Глава 4

Теорема на Хилберт за нулите

В глава 3 доказахме, че ако полето L е разширение на полето k и $a \in L$ е алгебричен над k, то пръстенът $k[a]$ на полиномите на a с коефициенти от k е поле. С индукция по n получаваме, че ако L е разширение на k и $a_1, \ldots, a_n \in L$ са алгебрични над k, то крайнопородената k-алгебра $k[a_1, \ldots, a_n]$ е подполе на L. По-точно, ако $k[a_1, \ldots, a_{n-1}]$ е поле по индукционно предположение, то алгебричният над k елемент $a_n \in L$ е алгебричен и над $k[a_1, \ldots, a_{n-1}]$. В резултат, $k[a_1, \ldots, a_{n-1}][a_n] = k[a_1, \ldots, a_{n-1}, a_n]$ е поле. Всъщност, крайнопородена алгебра $k[a_1, \ldots, a_n]$ над поле k е поле тогава и само тогава, когато $a_1, \ldots, a_n$ са алгебрични над k. В настоящия въпрос ще докажем, че ако k е безкрайно поле и крайнопородената k-алгебра $k[a_1, \ldots, a_n]$ е поле, то $a_1, \ldots, a_n$ са алгебрични над k. Твърдението е вярно над произволно поле k и следва от Теоремата за продължение на хомоморфизми в алгебрично затворено поле до пръстен на нормиране.

Теорема 6. *Ако k е безкрайно поле, а разширението L на k е крайнопородена k-алгебра, $L = k[a_1, \ldots, a_n]$ за някакви $a_1, \ldots, a_n \in L$, то $a_1, \ldots, a_n$ са алгебрични над k.*
В частност, L е крайномерно линейно пространство над k.

Доказателство: Да допуснем, че не всички пораждащи $a_1, \ldots, a_n$ на k-алгебрата $L = k[a_1, \ldots, a_n]$ са алгебрични над k. След евентуална пермутация на пораждащите $a_1, \ldots, a_n$ избираме максимално трансцендентно над k подмножество $\{a_1, \ldots, a_m\}$ на $\{a_1, \ldots, a_n\}$. Тогава за $\forall m+1 \leq i \leq n$ съществува нетъждествено нулев полином $h_i(x_1, \ldots, x_m, x_i) \in k[x_1, \ldots, x_m, x_i]$, така че $h_i(a_1, \ldots, a_m, a_i) = 0$. Представяме $h_i(x_1, \ldots, x_m, x_i) = \sum\limits_{j=0}^{\alpha_i} h_{i,j}(x_1, \ldots, x_m) x_i^j$ като полином на x_i с коефициенти $h_{i,j}(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$. Условието $h_i(x_1, \ldots, x_m, x_i) \not\equiv 0$ се свежда до $h_{i,\alpha_i}(x_1, \ldots, x_m) \not\equiv 0$. Тогава

$$0 = h_i(a_1, \ldots, a_m, a_i) = \sum_{j=0}^{\alpha_i} h_{i,j}(a_1, \ldots, a_m) a_i^j$$

е нетривиална полиномиална зависимост на a_i с коефициенти от $k[a_1, \ldots, a_m]$. Оттук, a_i са алгебрични над полето от частни $k(a_1, \ldots, a_m)$ на $k[a_1, \ldots, a_m]$ за всички $m+1 \leq i \leq n$.
Полето $L = k[a_1, \ldots, a_n]$ съвпада със своето поле от частни $k(a_1, \ldots, a_n)$. Твърдим, че $L = k(a_1, \ldots, a_m)[a_{m+1}, \ldots, a_n]$ е $k(a_1, \ldots, a_m)$-алгебрата, породена от $a_{m+1}, \ldots, a_n$. Включването

$$L = k[a_1, \ldots, a_n] = k[a_1, \ldots, a_m][a_{m+1}, \ldots, a_n] \subseteq k(a_1, \ldots, a_m)[a_{m+1}, \ldots, a_n]$$

е ясно. Обратно,

$$k(a_1, \ldots, a_m)[a_{m+1}, \ldots, a_n] \subseteq k(a_1, \ldots, a_n) = L$$

следва от това, че $k(a_1, \ldots, a_m)$ е подполе на полето $k(a_1, \ldots, a_n)$, пораждащите $a_{m+1}, \ldots a_n$ принадлежат на $k(a_1, \ldots, a_n)$ и L е пръстен. Представянето

$L = k(a_1, \ldots, a_m)[a_{m+1}, \ldots, a_n]$ ни дава възможност да приложим основното Твърдение 3.17 за крайнопородени модули и алгебри над ньотеров пръстен. По-точно, полето k е ньотеров пръстен, а $k(a_1, \ldots, a_m) \supseteq k$ е подпръстен на крайнопородената k-алгебра L. Понеже всяко от $a_{m+1}, \ldots, a_n$ е алгебрично над полето $k(a_1, \ldots, a_m)$, полето $L = k(a_1, \ldots, a_m)[a_{m+1}, \ldots, a_n]$ е крайномерно линейно пространство над $k(a_1, \ldots, a_m)$ съгласно Твърдение 3.21. Следователно $k(a_1, \ldots, a_m)$ е крайнопородена k-алгебра. С други думи, съществуват нетъждествено нулеви полиноми $f_i(x_1, \ldots, x_m), g_i(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$, така че

$$k(a_1, \ldots, a_m) = k\left[\frac{f_1(a_1, \ldots, a_m)}{g_1(a_1, \ldots, a_m)}, \ldots, \frac{f_t(a_1, \ldots, a_m)}{g_t(a_1, \ldots, a_m)}\right].$$

