Глава 3

Теорема на Hilbert за нулите и някои нейни следствия

1. Крайно породени подалгебри на крайно породени алгебри над ньотерова област

Започваме с едно техническо твърдение, което ще използваме по-нататък.

Твърдение 3.1. *Да разгледаме ньотерова комутативна област с единица R, крайно породена R-алгебра $R[a_1, \ldots, a_n]$ и такъв подпръстен с единица S на $R[a_1, \ldots, a_n]$, че $R[a_1, \ldots, a_n]$ е крайно породен S-модул. Тогава S е крайно породена R-алгебра.*

Доказателство: Нека

$$R[a_1, \ldots, a_n] = Sb_1 + \ldots + Sb_m.$$

Без ограничение на общността ще считаме, че $b_m = 1_R$, присъединявайки единицата на R към пораждащата система на $R[a_1, \ldots, a_n]$ като S-модул. От $a_p \in R[a_1, \ldots, a_n]$ за $\forall 1 \leq p \leq n$ следва съществуването на $\alpha_{p1}, \ldots, \alpha_{pm} \in S$, така че

$$a_p = \sum_{i=1}^{m} \alpha_{pi} b_i.$$

От друга страна, за произволни $1 \leq i, j \leq m$ елементите $b_i, b_j \in R[a_1, \ldots, a_n]$ имат произведение $b_i b_j \in R[a_1, \ldots, a_n]$, така че

$$b_i b_j = \sum_{k=1}^{m} \alpha_{ijk} b_k$$

за подходящи $\alpha_{ijq} \in S$. Образуваме подпръстена с единица

$$S_o := R[\alpha_{pi}, \alpha_{ijk} \ \mid \ 1 \leq p \leq n, \ \ 1 \leq i, j, k \leq m]$$

на $R[a_1, \ldots, a_n]$, съдържащ R. Тогава $R[a_1, \ldots, a_n]$ е S_o-модул и S_o-алгебра. В качеството си на крайно породена алгебра над ньотеровата комутативна област с единица R, пръстенът S_o е ньотеров. Твърдим, че $R[a_1, \ldots, a_n]$ се поражда като S_o-модул от пораждащите си $b_1, \ldots, b_m$ като S-модул, т.е.

$$R[a_1, \ldots, a_n] = S_o b_1 + \ldots + S_o b_m.$$

Модулът $R[a_1, \ldots, a_n]$ над S_o съдържа S_o-модула $M_o := S_o b_1 + \ldots + S_o b_m$, защото $b_1, \ldots, b_m \in R[a_1, \ldots, a_n]$. За обратното включване, $(M_o, +)$ е подгрупа на $(R[a_1, \ldots, a_n], +)$, защото M_o е S_o-подмодул на $R[a_1, \ldots, a_n]$. За произволни $x = \sum\limits_{i=1} m s_i b_i, y = \sum\limits_{i=1}^{m} t_i b_i \in M_o$, произведението $xy = \sum\limits_{i=1}^{m} \sum\limits_{j=1}^{m} s_i t_j b_i b_j$ принадлежи на M_o, защото $b_i b_j = \sum\limits_{k=1}^{m} \alpha_{ijk} b_k \in M_o$. Следователно M_o е подпръстен на $R[a_1, \ldots, a_n]$. От $R = R1_R = Rb_m \subset M_o$ и $a_p = \sum\limits_{i=1}^{m} \alpha_{pi} b_i \in M_o$ следва, че $R[a_1, \ldots, a_n] \subseteq M_o$, така че $R[a_1, \ldots, a_n] = M_o$.

По построение, S_o е подпръстен на S, така че S е S_o-модул. Пръстенът S_o е ньотеров, а пръстенът S е S_o-подмодул на крайно породения S_o-модул $R[a_1, \ldots, a_n]$. Съгласно Лема 2.16,

$$S = S_o\sigma_1 + \ldots + S_o\sigma_l$$

е крайно породен S_o-модул. От една страна,

$$S = S_o\sigma_1 + \ldots + S_o\sigma_l \subseteq S_o[\sigma_1, \ldots, \sigma_l].$$

От друга страна,

$$S_o[\sigma_1, \ldots, \sigma_l] \subseteq S,$$

защото S_o е подпръстен на S, $\sigma_1, \ldots, \sigma_l \in S$ и S е затворено относно умножение и събиране на свои елементи. Следователно

$$S = S_o[\sigma_1, \ldots, \sigma_l] = R[\alpha_{pq}, \alpha_{ijq} \mid 1 \leq p \leq n, \quad 1 \leq i, j, q \leq m][\sigma_r \mid 1 \leq r \leq l] =$$
$$= R[\alpha_{pq}, \alpha_{ijq}, \sigma_r \mid 1 \leq p \leq n, \quad 1 \leq i, j, q \leq m, \quad 1 \leq r \leq l]$$

е крайно породена R-алгебра, Q.E.D.

2. Алгебричност на разширенията, които са крайно породените алгебри

Задача 3.2. *Да се докаже, че всяка крайна комутативна област с единица R е поле.*

Упътване: За произволен елемент $r \in R \setminus \{0\}$ докажете, че умножението $\mu_r : R \to R$, $\mu_r(x) = rx$ с r е изоморфизъм на множества.

