Глава 17

Въпрос 17: Теорема на Хилберт за нулите

Определение 17.1. *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 17.2. *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, така че 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.

Лема 17.3. *Всеки собствен идеал $I \lhd R$, $I \subsetneqq R$ в комутативен пръстен с единица R се съдържа в максимален идеал $\mathfrak{M} \lhd R$.*

Доказателство: Ще приложим Лемата на Цорн към множеството

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

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 горна граница, то по

Лемата на Цорн Σ има 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.

Лема 17.4. *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 $|k| = p^n$ и установява, че всяко алгебрично затворено поле k е безкрайно, Q.E.D.
Характеризацията на максималните идеали $\mathfrak{M}$ в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от алгебрично затворено поле използва следната общо алгебрична

Лема 17.5. *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 някое a_i не е алгебрично над k и да изберем максимално алгебрично независимо над k подмножество на $a_1, \ldots, a_n$. След евентуална преномерация на $a_1, \ldots, a_n$ можем да считаме, че единственият полином $g(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m]$ с $g(a_1, \ldots, a_m) = 0$ е тъждествено нулевият $0 \in k[y_1, \ldots, y_m]$, а за всяко $m+1 \leq i \leq n$ съществува $h_i \neq 0 \in k[y_1, \ldots, y_m, y_i]$ с $h(a_1, \ldots, a_m, a_i) = 0$.
Полето от частни $k(a_1, \ldots a_n)$ на $k[a_1, \ldots a_n] = L$ се съдържа, а оттам и съвпада с L, доколкото L е поле. Полето

$$L_o := k(a_1, \ldots, a_m)$$

на рационалните функции на $a_1, \ldots, a_m$ с коефициенти от k е подполе на L, съдържащо полето k. Полиномите

$$h_i(a_1, \ldots, a_m, y_i) \in k[a_1, \ldots, a_m][y_i] \subset L_o[y_i]$$

с корени a_i за $m+1 \leq i \leq n$ не се анулират тъждествено защото $a_1, \ldots, a_m$ са алгебрично независими над k. По този начин, всички a_i с $m+1 \leq i \leq n$ се оказват алгебрични над L_o. От една страна,

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

От друга страна,

$$L_o[a_{m+1}, \ldots, a_n] \subseteq L,$$

доколкото L е пръстен, съдържащ L_o и $a_{m+1}, \ldots, a_n \in L$. Следователно $L = L_o[a_{m+1}, \ldots, a_n]$ е крайнопородена L_o-алгебра с алгебрични над L_o пораждащи $a_{m+1}, \ldots, a_n$. Съгласно Твърдение 16.17, L се оказва крайнопороден L_o-модул. Сега полето k е ньотеров пръстен, разширението $L = k[a_1, \ldots, a_n]$ е крайнопородена k-алгебра, а L_o е такова подполе на L, съдържащо k, над което L е крайномерно L_o-линейно пространство. Съгласно Твърдение 16.13 е крайнопородена k-алгебра. По-точно, съществуват полиноми $f_1, \ldots, f_t, g_1, \ldots, g_t \in$

$k[x_1,\dots,x_n]$, така че $g_i(a_1,\dots a_m)\neq 0\in L_o$ за всички $1\leq i\leq m$ и

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

За произволно $\lambda\in k$, $\lambda\neq a_m$ разглеждаме

$$\frac{1}{a_m-\lambda}\in k(a_1,\dots,a_m)=L_o=k\left[\frac{f_1(a_1,\dots,a_m)}{g_1(a_1,\dots,a_m)},\dots,\frac{f_t(a_1,\dots,a_m)}{g_t(a_1,\dots,a_m)}\right].$$

Привеждайки под общ знаменател можем да представим със вида

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

чрез някакъв полином $F\in k[x_1,\dots,x_m]$ и неотрицателни цели $d_1,\dots,d_t$. Последното равенство е еквивалентно на

$$(a_m-\lambda)F(a_1,\dots,a_m)=g_1(a_1,\dots,a_m)^{d_1}\dots g_t(a_1,\dots,a_m)^{d_t}.$$

Доколкото $a_1,\dots,a_m$ са алгебрично независими над k, оттук следва равенството на полиноми

$$(x_m-\lambda)F(x_1,\dots,x_m)=g_1(x_1,\dots,x_m)^{d_1}\dots g_t(x_1,\dots,x_m)^{d_t}$$