За $\forall \lambda \in k$ частното $\frac{1}{a_m - \lambda} \in k(a_1, \ldots, a_m)$ е полином на $\frac{f_1(a_1, \ldots a_m)}{g_1(a_1, \ldots a_m)}, \ldots, \frac{f_t(a_1, \ldots a_m)}{g_t(a_1, \ldots a_m)}$ с коефициенти от k. Привеждайки под общ знаменател преставяме

$$\frac{1}{a_m - \lambda} = \frac{f_0(a_1, \ldots, a_m)}{g_1(a_1, \ldots, a_m)^{d_1} \ldots g_t(a_1, \ldots, a_m)^{d_t}}$$

чрез полином $f_0(a_1, \ldots, a_m) \in k[a_1, \ldots, a_m]$ и някакви неотрицателни степенни показатели d_i на $g_i(a_1, \ldots, a_m) \in k[a_1, \ldots, a_m] \setminus \{0\}$. Равенството

$$(a_m - \lambda) f_0(a_1, \ldots, a_m) = g_1(a_1, \ldots, a_m)^{d_1} \ldots g_t(a_1, \ldots, a_m)^{d_t}$$

изисква анулирането на $g_i(a_1, \ldots, a_{m-1}, \lambda) = 0$ за някое $1 \leq i = i(\lambda) \leq t$. Доколкото елементите $\lambda \in k$ са безбройно много, а полиномите $g_1, \ldots, g_t$ са краен брой, съществува $1 \leq j \leq t$, така че $g_j(a_1, \ldots, a_{m-1}, x) = 0$ има безбройно много корени $x \in k$. По-точно, ако $g_j(a_1, \ldots, a_{m-1}, a_m) = \sum\limits_{s=0}^{\delta_j} g_{j,s}(a_1, \ldots, a_{m-1}) a_m^s$ е полином на a_m от степен δ_j с коефициенти $g_{j,s}(a_1, \ldots, a_{m-1}) \in k[a_1, \ldots, a_{m-1}]$, то избирайки $\delta_j + 1$ различни корена $\lambda_0, \lambda_1, \ldots, \lambda_{\delta_j}$ на $g_j(a_1, \ldots, a_{m-1}, x) = 0$ получаваме хомогенна линейна система

$$\begin{pmatrix} \lambda_0^0 & \lambda_0^1 & \ldots & \lambda_0^{\delta_j} \\ \lambda_1^0 & \lambda_1^1 & \ldots & \lambda_1^{\delta_j} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_{\delta_j}^0 & \lambda_{\delta_j}^1 & \ldots & \lambda_{\delta_j}^{\delta_j} \end{pmatrix} \begin{pmatrix} g_{j,0}(a_1, \ldots, a_{m-1}) \\ g_{j,1}(a_1, \ldots, a_{m-1}) \\ \ldots \\ g_{j,\delta_j}(a_1, \ldots, a_{m-1}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}$$

за $(g_{j,0}(a_1, \ldots, a_{m-1}), g_{j,1}(a_1, \ldots, a_{m-1}), \ldots, g_{j,\delta_j}(a_1, \ldots, a_{m-1}))$. Матрицата на тази хомогенна линейна система е транспонирана на матрицата на Вандермонд на различните $\lambda_0, \lambda_1 \ldots, \lambda_{\delta_j} \in k$. Следователно системата е от максимален ранг $\delta_j + 1$ и има само нулевото решение $g_{j,s}(a_1, \ldots, a_{m-1}) = 0$ за $\forall 0 \leq s \leq \delta_i$. В резултат, $g_j(a_1, \ldots, a_{m-1}, a_m) = 0$, което е противоречие. Следователно всяко едно от $a_1, \ldots, a_n$ е алгебрично над k.

Съгласно Твърдение 3.21, крайнопородената k-алгебра $L = k[a_1, \ldots, a_n]$ с алгебрични над k пораждащи $a_1, \ldots, a_n$ е крайнопороден k-модул. С други думи, полето L е крайномерно линейно пространство над k, Q.E.D.

Определение 4.1. *Идеалът $\mathfrak{M}$ в комутативния пръстен с единица R се нарича максимален, ако $\mathfrak{M} \subsetneqq R$ и единственият идеал I в R, съдържащ строго $\mathfrak{M}$ е $I = R$.*

Лема 4.2. *Нека R е комутативен пръстен с единица. В такъв случай, идеалът $\mathfrak{M} \lhd R$ е максимален тогава и само тогава, когато фактор-пръстенът $R/\mathfrak{M}$ е поле.*

Доказателство: Ако $\mathfrak{M} \lhd R$ е максимален идеал, то произволен елемент $r \in R \setminus \mathfrak{M}$ определя идеал $\mathfrak{M} + rR \lhd R$, съдържащ строго $\mathfrak{M}$. Следователно $\mathfrak{M} + rR = R$,

така че съществуват $\mu \in \mathfrak{M}$ и $s \in R$, свързани с равенството $\mu + rs = 1_R$. В резултат,

$$(r + \mathfrak{M})(s + \mathfrak{M}) = rs + \mathfrak{M} = 1_R - \mu + \mathfrak{M} = 1_R + \mathfrak{M}$$

и всеки ненулев клас $\mathfrak{M} \neq r + \mathfrak{M} \in R/\mathfrak{M}$ е обратим в $R/\mathfrak{M}$. По този начин установяваме, че комутативният пръстен с единица $R/\mathfrak{M}$ е поле.
Обратно, ако фактор-пръстенът $R/\mathfrak{M}$ на R по идеала $\mathfrak{M} \lhd R$ е поле, то всеки идеал $I \lhd R$, съдържащ строго $\mathfrak{M}$, притежава елемент $x_o \in I \setminus \mathfrak{M}$. Класът $x_o + \mathfrak{M} \neq \mathfrak{M}$ на x_o в $R/\mathfrak{M}$ е ненулев и съществува негов обратен $(x_o + \mathfrak{M})^{-1} = y_o + \mathfrak{M} \in R/\mathfrak{M}$, изпълняващ условието

$$1_R + \mathfrak{M} = (x_o + \mathfrak{M})(y_o + \mathfrak{M}) = x_o y_o + \mathfrak{M}.$$

