Глава 5

Теорема на Hilbert за базиса и Теорема на Hilbert за нулите

1. Ньотерови пръстени и модули над тях

Определение 5.1. *Комутативният пръстен с единица R е ньотеров, ако всеки идеал I в R е крайно породен, т.е. $I = \langle x_1, \ldots, x_k \rangle = Rx_1 + \ldots + Rx_k$ за някои $x_1, \ldots, x_k \in R$.*

Твърдение 5.2. *Комутативният пръстен с единица R е ньотеров тогава и само тогава, когато всяка ненамаляваща редица от идеали*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots \tag{5.1}$$

се стабилизира след краен брой стъпки.
В частност, ако R е ньотеров пръстен, то всяко пораждащо подмножество S на идеал $\langle S \rangle \lhd R$ има крайно пораждащо подмножество $\{s_1, \ldots, s_n\} \subseteq S$, $\langle S \rangle = \langle s_1, \ldots, s_n \rangle$.

Доказателство: Нека R е ньотеров пръстен и (5.1) е ненамаляваща редица от идеали Твърдим, че $I := \cup_{s=1}^{\infty} I_s$ е идеал в R. Наистина, за произволни $a, b \in I$ съществуват $p, q \in \mathbb{N}$, така че $a \in I_p$, $b \in I_q$. Ако $n := \max(p, q)$, то $a, b \in I_n$ и $a - b \in I_n \lhd R$. За $\forall a \in I_p$ и $\forall r \in R$, имаме $ar \in I_p \subseteq I$, така че I е идеал в R. По определението за ньотеровост, идеалът $I = \langle a_1, \ldots, a_k \rangle = Ra_1 + \ldots + Ra_k$ е крайнопороден. Ако $a_j \in I_{n_j}$ и $n := \max(n_1, \ldots, n_k)$, то за всяко $m \geq n$ е в сила $I \subseteq I_n \subseteq I_m \subseteq I$. Следователно $I = I_n = I_{n+1} = \ldots$ и редицата (5.1) се стабилизира след краен брой стъпки.
Ще докажем, че ако всяка ненамаляваща редица от идеали 5.1 се стабилизира след краен брой стъпки, то всяко множество $S \subseteq R$ има крайно подмножество $\{s_1, \ldots, s_n\} \subseteq S$, така че $\langle S \rangle = \langle s_1, \ldots, s_n \rangle$. Оттук следва, че условието за стабилизация на ненамаляващите редици от идеали е достатъчно за ньотеровостта на пръстена. Освен това, ако R е ньотеров пръстен то всяко пораждащо множество на идеал има крайно пораждащо подмножество, защото стабилизацията на ненамаляващите редици от идеали е необходимо условие за ньотеровост.
С допускане на противното, нека $S \subseteq R$ е такова подмножество, че идеалът $I = \langle S \rangle$ няма крайна пораждаща система $\{s_1, \ldots, s_n\} \subseteq S$. Тогава избираме $\sigma_1 \in S$. С индукция по $n \in \mathbb{N}$, ако $\sigma_1, \ldots, \sigma_n \in S$ са такива, че $\sigma_i \in S \setminus \langle \sigma_1, \ldots, \sigma_{i-1} \rangle$ за $\forall 2 \leq i \leq n$, то съществува $\sigma_{n+1} \in S \setminus \langle \sigma_1, \ldots, \sigma_n \rangle$. В противен случай, от $S \subseteq I_n := \langle \sigma_1, \ldots, \sigma_n \rangle$ следва $\langle S \rangle \subseteq I_n$, защото I_n е затворено относно събиране на свои елементи и умножение с елементи на R. Комбинирайки с $I_n \subseteq \langle S \rangle$ получаваме $I = I_n$, така че крайното подмножество $\{\sigma_1, \ldots, \sigma_n\} \subseteq S$ поражда I. Това противоречи на допускането и доказва съществуването на безкрайна редица $\{\sigma_n\}_{n=1}^{\infty} \subseteq S$, изпълняваща условието $\sigma_n \in S \setminus I_{n-1} := \langle \sigma_1, \ldots, \sigma_{n-1} \rangle$ за $\forall n \geq 2$. Безкрайната редица от идеали $I_{n-1} \subsetneq I_n$ е строго растяща. Противоречието с предположението за стабилизация на ненамаляващите редици от идеали и доказва твърдението, Q.E.D.
Модул M над комутативен пръстен с единица R е линейно пространство над R. По-точно:

Определение 5.3. *Непразното множество M е модул над комутативния прѣстен с единица R, ако в M са определени събиране*

$$M \times M \longrightarrow M,$$

$$(x, y) \mapsto x + y \quad \text{за} \quad x, y \in M$$

и умножение

$$R \times M \longrightarrow M,$$

$$(r, x) \mapsto rx \quad \text{на } x \in M \text{ с } r \in R,$$

изпѣлняващи свойствата:
(i) асоциативност на събирането: $(x + y) + z = x + (y + z)$ *за* $\forall x, y, z \in M$;
(ii) комутативност на събирането : $x + y = y + x$ *за* $\forall x, y \in M$;
(iii) съществува нулев елемент 0_M, *така че* $x + 0_M = x$ *за* $\forall x \in M$;
(iv) за $\forall x \in M$ *съществува противоположен елемент* $\exists(-x) \in M$, *така че* $x + (-x) = 0_M$;
(v) дистрибутивен закон над скаларен множител: $(r+s)x = rx+sx$ *за* $\forall r, s \in R$, $\forall x \in M$;
(vi) дистрибутивен закон над векторен множител: $r(x + y) = rx + ry$ *за* $\forall r \in R$, $\forall x, y \in M$;
(vii) $(rs)x = r(sx)$ *за* $\forall r, s \in R$, $\forall x \in M$;
(viii) $1_R x = x$ *за* $\forall x \in M$ *и* $1_R \in R$.

Абелева група $(M, +)$ е R-модул тогава и само тогава, когато съществува изображение $R \times M \to M$, $(r, x) \mapsto rx$, изпълняващо свойствата (v)-(viii) от Определение 5.3.
Всеки комутативен прѣстен с единица R е модул над себе си.

Определение 5.4. *Изображението* $\varphi : M \to N$ *е хомоморфизъм на R-модула M в R-модула N, ако*

$$\varphi\left(\sum_{i=1}^{n} r_i x_i\right) = \sum_{i=1}^{n} r_i \varphi(x_i)$$

за произволни $r_1, \ldots, r_n \in R$ *и* $x_1, \ldots, x_n \in M$.
Взаимно еднозначните хомоморфизми на R-модули се наричат изоморфизми на R-модули.