Лема 3.3. *Нека R е факториална ньотерова комутативна област с единица, която не е поле. Ако обединението $R^* \cup \{0\}$ на мултипликативната група R^* с нулата 0 на R е подгрупа на адитивната група $(R, +)$ на R, то R съдържа безбройно много неразложими елементи.*
В частност, R е безкраен пръстен.

Доказателство: Да допуснем, че R съдържа краен брой неразложими елементи $p_1, \ldots, p_m$ и да разгледаме

$$r := p_1 \ldots p_m + 1 \in R.$$

Ако $r = 0$, то от $p_1 \ldots p_m = (-1) \in R^*$ следва обратимостта на всички p_i, противно на условието $p_i \notin R^*$ от определението за неразложим елемент.
Ако $r \in R^*$, то

$$p_1 \ldots p_m = r - 1 \in R^* \cup \{0\},$$

защото подгрупата $(R^* \cup \{0\}, +)$ на $(R, +)$ съдържа разликата на елементите си r и 1. Вече доказахме, че $p_1 \ldots p_m \notin R^*$. В областта R, ненулевите елементи $p_1, \ldots, p_m$ имат ненулево произведение $p_1 \ldots p_m \in R \setminus \{0\}$, така че $r \notin R^*$.
Произволен елемнт $r \in R \setminus (R^* \cup \{0\})$ има единствено с точност до множители от R^* разлагане $r = p_1^{d_1} \ldots p_m^{d_m}$ с $u \in R^*$, $d_i \in \mathbb{Z}^{\geq 0}$ за $\forall 1 \leq i \leq m$ и поне едно $d_{i_o} \geq 1$. Тогава p_{i_o} дели r и $p_1 \ldots p_m$, така че p_{i_o} дели 1 и $p_{i_o} \in R^*$. Противоречието доказва, че R има безбройно много неразложими елементи, Q.E.D.

Следствие 3.4. *За произволно поле k, полиномиалният пръстен $k[x_1, \ldots, x_n]$ съдържа безбройно много неразложими елементи и полето*

$$k(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \;\middle|\; f, g \in k[x_1, \ldots, x_n], \quad g(x_1, \ldots, x_n) \not\equiv 0 \right\}$$

на рационалните функции на $x_1, \ldots, x_n$ с коефициенти от k не е крайно породена k-алгебра.

Доказателство: Пръстенът $k[x_1,\ldots,x_n]$ е факториална ньотерова комутативна област с единица. Мултипликативната група $k[x_1,\ldots,x_n]=k^*$ не изчерпва ненулевите елементи на $k[x_1,\ldots,x_n]$, така че $k[x_1,\ldots,x_n]$ не е поле. Обединението $k[x_1,\ldots,x_n]^*\cup\{0\}=k^*\cup\{0\}=k$ е подгрупа на $(k[x_1,\ldots,x_n],+)$ и съгласно Лема 3.3, съществуват безбройно много неразложими полиноми $p(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$.
Да допуснем, че полето $k(x_1,\ldots,x_n)$ на рационалните функции на $x_1,\ldots,x_n$ с коефициенти от k е крайно породена k-алгебра. Тогава съществуват краен брой полиноми $f_i(x_1,\ldots,x_n),g_i(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$, $1\leq i\leq t$, така че

$$k(x_1,\ldots,x_n)=k\left[\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)},\ldots,\frac{f_t(x_1,\ldots,x_n)}{g_t(x_1,\ldots,x_n)}\right].$$

За произволен неразложим елемент $p(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$, който не дели нито един от полиномите $g_1(x_1,\ldots,x_n),\ldots,g_t(x_1,\ldots,x_n)$ условието

$$\frac{1}{p(x_1,\ldots,x_n)}\in k(x_1,\ldots,x_n)=k\left[\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)},\ldots,\frac{f_t(x_1,\ldots,x_n)}{g_t(x_1,\ldots,x_n)}\right]$$

води до $pf=g_1^{k_1}\ldots g_t^{k_t}$ за някакви неотрицателни цели k_i, $1\leq i\leq t$ и някакъв полином $f\in k[x_1,\ldots,x_n]$. Това изисква p да дели някой от полиномите $g_1,\ldots,g_t$. Противоречието доказва, че $k(x_1,\ldots,x_n)$ не е крайно породена k-алгебра, Q.E.D.

Задача 3.5. *Нека R е факториална ньотерова комутативна област с единица, чието поле от частни $Q\neq R$ и $(R^*\cup\{0\},+)$ е подгрупа на $(R,+)$. Да се докаже, че Q не е крайно породена $\mathbb{Z}$-алгебра.*

Следващата задача илюстрира съществуването на факториални ньотерови комутативни области с единица R с безбройно много неразложими елементи, за които обединението $R^*\cup\{0\}$ не е подгрупа на $(R,+)$

Задача 3.6. *Да се докаже, че полето $\mathbb{Q}$ на рационалните числа не е крайно породена $\mathbb{Z}$-алгебра.*

Упътване: Използвайте съществуването на безбройно много прости числа.

Твърдение 3.7. *Ако полето L е крайно породена алгебра $L=k[a_1,\ldots,a_n]$ над своето подполе k, то $a_1,\ldots,a_n$ са алгебрични над k.*
В частност, L е крайно разширение на k, $[L:k]:=\dim_k(L)<\infty$.