Следователно $1_R = x_o y_o + \mu$ за някакъв елемент $\mu \in \mathfrak{M}$. По този начин $1_R \in I$ съгласно $x_o \in I \lhd R$ и $\mathfrak{M} \subset I$. Условието $1_R \in I$ е еквивалентно на $I = R$. С това установихме, че идеалът $\mathfrak{M} \lhd R$ е максимален, Q.E.D.
Комбинирайки с Лема 3.8 забелязваме, че всеки максимален идеал $\mathfrak{M} \lhd R$ е прост, защото всяко поле $R/\mathfrak{M}$ е област на цялост.

Лема 4.3. *Всеки собствен идеал $I \lhd R$, $I \subsetneq R$ в комутативен пръстен с единица R се съдържа в максимален идеал $\mathfrak{M} \lhd R$.*

Доказателство: Ще приложим Лемата на Цорн към множеството

$$\Sigma = \{J \lhd R \,|\, I \subseteq J \subsetneq R\},$$

наредено относно теоретико-множественото включване. Преди всичко, $I \in \Sigma$, така че $\Sigma \neq \emptyset$. Произволна ненамаляваща редица

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq J_{n-1} \subseteq J_n \subseteq J_{n+1} \subseteq \ldots$$

от собствени идеали на R, съдържащи I, има горна граница

$$J_\infty := \cup_{n=1}^{\infty} J_n \in \Sigma.$$

По-точно, J_∞ е идеал в R, защото за произволни $a, b \in J_\infty$ съществуват $n, l \in \mathbb{N}$, така че $a \in J_n$, $b \in J_l$. Полагайки $m := \max(n, l)$ получаваме, че $a, b \in J_m$, откъдето $a - b \in J_m \subseteq J_\infty$, защото $J_m \lhd R$. За произволни $a \in J_n \subseteq J_\infty$ и $r \in R$ е в сила $ar \in J_n \subseteq J_\infty$, доколкото $J_n \lhd R$. Това установява, че $J_\infty \lhd R$. От $I \subseteq J_1 \subseteq \ldots \subseteq J_n \subseteq J_{n+1} \subseteq \ldots$ е ясно, че $I \subseteq J_\infty$. Ако допуснем, че $J_\infty = R$, то $1_R \in J_\infty$, така че $1_R \in J_n$ за някакво естествено n. Сега $J_n = R$ противоречи на избора на $J_n \in \Sigma$. По построение е ясно, че $J_\infty \supseteq J_n$ за $\forall n \in \mathbb{N}$. Щом всяка ненамаляваща редица $\{J_n\}_{n\in\mathbb{N}}$ от идеали J_n от Σ има точна горна граница, то по Лемата на Цорн Σ съществува максимален елемент $\mathfrak{M} \in \Sigma$. Ясно е, че $\mathfrak{M}$ е максимален идеал в R, защото ако $I_o \lhd R$ и $\mathfrak{M} \subsetneqq I_o$, то $I_o \notin \Sigma$ съгласно максималността на $\mathfrak{M} \in \Sigma$. Доколкото $I_o \lhd R$ и $I \subseteq I_o$, оттук следва $I_o = R$, Q.E.D.
За описанието на максималните идеали в прсътена на полиномите $k[x_1, \ldots, x_n]$ с коефициенти от алгебрично затворено поле k ни трябва следната

Лема 4.4. *Всяко алгебрично затворено поле k е безкрайно.*

Доказателство: Ако допуснем, че алгебрично затвореното поле k е крайно, то характеристиката $char(k) = p$ на k е просто число p. Разглеждайки k като линейно пространство над простото си подполе $k_o \simeq \mathbb{Z}_p$, стигаме до извода, че k има p^n елемента за някое естествено число n. Полиномът $f(x) = x^{p^{2n}} - x \in k_o[x] \subseteq k[x]$ има само прости (т.е. еднократни) корени $\alpha_1, \ldots, \alpha_{p^{2n}}$. В противен случай $f(x) = (x - \alpha)^k g(x)$ за някакво естествено число $k \geq 2$ и формалната производна $f'(x) = (x - \alpha)^{k-1}[kg(x) + (x - \alpha)g'(x)]$ има общ корен α с $f(x)$. Но $f'(x) = p^{2n} x^{p^{2n}-1} - 1 = -1$ няма корени в нито едно разширение на k_o. По

този начин, $f(x)$ има p^{2n} различни корена $\alpha_1, \ldots, \alpha_{p^{2n}}$, които трябва да са от k съгласно алгебричната затвореност на k. Това противоречи на $\mathrm{card}(k) = p^n$ и установява, че всяко алгебрично затворено поле k е безкрайно, Q.E.D.

Твърдение 4.5. *Ако k е алгебрично затворено поле, то всеки максимален идеал $\mathfrak{M}$ в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от k е от вида*

$$\mathfrak{M} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

за някакви $a_1, \ldots, a_n \in k$.