Задача 5.5. *Да се докаже, че изображението* $\varphi : M \to N$ *на R модули M и N е хомоморфизъм на R-модули тогава и само тогава, когато за произволни* $x, y \in M$ *и произволно* $r \in R$ *са в сила равенствата*

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{и} \quad \varphi(rx) = r\varphi(x).$$

Определение 5.6. *Непразното подмножество N на модул M над комутативен прѣстен с единица R е R-подмодул, ако заедно с произволни свои елементи* $n_1, \ldots, n_k \in N$ *съдържа всички техни R-линейни комбинации*

$$r_1 n_1 + \ldots + r_k n_k.$$

Задача 5.7. *Нека R е комутативен прѣстен с единица, M е R-модул. Да се докаже, че:*
(i) непразното подмножество $N \subseteq M$ *е R-подмодул тогава и само тогава, когато за произволни* $x, y \in N$ *и произволно* $r \in R$ *са в сила* $x + y \in N$ *и* $rx \in N$;
(ii) ако N е R-подмодул на M, то $(N, +)$ е подгрупа на $(M, +)$.
В частност, ако N е подмодул на M, то $(N, +)$ е абелева група.

Задача 5.8. *Нека $(M,+)$ е адитивно записана абелева група. За произволно естествено n определяме $nx = x + \ldots + x$ като n-кратната сума на x. Полагаме $0x = 0 \in M$ за $0 \in \mathbb{Z}$ и $(-n)x = -(nx)$ за $\forall n \in \mathbb{N}$. Да се докаже, че:*
(i) M е $\mathbb{Z}$-модул относно така определеното изображение

$$\mathbb{Z} \times M \longrightarrow M,$$

$$(n,x) \mapsto nx \quad за \quad \forall n \in \mathbb{Z}, \quad \forall x \in M;$$

(ii) $(N,+)$ е подгрупа на $(M,+)$ тогава и само тогава, когато N е $\mathbb{Z}$-подмодул на M;
(iii) изображението $\varphi : M \to M_1$ в адитивно записана абелева група $(M_1,+)$ е хомоморфизъм на групи тогава и само тогава, когато е хомоморфизъм на $\mathbb{Z}$-модули.

Лема-Определение 5.9. *Нека R е комутативен пръстен с единица, M е R-модул, а N е R-подмодул на M. Умножението на елементи $x \in M$ на модула с елементи $r \in R$ на пръстена индуцира коректно определено умножение*

$$R \times (M,+)/(N,+) \longrightarrow (M,+)/(N,+),$$

$$(r, m+N) \mapsto r(m+N) = rm + N$$

на елементи $m+N$ на фактор-групата $(M,+)/(N,+)$ с елементи $r \in R$ и превръща M/N в R-модул.
Модулът M/N над R се нарича фактор-модул на M относно N.
Вземайки предвид, че всеки идеал I в R е R-модул, стигаме до извода, че произволен фактор-пръстен R/I има структура на R-модул.

Доказателство: Подгрупата $(N,+)$ на абелевата група $(M,+)$ е нормална, така че фактор-групата $(M,+)/(N,+)$ е коректно определена. За коректността на умножението на елементи $m+N$ на $(M,+)/(N,+)$ с елементи r на R забелязваме, че ако $m+N = m'+N$, то $m'-m \in N$, така че $rm'-rm = r(m'-m) \in N$, защото N е R-подмадул на M. Оттук $rm+N = rm'+N$ и произведението $r(m+N) = rm+N$ не зависи от избора на представител m на съседния клас $m+N$ по модул $(N,+)$.
Непосредствено се проверява, че

$$(r+s)(m+N) = (r+s)m + N = rm + sm + N =$$

$$= (rm+N) + (sm+N) = r(m+N) + s(m+N),$$

$$r[(m_1+N)+(m_2+N)] = r(m_1+m_2+N) = r(m_1+m_2) + N =$$

$$= rm_1 + rm_2 + N = (rm_1+N) + (rm_2+N) = r(m_1+N) + r(m_2+N),$$

$$(rs)(m+N) = (rs)m + N = r(sm) + N = r(sm+N) = r[s(m+N)] \quad \text{и}$$

$$1_R(m+N) = 1_R m + N = m + N$$

за произволни $m+N, m_1+N, m_2+N \in M/N$, и произволни $r, s \in R$, Q.E.D.

Задача 5.10. (Теорема за хомоморфизмите на модули) *Да се докаже, че ако $\varphi : M \to N$ е хомоморфизъм на R-модули, то ядрото*

$$\ker\varphi := \{\mu \in M \;\mid\; \varphi(\mu) = 0_N\}$$

на φ е R-подмодул на M, образът

$$\mathrm{im}\varphi := \{\varphi(m) \;\mid\; m \in M\}$$

е R-подмодул на N и изображението

$$\overline{\varphi} : M/\ker\varphi \longrightarrow \mathrm{im}\varphi,$$

$$\overline{\varphi}(m + \ker\varphi) = \varphi(m) \quad за \quad \forall m + \ker\varphi \in M/\ker\varphi$$

е коректно определен изоморфизъм на R-модули.

Упътване: Проверете първо, че $0_R.y = 0_N$ за $\forall y \in N$, $r.0_N = 0_N$ за $\forall r \in R$ и $\varphi(x_1 - x_2) = \varphi(x_1) - \varphi(x_2)$ за $\forall x_1, x_2 \in M$.

Задача 5.11. *Нека R е комутативен пръстен с единица, M е R-модул, а $x \in M$ е елемент на M. Определяме анулатора на x в R като множеството*

$$A_x = \{r \in R \mid rx = 0_M\}.$$

Да се докаже, че:
(i) A_x е идеал в R;
(ii) подмножеството $Rx = \{rx \mid r \in R\}$ на M е R-подмодул;
(iii) изображението

$$\overline{\varphi} : R/A_x \longrightarrow Rx,$$
$$\overline{\varphi}(r + A_x) = rx \quad за \quad \forall r + A_x \in R/A_x$$

на фактор-пръстена R/A_x е коректно зададен изоморфизъм на R-модули.