от $k[x_1,\dots,x_m]$. По този начин, неразложимият над k полином $x_m-\lambda\in k[x_m]\subseteq k[x_1,\dots,x_m]$ се оказва делител на $g_i(x_1,\dots,x_m)$ за някое $1\leq i\leq t$. Вземайки предвид, че k е безкрайно поле, стигаме до извода, че поне един от полиномите $g_i\in k[x_1,\dots,x_m]$ има безбройно много линейни делители от вида $x_m-\lambda\in k[x_1,\dots,x_m]$ с $\lambda\in k$. Полученото противоречие доказва, че $a_1,\dots,a_m$ са алгебрични над k.
Прилагайки Твърдение 16.17 към крайнопородената k-алгебра $L=k[a_1,\dots,a_n]$ с алгебрични над k пораждащи $a_1,\dots,a_n\in L$ получаваме, че L е крайномерно линейно пространство над своето подполе k, Q.E.D.
Сега сме в състояние да опишем максималните идеали $\mathfrak{M}$ в пръстена $k[x_1,\dots,x_n]$ на полиномите с коефициенти от алгебрично затворено поле k.

Твърдение 17.6. *Ако k е алгебрично затворено поле, то всеки максимален идеал $\mathfrak{M}$ в пръстена $k[x_1,\dots,x_n]$ на полиномите на $x_1,\dots,x_n$ с коефициенти от k е от вида*

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

за някакви $a_1,\dots,a_n\in k$.

Доказателство: Ако $\mathfrak{M}$ е максимален идеал в $k[x_1,\dots,x_n]$, то фактор-пръстенът

$$L:=k[x_1,\dots,x_n]/\mathfrak{M}$$

е поле съгласно Лема 17.2.
Ядрото $\mathfrak{M}$ на естествения хомоморфизъм

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

$$\pi_{\mathfrak{M}}\left(\sum_{\alpha\in A}c_\alpha x_1^{\alpha_1}\dots x_n^{\alpha_n}\right)=\sum_{\alpha\in A}c_\alpha x_1^{\alpha_1}\dots x_n^{\alpha_n}+\mathfrak{M}$$

пресича полето k само в 0, защото всяко $0\neq a_o\in k\cap\mathfrak{M}$ е обратимо в k и води до $1_k=a_o^{-1}a_o\in k\cap\mathfrak{M}$, а оттам и до $k[x_1,\dots,x_n]=\mathfrak{M}$, което противоречи на определението за максимален идеал. Следователно ограничението

$$\pi_{\mathfrak{M}}|_k:k\longrightarrow\pi_{\mathfrak{M}}(k)\subset L$$

е влагане на полето k в полето L. Оттук нататък ще отъждествяваме полето k с неговия образ $\pi_{\mathfrak{M}}(k)=(k+\mathfrak{M})/\mathfrak{M}\subset k[x_1,\dots,x_n]/\mathfrak{M}=L$ и ще считаме, че L е k-алгебра.

Събирането и умножението във фактор-пръстена $L = k[x_1, \ldots, x_n]/\mathfrak{M}$ изпълняват тъждествата

$$\sum_{\alpha \in A} c_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n} + \mathfrak{M} = \sum_{\alpha \in A} c_\alpha (x_1 + \mathfrak{M})^{\alpha_1} \ldots (x_n + \mathfrak{M})^{\alpha_n}$$

за произволни крайни множества A от наредени n-торки $\alpha = (\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^n$ с неотрицателни компоненти α_i и $c_\alpha \in k$. Това дава възможност да отъждествим

$$L = k[x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M}]$$

с полиномите на $x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M} \in L$ с коефициенти от k. Алгебрично затвореното поле k е безкрайно, а неговото разширение $L = k[x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M}]$ е крайнопородена k-алгебра, така че $x_1 + \mathfrak{M}, \ldots, x_n + \mathfrak{M}$ са алгебрични над k съгласно Лема 17.5. Но тогава алгебричната затвореност на k изисква $x_i + \mathfrak{M} \in \pi_{\mathfrak{M}}(k) = (k + \mathfrak{M})/\mathfrak{M}$ за всяко $1 \leq i \leq n$. С други думи, съществуват $a_i \in k$, така че $x_i + \mathfrak{M} = a_i + \mathfrak{M}$. Оттук получаваме, че $x_i - a_i \in \mathfrak{M}$, така че идеалът

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

се съдържа в $\mathfrak{M}$. Да разгледаме "остойностяващото изображение"

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

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

Възоснова на

$$\varepsilon_a(f + g) = (f + g)(a) = f(a) + g(a) = \varepsilon_a(f) + \varepsilon_a(g) \text{ и}$$

$$\varepsilon_a(fg) = (fg)(a) = f(a)g(a) = \varepsilon_a(f)\varepsilon_a(g)$$

изображението ε_a е хомоморфизъм на пръстени. По определение, ядрото

$$Ker(\varepsilon_a) := \{f \in k[x_1, \ldots, x_n] \,|\, \varepsilon_a(f) = f(a) = 0\}.$$