Доказателство: Да разгледаме естествения хомоморфизъм

$$\pi_{\mathfrak{M}} : k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n]/\mathfrak{M},$$

$$\pi_{\mathfrak{M}}(f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n) + \mathfrak{M}$$

с ядро $Ker(\pi_{\mathfrak{M}}) = \mathfrak{M}$ и образ $Im(\pi_{\mathfrak{M}}) = k[x_1, \ldots, x_n]/\mathfrak{M}$. Поради максималността на идеала $\mathfrak{M} \lhd k[x_1, \ldots, x_n]$, фактор-пръстенът $L = k[x_1, \ldots, x_n]/\mathfrak{M}$ е поле. Твърдим, че $Ker(\pi_{\mathfrak{M}}) \cap k = \{0\}$, така че хомоморфизмът $\pi_{\mathfrak{M}}$ се ограничава до влагане $\pi_{\mathfrak{M}} : k \to L$. В противен случай, съществуването на $\lambda \in \mathfrak{M} \cap k^*$ води до $1 \in \mathfrak{M}$ и противоречи на определението за максимален идеал. От сега нататък ще отъждествяваме k с $\pi_{\mathfrak{M}}(k) = (k + \mathfrak{M})/\mathfrak{M}$. Разширението $L = k[x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M}]$ на безкрайното поле k е крайнопородена k-алгебра, така че $x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M}$ са алгебрични над k съгласно Алгебричния вариант на Теоремата на Хилберт за нулите - Теорема 6. Сега алгебричната затвореност на k води до $x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M} \in (k + \mathfrak{M})/\mathfrak{M} \simeq k$. С други думи, съществуват $a_1, \ldots, a_n \in k$, така че $x_i + \mathfrak{M} = a_i + \mathfrak{M}$ за всички $1 \leq i \leq n$.
Твърдим, че $\mathfrak{M}$ съвпада с идеала $\mathfrak{M}_a := \langle x_1 - a_1, \ldots, x_n - a_n \rangle \lhd k[x_1, \ldots, x_n]$. Включването $\mathfrak{M} \supseteq \mathfrak{M}_a$ е ясно от $x_i - a_i \in \mathfrak{M}$ за $\forall 1 \leq i \leq n$. Достатъчно е да проверим, че идеалът $\mathfrak{M}_a \lhd k[x_1, \ldots, x_n]$ е максимален, за да получим $\mathfrak{M} = \mathfrak{M}_a$ и да докажем твърдението. Да отбележим, че естественият хомоморфизъм

$$\pi_{\mathfrak{M}_a} : k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n]/\mathfrak{M}_a,$$

$$\pi_{\mathfrak{M}_a}(f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n) + \mathfrak{M}_a = f(a_1, \ldots, a_n) + \mathfrak{M}_a$$

съвпада с остойностяващото изображение

$$\varepsilon_a : k[x_1, \ldots, x_n] \longrightarrow k,$$

$$\varepsilon_a(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$$

в точката $a = (a_1, \ldots, a_n) \in k^n$, съгласно $x_i \equiv a_i (\mathrm{mod}\, \mathfrak{M}_a)$ за $\forall 1 \leq i \leq n$ и факта, че $\pi_{\mathfrak{M}_a}$ е хомоморфизъм на пръстени. Използваме също, че собственият идеал $\mathfrak{M}_a \lhd k[x_1, \ldots, x_n]$ пресича полето k само в $\mathfrak{M}_a \cap k = \{0\}$, за да отъждествим $Im(\pi_{\mathfrak{M}_a}) = k$. Щом фактор-пръстенът $k[x_1, \ldots, x_n]/\mathfrak{M}_a = Im(\pi_{\mathfrak{M}_a})$ е поле, идеалът $\mathfrak{M}_a \lhd k[x_1, \ldots, x_n]$ е максимален и съвпада с $\mathfrak{M}$, Q.E.D.
С помощта на Твърдение 4.5 ще докажем следното

Следствие 4.6. **(Слаба форма на Теоремата на Хилберт за нулите)** *Нека J е идеал в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от алгебрично затвореното поле k. Ако афинното многообразие $V(J) = \emptyset$ е празното множество $\emptyset$, то идеалът J съвпада с целия пръстен*

$$J = k[x_1, \ldots, x_n].$$

Доказателство: Ако допуснем, че $J \subsetneqq k[x_1, \ldots, x_n]$ е собствен идеал, то съгласно Лема 4.3 съществува максимален идеал $\mathfrak{M} \lhd k[x_1, \ldots, x_n]$, съдържащ J. Непосредствено се проверява, че включването на идеалите $J \subseteq \mathfrak{M}$ води до обратното включване $V(J) \supseteq V(\mathfrak{M})$ на съответните афинни многообразие. Именно, ако $a \in V(\mathfrak{M}) \subseteq k^n$, то за всеки полином $f \in \mathfrak{M}$ е в сила

$f(a_1,\ldots,a_n)=0$. В частност, за всички $f\in J\subseteq\mathfrak{M}$ имаме $f(a_1,\ldots,a_n)=0$, така че $a\in V(J)$. В Твърдение 4.5 установихме, че всеки максимален идеал $\mathfrak{M}$ в пръстена $k[x_1,\ldots,x_n]$ на полиномите на $x_1,\ldots,x_n$ с коефициенти от алгебрично затвореното поле k има вида

$$\mathfrak{M}=\langle x_1-a_1,\ldots,x_n-a_n\rangle$$

за някакви $a_1,\ldots,a_n\in k$. Следователно афинното многообразие

$$V(\mathfrak{M})=V(x_1-a_1,\ldots,x_n-a_n)=\{a=(a_1,\ldots,a_n)\}$$

се състои от точката $a\in k^n$. По този начин, $V(J)\neq\emptyset$ за всеки собствен идеал $J\lhd k[x_1,\ldots,x_n]$. С други думи, ако $V(J)=\emptyset$, то $J=k[x_1,\ldots,x_n]$, Q.E.D.
Алгебричната затвореност на полето k от Следствие 4.6 е съществена, както се вижда от следния