Упътване: За (iii) е достатъчно да проверите, че изображението

$$\varphi : R \longrightarrow Rx,$$
$$\varphi(r) = rx \quad \text{за} \quad \forall r \in R$$

е хомоморфизъм на R-модули с ядро $\ker\varphi = A_x$ и образ $\mathrm{im}\varphi = Rx$.

Задача 5.12. *Нека R е комутативен пръстен с единица, M е R-модул, $x, y \in M$. Да се докаже, че:*
(i) $Rx + Ry$ е подмодул на M, съдържащ Ry;
(ii) $Rx \cap Ry$ е подмодул на M, съдържащ се в Rx;
(iii) фактор-модулите $Rx/(Rx \cap Ry)$ и $(Rx + Ry)/Ry$ са изоморфни.

Упътване: За (iii) е достатъчно да проверите, че

$$\varphi : Rx \longrightarrow (Rx + Ry)/Ry,$$
$$\varphi(rx) = rx + Ry \quad \text{за} \quad \forall rx \in Rx$$

е хомоморфизъм на R-модули с ядро $\ker\varphi = Rx \cap Ry$ и образ

$$\mathrm{im}\varphi = (Rx + Ry)/Ry.$$

Определение 5.13. *Модулът M над комутативния пръстен с единица R е крайно породен, ако съществуват краен брой елементи $x_1, \ldots, x_n \in M$, така че $M = \{r_1x_1 + \ldots + r_nx_n \mid r_i \in R\}$ се състои от R-линейните комбинации на тези елементи. В такъв случай бележим $M = Rx_1 + \ldots + Rx_n$.*

Лема 5.14. *Ако R е ньотеров комутативен пръстен с единица, а M е крайно породен R-модул, то всеки R-подмодул N на M е крайно породен над R.*

Доказателство: С индукция по броя n на пораждащите $\mu_1, \ldots, \mu_n$ на $M = R\mu_1 + \ldots + R\mu_n$, ако $M = R\mu_1$, то за произволен R-подмодул N на $M = R\mu_1$ множеството

$$C_N = \{r \in R \mid r\mu_1 \in N\}$$

на коефициентите на елементите на N е идеал в R. Пръстенът R е ньотеров, така че съществуват краен брой пораждащи $r_1, \ldots, r_l$ на $C_N = \langle r_1, \ldots, r_l\rangle = Rr_1 + \ldots + Rr_l$. Тогава $N = Rr_1\mu_1 + \ldots + Rr_l\mu_1$ е крайно породен R-модул.
Ако $M = R\mu_1 + \ldots + R\mu_{n-1} + R\mu_n$ има $n \geq 2$ пораждащи, то фактор-модулът $M/R\mu_n = R(\mu_1 + R\mu_n) + \ldots + R(\mu_{n-1} + R\mu_n)$ има $n - 1$ пораждащи, защото всеки елемент на $M/R\mu_n$ е от вида $\sum\limits_{i=1}^{n} r_i\mu_i + R\mu_n = \sum\limits_{i=1}^{n-1} r_i(\mu_i + R\mu_n)$. Сумата $N + R\mu_n = \{y + r\mu_n \mid y \in N, \ r \in R\}$ е R-подмодул на M, съдържащ $R\mu_n$, така че фактор-модулът $(N + R\mu_n)/R\mu_n$ е коректно определен R-подмодул

на $M/R\mu_n$. По индукционно предположение, подмодулът $(N + R\mu_n)/R\mu_n$ на $(n-1)$-породения R-модул $M/R\mu_n$ е крайно породен, т.е.

$$(N + R\mu_n)/R\mu_n = R(\nu_1 + R\mu_n) + \ldots + R(\nu_m + R\mu_n)$$

за някакви елементи $\nu_1, \ldots, \nu_m \in N$.
От друга страна, R-подмодулът $N \cap R\mu_n$ на $R\mu_n$ е крайно породен или

$$N \cap R\mu_n = R\lambda_1 + \ldots + R\lambda_l$$

за подходящи $\lambda_1, \ldots, \lambda_l \in N \cap R\mu_n$.
Твърдим, че

$$N = R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m \tag{5.2}$$

се поражда от $\lambda_1, \ldots, \lambda_l, \nu_1, \ldots, \nu_m \in N$ като R-модул. Включването

$$R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m \subseteq N$$

следва от $\lambda_j, \nu_i \in N$. Всеки елемент $x \in N$ отговаря на елемент

$$x + R\mu_n = \sum_{i=1}^{m} r_i(\nu_i + R\mu_n) = \sum_{i=1}^{m} r_i\nu_i + R\mu_n \in (N + R\mu_n)/R\mu_n.$$

Следователно $x_o := x - \sum\limits_{i=1}^{m} r_i\nu_i \in N \cap R\mu_n$, откъдето $x_o = \sum\limits_{j=1}^{l} s_j\lambda_j$ за подходящи $s_j \in R$. По този начин получаваме, че

$$x = \sum_{j=1}^{l} s_j\lambda_j + \sum_{i=1}^{m} r_i\nu_i \in R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m.$$

Това доказва $N \subseteq R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m$ и (5.2), Q.E.D.

Задача 5.15. *Нека k е поле, а $M = k[x]\mu_1 + k[x]\mu_2$ е $k[x]$-модул с два пораждащи μ_1 и μ_2. Да се докаже, че всеки $k[x]$-подмодул N на M може да се породи от не повече от два елемента.*

Упътване: Използвайте, че $k[x]$ е област на главни идеали.

Твърдение 5.16. *Ако R е нътеров комутативен пръстен с единица, то пръстенът $R[x]$ на полиномите на една променлива x с коефициенти от R е нътеров комутативен пръстен с единица.*

Доказателство: Допускаме, че пръстенът $R[x]$ не е нътеров и разглеждаме идеал $I \lhd R[x]$, който не е крайно породен. Избираме $f_1 \in I \setminus \{0\}$ от минимална степен. С индукция по броя на избраните полиноми, да предположим, че сме фиксирали $f_1, \ldots, f_{j-1} \in I$ с $f_i \in I \setminus \langle f_1, \ldots, f_{i-1}\rangle$ от минимална степен за всяко $2 \leq i \leq j-1$. Вземаме $f_j \in I \setminus \langle f_1, \ldots, f_{j-1}\rangle$ от минимална степен. По този начин получаваме безкрайна редица от полиноми $f_1, \ldots, f_j, \ldots$. Твърдим, че $\deg(f_{m+1}) \geq \deg(f_i)$ за $\forall 1 \leq i \leq m$. В противен случай, съгласно $f_{m+1} \in S \setminus \langle f_1, \ldots, f_{i-1}\rangle$ би трябвало да изберем f_{m+1} за i-ти член на конструираната редица от полиноми. Оттук, степените на избраните полиноми образяват ненамаляваща редица

$$\deg f_1 \leq \deg f_2 \leq \ldots \leq \deg f_{n-1} \leq \deg f_n \leq \ldots.$$

Нека

$$J = \langle LC(f_n) \mid n \in \mathbb{N}\rangle$$

е идеалът в R, породен от старшите коефициенти $LC(f_n) \in R$ на всички полиноми от редицата $\{f_n\}_{n=1}^{\infty} \subseteq R[x]$. Съгласно Твърдение 5.2, съществува крайно подмножество $\{LC(f_{i_1}), \ldots, LC(f_{i_s})\} \subseteq \{LC(f_n) \mid n \in \mathbb{N}\}$ от пораждащи на J.