Произволен моном $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ на $x_1, \ldots, x_n$ се различава от същия моном $a_1^{\alpha_1} \ldots a_n^{\alpha_n}$ на с полином от идеала $\mathfrak{M}_a$, съгласно

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} = [a_1 + (x_1 - a_1)]^{\alpha_1} \ldots [a_n + (x_n - a_n)]^{\alpha_n} =$$

$$a_1^{\alpha_1} \ldots a_n^{\alpha_n} + (x_1 - a_1)g_1 + \ldots + (x_n - a_n)g_n$$

за подходящи полиноми $g_1, \ldots, g_n \in k[x_1, \ldots, x_n]$. Оттук, за произволен полином $f(x_1, \ldots, x_n) = \sum_{\alpha \in A} c_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in Ker(\varepsilon_a)$ получаваме, че

$$f(x_1, \ldots, x_n) = f(a_1, \ldots, a_n) + (x_1 - a_1)G_1 + \ldots + (x_n - a_n)G_n =$$

$$(x_1 - a_1)G_1 + \ldots + (x_n - a_n)G_n \in \mathfrak{M}_a$$

с някакви $G_1, \ldots, G_n \in k[x_1, \ldots, x_n]$. С други думи, $Ker(\varepsilon_a) \subseteq \mathfrak{M}_a$. Обратно, всеки полином $(x_1 - a_1)h_1 + \ldots + (x_n - a_n)h_n \in \mathfrak{M}_a$ принадлежи на $Ker(\varepsilon_a)$, така че $Ker(\varepsilon_a) = \mathfrak{M}_a$. Образът $Im(\varepsilon_a) = k$, доколкото за $\forall a_o \in k$ тъждественият полином има стойност a_o за $x_i = a_i$. Сега теоремата за хомоморфизмите на пръстени предоставя изоморфизма на пръстени

$$\overline{\varepsilon_a} : k[x_1, \ldots, x_n]/\mathfrak{M}_a = k[x_1, \ldots, x_n]/Ker(\varepsilon_a) \longrightarrow Im(\varepsilon_a) = k,$$

$$\overline{\varepsilon_a}(f + \mathfrak{M}_a) = \overline{\varepsilon_a}(f + Ker(\varepsilon_a)) = \varepsilon_a(f) = f(a).$$

Вземайки предвид, че k е поле, прилагаме Лема 17.2 и стигаме до извода, че идеалът $\mathfrak{M}_a \lhd k[x_1, \ldots, x_n]$ е максимален. Следователно включването $\mathfrak{M}_a \subseteq \mathfrak{M}$ е съвпадение $\mathfrak{M}_a = \mathfrak{M}$, Q.E.D.

Да напомним, че афинното многообразие $V(J)$ на идеал $J \lhd k[x_1, \ldots, x_n]$ се определя като множеството

$$V(J) := \{a \in k^n \,|\, f(a) = f(a_1, \ldots, a_n) = 0 \text{ за } \forall f \in J\}$$

на точките $a = (a_1, \ldots, a_n) \in k^n$, в които се анулират всички полиноми от J. Идеалът $I(S)$ на подмножество $S \subset k^n$ се състои от полиномите, които се анулират върху S,

$$I(S) := \{f \in k[x_1, \ldots, x_n] \,|\, f(a_1, \ldots, a_n) = 0 \text{ за } \forall (a_1, \ldots, a_n) \in S\}.$$

С помощта на Твърдение 17.6 ще докажем следната слаба форма на Теоремата на Хилберт за нулите:

Следствие 17.7. *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 17.3 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 17.6 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 $V(\mathfrak{M}) = V(x_1 - a_1, \ldots, x_n) = \{a = (a_1, \ldots, a_n)\}$ 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.
За да формулираме и да докажем общата форма на Теоремата на Хилберт за нулите е необходимо следното

Определение 17.8. *Ако I е идеал в комутативния пръстен с единица R, то множеството*

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

се нарича радикал на идеала I.

Лема 17.9. *Нека I е идеал в комутативния пръстен с единица R. Тогава радикалът $r(I)$ на I е идеал в R, съдържащ I.*

Доказателство: За произволни $r, s \in r(I)$ съществуват $m, n \in \mathbb{N}$, така че $r^m, s^n \in I$. В резултат,

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

доколкото $r^{m+n-1-i} \in I$ за $0 \leq i \leq n-1$ и $s^i \in I$ за $n \leq i \leq m+n-1$. По този начин, $r - s \in r(I)$ и $(r(I), +)$ е подгрупа на $(R, +)$. За $r \in r(I)$ с $r^m \in I$ и произволно $t \in R$ е в сила $(rt)^m = r^m t^m \in I$, така че $r(I)$ е идеал в R.
По определение, ако $r \in I$, то $r = r^1 \in I$ и $r \in r(I)$. Следователно $I \subseteq r(I)$, Q.E.D.