Пример 4.7. *Идеалът $J=\langle x^2+1\rangle\lhd\mathbb{Q}[x]$ има празно афинно множество $V(J)=\emptyset$ в $\mathbb{Q}$, но не съвпада с целия полиномиален пръстен $\mathbb{Q}[x]$.*

По-точно, полиномът $x^2+1\in\mathbb{Q}[x]$ е неразложим над $\mathbb{Q}$. Всеки полином $g(x)\in\mathbb{Q}[x]\backslash J$ е взаимно прост с x^2+1. По тъждеството на Безу съществуват полиноми $u(x),v(x)\in\mathbb{Q}[x]$ със свойството $(x^2+1)u(x)+g(x)v(x)=1$. Следователно всеки ненулев елемент $g+J$ на фактор-пръстена $\mathbb{Q}[x]/J$ е обратим, $(g+J)(v+J)=gv+J=1-(x^2+1)u+J=1+J$. Затова $\mathbb{Q}[x]/J$ е поле и идеалът $J\lhd\mathbb{Q}[x]$ е максимален. В частност, $J\neq\mathbb{Q}[x]$. Ако точка $a\in\mathbb{Q}$ принадлежи на афинното многообразие $V(J)\subseteq\mathbb{Q}$, то $a^2+1=0$, което противоречи на неотрицателността на квадратите на рационалните числа. Следователно $V(J)=\emptyset$.

Определение 4.8. *Радикал на идеал $I\lhd R$ в комутативен пръстен с единица R се нарича множеството*

$$r(I):=\{r\in R\ \mid\ \exists n\in\mathbb{N},r^n\in I\}.$$

Лема 4.9. *Ако $I\lhd R$ е идеал в комутативен пръстен с единица R, то радикалът $r(I)\lhd R$ е идеал, съдържащ $I\subseteq r(I)$.*

Доказателство: Ако $a,b\in r(I)$, $a^m\in I$, $b^n\in I$, то

$$(a-b)^{m+n-1}=\sum_{i=0}^{m+n-1}\left(\begin{array}{c}m+n-1\\ i\end{array}\right)(-1)^i a^{m+n-1-i}b^i\in I,$$

защото за $i\geq n$ следва, че $b^i\in I$, а за $i<n$ се получава, че $m+n-1-i\geq m$, така че $a^{m+n-1-i}\in I$. Освен това, за $\forall a\in r(I)$, $\forall r\in R$ е в сила $ar\in r(I)$, защото от $a^m\in I$ следва, че $(ra)^m=r^m a^m\in I\lhd R$. Следователно $r(I)\lhd R$. Накрая $I\subseteq r(I)$, доколкото $a=a^1\in I$ означава, че $a\in r(I)$, Q.E.D.

Определение 4.10. *Идеалът I на комутативен пръстен с единица R се нарича радикален, ако съвпада с радикала си $r(I)=I$.*

Лесно се вижда, че радикалът $r(I)$ на произволен идеал $I\lhd R$ е радикален идеал, т.е. $r(r(I))=r(I)$.
Идеалът $I(X)=\{f(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]\,|\,f(a)=0\ \text{за}\ \forall a\in X\}$ на афинно многообразие $X\subseteq k^n$ е радикален, защото ако $f(x_1,\ldots,x_n)^m$ се анулира върху X, то $f(x_1,\ldots,x_n)$ се анулира върху X.

Определение 4.11. *Елементът x на комутативен пръстен с единица S е нилпотентен, ако съществува естествено n, така че $x^n=0_S$.*

Лема 4.12. *Идеалът I в комутативен пръстен с единица R е радикален тогава и само тогава, когато фактор-пръстенът R/I няма ненулеви нилпотенти.*

Доказателство: Ако $I \lhd R$ е радикален идеал и $(r+I)^n = I$ за някое $r \in R$, то $r^n \in I$, така че $r \in r(I) = I$ и $r + I = I$. С други думи, фактор-пръстенът R/I по радикалния идеал I няма ненулеви нилпотентни елементи.
Обратно, ако фактор-пръстенът R/I по идеала $I \lhd R$ няма ненулеви нилпотентни елементи, то за всяко $r \in R$ с $r^n \in I$ за някое $n \in \mathbb{N}$ имаме $(r+I)^n = r^n + I = I$. Следователно $r + I = I$ и $r \in I$. Това означава съвпадение $r(I) = I$, Q.E.D.
Всеки прост идеал $\mathfrak{p} \lhd R$ е радикален, защото в областта $R/\mathfrak{p}$ няма ненулеви нилпотентни елементи. В частност, всеки максимален идеал $\mathfrak{M} \lhd R$ е радикален.

ТЕОРЕМА 7. **(Теорема на Хилберт за нулите)** *Ако $J \lhd k[x_1, \ldots, x_n]$ е идеал в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от алгебрично затворено поле k, то радикалът*

$$r(J) = IV(J)$$

съвпада с идеала на афинното многообразие $V(J)$ на J.