Доказателство: Полето от частни $k(a_1,\ldots,a_n)$ на $L=k[a_1,\ldots,a_n]$ се съдържа в L, защото L е поле. Комбинирайки с $L=k[a_1,\ldots,a_n]\subseteq k(a_1,\ldots,a_n)$ получаваме, че $L=k(a_1,\ldots,a_n)$.
Да допуснем, че някой пораждащ a_i на L над k не е алгебричен над k и да изберем максимално трансцендентно (т.е. алгебрично независимо) подмножество $a_1,\ldots,a_m$ на $a_1,\ldots,a_n$. Трансцендентността на $a_1,\ldots,a_m$ над k означава липсата на нетъждествено нулева полиномиална зависимост на $a_1,\ldots,a_m$ с коефициенти от k. Тогава за $\forall m+1\leq i\leq n$ съществува нетъждествено нулев полином $h_i(y_1,\ldots,y_m,y_i)\in k[y_1,\ldots,y_m,y_i]$, зависещ от y_i, който изпълнява равенството $h_i(a_1,\ldots,a_m,a_i)=0$.
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 $k(a_1,\ldots,a_n)=L$, съдържащо k. Полиномите

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

с корени a_i не се анулират тъждествено съгласно алгебричната независимост на $a_1,\ \ldots,a_m$. По този начин, всички a_i за $m+1\leq i\leq n$ се оказват алгебрични над L_o. От една страна имаме влагания на пръстени

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

От друга страна, $L_o[a_{m+1},\dots,a_n]$ е подпръстен на L, защото L_o е подполе на L, $a_{m+1},\dots,a_n \in L$ и полето L е затворено относно умножение и събиране на свои елементи. Следователно $L = L_o[a_{m+1},\dots,a_n]$ е крайно породена L_o-алгебра.
Алгебричните над L_o елементи $a_{m+1},\dots,a_n$ са цели над L_o, така че L е крайно породен L_o-модул или крайномерно линейно пространство над L_o. Прилагаме Лема 3.1 към ньотеровата област с единица k, крайно породената k-алгебра $L = k[a_1,\dots,a_n]$ и подпръстена L_o на L, съдържащ k. Понеже L е крайномерно линейно пространство над L_o, полето

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

е крайно породена k-алгебра за някакви полиноми

$$f_i(x_1,\dots,x_m), g_i(x_1,\dots,x_m) \in k[x_1,\dots,x_m], \quad g_i(a_1,\dots,a_m) \not\equiv 0.$$

Естественият епиморфизъм $\pi_A : k[x_1,\dots,x_m] \to k[a_1,\dots,a_m]$ на крайно породената k-алгебра $k[a_1,\dots,a_m]$ е изоморфизъм, съгласно трансцендентността на $a_1,\dots,a_m$. Той индуцира изоморфизъм $\pi_A : k(x_1,\dots,x_m) \to L_o = k(a_1,\dots,a_m)$ на съответните полета от частни, така че

$$k(x_1,\dots,x_m) = k\left[\frac{f_1(x_1,\dots,x_m)}{g_1(x_1,\dots,x_m)},\dots,\frac{f_t(x_1,\dots,x_m)}{g_t(x_1,\dots,x_m)}\right]$$

се оказва крайно породена k-алгебра. Това противоречи на Следствие 3.4 и доказва алгебричността на $a_1,\dots,a_n$ над k.
Алгебричните над k пораждащи $a_1,\dots,a_n$ на k-алгебрата $L = k[a_1,\dots,a_n]$ са цели над k, така че L е крайно породен k-модул. С други думи, L е крайномерно линейно пространство над k и $[L:k] := \dim_k(L) < \infty$, Q.E.D.

Задача 3.8. *Да се докаже, че ако поле F е крайно породена $\mathbb{Z}$-алгебра $F = \mathbb{Z}[a_1,\dots,a_n]$, то F е крайно поле.*

Упътване: Ако P е простото подполе на F, то $F = P[a_1,\dots,a_n]$ е крайно породена P-алгебра. Приложете Твърдение 3.7, за да получите, че F е крайномерно линейно пространство над P.
Ако допуснем, че F е безкрайно поле, то $P \simeq \mathbb{Q}$ е изоморфно на полето на рационалните числа. Приложете Твърдение 3.1 към ньотеровата комутативна област с единица $\mathbb{Z}$, крайно породената $\mathbb{Z}$-алгебра $F = \mathbb{Z}[a_1,\dots,a_n]$ и подпръстена $P \simeq \mathbb{Q}$ на F, съдържащ $\mathbb{Z}$, за да получите противоречие.

3. Максимални идеали в крайно породени алгебри над поле

Определение 3.9. *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 целият пръстен $I = R$.*

Лема 3.10. *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 $\Sigma \neq \emptyset$. Казваме, че $\{J_\alpha\}_{\alpha\in A} \subseteq \Sigma$ е линейно наредено подмножество, ако за произволни $\alpha,\beta \in A$ е в сила $J_\alpha \subseteq J_\beta$ или $J_\beta \subseteq J_\alpha$. Твърдим, че произволно линейно наредено подмножество $\{J_\alpha\}_{\alpha\in A} \subseteq \Sigma$ има горна граница $J_\infty := \cup_{\alpha\in A} J_\alpha$. По-точно, J_∞ е идеал в R, защото за произволни $a,b \in J_\infty$ съществуват $\alpha,\beta \in A$, така че $a \in J_\alpha$, $b \in J_\beta$. За $J_\alpha \subseteq J_\beta$ имаме $a - b \in J_\beta \lhd R$. В случая $J_\beta \subseteq J_\alpha$ забелязваме, че $a - b \in J_\alpha \subseteq J_\infty$. За произволни $a \in J_\alpha \subseteq J_\infty$