Теорема 13. (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 $f(a') =$ 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 17.7, 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

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

сменяме 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

$$1 = \sum_{j=0}^{d} h_j(x_1, \ldots, x_n)y^j + (yf(x_1, \ldots, x_n) - 1)G_0(x_1, \ldots, x_n, y). \tag{17.1}$$

Нека $m \leq d$ е максималното неотрицателно цяло число с $h_m \neq 0 \in k[x_1, \ldots, x_n]$. Ако $m = 0$, то $1 = h_0(x_1, \ldots, x_n) + (yf - 1)G_0$ изисква $G_0 = 0 \in k[x_1, \ldots, x_n, y]$, така че $1 = h_0(x_1, \ldots, x_n) \in J$. Следователно $J = k[x_1, \ldots, x_n]$, така че

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

За $m > 0$ полагаме $y = \frac{1}{f}$ в (17.1) и получаваме

$$1 = \sum_{j=0}^{m} \frac{h_j}{f^j} = \frac{f^m h_0 + f^{m-1} h_1 + \ldots + f h_{m-1} + h_m}{f^m} = \frac{h}{f^m}$$

с $h \in J$. В резултат, $f^m = h \in J$ или $f \in r(J)$, Q.E.D.
Да напомним, че идеалът I в комутативен пръстен с единица R се нарича радикален, ако

$$r(I) = I.$$

Радикалът $r(I)$ на произволен идеал $I \lhd R$ е радикален идеал, защото

$$r(r(I)) = \{r \in R \,|\, \exists m \in \mathbb{N} : r^m \in r(I)\} =$$

$$\{r \in R \,|\, \exists m, n \in \mathbb{N} : (r^m)^n = r^{mn} \in I\} \subseteq r(I).$$

Включването $r(r(I)) \supseteq r(I)$ е доказано в Лема 17.9.

Следствие 17.10. *Ако k е алгебрично затворено поле, то за всяко естествено число n афинните многообразия $X \subset k^n$ са във взаимно-еднозначно съответствие с радикалните идеали $J \lhd k[x_1, \ldots, x_n]$ в пръстена на полиномите на $x_1, \ldots, x_n$ с коефициенти от k.*

Доказателство: На произволно афинно многообразие $X \subset k^n$ съпоставяме идеала му $I(X) \lhd k[x_1, \ldots, x_n]$. Твърдим, че многообразието на този идеал

$$VI(X) = X$$

съвпада с X. От една страна, $X \subseteq VI(X)$, защото $I(X)|_X \equiv 0$. Ако допуснем, че включването $VI(X) \supsetneq X$ е строго, то съществува полином $f \in k[x_1, \ldots, x_n]$, така че $f|_X \equiv 0$ и $f|_{VI(X)} \not\equiv 0$. Но тогава $f \in I(X)$, а $I(X)|_{VI(X)} \equiv 0$, така че $f|_{VI(X)} \equiv 0$. Противоречието доказва, че $VI(X) = X$.
Както вече отбелязахме във въпрос 3, идеалът $I(X) \lhd k[x_1, \ldots, x_n]$ на произволно афинно многообразие $X \subseteq I(X)$ е радикален, доколкото $f^m \in I(X)$ за произволни $f \in k[x1, \ldots, x_n]$ и $m \in \mathbb{N}$ означава, че $f^m|_X \equiv 0$. Оттук $f|_X \equiv 0$, така че $r(I(X)) \subseteq I(X) \subseteq r(I(X))$, т.е. $r(I(X)) = I(X)$. Радикалността на $I(X)$ може да се изведе и от Теоремата на Хилберт за нулите $r(I(X)) = IVI(X)$, с помощта на следствието $IVI(X) = I(X)$ на $VI(X) = X$.
Обратно, за всеки радикален идеал $J \lhd k[x_1, \ldots, x_n]$ определяме афинно многообразие $V(J) \subset k^n$.
Различни афинни многообразия $X \subseteq k^n$ и $Y \subseteq k^n$ отговарят на различни радикални идеали $I(X) \lhd k[x_1, \ldots, x_n]$ и $I(Y) \lhd k[x_1, \ldots, x_n]$, доколкото $I(X) = I(Y)$ води до