Доказателство: Включването $r(J) \subseteq IV(J)$ се проверява непосредствено. По-точно, ако $f \in r(J)$, то съществува естествено число m, така че $f^m \in J$. Съгласно определението на афинното многообразие $V(J)$ имаме $f^m|_{V(J)} \equiv 0$. Оттук следва, че $f|_{V(J)} \equiv 0$ или $f \in IV(J)$.
За обратното включване $IV(J) \subseteq r(J)$ ще приложим трика на Рабинович. Нека $f \in IV(J)$, т.е. $f|_{V(J)} \equiv 0$. Въвеждаме нова променлива y и разглеждаме идеала

$$J_o := \langle J, yf - 1 \rangle \lhd k[x_1, \ldots, x_n, y].$$

Ако $a \in V(J_o) \subset k^{n+1}$, то $a = (a', a_{n+1})$ с $a' \in k^n$ и $a_{n+1} \in k$. При това, $a' \in V(J)$, така че $f(a') = 0$ и $(yf-1)(a) = (yf-1)(a', a_{n+1}) = a_{n+1}f(a') - 1 = -1 \neq 0$. Това противоречи на $yf - 1 \in J_o$, $a \in V(J_o)$ и доказва, че $V(J_o) = \emptyset$. Съгласно слабата форма на Теоремата на Хилберт за нулите - Следствие 4.6, оттук получаваме, че

$$J_o := \langle J, yf - 1 \rangle = k[x_1, \ldots, x_n, y]$$

съвпада с целия полиномиален пръстен. По този начин, съществуват краен брой полиноми $f_1, \ldots, f_\nu \in J$ и $G_0, G_1, \ldots, G_\nu \in k[x_1, \ldots, x_n, y]$, така че

$$1 = \sum_{i=1}^{\nu} f_i G_i + (yf - 1)G_0.$$

За $1 \leq i \leq \nu$ да представим

$$G_i(x_1, \ldots, x_n, y) = \sum_{j=0}^{d_i} g_{ij}(x_1, \ldots, x_n) y^j$$

като полиноми на y с коефициенти $g_{ij}(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Ако $d := \max(d_1, \ldots, d_\nu)$, то след евентуално дописване на някои $g_{ij}y^j$ с $g_{ij} = 0 \in k[x_1, \ldots, x_n]$ имаме

$$G_i(x_1, \ldots, x_n, y) = \sum_{j=0}^{d} g_{ij}(x_1, \ldots, x_n) y^j$$

за всички $1 \leq i \leq \nu$. Сега в

$$1 = \sum_{i=1}^{\nu} \sum_{j=0}^{d} f_i(x_1, \ldots, x_n) g_{ij}(x_1, \ldots, x_n) y^j + (yf(x_1, \ldots, x_n) - 1)G_0(x_1, \ldots, x_n, y)$$

разменяме реда на сумиране и получаваме

$$1=\sum_{j=0}^{d}\left(\sum_{i=1}^{\nu}f_i(x_1,\ldots,x_n)g_{ij}(x_1,\ldots,x_n)\right)y^j+(yf(x_1,\ldots,x_n)-1)G_0(x_1,\ldots,x_n,y).$$

Полиномите

$$h_j(x_1,\ldots,x_n):=\sum_{i=1}^{\nu}f_i(x_1,\ldots,x_n)g_{ij}(x_1,\ldots,x_n)$$

принадлежат на идеала $J\lhd k[x_1,\ldots,x_n]$ и представят 1 във вида

$$1=\sum_{j=0}^{d}h_j(x_1,\ldots,x_n)y^j+(yf(x_1,\ldots,x_n)-1)G_0(x_1,\ldots,x_n,y). \tag{4.1}$$

Ако $h_j(x_1,\ldots,x_n)\equiv 0$ за $\forall 1\leq j\leq d$, то

$$H_o(x_1,\ldots,x_n,y)=(yf(x_1,\ldots,x_n)-1)G_0(x_1,\ldots,x_n,y)\in k[x_1,\ldots,x_n].$$

Разглеждайки $G_0(x_1,\ldots,x_n,y)=\sum\limits_{j=0}^{d_0}g_{0,j}(x_1,\ldots,x_n)y^j$ като полином на y с коефициенти $g_{0,j}(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$, представяме

$$H_o(x_1,\ldots,x_n,y)=g_{0,d_0}(x_1,\ldots,x_n)f(x_1,\ldots,x_n)y^{d_0+1}+$$

$$\sum_{j=1}^{d_0}\left[g_{0,j-1}(x_1,\ldots,x_n)f(x_1,\ldots,x_n)-g_{0,j}(x_1,\ldots,x_n)\right]y^j-g_{0,0}(x_1,\ldots,x_n).$$

Ако $G_0(x_1,\ldots,x_n,y)\not\equiv 0$, то без ограничение на общността можем да считаме, че $g_{0,d_0}(x_1,\ldots,x_n)\not\equiv 0$. Това противоречи на $H_o(x_1,\ldots,x_n,y)\in k[x_1,\ldots,x_n]$ и доказва, че $G_0(x_1,\ldots,x_n,y)\equiv 0$. Следователно $1=h_0(x_1,\ldots,x_n)\in J$ или $J=k[x_1,\ldots,x_n]$. Непосредствено се проверява, че

$$r(J)=r(k[x_1,\ldots,x_n])=k[x_1,\ldots,x_n]=I(\emptyset)=IV(k[x_1,\ldots,x_n])=IV(J).$$

Ако съществува естествено j с $h_j(x_1,\ldots,x_n)\not\equiv 0$ и m е максималното естествено с $h_m(x_1,\ldots,x_n)\not\equiv 0$, то полагаме $y=\frac{1}{f}$ в (4.1) и получаваме

$$1=\sum_{j=0}^{m}\frac{h_j}{f^j}=\frac{f^mh_0+f^{m-1}h_1+\ldots+fh_{m-1}+h_m}{f^m}=\frac{h}{f^m}$$

с $h\in J$. В резултат, $f^m=h\in J$ или $f\in r(J)$, Q.E.D.

Преди да разгледаме някои следствия от Теоремата на Хилберт за нулите, да опишем Зариски затворената обвивка на подмножество $M\subseteq k^n$ на афинното пространство k^n.