и $r \in R$ е в сила $ar \in J_\alpha \subseteq J_\infty$, доколкото $J_\alpha \lhd R$. Това установява, че $J_\infty \lhd R$. От $I \subseteq J_\alpha$ за $\forall \alpha \in A$ следва, че $I \subseteq J_\infty$. Ако допуснем, че $J_\infty = R$, то $1_R \in J_\infty$, така че $1_R \in J_\alpha$ за някое $\alpha \in A$, противно на $1_R \notin J_\alpha$ за $\forall \alpha \in A$. Следователно $J_\infty \in \Sigma$ и $J_\infty \supseteq J_\alpha$ за $\forall \alpha \in A$. Това доказва, че всяко линейно наредено подмножество $\{J_\alpha\}_{\alpha \in A} \subseteq \Sigma$ има горна граница $J_\infty \in \Sigma$.
По Лемата на Zorn, щом всяко линейно наредено подмножество на Σ има горна граница, то съществува максимален елемент $\mathfrak{M}$ на Σ. Идеалът $I \subseteq \mathfrak{M} \subsetneq R$ е максимален, защото ако $I_o \lhd R$ и $\mathfrak{M} \subsetneqq I_o$, то $I_o \notin \Sigma$. От $I \subseteq \mathfrak{M} \subseteq I_o$ за идеала I_o в R следва, че $I_o = R$, Q.E.D.

Лема 3.11. *Идеалът $\mathfrak{M}$ в комутативен пръстен с единица 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 за произволен елемент $r \in R \setminus \mathfrak{M}$, идеалът $\mathfrak{M} + rR \lhd R$ съдържа 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 $I = R$. Това доказва, че идеалът $\mathfrak{M} \lhd R$ е максимален, Q.E.D.

Задача 3.12. *Нека k е поле, I е собствен идеал в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от k. Да се докаже, че съществува крайно разширение $F \supseteq k$ и елементи $a_1, \ldots, a_n$ на полето F, такива че $f(a_1, \ldots, a_n) = 0$ за $\forall f \in I$.*

Упътване: Изберете максимален идеал $\mathfrak{M}$ в $k[x_1, \ldots, x_n]$, съдържащ I. Разгледайте полето $F = k[x_1, \ldots, x_n]/\mathfrak{M}$ и елементите $a_i = x_i + \mathfrak{M}$ за $\forall 1 \leq i \leq n$.

Лема 3.13. *Нека k е поле, $A = k[a_1, \ldots, a_n]$ е крайно породена k-алгебра с единица, а $I \subsetneq A$ е собствен идеал в A. Тогава естественият епиморфизъм*

$$\psi : k \longrightarrow k + I/I,$$
$$\psi(a) = a + I$$

е изоморфизъм на пръстени.

Доказателство: От $\psi(a+b) = a+b+I = (a+I)+(b+I) = \psi(a)+\psi(b)$ и $\psi(ab) = ab + I = (a + I)(b + I) = \psi(a)\psi(b)$ за $\forall a, b \in k$ следва, че ψ е хомоморфизъм на пръстени. Всеки елемент на фактор-пръстена $k + I/I$ е от вида $a + I = \psi(a)$ за някое $a \in k$, така че $\mathrm{im}(\psi) = k + I/I$. Ако $a \in \ker(\psi)$, то $a + I = I$ и $a \in k \cap I$. Полето k е подпръстен на A. По-точно, можем да отъждествим k с k-линейната обвивка на единицата 1_A на A, защото анулаторът на 1_A в k е нулев. Сечението $k \cap I$ е идеал в k, защото $(k, +)$ и $(I, +)$ са подгрупи на $(A, +)$ и $k \cap I$ е затворено относно умножение с елементи от k. Ако $k \cap I = k$, то $1_k = 1_A \in I$ и $I = A$, противно на допускането $I \subsetneq A$. Следователно $k \cap I = \{0\}$ и по Теоремата за хомоморфизмите

$$k = k/(k \cap I) = k/\ker(\psi) \simeq \mathrm{im}(\psi) = k + I/I,$$

Q.E.D.

ТВЪРДЕНИЕ 3.14. *Нека k е поле, $R = k[r_1, \ldots, r_n]$ е крайно породена k-алгебра и $\mathfrak{M}$ е максимален идеал в R. Тогава полето $R/\mathfrak{M}$ е крайно разширение на k. Още повече, ако k е алгебрично затворено поле, то $R/\mathfrak{M} \simeq k$ и съществуват елементи $a_1, \ldots, a_n \in k$, така че $\mathfrak{M} = \langle r_1 - a_1, \ldots, r_n - a_n \rangle$.*

Доказателство: Фактор-пръстенът

$$L = R/\mathfrak{M} = k[r_1, \ldots, r_n]/\mathfrak{M} = (k + \mathfrak{M})/\mathfrak{M}[r_1 + \mathfrak{M}, \ldots, r_n + \mathfrak{M}]$$