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

. Единственото нещо, за което използваме алгебричната затвореност на полето k, а оттам и Теоремата на Хилберт за нулите е реализацията на произволен радикален идеал $J \lhd k[x_1, \ldots, x_n]$ като идеал $J = I(X)$ на подходящо афинно многообразие $X \subseteq k^n$. По-точно, $X = V(J)$, така че

$$I(X) = IV(J) = r(J) = J$$

. Това установява взаимната еднозначност на съответствието между афинни многообразия $X \subseteq k^n$ и радикални идеали $J \lhd k[x_1, \ldots, x_n]$ над алгебрично затворено поле k, Q.E.D.
Ако полето k не е алгебрично затворено, то съществуват радикални идеали $J \lhd k[x_1, \ldots, x_n]$, които не могат да се реализират като идеали $I(X)$ на афинни многообразия $X \subseteq k^n$.

Пример 17.11. *Идеалът $J = \langle x^2 + 1 \rangle \lhd \mathbb{Q}[x]$ е радикален, но не съществува афинно многообразие $X \subseteq \mathbb{Q}$ с $I(X) = J$.*

Наистина, ако $f^m \in J = \langle x^2+1\rangle$ за някакъв полином $f \in \mathbb{Q}[x]$, то $f \in J = \langle x^2+1\rangle$, доколкото делимостта на f^m с неразложимия над $\mathbb{Q}$ полином $x^2+1 \in \mathbb{Q}[x]$ води до делимост на множителя f на f^m с x^2+1. Следователно $r(J) = J$ и $J = \langle x^2+1\rangle \lhd \mathbb{Q}[x]$ е редикален идеал. Ако допуснем, че съществува непразно афинно многообразие $X \subseteq \mathbb{Q}$ с $I(X) = J = \langle x^2+1\rangle$, то за всяка точка $a \in X \subseteq \mathbb{Q}$ трябва да е изпълнено $a^2+1 = 0$. Доколкото квадратите на рационалните числа са неотрицателни, оттук следва, че $X = \emptyset$. Но тогава $I(X) = \mathbb{Q}[x] \neq J$ е противоречие, доказващо несъществуването на афинно многообразие $X \subseteq \mathbb{Q}$ с идеал $I(X) = J = \langle x^2+1\rangle \lhd \mathbb{Q}[x]$.
Накрая да завършим със следната лесна

Лема 17.12. *Ако $I = \langle f\rangle$ е главен идеал в пръстена $k[x_1,\ldots,x_n]$ на полиномите на $x_1,\ldots,x_n$ с коефициенти от поле k и*

$$f = f_1^{d_1}\ldots f_m^{d_m}$$

е разлагането на f в произведение на различни неразложими над k множители f_i, то радикалът

$$r(I) = r(\langle f\rangle) = \langle f_1 f_2 \ldots f_m\rangle$$

е главният идеал, породен от произведението $f_1\ldots f_m$ на различните неразложими над k множители на f.

Доказателство: Преди всичко, $f_1\ldots f_m \in r(\langle f\rangle)$, защото за $d := \max(d_1,\ldots,d_m)$ имаме

$$(f_1\ldots f_m)^d = (f_1^{d_1}\ldots f_m^{d_m})(f_1^{d-d_1}\ldots f_m^{d-d_m}) = f(f_1^{d-d_1}\ldots f_m^{d-d_m}) \in \langle f\rangle.$$

Обратно, ако $g \in r(\langle f\rangle)$, то съществува естествено число N, така че $g^N = fh$ за подходящ полином $h \in k[x_1,\ldots,x_n]$. Разлагаме g в произведение на неразложими над k множители

$$g = g_1^{\delta_1}\ldots g_l^{\delta_l}$$

и получаваме

$$g_1^{N\delta_1}\ldots g_l^{N\delta_l} = f_1^{d_1}\ldots f_m^{d_m}h.$$

Съгласно единствеността на разлагането на полиноми на $x_1,\ldots,x_n$ в произведение от неразложими над k множители, за $\forall 1 \leq i \leq m$ съществува $1 \leq j(i) \leq l$, така че

$$g_{j(i)} = f_i a_i$$

за подходящо $a_i \in k^*$. За $i_1 \neq i_2$ полиномите $g_{j(i_1)}$ и $g_{j(i_2)}$ не съвпадат с точност до мултипликативна константа, така че $f_1\ldots f_m$ дели g. По този начин $g \in \langle f_1\ldots f_m\rangle$ или $r(\langle f\rangle) \subseteq \langle f_1\ldots f_m\rangle$, откъдето $r(\langle f\rangle) = \langle f_1\ldots f_m\rangle$, Q.E.D.