak olyan $v_1,\ldots,v_r\in R'$ elemek, melyekre $1=v_ib_i$. Legyen $S=R''[v_1,\ldots,v_r]$. Ekkor $SJ=S$ és mivel a v_i-l egészek R'' felett, S egy végesen generált R''-modulus. A Nakayama-lemma miatt ez csak úgy lehetne, ha valamely $d\in R''\setminus J$-re $0=dS\supseteq dR''$ lenne, ami képtelenség.

Rang és pontok ősképe

Alaphelyzet. Legyen F egy algebrailag zárt test, $S = F[x_1, \ldots, x_n]$, $f_1, \ldots, f_r \in L$ $R = F[f_1, \ldots, f_r]$, K az R-nek, L pedig az S hányadostestje ($L = F(x_1, \ldots, x_n)$). Tegyük fel, hogy S végesen generált R-modulus. Ekkor persze L véges bővítése K-nak. Legyen $d = \dim_K L$ (ezt hívjuk S rangjának R fölött).

Legyen $\beta = (\beta_1, \ldots, \beta_r) \in F^r$. Ekkor Az $M_\beta = R \cdot \{f_1 - \beta_1, \ldots, f_r - \beta_r\}$ ideál vagy az egész R, vagy egy maximális ideál R-ben. A $\{\alpha = (\alpha_1, \ldots, \alpha_n) \in F^n | f_i(\alpha) = \beta_i \ i = 1, \ldots, r\}$ halmaz (azaz, a $(\beta + 1, \ldots, \beta_r) \in F^r$ pont ősképe az $(f_1, \ldots, f_r)$ együttesből képzett $F^n \to F^n$ leképezésnél) az S gyűrűnek az SM_β ideált tartalmazó maximális ideáljainak felel meg ($M_\beta = R$ esetén tehát üres).

Lemma. Ha R egész-zárt, akkor S-nek legfeljebb d darab SM_β-t tartalmazó maximális ideálja van.
Biz.: Legyen $M = M_\beta$ és tegyük fel, hogy $M \neq R$. Legyenek $J_1, \ldots, J_s$ s darab különböző SM-et tartalmazó maximális ideál S-ben. Meg kell mutatni, hogy $s \leq d$. Legyen $J = \cap_{i=1}^s J_i$. Nyilvánvaló, hogy $J \supseteq M$ és a kínai maradéktétel szerint $S/J \cong F^s$. F^s-ben létezik olyan elem, amelynek a F feletti minimálpolinomja s-edfokú: például páronként különböző $\gamma_1, \ldots, \gamma_s \in F$ elemekre a $(\gamma_1, \ldots, \gamma_s)$. Legyen tehát $u \in S$ egy olyan elem, amelyre $u + J$ minimálpolinomja S/J-ben s-edfokú. Mivel $u \in S$ egész R felett, és R egész-zárt, u-nak a K test felett számított minimálpolinomja R-beli együtthatós. Ezt redukálva M szerint azt kapjuk, hogy $u + M$ gyöke egy (1 főegyütthatós, tehát nem 0) d-edfokú F feletti polinomnak. De akkor $u + J$ is gyöke ugyanennek. Ez csak úgy lehet, hogyha $s \leq d$.

Példa. $S = F[y]$, $R = F[f]$, ahol $f(y) \in F[y]$ d-edfokú, $M = R \cdot f(y)$. Ekkor $S \cong R[x]/R[x] \cdot (f(x) - f(y))$, $K = K(f)$ és $L \cong K[x]/K[x]/K[x] \cdot (f(x) - f(y))$. Így $\dim_K L = d$. $M = Rf(y)$-ra az SM feletti maximális ideálok az $f(x)$ polinom gyökeinek felelnek meg.

Lemma. Tegyük fel, hogy R valamely $M = M_\beta$ maximális ideáljára $SM = \cap_{i=1}^s J_i$, ahol $J_1, \ldots, J_s$ s darab különböző maximális ideál S-ben. Ekkor $d \leq s$.
Biz.: A kínai maradéktétel szerint S/SM egy s-dimenziós algebra $R/M \cong F$ felett. Legyenek $u_1, \ldots, u_s \in S$ elemek melyekre az $u_1 + SM, \ldots, u_s + SM$ rendszer egy bázis S/SM-ben. Ekkor $u_1, \ldots, u_s$ és SM együtt R-modulusként generálják S-t. Legyen V az $u_1, \ldots, u_s$ elemek által generált K-lineáris altér L-ben. Tegyük fel, hogy $V < L$. Tekintsük a szokásos $L \to W = L/V$ homomorfizmust. S-nek Q képe ennél egy olyan végesen generált R-részmodulusa W-nek, mely K felett kifeszíti W-t. Az $u_1, \ldots, u_s$ elemek itt 0-ba képződtek, tehát $MQ = Q$. Ez nem lehetséges a Nakayama-lemma miatt. Ugyanis semelyik nem 0 R-beli d elemre nem igaz, hogy $dQ = 0$, azaz $dE \subseteq V$ lenne.