Определение 4.13. *Затворената обвивка $\overline{M}$ на подмножество M на топологично пространство X е сечението*

$$\overline{M}=\cap_{Z\supseteq M}Z$$

на всички затворени подмножества $Z\subseteq X$, съдържащи M.

Ясно е, че M е затоврено тогава и само тогава, когато $M=\overline{M}$.

Лема 4.14. *Ако $M\subseteq k^n$ е подмножество на афинното пространство k^n, то Зариски затворената обвивка*

$$\overline{M}=VI(M)$$

съвпада с афинното многообразие на идеала $I(M)\lhd k[x_1,\ldots,x_n]$.
В частност, ако $X\subseteq k^n$ е афинно многообразие, то $X=VI(X)$.

Доказателство: По определение, всеки полином $f \in I(M)$ се анулира върху M, така че $M \subseteq VI(M)$. Следователно затвореното множество $VI(M)$ участва в сечението $\cap_{Z \supseteq M} Z = \overline{M}$ и го съдържа, $VI(M) \supseteq \overline{M}$.
Обратно, $VI(M) \subseteq \overline{M} = \cap_{Z \supseteq M} Z$. Достатъчно е да проверим, че $VI(M) \subseteq Z$ за всяко Зариски затворено подмножество $Z \subseteq k^n$, съдържащо M. По определение, $Z = V(J)$ за някакъв идеал $J \lhd k[x_1, \ldots, x_n]$. Условието $M \subseteq V(J)$ означава анулиране на всички полиноми $f \in J$ в точките $a \in M$, $f(a) = 0$ Следователно $J \subseteq I(M)$, откъдето $Z = V(J) \supseteq VI(M)$, Q.E.D.

Следствие 4.15. *Ако k е алгебрично затворено поле, то за всяко естествено число n непразните афинни многообразия $X \subseteq k^n$ са във взаимно-еднозначно съответствие със собствените радикални идеали $J \lhd k[x_1, \ldots, x_n]$ в пръстена на полиномите $k[x_1, \ldots, x_n]$ на $x_1, \ldots, x_n$ с коефициенти от k.*

Доказателство: Както вече споменахме, идеалът

$$I(X) = \{f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \,|\, f(a) = 0 \text{ за } \forall a \in X\}$$

на непразно афинно многообразие $X \subseteq k^n$ е радикален. От друга страна, всеки собствен радикален идеал $J \lhd k[x_1, \ldots, x_n]$ определя непразно афинно многообразие

$$V(J) = \{a \in k^n \,|\, f(a) = 0 \text{ за } \forall f \in J\}.$$

Теоремата на Хилберт за нулите дава $IV(J) = r(J) = J$. Съгласно Лема 4.14 имаме $VI(X) = X$, така че съответствието между непразни афинни монгообразия $X \subseteq k^n$ и собствени радикални идеали $J \lhd k[x_1, \ldots, x_n]$ е взаимно еднозначно, Q.E.D.

Следствие 4.16. *(i) Произволни афинни многообразия $X \subsetneqq Y \subseteq k^n$ отговарят на радикални идеали $I(X) \supsetneqq I(Y)$.*
(ii) Ако k е алгебрично затворено поле и $J_1 \subsetneqq J_2 \subseteq k[x_1, \ldots, x_n]$ са радикални идеали, то $V(J_1) \supsetneqq V(J_2)$.

Доказателство: (i) Непосредствено се вижда, че ако $X \subseteq Y$, то $I(X) \supseteq I(Y)$. Допускането $I(X) = I(Y)$ води до

$$X = VI(X) = VI(Y) = Y,$$

съгласно Лема 4.14.
(ii) От $J_1 \subseteq J_2$ следва $V(J_1) \supseteq V(J_2)$. Ако $V(J_1) = V(J_2)$, то Теоремата на Хилберт за нулите дава

$$J_1 = r(J_1) = IV(J_1) = IV(J_2) = r(J_2) = J_2,$$

Q.E.D.
За да изучим идеалите на непразните проективни многообразия $X \subseteq \mathbb{P}^n$, да разгледаме проекцията

$$\Pi : k^{n+1} \setminus \{0^{n+1}\} \longrightarrow \mathbb{P}^n,$$

$$\Pi(x_0, x_1, \ldots, x_n) = [x_0 : x_1 : \ldots : x_n].$$

Ако към праобраза $\Pi^{-1}(X) \subseteq k^{n+1} \setminus \{0^{n+1}\}$ на $X \subseteq \mathbb{P}^n$ присъединим началото $0^{n+1} \in k^{n+1}$, то получаваме афинно многообразие

$$\widehat{X} = \Pi^{-1}(X) \cup \{0^{n+1}\} \subseteq k^{n+1}$$

със същия идеал $I(\widehat{X}) = I(X)$ като X. Първо, идеалът $I(\widehat{X}) \lhd k[x_0, x_1, \ldots, x_n]$ е радикален. Второ, афинното многообразие $\widehat{X} \subseteq k^{n+1}$ е инвариантно под действието на k^* или $\widehat{X} \subseteq k^{n+1}$ е конус с център в началото 0^{n+1}. Следователно идеалът $I(\widehat{X}) \subseteq k[x_0, x_1, \ldots, x_n]$ е хомогенен. Трето, многообразието $\widehat{X} \subseteq k^{n+1}$ съдържа строго началото 0^{n+1}, така че $I(\widehat{X}) \subsetneqq I(0^{n+1}) = \mathfrak{M}_o = \langle x_0, \ldots, x_n \rangle$. С това получаваме следното

Следствие 4.17. *Нека k е алгебрично затворено поле. Тогава непразните проективни многообразия $X \subseteq \mathbb{P}^n$ са във взаимно-еднозначно съответствие с радикалните хомогенни идеали $J \lhd k[x_0, x_1 \ldots, x_n]$, които се съдържат строго в максималния идеал $\mathfrak{M}_o = \langle x_0, x_1, \ldots, x_n \rangle$.*

В останалата част от въпроса ще изложим някои зависимости между операции с полиномиални идеали и операции с афинни многообразия. Неопсредствените проверки ще бъдат изпуснати.