Оттук, за $m := \max(i_1, \ldots, i_s)$ имаме $J = \langle LC(f_1), \ldots, LC(f_m)\rangle$. Представяме $LC(f_{m+1}) \in J = \langle LC(f_1), \ldots, LC(f_m)\rangle$ във вида

$$LC(f_{m+1}) = \sum_{i=1}^{m} LC(f_i)r_i$$

чрез подходящи $r_i \in R$. Полиномът

$$f'_{m+1} = f_{m+1} - \sum_{i=1}^{m} x^{\deg(f_{m+1})-\deg(f_i)} f_i r_i,$$

е от степен $\deg(f'_{m+1}) < \deg(f_{m+1})$, защото коефициентът на $x^{\deg(f_{m+1})}$ в f'_{m+1} се анулира. Съгласно избора на $f_{m+1} \in I \setminus \langle f_1, \ldots, f_m\rangle$ от минимална степен, $f'_{m+1} \in \langle f_1, \ldots, f_m\rangle$. В резултат, $f_{m+1} = f'_{m+1} + \sum\limits_{i=1}^{m} x^{\deg(f_{m+1})-\deg(f_i)} f_i r_i \in \langle f_1, \ldots, f_m\rangle$, което противоречи на избора на f_{m+1} и доказва ньотеровостта на $R[x]$, Q.E.D.
Като непосредствено следствие от Твърдение 5.16 получаваме следното

Следствие 5.17. *Ако R е ньотеров комутативен пръстен с единица, то пръстенът $R[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от R е ньотеров комутативен пръстен с единица.*

Доказателство: С индукция по брой на променливите n, ако $R[x_1, \ldots, x_{n-1}]$ е ньотеров комутативен пръстен с единица, то $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ е ньотеров комутативен пръстен с единица, Q.E.D.
Вземайки предвид, че пръстенът на полиномите $R[x_1, \ldots, x_n]$ с коефициенти от комутативна област с единица R е комутативна област с единица и Следствие 5.17, получаваме следната

Теорема 9. **(Теорема на Hilbert за базиса)** *Пръстенът на полиномите $k[x_1, \ldots, x_n]$ на няколко променливи с коефициенти от поле k е ньотерова комутативна област с единица.*

Следствие 5.18. *Всяко афинно алгебрично множество $V \subset k^n$ е множество на нулите $Z = Z(f_1, \ldots, f_m)$ на краен брой полиноми*

$$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n].$$

Доказателство: Нека $S \subseteq k[x_1, \ldots, x_n]$ е множество от полиноми, а $Z = Z(S) \subseteq \overline{k}^n$ е афинното алгебрично множество на нулите на S. По Лема 4.14 (iv), $Z = Z(\langle S\rangle)$ съвпада с множеството на нулите на идеала $\langle S\rangle \lhd \overline{k}[x_1, \ldots, x_n]$, породен от S. Съгласно Теорема 9 и Твърдение 5.2, съществува крайна пораждаща система $\{f_1, \ldots f_m\} \subseteq S$ на идеала $\langle S\rangle$, така че $Z(\langle S\rangle) = Z(\langle f_1, \ldots, f_m\rangle) = V(f_1, \ldots, f_m)$, Q.E.D.

Определение 5.19. *Ако R и S са комутативни пръстени с единица, S е R-модул и*

$$r(s_1 s_2) = (rs_1)s_2 \quad за \quad \forall s_1, s_2 \in S, \quad \forall r \in R,$$

то казваме, че S е R-алгебра.

Пример 5.20. *Пръстенът $R[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от комутативен пръстен с единица R е R-алгебра.*

Определение 5.21. *Хомоморфизъм $\varphi : S_1 \to S_2$ на R-алгебри е хомоморфизъм на пръстени, който е и хомоморфизъм на R-модули.*

Задача 5.22. *Да се докаже, че изображението $\varphi : S_1 \to S_2$ на R-алгебри е хомоморфизъм на R-алгебри тогава и само тогава, когато са изпълнени едновременно следните три условия:*
(i) $\varphi(s+t) = \varphi(s) + \varphi(t)$ за $\forall s, t \in S_1$;
(ii) $\varphi(\rho s) = \rho\varphi(s)$ за $\forall \rho \in R$, $\forall s \in S_1$;
(iii) $\varphi(st) = \varphi(s)\varphi(t)$ за $\forall s, t \in S_1$‘.

Определение 5.23. *Непразното подмножество S_o на R-алгебра S е R-подалгебра, ако S_o е подпръстен с единица на S и R-подмодул на S.*

Задача 5.24. *Да се докаже, че непразното подмножество S_o на R-алгебра S е R-подалгебра тогава и само тогава, когато за произволни $x, y \in S_o$ и произволно $r \in R$ са в сила $x - y, xy, rx, 1_S \in S_o$.*

Задача 5.25. *Нека S е комутативен пръстен с единица 1, а $\mathbb{Z}$ е пръстенът на целите числа. Да се докаже, че:*
(i) S е $\mathbb{Z}$-алгебра относно изображението $\mathbb{Z} \times S \to S$, $(n, s) \mapsto ns$, описано в Задача 5.8;
(ii) всеки подпръстен S_o на S е $\mathbb{Z}$-подалгебра;
(iii) всеки хомоморфизъм $\varphi : S \to S'$ на комутативни пръстени с единица е хомоморфизъм на $\mathbb{Z}$-алгебри.