е разширение на полето $(k + \mathfrak{M})/\mathfrak{M} \simeq k$, което в същото време е крайно породена алгебра над $(k+\mathfrak{M})/\mathfrak{M}$. Съгласно Лема 3.7, елементите $r_1+\mathfrak{M}, \ldots, r_n+\mathfrak{M}$ са алгебрични над $(k + \mathfrak{M})/\mathfrak{M} \simeq k$ и полето $L = R/\mathfrak{M}$ е крайно разширение на полето k.
Ако полето k е алгебрично затворено, то алгебричните над $(k + \mathfrak{M})/\mathfrak{M} \simeq k$ елементи $r_i+\mathfrak{M} \in k[r_1, \ldots, r_n]/\mathfrak{M}$ принадлежат на $(k+\mathfrak{M})/\mathfrak{M}$ или съществуват $a_i \in k$ с $r_i + \mathfrak{M} = a_i + \mathfrak{M}$ за всички $1 \leq i \leq n$. Твърдим, че идеалът $\mathfrak{M}_o := \langle r_1 - a_1, \ldots, r_n - a_n \rangle \lhd R = k[r_1, \ldots, r_n]$ е максимален. За целта разглеждаме фактор-пръстена

$$R/\mathfrak{M}_o = k[r_1, \ldots, r_n]/\mathfrak{M}_o \simeq (k + \mathfrak{M}_o)/\mathfrak{M}_o\,[r_1 + \mathfrak{M}_o, \ldots, r_n + \mathfrak{M}_o] =$$
$$= (k + \mathfrak{M}_o)/\mathfrak{M}_o[a_1 + \mathfrak{M}_o, \ldots, a_n + \mathfrak{M}_n] \subseteq (k + \mathfrak{M}_o)/\mathfrak{M}_o.$$

Понеже полето $(k+\mathfrak{M}_o)/\mathfrak{M}_o$ е подпръстен на $R/\mathfrak{M}_o$, оттук следва съвпадението $R/\mathfrak{M}_o = (k + \mathfrak{M}_o)/\mathfrak{M}_o \simeq k$. По този начин, $R/\mathfrak{M}_o$ е поле и идеалът $\mathfrak{M}_o \lhd A$ е максимален.
От $r_i - a_i \in \mathfrak{M}$ за $\forall 1 \leq i \leq n$ получаваме, че $\mathfrak{M}_o \subseteq \mathfrak{M}$. Съгласно максималността на идеала $\mathfrak{M}_o \lhd R$ и $\mathfrak{M} \neq R$, това е достатъчно за $\mathfrak{M}_o = \mathfrak{M}$, Q.E.D.

ЗАДАЧА 3.15. *Нека k е поле, а $p(x) \in k[x]$ неразложим над k полином от степен $d \in \mathbb{N}$. Да се докаже, че фактор-пръстенът $F = k[x]/\langle p \rangle$ е поле и F е разширение на k от степен $[F : k] = \dim_k(F) = d$. Да се намери базис на F над k.*

4. Теорема на Hilbert за нулите

ЛЕМА-ОПРЕДЕЛЕНИЕ 3.16. *Нека R е комутативен пръстен с единица R, а I е идеал в R. Тогава множеството*

$$r(I) = \{x \in R \;\mid\; x^n \in I \quad \text{за някое } n \in \mathbb{N}\}$$

е идеал в R, съдържащ I и се нарича радикал на идеала I.
В частност, радикалът $\mathfrak{N} = r(\{0\})$ на нулевия идеал $\{0\} \lhd R$ е идеал в R, който се нарича нил-радикал на R. Съгласно

$$\mathfrak{N} = \{x \in R \;\mid\; x^n = 0 \quad \text{за някое } n \in \mathbb{N}\},$$

нил-радикалът се състои от нилпотентните елементи на R.

Доказателство: Ако $x, y \in r(I)$, то съществуват $m, n \in \mathbb{N}$, така че $x^m \in I$ и $y^n \in I$. В резултат,

$$(x - y)^{m+n-1} = \sum_{i=0}^{n-1} (-1)^i \binom{m+n-1}{i} x^{m+n-1-i} y^i +$$
$$+ \sum_{i=n}^{m+1n-1} (-1)^i \binom{m+n-1}{i} x^{m+n-i} y^i \in I,$$

защото $x^{m+n-1-i} \in I$ за $0 \leq i \leq n-1$ и $y^i \in I$ за $n \leq i \leq m+n-1$. Следователно $x - y \in r(I)$ и $(r(I), +)$ е подгрупа на $(R, +)$.

За произволно $x \in r(I)$ с $x^m \in I$ за някое $m \in \mathbb{N}$ и произволно r е в сила $rx \in r(I)$, съгласно $(rx)^m = r^m x^m \in I \lhd R$. Следователно $r(I)$ е идеал в R. Непосредствено се вижда, че всеки елемент на I се съдържа в $r(I)$, Q.E.D.

Твърдение 3.17. *Ако R е комутативен пръстен с единица, то нил-радикалът*

$$\mathfrak{N} = \cap_{\mathfrak{p} \lhd R} \mathfrak{p}$$

на R съвпада със сечението на всички прости идеали $\mathfrak{p} \lhd R$.
Радикалът

$$r(I) = \cap_{I \subseteq \mathfrak{p} \lhd R} \mathfrak{p}$$

на произволен идеал $I \lhd R$ съвпада със сечението на простите идеали $\mathfrak{p}$ в R, съдържащи I.

