Глава 2

Теорема на Hilbert за базиса. Еднозначно разлагане на полиноми.

1. Ньотерови пръстени

Определение 2.1. *Комутативният пръстен с единица R е ньотеров, ако всеки идеал I в R е крайно породен, $I = \langle x_1, \ldots, x_k \rangle$ за някои $x_1, \ldots, x_k \in R$.*

Твърдение 2.2. *Комутативният пръстен с единица R е ньотеров тогава и само тогава, когато всяка ненамаляваща редица от идеали*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots \tag{2.1}$$

се стабилизира след краен брой стъпки.
В частност, ако R е ньотеров пръстен, то всяко пораждащо подмножество S на идеал $\langle S \rangle \triangleleft R$ 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 (2.1) 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 $a - b \in I_n \triangleleft R$. 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 (2.1) се стабилизира след краен брой стъпки.
Ще докажем, че ако всяка ненамаляваща редица от идеали 2.1 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. Това противоречи на предположението за стабилизация на ненамаляващите редици от идеали и доказва твърдението, Q.E.D.

Определение 2.3. *Идеалът I в комутативен пръстен с единица R е главен, ако се състои от кратните на някакъв свой елемент,*

$$I = \langle \alpha \rangle := \{\alpha r \mid r \in R\} \quad \text{за някое} \quad \alpha \in R.$$

Комутативна област с единица R е област на глевни идеали, ако всеки идеал I в R е главен, $I = \langle \alpha \rangle$ за някое $\alpha \in I$.

Областите на главни идеали са частни случаи на ньотерови комутативни области. Следващата задача илюстрира съществуването на пораждаща система S на главен идеал $I = \langle \alpha \rangle$ с $\langle s \rangle \subsetneq I$ за всяко $s \in S$.

Задача 2.4. *Нека S е множеството на естествените числа от вида $2p$, където p пробягва нечетните прости числа, а I е идеалът в $\mathbb{Z}$, породен от S. Да се докаже, че:*
(i) идеалът I е главен и да се намери пораждащ на I;
(ii) не съществува елемент на S, пораждащ I;
(iii) всеки два различни елемента на S пораждат I.

2. Модули над комутативен пръстен с единица

Модул M над комутативен пръстен с единица R е линейно пространство над R. По-точно:

Определение 2.5. *Непразното множество M е модул над комутативния пръстен 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

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

изпълняващи 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 2.5.
Всеки комутативен пръстен с единица R е модул над себе си.

Определение 2.6. *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 2.7. *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*

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

Определение 2.8. *Непразното подмножество N на модул M над комутативен пръстен 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 2.9. *Нека R е комутативен пръстен 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 2.10. *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 2.11. *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 2.12. (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

$$\overline{\varphi} : M/\ker\varphi \longrightarrow \mathrm{im}\varphi,$$
$$\overline{\varphi}(m + \ker\varphi) = \varphi(m) \quad \textit{за} \quad \forall m + \ker\varphi \in M/\ker\varphi$$

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 2.13. *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

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

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 2.14. *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 2.15. *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 2.16. *Ако R е нъотеров 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 нъотеров, 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

$$N = R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m \tag{2.2}$$

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 (2.2), Q.E.D.

Задача 2.17. *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.

3. Алгебри над комутативен пръстен с единица. Цяла зависимост.

Определение 2.18. *Ако R и S са комутативни пръстени с единица, S е R-модул и*

$$r(s_1s_2) = (rs_1)s_2 \quad за \quad \forall s_1, s_2 \in S, \quad \forall r \in R,$$

то казваме, че S е R-алгебра.

Пример 2.19. *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 2.20. *Хомоморфизъм $\varphi : S_1 \to S_2$ на R-алгебри е хомоморфизъм на пръстени, който е и хомоморфизъм на R-модули.*

Задача 2.21. *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 2.22. *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 2.23. *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 2.24. *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 2.10;
(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 2.25. *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*

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

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

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

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

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.
В частния случай, когато $S = R[a_1, \ldots, a_n]$ е крайно породена R-алгебра над комутативен подпръстен R на S с единица, ще дадем необходими и достатъчни условия за крайната породеност на S като R-модул.

Определение 2.26. *Нека R е подпръстен с единица на комутативния пръстен с единица S. Елементът $s \in S$ е цял над R, ако изпълнява полиномиално съотношение*

$$s^n + r_{n-1}s^{n-1} + \ldots + r_1 s + r_0 = 0$$

с коефициенти $r_i \in R$ и старши коефициент $1 = 1_R = 1_S$.