Определение 5.26. *Комутативният пръстен с единица S е крайнопородена алгебра над комутативния пръстен с единица R, ако съществуват елементи $a_1, \ldots, a_n \in S$, така че*

$$S = R[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in R[x_1, \ldots, x_n]\}$$

се състои от полиномите на $a_1, \ldots, a_n$ с коефициенти от R.

Ясно е, че всяка крайнопородена алгебра $S = R[a_1, \ldots, a_n]$ над комутативен пръстен с единица R е R-алгебра, защото $R[a_1, \ldots, a_n]$ е R-модул и R е подпръстен на $R[a_1, \ldots, a_n]$, така че

$$r(f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = (rf(a_1, \ldots, a_n))g(a_1, \ldots, a_n)$$

за $r \in R$ и $f(a_1, \ldots, a_n), g(a_1, \ldots, a_n) \in R[a_1, \ldots, a_n]$ е непосредствено следствие от асоциативността на умножението в $R[a_1, \ldots, a_n]$.
Ако $A = \{a_1, \ldots, a_n\}$ е множеството на пораждащите на R-алгебрата $S = R[a_1, \ldots, a_n]$, то естественото изображение

$$\pi_A : R[x_1, \ldots, x_n] \longrightarrow R[a_1, \ldots, a_n] = S,$$
$$\pi_A(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$$

е хомоморфизъм на R-алгебри с образ $Im(\pi_A) = R[a_1, \ldots, a_n]$. За целта е достатъчно да се отбележи, че

$$\pi_A(f(x_1, \ldots, x_n)g(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)g(a_1, \ldots, a_n),$$
$$\pi_A(f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) \quad \text{и}$$
$$\pi_A(rf(x_1, \ldots, x_n)) = rf(a_1, \ldots, a_n)$$

за произволни $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$, $r \in R$. Ядрото

$$I_A := Ker(\pi_A) = \{f \in R[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0\}$$

на този хомоморфизъм се нарича идеал на тъждествата на A. Съгласно теоремата за хомоморфизмите на пръстени, индуцираното изображение

$$\overline{\pi_A} : R[x_1, \ldots, x_n]/I_A \longrightarrow R[a_1, \ldots, a_n],$$
$$\overline{\pi_A}(f + I_A) = f(a_1, \ldots, a_n)$$

е изоморфизъм на пръстени. Още повече,

$$\overline{\pi_A}(r(f+I_A)) = \overline{\pi_A}(rf+I_A) = (rf)(a_1,\ldots,a_n) = rf(a_1,\ldots,a_n) = r\overline{\pi_A}(f+I_A)$$

за $\forall r \in R$ и $\forall f \in R[x_1,\ldots,x_n]$, така че $\overline{\pi_A}$ е изоморфизъм на R-алгебри.

Лема 5.27. *Ако $\varphi : R \to S$ е хомоморфизъм на комутативни пръстени с единица и R е ньотеров пръстен, то образът $Im(\varphi) := \{\varphi(r) \,|\, r \in R\}$ на φ е ньотеров пръстен.*

Доказателство: Трябва да докажем, че произволен идеал $I \lhd Im(\varphi)$ е крайнопороден. За целта използваме, че пълният праобраз

$$\varphi^{-1}(I) := \{r \in R \,|\, \varphi(r) \in I\}$$

е идеал в R. Наистина, за $\forall a,b \in \varphi^{-1}(I)$ и $r \in R$ е в сила $a-b, ar \in \varphi^{-1}(I)$ съгласно $\varphi(a-b) = \varphi(a)-\varphi(b) \in I$ и $\varphi(ar) = \varphi(a)\varphi(r) \in I$ за $\varphi(a), \varphi(b) \in I$. Доколкото пръстенът R е ньотеров, идеалът $\varphi^{-1}(I) \lhd R$ е крайнопороден, т.е. съществуват $r_1,\ldots,r_n \in \varphi^{-1}(I)$, така че

$$\varphi^{-1}(I) = \langle r_1,\ldots,r_n\rangle = \left\{ \sum_{i=1}^{n} r_i s_i \,\middle|\, s_i \in R,\, 1 \le i \le n \right\}.$$

Твърдим, че

$$I = \langle \varphi(r_1),\ldots,\varphi(r_n)\rangle = \left\{ \sum_{i=1}^{n} \varphi(r_i)\varphi(s_i) \,\middle|\, s_i \in R,\, 1 \le i \le n \right\}$$

се поражда от $\varphi(r_1),\ldots,\varphi(r_n)$ като идеал в пръстена $Im(\varphi) = \{\varphi(s) \,|\, s \in R\}$. Наистина, всеки елемент на $I \lhd Im(\varphi)$ е от вида $\varphi(r)$ за някое $r \in R$. По определението на $\varphi^{-1}(I)$ имаме $r \in \varphi^{-1}(I)$, така че $r = \sum_{i=1}^{n} r_i s_i$ за подходящи $s_1,\ldots,s_n \in R$. Следователно $\varphi(r) = \sum_{i=1}^{n} \varphi(r_i)\varphi(s_i) \in \langle \varphi(r_i),\ldots,\varphi(r_n)\rangle$, така че идеалът $I = \langle \varphi(r_1),\ldots,\varphi(r_n)\rangle$ е крайнопороден и пръстенът $Im(\varphi)$ е ньотеров, Q.E.D.

Следствие 5.28. *Ако R е ньотеров комутативен пръстен с единица, то всяка крайнопородена R-алгебра $S = R[a_1,\ldots,a_n]$ е също ньотеров комутативен пръстен с единица.*

Доказателство: Нека $\pi_A : R[x_1,\ldots,x_n] \to S = R[a_1,\ldots,a_n]$ е естественият епиморфизъм, отговарящ на пораждащата система $a_1,\ldots,a_n$ на $S = R[a_1,\ldots,a_n]$. Съгласно Следствие 5.17, полиномиалният пръстен $R[x_1,\ldots,x_n]$ е ньотеров комутативен пръстен с единица. Прилагайки Лема 5.27 получаваме, че $Im(\pi_A) = R[a_1,\ldots,a_n] = S$ е ньотеров комутативен пръстен с единица, Q.E.D.