Доказателство: Ако $x \in \mathfrak{N}$, то съществува $n \in \mathbb{N}$, така че $x^n = 0$ принадлежи на всеки прост идеал $\mathfrak{p}$ в R. Оттук $x \in \mathfrak{p}$ и нил-радикалът $\mathfrak{N} \subseteq \cap_{\mathfrak{p} \lhd R} \mathfrak{p}$ се съдържа в сечението на простите идеали $\mathfrak{p}$ в R.
Обратното включване $\cap_{\mathfrak{p} \lhd R} \mathfrak{p} \subseteq \mathfrak{N}$ е еквивалентно на включването

$$R \setminus \mathfrak{n} \subseteq R \setminus (\cap_{\mathfrak{p} \lhd R} \mathfrak{p})$$

на съответните допълнения. За произволен елемент $x \in R \setminus \mathfrak{N}$ разглеждаме множеството

$$\Sigma_x := \{J \lhd R \ \mid \ x \notin r(J)\}$$

на идеалите J в R, чиито радикали $r(J) \lhd R$ не съдържат x. Множеството $\Sigma_x \neq \emptyset$ не е празно, защото нулевият идеал $\{0\} \in \Sigma_x$. Произволно линейно наредено подмножество $\{J_\alpha\}_{\alpha \in A} \subseteq \Sigma_x$ има горна граница $J_\infty := \cup_{\alpha \in A} J_\alpha$. Както в доказателството на Лема 3.10 проверяваме, че J_∞ е идеал в R. Ако $x \in r(J_\infty)$, то $x^n \in J_\infty$ за някое $n \in \mathbb{N}$. Следователно $x^n \in J_\alpha$ за някое $\alpha \in A$ и $x \in r(J_\alpha)$, противно на избора на $J_\alpha \in \Sigma_x$. Следователно $x \notin r(J_\infty)$ и $J_\infty \in \Sigma_x$. Ясно е, че $J_\infty \supseteq J_\alpha$ за $\forall \alpha \in A$. Съгласно Лемата на Zorn, Σ_x има максимален елемент J. Достатъчно е да докажем, че идеалът J е прост, за да получим съвпадението $\mathfrak{N} = \cap_{\mathfrak{p} \lhd R} \mathfrak{p}$ на нил-радикала $\mathfrak{N}$ със сечението на простите идеали в R. Ако идеалът $J \lhd R$ не е прост, то съществуват $a, b \in R \setminus J$ с $ab \in J$. Тогава идеалите $J_1 := J + \langle a \rangle \supsetneq J$ и $J_2 := J + \langle b \rangle \supsetneq J$ не принадлежат на Σ_x заради максималността на $J \in \Sigma_x$. Следователно съществуват $m, n \in \mathbb{N}$ с $x^m = \alpha + ar_1 \in J_1$, $x^n = \beta + br_2 \in J_2$ за някои $\alpha, \beta \in J$, $r_1, r_2 \in R$. Оттук, $x^{m+n} = (\alpha\beta + \alpha b r_2 + \beta a r_1) + ab r_1 r_2 \in J$ и $x \in r(J)$, противно на избора на $J \in \Sigma_x$. Това доказва, че идеалът J е прост и $\mathfrak{N} = \cap_{\mathfrak{p} \lhd R} \mathfrak{p}$.
Идеалите $\overline{J}$ в R/I са от вида J/I за някакъв идеал $J \lhd R$, съдържащ I. Наистина, ако $I \subseteq J \lhd R$, то $\overline{J} = J/I \lhd R/I$. За произволен идеал $\overline{J} \lhd R/I$, множеството

$$J := \{x \in R \ \mid \ x + I \in \overline{J}\}$$

е идеал в R, съдържащ I и $J/I = \{x + I \ \mid \ x \in J\} = \overline{J}$. По-точно, ако $x, y \in J$, то $(x + I) - (y + I) = x - y + I \in \overline{J} \lhd R/I$, така че $x - y \in J$ и $(J, +)$ е подгрупа на $(R, +)$. За $\forall x \in J$ и $\forall r \in R$ имаме $(r + I)(x + I) = rx + I \in \overline{J} \lhd R/I$, откъдето $rx \in J$ и $J \lhd R$ е идеал в R. За $\forall x \in I$ е в сила $x + I = I \in \overline{J}$, защото нулевият елемент I на R/I принадлежи на всеки идеал $\overline{J} \lhd R/I$. Съвпадението $J/I = \overline{J}$ е непосредствено следствие от определението на J.
Фактор-пръстенът $(R/I)/\overline{J} \simeq R/J$ на идеал $\overline{J} \lhd R/I$ съвпада с фактор-пръстена R/J по неговото повдигане $J \lhd R$. По-точно, изображението

$$\varphi : R/I \longrightarrow R/J,$$

$$\varphi(r + I) = r \in J \quad \text{за} \quad \forall r \in R$$

е коректно определен епиморфизъм на пръстени, съгласно $I \subseteq J$. Ядрото на φ е $\ker(\varphi) = J/I = \overline{J}$ и индуцираното изображение

$$\overline{\varphi} : (R/I)/\overline{J} \longrightarrow R/J,$$
$$\overline{\varphi}((r+I)+\overline{J}) = r + J \quad \text{за} \quad \forall r \in R$$