A tétel bizonyítása:

Feltehető, hogy F algebrailag zárt. Legyenek $f_i = (x_1 - a_{i1}) \cdots (x_t - a_{it})$ $(i = 1, \ldots, t)$, $R = K[f_1, \ldots, f_t]$, $S = K[x_1, \ldots, x_t]$. Megmutatjuk, hogy

- S végesen generált R-modulus, azaz minden x_i egész R felett
- S rangja R fölött éppen $t!$. Ezt úgy tesszük, hogy az $f_1 - 0, \ldots, f_t - 0$ által generált S-beli ideált előíllítjuk $t!$ maximális ideál metszeteként.

Végesség:. Indukcióval. A $t = 1$ eset triviális: ekkor $S = R$. Tegyük fel, hogy $t > 1$, és $t - 1$-re már megvagyunk. Tegyük fel, hogy x_1 nem egész R felett. Az egészekről szóló fejezet végén található lemma miatt létezik egy $T \supseteq R[\frac{1}{x_1 - a_{11}}, \ldots, \frac{1}{x_1 - a_{t1}}]$ K-ban egész-zárt részgyűrű, melyen a $J = T\{\frac{1}{x_1 - a_{11}}, \ldots, \frac{1}{x_1 - a_{t1}}\}$ ideál valódi. Legyenek $g_j = f_j/(x_1 - a_{j1}) \in J$. Az indukciós feltevés miatt $x_2, \ldots, x_t$ egész $F[g_2, \ldots, g_t] \subseteq T$ felett, tehát $x_2, \ldots, x_t \in T$. Látható, hogy a $g_1, \ldots, g_t$ polinomoknak nincs közös gyöke F^{t-1}-ben, tehát a Nullstellensatz miatt vannak olyan $h_1, \ldots, h_t \in F[x_2, \ldots, x_t] \subseteq T$ polinomok, melyekre $\sum h_i g_i = 1$. Mivel $g_i \in J$, ebből a $J = T$ ellentmondás következik. Tehát x_1 egész R fölött. Hasonlóan, $x_2, \ldots, x_t$ is egész R-fölött, így S végesen generált R-modulus.

A rang meghatározása:. Legyen $M = M_0$ R-ben az f_i polinomok által generált ideál. Mivel S végesen generált R-modulus, az f_i polinomok algebrailag függetlenek, következésképp $R \cong F[x_1, \ldots, x_t]$, mely izomorfizmusnál x_i-nek f_i felel meg, így M egy maximális ideálja R-nek.

Legyen $u_i(x) = \prod_{j=1}^t (x_i - a_{ji})$. Belátjuk, hogy $u_i \in SM$. Szimmetriaokokból elegendő ezt $i = 1$-re igazolni. Legyenek $g_j = f_1/(x - a_{j1})$, mint fent. Mivel a g_j-knek nincs közös gyöke F^{t-1}-ben, a Nullstellensatz miatt vannak olyan $h_1, \ldots, h_t \in F[x_2, \ldots, x_t] \subseteq S$ polinomok, melyekre $\sum h_i g_i = 1$. Ezt megszorozva u_1-gyel azt kapjuk, hogy $u_1 = \sum u_1 h_i g_i = \sum \frac{u_1}{(x - a_{i1})} h_i g_i$. Mivel $\frac{u_1}{(x_1 - a_{i1})} = \prod_{j \neq i} (x_1 - a_{j1}) \in F[x_1] \subseteq S$, ez azt jelenti, hogy $u_1 \in SM$.

Legyen J az $u_1, \ldots, u_s$ polinomok által generált ideál S-ben. Tudjuk, hogy $SM \supseteq J$. Az Alon-féle Nullstellensatz miatt J a következő t^t darab maximális ideál metszete: $J_{i_1, \ldots, i_t} = (x_1 - a_{i_1 1}, \ldots, x_t - a_{i_t t})$. Mivel $SM \supseteq J$, SM ezek közül az őt tartalmazó maximális ideálok metszeteként áll elő. Ezekből $t!$ darab van: azok, amelyekre $i_1, \ldots, i_t$ az $\{1, \ldots, t\}$ halmaz egy permutációja. Tehát, az előző fejezet második lemmája szerint $\dim_K L \leq t!$. Így az első lemma miatt egy tetszőleges $(b_1, \ldots, b_t) \in F^t$ pont ősképe legfeljebb $t!$ elemű. (És, mivel a $(0, \ldots, 0)$ őslépe éppen $t!$ elemű, $\dim_K L \geq t!$ is igaz.)