Определение 4.18. *Ако I и J са идеали в комутативен пръстен с единица R, то множеството*

$$I + J = \{x + y \,|\, x \in I,\, y \in J\}$$

се нарича сума на идеалите I и J.

Лема 4.19. *Нека I и J са идеали в комутативния пръстен с единица R. Тогава:*
(i) $I + J$ е идеал в R;
(ii) $I + J$ е минималният идеал в R, съдържащ $I \cup J$, т.е. $I + J$ е идеал в R, съдържащ $I \cup J$ и ако идеал $K \lhd R$ съдържа $I \cup J$, то K съдържа $I + J$;
(iii) ако $I = \langle M \rangle$ се поражда от множество M, а $J = \langle N \rangle$ се поражда от множество N, то $I + J = \langle M \cup N \rangle$ се поражда от обединението $M \cup N$ на M и N.

Лема 4.20. *Ако I и J са идеали в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k, то афинното многообразие*

$$V(I + J) = V(I) \cap V(J)$$

на тяхната сума е сечение на афинните многообразия на I и J.

Вече знаем, че обединението $X \cup Y$ на афинни многообразия в k^n е афинно многообразие в k^n. Следващата лема описва уравненията на $X \cup Y$ чрез уравненията на X и Y.

Лема 4.21. *Ако $X = V(M)$ и $Y = V(N)$ са множествата на общите нули на фамилии от полиноми $M, N \subseteq k[x_1, \ldots, x_n]$, то*

$$X \cup Y = V\left(f(x_1, \ldots, x_n)g(x_1, \ldots, x_n) \,|\, \forall f(x_1, \ldots, x_n) \in M,\, \forall g(x_1, \ldots, x_n) \in N\right)$$

е множеството на общите нули на всевъзможните произведения на полином от M с полином от N.

Включването

$$V(f(x_1, \ldots, x_n)g(x_1, \ldots, x_n) \,|\, \forall f(x_1, \ldots, x_n) \in M,\, \forall g(x_1, \ldots, x_n) \in N) \subseteq X \cup Y$$

следва чрез допускане на противното.

Лема 4.22. *Ако X и Y са афинни многообразия в k^n, то радикалният идеал*

$$I(X \cup Y) = I(X) \cap I(Y)$$

на обединението $X \cup Y$ е сечение на радикалните идеали на X и Y.

Определение 4.23. *Ако I и J са идеали в комутативния пръстен с единица R, то произведението им е множеството*

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \,\middle|\, x_i \in I,\, y_i \in J,\, n \in \mathbb{N} \right\}.$$

Лема 4.24. *Ако I и J са идеали в комутативния пръстен с единица R, то*
(i) произведението им IJ е идеал в R;
(ii) ако $I = \langle M \rangle$ и $J = \langle N \rangle$ се пораждат от множества M и N, то

$$IJ = \langle xy \,|\, \forall x \in M, \forall y \in N \rangle$$

се поражда от всевъзможните произведения на елемент от M с елемент от N.

Лема 4.25. *Ако I и J са идеали в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k, то афинното многообразие*

$$V(IJ) = V(I) \cup V(J),$$

отговарящо на произведението им IJ е обединение на афинните многообразия, съответстващи на I и J.

Условието $V(IJ) \subseteq V(I) \cup V(J)$ се установява с допускане на противното.
Непосредствено се проверява, че сечението $I \cap J$ на идеали I и J в пръстен R е идеал, съдържащ произведението. В случая на полиномиални идеали $I, J \subseteq k[x_1, \ldots, x_n]$, съответните афинни многообразия $V(IJ) = V(I \cap J)$ съвпадат.

Лема 4.26. *Ако I и J са идеали в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k, то афинното многообразие*

$$V(I \cap J) = V(I) \cup V(J)$$

на сечението $I \cap J$ е обединение на афинните многообразия на I и J.

Тук $V(I \cap J) \subseteq V(I) \cup V(J)$ се доказва с допускане на противното и използване на $IJ \subseteq I \cap J$.
Преди да изучим идеала на сечение на афинни многообразия, да опишем уравненията на такова сечение.

Лема 4.27. *Ако $X = V(M)$ и $Y = V(N)$ са афинни многообразия в k^n, зададени като нулите на фамилии от полиноми $M, N \subseteq k[x_1, \ldots, x_n]$, то сечението им*

$$X \cap Y = V(M \cup N)$$

е множеството на нулите на $M \cup N$.

За разлика от разглежданите до сега свойства на операциите с полиномиални идеали и афинни многообразия, идеалът на сечение на афинни многообразия се описва с помощта на Теоремата на Хилберт за нулите.

Следствие 4.28. *Ако k е алгебрично затворено поле, а X и Y са афинни многообразия в k^n, то идеалът*

$$I(X \cap Y) = r(I(X) + I(Y))$$

на тяхното сечение $X \cap Y$ е радикалът на сумата на идеалите на X и Y.

Доказателство: Съгласно Следствие 4.14 имаме $X = VI(X)$ и $Y = VI(Y)$. Следователно

$$X \cap Y = VI(X) \cap VI(Y) = V(I(X) + I(Y)),$$

след прилагане на Лема 4.20. Използвайки теоремата на Хилберт за нулите, получаваме, че

$$I(X \cap Y) = IV(I(X) + I(Y)) = r(I(X) + I(Y)),$$

Q.E.D.