Твърдение 2.27. *Нека R е подпръстен с единица на комутативен пръстен с единица S, а s е елемент на S. Тогава следните условия са еквивалентни:*
(i) s е цял над R;
(ii) подпръстенът $R[s]$ на S е крайно породен R-модул;
(iii) подпръстенът $R[s]$ на S се съдържа в подпръстен с единица S_o на S, който е крайно породен R-модул $S_o = Rs_1 + \ldots + Rs_n$.

Доказателство: $(i) \Rightarrow (ii)$ Ако s е цял над R, то

$$s^n = \sum_{i=0}^{n-1}(-r_i)s^i \in R1_S + Rs + \ldots Rs^{n-1} = R^{(n)}[s]$$

принадлежи на R-модула $R^{(n)}[s]$ на полиномите на s от степен $\leq n-1$ с коефициенти от R. С индукция по $m \geq n$, ако $s^m = \sum\limits_{j=0}^{n-1} \rho_{m,j}s^j \in R^{(n)}[s]$, то

$$s^{m+1} = \sum_{j=0}^{n-2} \rho_{m,j}s^{j+1} + \rho_{m,n-1}s^n = \sum_{i=1}^{n-1} \rho_{m,i-1}s^i + \rho_{m,n-1}\left[\sum_{i=0}^{n-1}(-r_i)s^i\right] =$$

$$= -\rho_{m,n-1}r_0 + \sum_{i=1}^{n-1}(\rho_{m,i-1} - \rho_{m,n-1}r_i)s^i \in R^{(n)}[s],$$

така че $R[s] = \sum\limits_{j=0}^{\infty} Rs^j \subseteq R^{(n)}[s] = R1_S + Rs + \ldots + Rs^{n-1} \subseteq R[s]$ и $R[s] = R^{(n)}[s]$ е крайно породен R-модул.
Импликацията $(ii) \Rightarrow (iii)$ е тривиална с $S_o := R[s]$.
$(iii) \Rightarrow (i)$ Нека S_o е подпръстен с единица на S, съдържащ $R[s]$, който е крайно породен R-модул, $S_o = Rs_1 + \ldots + Rs_n$. Тогава умножението с s е изображение $\mu_s : S_o \to S_o$, $\mu_s(\sigma) = s\sigma$ на S_o в себе си. Още повече, μ_s е хомоморфизъм на R-модули, защото

$$\mu_s(\sigma + \tau) = s(\sigma + \tau) = s\sigma + s\tau = \mu_s(\sigma) + \mu_s(\tau) \quad \text{и}$$

$$\mu_s(r\sigma) = s(r\sigma) = (sr)\sigma = (rs)\sigma = r(s\sigma) = r\mu_s(\sigma) \quad \text{за} \quad \forall \sigma, \tau \in S_o, \quad \forall r \in R.$$

За $\forall 1 \leq i \leq n$ съществуват $r_{i,j} \in R$, така че $S_o \ni \mu_s(s_i) = \sum\limits_{j=1}^{m} r_{i,j}s_j$. Образуваме $m \times m$-матрицата $\mu_s E_m$ и $m \times m$-матрицата $M_o = (r_{i,j})_{i,j=1}^{m}$. Забелязваме, че

$$(\mu_s E_m - M_o)\begin{pmatrix} s_1 \\ \dots \\ s_i \\ \dots \\ s_m \end{pmatrix} = \begin{pmatrix} \mu_s(s_1) - \sum\limits_{j=1}^{m} r_{1,j}s_j \\ \dots \\ \mu_s(s_i) - \sum\limits_{j=1}^{m} r_{i,j}s_j \\ \dots \\ \mu_s(s_m) - \sum\limits_{j=1}^{m} r_{m,j}s_j \end{pmatrix} = \begin{pmatrix} 0 \\ \dots \\ 0 \\ \dots \\ 0 \end{pmatrix}.$$