е коректно определен изоморфизъм на пръстени, съгласно Теоремата за хомоморфизмите.
Идеалът $\overline{J} \lhd R/I$ е прост тогава и само тогава, когато повдигането му $J \lhd R$ е прост идеал. Еквивалентно, фактор-пръстенът $(R/I)/\overline{J}$ е област на цялост точно когато R/J е област на цялост.
Да забележим, че нил-радикалът на R/I е

$$\mathfrak{N}(R/I) = \{r + I \in R/I \ \mid \ (r+I)^n = I \quad \text{за някое} \quad n \in \mathbb{N}\} =$$
$$= \{r + I \in R/I \ \mid \ r^n \in I \quad \text{за някое} \quad n \in \mathbb{N}\} = r(I)/I.$$

Вземайки предвид, че $\mathfrak{N}(R/I)$ е сечението на простите идеали $\overline{\mathfrak{p}} \lhd R/I$, получаваме, че

$$r(I)/I = \cap_{\overline{\mathfrak{p}} \lhd R/I} \overline{\mathfrak{p}} = \cap_{I \subseteq \mathfrak{p} \lhd R} (\mathfrak{p}/I) = (\cap_{I \subseteq \mathfrak{p} \lhd R} \mathfrak{p})/I$$

е факторът на сечението $\cap_{I \subseteq \mathfrak{p} \lhd R} \mathfrak{p}$ на простите идеали $\mathfrak{p}$ в R, съдържащи I.
Твърдим, че

$$r(I) = \cap_{I \subseteq \mathfrak{p} \lhd R} \mathfrak{p}.$$

По-общо, ако J_1 и J_2 са идеали в R, съдържащи идеала I и факторите $J_1/I = J_2/I$ съвпадат, то и идеалите $J_1 = J_2$ съвпадат. Наистина, за всяко $x_1 \in J_1$ съществува $x_2 \in J_2$, така че $x_1 + I = x_2 + I$. Тогава $x = x_1 - x_2 \in I \subseteq J_2$, така че $x_1 = x + x_2 \in J_2$ и $J_1 \subseteq J_2$. Аналогично проверяваме, че $J_2 \subseteq J_1$, откъдето $J_1 = J_2$, Q.E.D.

ТЕОРЕМА 3. **(Теорема на Hilbert за нулите)** *Нека k е алгебрично затворено поле, I е идеал в $k[x_1, \ldots, x_n]$,*

$$V(I) = \{a = (a_1, \ldots, a_n) \in k^n \ \mid \ f(a_1, \ldots, a_n) = 0 \quad \textit{за} \quad \forall f \in I\}$$

е афинното алгебрично множество, определено от I, а

$$IV(I) = \{g \in k[x_1, \ldots, x_n] \ \mid \ g(a_1, \ldots, a_n) = 0 \quad \textit{за} \quad \forall a = (a_1, \ldots, a_n) \in V(I)\}$$

е идеалът на $V(I)$ в $k[x_1, \ldots, x_n]$. Тогава

$$IV(I) = r(I)$$

за радикала $r(I) \lhd k[x_1, \ldots, x_n]$ на I.

Доказателство: Включването $r(I) \subseteq IV(I)$ е тривиално, защото ако $f^m \in I$ за полином $f \in k[x_1, \ldots, x_n]$ и $m \in \mathbb{N}$, то $f^m(a_1, \ldots, a_n) = 0$ за всяка точка $(a_1, \ldots, a_n) \in V(I)$. Поради липсата на делители на нулата в полето k, оттук следва $f(a_1, \ldots, a_n) = 0$, така че $f \in IV(I)$.
Обратното включване $IV(I) \subseteq r(I)$ е еквивалентно на включването

$$k[x_1, \ldots, x_n] \setminus r(I) \subseteq k[x_1, \ldots, x_n] \setminus IV(I)$$

на съответните допълнения. Ако $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \setminus r(I)$, то съгласно Твърдение 3.17 съществува прост идеал $\mathfrak{p} \lhd k[x_1, \ldots, x_n]$, съдържащ I, така че $f(x_1, \ldots, x_n) \notin \mathfrak{p}$. Фактор-пръстенът

$$R_1 := k[x_1, \ldots, x_n]/\mathfrak{p} = (k + \mathfrak{p})/\mathfrak{p}[x_1 + \mathfrak{p}, \ldots, x_n + \mathfrak{p}]$$

е област на цялост и се влага в поле от частни Q_1. Понеже $f + \mathfrak{p} \neq \mathfrak{p}$ е ненулев елемент на R_1, съществува $(f + \mathfrak{p})^{-1} = \frac{1}{f+\mathfrak{p}} \in Q_1$ и можем да разгледаме подпръстена

$$R_2 = R_1\left[\frac{1}{f+\mathfrak{p}}\right] \simeq (k+\mathfrak{p})/\mathfrak{p}\left[x_1 + \mathfrak{p}, \ldots, x_n + \mathfrak{p}, \frac{1}{f+\mathfrak{p}}\right]$$

на Q_1, който е крайно породена k-алгебра. Произволен максимален идеал $\mathfrak{M}$ на R_2 не съдържа $f+\mathfrak{p}$, защото $f+\mathfrak{p} \in R_2^*$ е обратим в R_2. Полето

$$R_2/\mathfrak{M} \simeq (k+\mathfrak{M})/\mathfrak{M}\left[x_1+\mathfrak{M},\ldots,x_n+\mathfrak{M},\frac{1}{f+\mathfrak{p}}+\mathfrak{M}\right]$$

