

K -ciało algebraicznie domknięte (w szczególności nieskończone). $K[X] := K[X_1, \dots, X_n]$.

Dla dowolnego zbioru wielomianów (“układu równań”) $W \subseteq K[X]$ określamy jego zbiór zer: $Z(W) = \{x \in K^n \mid (\forall P(X) \in W)(P(x) = 0)\}$. Tej postaci podzbiory K^n nazywamy *zbiorami algebraicznymi*. Zauważmy, że $Z(W) = Z((W))$ – zbiór W i generowany przezeń ideał mają ten sam zbiór zer. Z tw. Hilberta o bazie wynika więc, że każdy zbiór algebraiczny można zadać skończonym układem równań wielomianowych. Jeśli dwa układy równań generują ten sam ideał, to ich zbiory rozwiązań są równe. Odwrotnie nie jest: X i X^2 mają ten sam zbiór zer, a generują różne ideały.

Lemat. Niech $x \in K^n$. Wtedy $m_x = \{P(X) \in K[X] \mid P(x) = 0\}$ jest maksymalnym ideałem $K[X]$.

Istotnie, ideał ten jest jądrem homomorfizmu ewaluacji $K[X] \ni P(X) \mapsto P(x) \in K$, a zatem iloraz $K[X]/m_x \simeq K$ jest ciałem.

Nullstellensatz. (czyli tw. Hilberta o zerach) Właściwy ideał $K[X]$ ma niepusty zbiór zer.

Dowód. Indukcja względem n . Niech $I \triangleleft K[X]$.

a) $I \cap K[X_1] = 0$.

W tym przypadku ideał J generowany przez I w $K(X_1)[X_2, \dots, X_n]$ też jest właściwy. Wybierzmy bazę Groebnera $G = (g_1, \dots, g_k)$ ideału J . Przy sprawdzaniu, że $S(g_i, g_j) \bmod G = 0$ pojawia się skończenie wiele współczynników – wymiernych funkcji zmiennej X_1 . Dobierzmy $z \in K$ tak, by wszystkie liczniki i mianowniki tych współczynników były niezerowe w z . Podstawmy to z w miejsce X_1 we wszystkich wielomianach g_i ; uzyskamy układ $G' \subseteq K[X_2, \dots, X_n]$, będący bazą Groebnera swego ideału (G') (w pierścieniu $K[X_2, \dots, X_n]$). Ten ideał jest właściwy: w przeciwnym razie pewne $g_i(z, X_2, \dots, X_n) \equiv 0$; ale wówczas g_i jest niezerową funkcją wymierną w $K(X_1)$ i $J = (g_i) = (1)$, wbrew właściwości J . Z założenia indukcyjnego wybieramy więc $(z_2, \dots, z_n) \in Z((G'))$, i wtedy $(z, z_2, \dots, z_n) \in Z(I)$.

b) Dla wszystkich i zachodzi $I \cap K[X_i] \neq 0$.

W tym przypadku weźmy generator f_1 ideału $I \cap K[X_1]$. Niech $z_1 \in K$ będzie pierwiastkiem f_1 , i niech $f_1 = (X_1 - z_1)q_1$. Mamy $1 \notin I_1 := I + K[X](X_1 - z_1)$ (w przeciwnym razie $1 = A(X) + B(X)(X_1 - z_1)$ dla pewnego $A(X) \in I$; wtedy jednak $q_1 = A(X)q_1 + B(X)f_1 \in I$ – sprzeczność z definicją f_1). Iterujemy tę procedurę: f_2 to generator $I_1 \cap K[X_2]$, $z_2 \in K$ – pewien pierwiastek f_2 , $1 \notin I_2 = I_1 + K[X](X_2 - z_2)$ itd. Ostatecznie $1 \notin I_n \supseteq m_z$ dla $z = (z_1, \dots, z_n)$, a z maksymalności m_z dostajemy $m_z = I_n \supseteq I$. Ostatecznie $z \in Z(I)$.

Odpowiedniość zbiór – ideał.

Ideałowi w $K[X]$ przypisaliśmy jego zbiór zer $Z(I)$. Podzbirowi $V \subseteq K^n$ przypiszemy jego ideał: $I(V) = \{P(X) \in K[X] \mid (\forall x \in V)(P(x) = 0)\}$. Jeśli V jest zbiorem algebraicznym, to $Z(I(V)) = V$; a jeśli nie, to nie. Ogólnie zbiór $Z(I(V))$ jest najmniejszym zbiorem algebraicznym zawierającym V , tzw. domknięciem Zariskiego V . Zbiorowi I i jego domknięciu Zariskiego odpowiadają te same ideały. Różnym zbiorom algebraicznym odpowiadają różne ideały.

Nie każdy ideał jest ideałem zbioru algebraicznego. Ideał I nazywamy *radykałnym*, jeśli z $f^k \in I$ wynika $f \in I$. Ideały zbiorów algebraicznych są radykalne. Ideał I można przerobić na radykalny: radykał I to ideał $\sqrt{I} := \{f \in K[X] \mid (\exists k)(f^k \in I)\}$. Ideał i jego radykał mają ten sam zbiór zer.

Tw. Dla dowolnego $J \triangleleft K[X]$ mamy $I(Z(J)) = \sqrt{J}$.

Dowód. Nietrivialne jest zawieranie $I(Z(J)) \subseteq \sqrt{J}$. Niech więc $f(X)$ zeruje się na $Z(J)$. W $K^{n+1} = K^n \times K$ rozważmy dwa rozłączne zbiory: $Z(J) \times K = Z(K[X, Y]J)$ oraz $Z(1 - Yf(X))$. Z tw. Hilberta o zerach wnioskujemy, że ideały $K[X, Y]J$ i $K[X, Y](1 - Yf(X))$ razem generują ideał niewłaściwy $K[X, Y]$. A zatem $1 = \sum_i A_i(X, Y)f_i + B(X, Y)(1 - Yf(X))$. Podstawiając $Y = \frac{1}{f(X)}$ i mnożąc przez dostatecznie wysoką potęgę $f(X)^N$ dostajemy $f(X)^N \in J$.

Wn. Odwzorowania Z oraz I są wzajemnie odwrotnymi bijekcjami między rodziną ideałów radykalnych w $K[X]$ a rodziną zbiorów algebraicznych w K^n .

Te bijekcje dostarczają algebraiczno-geometrycznej odpowiedniości. Punktom K^n odpowiadają ideały maksymalne; zbiorom nierozkładalnym – ideały pierwsze; sumie zbiorów – przekrój ideałów; przekrojowi zbiorów – radykał sumy ich ideałów itd.