Задача 5.29. *Да се докаже, че ако R е комутативен пръстен с единица и пръстенът на полиномите $R[x]$ на x с коефициенти от R е ньотеров, то R е ньотеров пръстен.*

Упътване: Допуснете противното и разгледайте безкрайна строго растяща редица

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_s \subsetneq I_{s+1} \subsetneq \ldots$$

от идеали I_s в R. Ако $J_s = I_s R[x]$ са идеалите в $R[x]$, полодени от I_s, то ненамаляващата редица

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq J_s \subseteq J_{s+1} \subseteq \ldots$$

от идеали в ньотеровия пръстен $R[x]$ се стабилизира след краен брой стъпки, $J_n = J_{n+1} = \ldots$ за някое $n \in \mathbb{N}$. Произволен елемент $\beta \in I_{n+1} \setminus I_n$ принадлежи

на идеала $I_{n+1}R[x] = J_{n+1} = J_n = I_nR[x]$ в $R[x]$, така че съществуват елементи $\alpha_1, \ldots, \alpha_m \in I_n$ и и полиноми $g_1(x), \ldots, g_m(x) \in R[x]$ с $\beta = \sum_{i=1}^{m} \alpha_i g_i(x)$. В частност, $\beta = \sum_{i=1}^{m} \alpha_i g_i(0) \in I_n \lhd R$, което противоречи на избора на β и доказва ньотеровостта на R.

2. Ньотеровост на топологията на Зариски

Определение 5.30. *Топологията $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$ се нарича ньотерова, ако всяка ненамаляваща редица от отворени подмножества*

$$U_1 \subseteq U_2 \subseteq \ldots \subseteq U_n \subseteq U_{n+1} \subseteq \ldots$$

се стабилизира след краен брой стъпки, $U_m = U_{m+1} = \ldots$ за някое $m \in \mathbb{N}$.

Твърдение 5.31. *Ако $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$ е ньотерова топология върху X, то всяко отворено покритие на X има крайно подпокритие.*

Доказателство: Да допуснем противното. Тогава съществува отворено покритие $X = \cup_{\gamma \in \Gamma} U_\gamma$, от което не може да се избере крайно подпокритие. Конструираме редица $\{U_{\gamma_i}\}_{i=1}^{n}$, $\gamma_i \in \Gamma$, започвайки с произволно U_{γ_1}. На всяка стъпка твърдим, че за вече избраните $U_{\gamma_1}, \ldots, U_{\gamma_n}$ съществува

$$U_{\gamma_{n+1}} \not\subseteq U_{\gamma_1} \cup \ldots \cup U_{\gamma_n}$$

с $\gamma_{n+1} \in \Gamma$. В противен случай $\cup_{\gamma \in \Gamma} U_\gamma = \cup_{i=1}^{n} U_{\gamma_i}$. Наличието на безкрайна строго растяща редица

$$U_{\gamma_1} \subsetneq \left(\cup_{i=1}^{2} U_{\gamma_i}\right) \subsetneq \ldots \subsetneq \left(\cup_{i=1}^{n} U_{\gamma_i}\right) \subsetneq \left(\cup_{i=1}^{n+1} U_{\gamma_i}\right) \subsetneq \ldots$$

от отворени подмножества на X противоречи на ньотеровостта на $\mathcal{U}$, Q.E.D.
Съществуват топологии $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$, които не са ньотерови, на всяко отворено покритие $X = \cup_{\beta \in B} U_\beta$, индексирано с подмножество $B \subseteq A$ има крайно подпокритие $X = U_{\beta_1} \cup \ldots \cup U_{\beta_n}$. Като пример разглеждаме затвореното кълбо

$$\overline{\mathbb{B}^n(\check{o}, r)} = \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^{n} x_i^2 \leq r \right\}$$

относно метричната топология, чиито отворени подмножества са обединенията на кълба. Топологично пространство X е компактно, ако е Хаусдорфово и всяко отворено покритие има крайно подпокритие. Съгласно Теоремата на Хайне-Борел, затвореното и ограничено подмножество $\overline{\mathbb{B}^n(\check{o}, 1)} \subset \mathbb{R}^n$ на метричното пространство $\mathbb{R}^n$ е компактно топологично пространство. Наличието на безкрайна строго растяща редица

$$\mathbb{B}^n\left(\check{o}, 1 - \frac{1}{2}\right) \subset \mathbb{B}^n\left(\check{o}, 1 - \frac{1}{3}\right) \subset \ldots \subset \mathbb{B}^n\left(\check{o}, 1 - \frac{1}{k}\right) \subset \mathbb{B}^n\left(\check{o}, 1 - \frac{1}{k+1}\right) \subset \ldots$$

от отворени подмножества на $\overline{\mathbb{B}^n(\check{o}, 1)}$ доказва, че метричната топология върху $\overline{\mathbb{B}^n(\check{o}, 1)}$ не е ньотерова.

Твърдение 5.32. *Топологията на Зариски върху афинно алгебрично множество $X \subset k^n$ е ньотерова.*

Доказателство: Нека

$$U_1 \subseteq U_2 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n \subseteq \ldots$$

е ненамаляваща редица от Зариски отворени подмножества на X. Допълненията им $Z_n := X - U_n$ образуват нерастяща редица от Зариски затворени подмножества

$$Z_1 \supseteq Z_2 \supseteq \ldots \supseteq Z_n \supseteq Z_{n+1} \supseteq \ldots$$

на X. Съответните идеали

$$I(Z_1) \subseteq I(Z_2) \subseteq \ldots \subseteq I(Z_n) \subseteq I(Z_{n+1}) \subseteq \ldots$$

се нареждат в ненамаляваща редица. Съгласно Теоремата на Hilbert за базиса, Теорема 9 и Твърдение 5.2, редицата от идеали $I(Z_m) = I(Z_{m+1}) = \ldots$ се стабилизира след краен брой стъпки. Оттук и редицата от афинни многообразия $Z_m = ZI(Z_m)$ се стабилизира след краен брой стъпки, $Z_m = Z_{m+1} = \ldots$. Следователно допълненията им $U_m = U_{m+1} = \ldots$ се стабилизират и топологията на Зариски върху X е ньотерова, Q.E.D.

3. Крайно породени подалгебри на крайно породени алгебри над ньотеров пръстен

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

Твърдение 5.33. *Да разгледаме ньотеров комутативен пръстен 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 5.14,

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

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

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

е крайно породена R-алгебра, Q.E.D.