е изоморфно на алгебрично затвореното поле k. Следователно съществуват $a_1,\ldots,a_n,a_0 \in k$, така че $x_i+\mathfrak{M}=a_i+\mathfrak{M}$ за $\forall 1 \leq i \leq n$ и $f+\mathfrak{M}=a_0+\mathfrak{M} \neq \mathfrak{M}$. Ако $g \in I \subseteq \mathfrak{p}$, то $g+\mathfrak{p}=\mathfrak{p}$ е нулевият елемент на R_1 и R_2, така че

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

е нулевият елемент на $R_2/\mathfrak{M}$. Следователно $g(a_1,\ldots,a_n) \in k \cap \mathfrak{M} = \{0\}$ и точката $(a_1,\ldots,a_n) \in V(I)$ се съдържа в нулите на идеала I. Ако допуснем, че $f \in IV(I)$, то $f(a_1,\ldots,a_n)=0$. В резултат,

$$a_0+\mathfrak{M}=f+\mathfrak{M}=f(x_1+\mathfrak{M},\ldots,x_n+\mathfrak{M})=f(a_1,\ldots,a_n)+\mathfrak{M}=\mathfrak{M}.$$

Противоречието доказва, че $f \notin IV(I)$. С други думи, $k[x_1,\ldots,x_n] \setminus r(I)$ се съдържа в $k[x_1,\ldots,x_n] \setminus IV(I)$, откъдето $IV(I) \subseteq r(I)$ и $IV(I)=r(I)$, Q.E.D.

Определение 3.18. *Идеалът I на комутативен пръстен с единица R се нарича радикален, ако съвпада с радикала си $r(I)=I$.*

Непосредствено се вижда, че радикалът $r(I)$ на произволен идеал I в комутативен пръстен с единица R е радикален идеал. По-точно, ако $x^n \in r(I)$ за някое $n \in \mathbb{N}$, то съществува $m \in \mathbb{N}$, така че $(x^n)^m = x^{mn} \in I$. Следователно $x \in r(I)$ и $r(r(I))=r(I)$.

Задача 3.19. *Да се докаже, че:*
(i) всеки прост идеал $\mathfrak{p}$ в комутативен пръстен с единица R е радикален;
(ii) всеки максимален идеал $\mathfrak{M}$ в комутативен пръстен с единица R е радикален;
(iii) 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 подмножество $X \subseteq k^n$ на афинно пространство k^n над поле k е радикален.

Упътване: За (ii) използвайте, че всяко поле е комутативна област с единица, така че всеки максимален идеал в комутативен пръстен с единица R е прост идеал.

Задача 3.20. **(Слаба форма на Теоремата на Hilbert за нулите)** *Да се докаже, че ако k е алгебрично затворено поле, а I е идеал в $k[x_1,\ldots,x_n]$ с празно множество на нулите $V(I)=\emptyset$, то $I=k[x_1,\ldots,x_n]$ съвпада с целия полиномиален пръстен $k[x_1,\ldots,x_n]$.*

Упътване: Допуснете, че $I \subsetneq k[x_1,\ldots,x_n]$ и изберете максимален идеан $\mathfrak{M}$ в $k[x_1,\ldots,x_n]$, съдържащ I. Тогава $\mathfrak{M}=\langle x_1-a_1,\ldots,x_n-a_n\rangle$ за някои $a_1,\ldots,a_n \in k$ и афинното алгебрично множество $\emptyset=V(I) \supseteq V(\mathfrak{M})=\{(a_1,\ldots,a_n)\}$.

Следствие 3.21. *Нека k е алгебрично затоварено поле. Тогава съществува взаимно еднозначно съответствие между афинните алгебрични множества $X=V(S) \subseteq k[x_1,\ldots,x_n]$, $S \subseteq k[x_1,\ldots,x_n]$ и радикалните идеали $I(X)=IV(S) \lhd k[x_1,\ldots,x_n]$.*

Доказателство: Всяко афинно алгебрично множество $X=V(S) \subseteq k^n$, $S \subseteq k[x_1,\ldots,x_n]$ отговаря на радикален идеал $IV(S)=IV(\langle S\rangle)=r(\langle S\rangle)$. Обратно, всеки радикален идеал $I=r(I) \lhd k[x_1,\ldots,x_n]$ отговаря на афинно алгебрично множество $V(I) \subseteq k^n$. Съответствието е взаимно еднозначно, защото съгласно Лема 1.31, $VI(X)=X$ за всяко афинно алгебрично множество $X \subseteq k^n$. от Теорема 3 на Hilbert за нулите, $IV(I)=r(I)=I$ за произволен радикален идеал $I=r(I) \lhd R$, Q.E.D.

Съгласно Следствие 3.21, ако k е алгебрично затворено поле и радикалните идеали $I_1 \subsetneq I_2 \lhd k[x_1, \ldots, x_n]$ се съдържат строго, то съответните им афинни алгебрични множества $V(I_2) \subsetneq V(I_2) \subseteq k^n$ също се съдържат строго. Аналогично, ако афинните алгебрични множества $V_1 \subsetneq V_2 \subseteq k^n$ се съдържат строго, то радикалните им идеали $I(V_2) \subsetneq I(V_1) \lhd k[x_1, \ldots, x_n]$ се съдържат строго.

Следствие 3.22. *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 1.31 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 1.16 (i). 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.