4. Алгебричност на разширенията, които са крайно породени алгебри

Лема 5.34. *Ако k е безкрайно поле, то толето*

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

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

Доказателство: Допускаме противното, т.е. че

$$k(x_1,\ldots,x_n) = k\left[\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)},\ldots,\frac{f_m(x_1,\ldots,x_n)}{g_m(x_1,\ldots,x_n)}\right]$$

е крайно породена k-алгебра. Тогава за $\forall\alpha\in k$ е в сила $\frac{1}{x_n-\alpha}\in k(x_1,\ldots,x_n)$, откъдето

$$\frac{1}{x_n-\alpha} = \frac{f_0(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)^{d_1}\ldots g_m(x_1,\ldots x_n)^{d_m}}$$

за полином $f_0(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$ и $d_1,\ldots,d_m\in\mathbb{Z}^{\ge 0}$. Оттук

$$(x_n-\alpha)f_0(x_1,\ldots,x_n) = g_1(x_1,\ldots,x_n)^{d_1}\ldots g_m(x_1,\ldots,x_n)^{d_m}$$

и съществува $1\le i=i(\alpha)\le m$, така че $g_i(x_1,\ldots,x_{n-1},\alpha)\equiv 0\in k[x_1,\ldots,x_{n-1}]$. Ако $g_i(x_1,\ldots,x_n)=\sum\limits_{j=0}^{s_i} c_{i,j}(x_1,\ldots,x_{n-1})x_n^j \in k[x_1,\ldots,x_{n-1}][x_n]=k[x_1,\ldots,x_n]$ за някакви полиноми $c_{i,j}(x_1,\ldots,x_{n-1})\in k[x_1,\ldots,x_{n-1}]$, то равенството

$$g_i(x_1,\ldots,x_{n-1},\alpha)=\sum_{j=0}^{s_i} c_{i,j}(x_1,\ldots,x_{n-1})\alpha^j\equiv 0$$

може да се запише във вида

$$\begin{pmatrix} 1 & \alpha & \ldots & \alpha^{s_i}\end{pmatrix}\begin{pmatrix} c_{i,0}(x_1,\ldots,x_{n-1})\\ c_{i,1}(x_1,\ldots,x_{n-1})\\ \ldots\\ c_{i,s_i}(x_1,\ldots,x_{n-1})\end{pmatrix}=0.$$

Елементите $\alpha\in k$ са безбройно много, а индексите $1\le i(\alpha)\le m$ са краен брой, така че след евентуална пермутация на пораждащите $\frac{f_i(x_1,\ldots,x_n)}{g_i(x_1,\ldots,x_n)}$ на $k(x_1,\ldots,x_n)$ като k-алгебра можем да считаме, че $g_1(x_1,\ldots,x_{n-1},\alpha)=0$ за

безбройно много стойности $\alpha \in k$. В частност, можем да намерим s_1+1 различни $\alpha_0, \alpha_1, \ldots, \alpha_{s_1} \in k$, така че

$$\begin{pmatrix} 1 & \alpha_0 & \ldots & \alpha_0^{s_1} \\ 1 & \alpha_1 & \ldots & \alpha_1^{s_1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha_{s_1} & \ldots & \alpha_{s_1}^{s_1} \end{pmatrix} \begin{pmatrix} c_{1,0}(x_1,\ldots,x_{n-1}) \\ c_{1,1}(x_1,\ldots,x_{n-1}) \\ \ldots \\ c_{1,s_1}(x_1,\ldots,x_{n-1}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}.$$

Матрицата на Вандермонд на различните елементи $\alpha_0, \alpha_1, \ldots, \alpha_{s_1} \in k$ е неособена и горното равенство е в сила тогава и само тогава, когато

$$c_{1,j}(x_1,\ldots,x_{n-1}) \equiv 0 \in k[x_1,\ldots,x_{n-1}] \quad \text{за} \quad \forall 0 \leq j \leq s_1.$$

В резултат, $g_1(x_1,\ldots,x_n) = \sum\limits_{j=1}^{s_1} c_{1,j}(x_1,\ldots,x_{n-1})x_n^j \equiv 0 \in k[x_1,\ldots,x_n]$, което противоречи на избора на $\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)} \in k(x_1,\ldots,x_n)$ и доказва, че $k(x_1,\ldots,x_n)$ не е крайно породена k-алгебра, Q.E.D.

Твърдение 5.35. *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, $L_o[a_{m+1},\ldots,a_n]$ е подпръстен на L, защото L_o е подполе на L, $a_{m+1},\ldots,a_n \in L$ и полето L е затворено относно умножение и събиране на свои елементи. Следователно $L = L_o[a_{m+1},\ldots,a_n]$ е крайно породена L_o-алгебра.
Алгебричните над L_o елементи $a_{m+1},\ldots,a_n$ пораждат крайно разширение $L = L_o[a_{m+1},\ldots,a_n] \supseteq L_o$.
Прилагаме Лема 5.33 към ньотеровата област с единица k, крайно породената k-алгебра $L = k[a_1,\ldots,a_n]$ и подпръстена L_o на L, съдържащ k, над който L е крайно породен L_o-модул. В резултат получаваме, че $L_o \simeq k(x_1,\ldots,x_m)$ е крайно породена k-алгебра. Това противоречи на Лема 5.34 и доказва алгебричността на $a_1,\ldots,a_n$ над k, откъдето и $[L:k] < \infty$, Q.E.D.

5. Максимални идеали в крайно породени алгебри над поле

Определение 5.36. *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 5.37. *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 5.38. *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 5.39. *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 5.40. *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 на простени

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

Q.E.D.

Твърдение 5.41. *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 5.35, 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 5.42. *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.*

6. Нил-радикал и радикал на идеал

Лема-Определение 5.43. *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 5.44. *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 5.37 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.

7. Теорема на Hilbert за нулите

ТЕОРЕМА 10. **(Теорема на Hilbert за нулите)** *Нека k е алгебрично затворено поле, I е идеал в $k[x_1, \ldots, x_n]$,*

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

е афинното алгебрично множество, определено от I, а

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

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

$$IZ(I) = r(I)$$

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

Доказателство: Включването $r(I) \subseteq IZ(I)$ 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 $(a_1, \ldots, a_n) \in Z(I)$. Поради липсата на делители на нулата в полето k, оттук следва $f(a_1, \ldots, a_n) = 0$, така че $f \in IZ(I)$.
Обратното включване $IZ(I) \subseteq r(I)$ е еквивалентно на включването

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

на съответните допълнения. Ако $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \setminus r(I)$, то съгласно Твърдение 5.44 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 $(f + \mathfrak{p})^{-1} = \frac{1+\mathfrak{p}}{f+\mathfrak{p}} \in Q_1$ и можем да разгледаме подпръстена

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

на Q_1, който е крайно породена k-алгебра.
Ако $\mathfrak{M}$ е максимален идеал в крайно породената алгебра R_2 над алгебрично затвореното поле $k \simeq k + \mathfrak{p}/\mathfrak{p}$, то фактор-пръстенът $R_2/\mathfrak{M} \simeq k$, съгласно Твърдение 5.41. Подпръстенът

$$\begin{aligned} R_1 + \mathfrak{M}/\mathfrak{M} \simeq R_1/R_1 \cap \mathfrak{M} = \\ (k + R_1 \cap \mathfrak{M}/R_1 \cap \mathfrak{M})\,[x_1 + R_1 \cap \mathfrak{M}, \ldots, x_n + R_1 \cap \mathfrak{M}] \simeq \\ k[x_1 + R_1 \cap \mathfrak{M}, \ldots, x_n + \mathfrak{M}] \end{aligned}$$

на $R_2/\mathfrak{M} \simeq k$ съдържа полето k и съвпада с него. Оттук $R_1 \cap \mathfrak{M}$ е максимален идеал в $R_1 = k[x_1, \ldots, x_n]/\mathfrak{p}$ и се представя като фактор $R_1 \cap \mathfrak{M} = \widetilde{\mathfrak{M}}/\mathfrak{p}$ на максимален идеал $\widetilde{\mathfrak{M}} \lhd k[x_1, \ldots, x_n]$, съдържащ $\mathfrak{p}$. Прилагането на Твърдение 5.41 към максималния идеал $\widetilde{\mathfrak{M}}$ на крайно породената алгебра $k[x_1, \ldots, x_n]$ над алгебрично затвореното поле k дава съществуването на $a_1, \ldots, a_n \in k$, така че

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

Твърдим, че $f \notin \widetilde{\mathfrak{M}}$. В противен случай $f + \mathfrak{p} \in \widetilde{\mathfrak{M}}/\mathfrak{p} = R_1 \cap \mathfrak{M} \subset \mathfrak{M}$, откъдето $1 + \mathfrak{p} = (f + \mathfrak{p}) \left(\frac{1+\mathfrak{p}}{f+\mathfrak{p}}\right) \in \mathfrak{M}$, защото $\frac{1+\mathfrak{p}}{f+\mathfrak{p}} \in R_2$ и $\mathfrak{M} \lhd R_2$ е идеал в R_2. Но от $1 + \mathfrak{p} \in \mathfrak{M}$ следва $\mathfrak{M} = R_2$, което е противоречие, доказващо $f \notin \widetilde{\mathfrak{M}}$.
Твърдим, че точката $a = (a_1, \ldots, a_n) \in Z(I)$ принадлежи на афинното алгебрично множество на нулите на I. Наистина, произволен полином

$$g \in I \subseteq \mathfrak{p} \subseteq \widetilde{\mathfrak{M}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

е от вида $g = \sum_{i=1}^{n} (x_i - a_i) g_i(x_1, \ldots, x_n)$ с $g_i \in k[x_1, \ldots, x_n]$ и $g(a_1, \ldots, a_n) = 0$. Ако допуснем, че $f \in IZ(I)$, то $f(a_1, \ldots, a_n) = 0$. Пръстените

$$k[x_1, \ldots, x_n] = k[x_1 - a_1, \ldots, x_n - a_n]$$

съвпадат, защото $x_i \in k[x_1 - a_1, \ldots, x_n - a_n]$ и $x_j - a_j \in k[x_1, \ldots, x_n]$ за всички $1 \leq i, j \leq n$. Това позволява изразяването на f във вида

$$f = \sum_{\alpha \in (\mathbb{Z}^{\geq 0})^n} c_\alpha (x_1 - a_1)^{\alpha_1} \ldots (x_n - a_n)^{\alpha_n}, \quad c_\alpha \in k.$$

Сега от $f(a_1, \ldots, a_n) = 0$ следва $c_{0^n} = 0$ и $f \in \langle x_1 - a_1, \ldots, x_n - a_n \rangle = \widetilde{\mathfrak{M}}$. Полученото противоречие установява, че $f \notin IZ(I)$ и доказва теоремата, Q.E.D.

Определение 5.45. *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 5.46. *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;
(ii) 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 5.47. **(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 $Z(I) = \emptyset$, 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 $\emptyset = Z(I) \supseteq Z(\mathfrak{M}) = \{(a_1, \ldots, a_n)\}$.

Следствие 5.48. *Нека k е алгебрично затворено поле. Тогава съществува взаимно еднозначно съответствие между афинните алгебрични множества $X = Z(S) \subseteq k[x_1, \ldots, x_n]$, $S \subseteq k[x_1, \ldots, x_n]$ и радикалните идеали $I(X) = IZ(S) \lhd k[x_1, \ldots, x_n]$.*

Доказателство: Всяко афинно алгебрично множество $X = Z(S) \subseteq k^n$, $S \subseteq k[x_1, \ldots, x_n]$ отговаря на радикален идеал $IZ(S) = IZ(\langle S \rangle) = r(\langle S \rangle)$. Обратно, всеки радикален идеал $I = r(I) \lhd k[x_1, \ldots, x_n]$ отговаря на афинно алгебрично множество $Z(I) \subseteq k^n$. Съответствието е взаимно еднозначно, защото съгласно Лема 4.23, $ZI(X) = X$ за всяко афинно алгебрично множество $X \subseteq k^n$. от Теорема 10 на Hilbert за нулите, $IZ(I) = r(I) = I$ за произволен радикален идеал $I = r(I) \lhd R$, Q.E.D.
Съгласно Следствие 5.48, 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 $Z(I_2) \subsetneq Z(I_2) \subseteq k^n$ също се съдържат строго. Аналогично, ако афинните алгебрични множества $Z_1 \subsetneq Z_2 \subseteq k^n$ се съдържат строго, то радикалните им идеали $I(Z_2) \subsetneq I(Z_1) \lhd k[x_1, \ldots, x_n]$ се съдържат строго.

Следствие 5.49. *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 4.23 имаме $X = ZI(X)$ и $Y = ZI(Y)$. Следователно

$$X \cap Y = ZI(X) \cap ZI(Y) = Z(I(X) + I(Y)),$$

след прилагане на Лема 4.18 (i). По Теоремата на Хилберт за нулите,

$$I(X \cap Y) = IZ(I(X) + I(Y)) = r(I(X) + I(Y)), Q.E.D.$$