Нека $(\mu_s E_m - M_o)^*$ е $m \times m$-матрицата, която в i-ти ред и j-ти стълб съдържа адюнгираното количество на (j,i)-тия елемент на $\mu_s E_m - M_o$. Тогава произведението $(\mu_s E_m - M_o)^*(\mu_s E_m - M_o) = \det(\mu_s E_m - M_o)E_m$ е скаларна матрица и

$$\begin{pmatrix} \det(\mu_s E_m - M_o)s_1 \\ \dots \\ \det(\mu_s E_m - M_o)s_i \\ \dots \\ \det(\mu_s E_m - M_o)s_m \end{pmatrix} = (\mu_s E_m - M_o)^*(\mu_s E_m - M_o)\begin{pmatrix} s_1 \\ \dots \\ s_i \\ \dots \\ s_m \end{pmatrix} =$$

$$= (\mu_s E_m - M_o)^*\begin{pmatrix} 0 \\ \dots \\ 0 \\ \dots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \dots \\ 0 \\ \dots \\ 0 \end{pmatrix}.$$

Полиномът

$$\det(\mu_s E_m - M_o) = \mu_s^m - \left(\sum_{i=1}^{m} r_{i,i}\right)\mu_s^{m-1} + c_2\mu_s^{m-2} + \ldots + c_{m-1}\mu_s + (-1)^m \det(M_o) \tag{2.3}$$

на μ_s с коефициенти $c_i \in R$ е хомоморфизъм $\det(\mu_s E_m - M_o) : S_o \to S_o$ на R-модули, действащ по правилото

$$\det(\mu_s E_m - M_o)(\sigma) = \left(\sum_{i=0}^{m} c_i \mu_s^{m-i}\right)(\sigma) = \sum_{i=0}^{m} c_i s^{m-i}\sigma$$

върху $\forall \sigma \in S_o$. Да отбележим, че $\det(\mu_s E_m - M_o)$ се анулира тъждествено върху S_o, защото се анулира върху всеки от пораждащите $s_1, \ldots, s_m$ на S_o като R-модул. В частност, стайността на $\det(\mu_s E_m - M_o)$ върху единицата $1_S = 1_R$ е

$$s^m - \left(\sum_{i=1}^{m} r_{i,i}\right)s^{m-1} + c_2 s^{m-2} + \ldots + c_{m-1}s + (-1)^m \det(M_o) = 0.$$

По определение, това означава, че $s \in S$ е цял над R, Q.E.D.

Следствие 2.28. *Нека R е комутативен подпръстен с единица на комутативен пръстен с единица S, а $s_1, \ldots, s_n \in S$ са елементи на S. В такъв случай, крайно породената R-алгебра $R[s_1, \ldots, s_n]$ е крайно породен R-модул тогава и само тогава, когато $s_1, \ldots, s_n$ са цели над R.*

Доказателство: Ако R е комутативен подпръстен с единица на комутативен пръстен с единица S, то S е R-алгебра. Да предположим, че крайно породената R-алгебра $R[s_1, \ldots, s_n]$ е крайно породен R-модул. Тогава съгласно Твърдение

2.27, всяко s_i е цяло над R, защото подпръстенът $R[s_i]$ на S се съдържа в подпръстена с единица $R[s_1, \ldots, s_n] \subseteq S$, който е крайно породен R-модул.
Ако $s_1, \ldots, s_n$ са цели над R, то с индукция по $1 \leq i \leq n$ ще докажем, че $A_i = R[s_1, \ldots, s_i]$ е крайно породен R-модул. По Твърдение 2.27, $A_1 = R[s_1]$ е крайно породен R-модул. Да допуснем, че $A_{i-1} := R[s_1, \ldots, s_{i-1}]$ е крайно породен R-модул. Тогава съществуват полиноми $f_j(s_1, \ldots, s_{i-1}) \in R[s_1, \ldots, s_{i-1}] = A_{i-1}$, така че $A_{i-1} = \sum_{j=1}^{m} Rf_j$. Разглеждаме $A_i := R[s_1, \ldots, s_{i-1}, s_i] = R[s_1, \ldots, s_{i-1}][s_i] = A_{i-1}[s_i]$ като A_{i-1}-алгебра. Понеже R е подпръстен на A_{i-1}, елементът $s_i \in S$ е цял над A_{i-1}. Съгласно Твърдение 2.27, пърстенът $A_i = A_{i-1}[s_i]$ е крайно породен A_{i-1}-модул. С други думи, съществуват полиноми $g_s(s_1, \ldots, s_i) \in A_{i-1}[s_i] = R[s_1, \ldots, s_i]$, така че

$$A_i = \sum_{s=1}^{p} A_{i-1}g_s = \sum_{s=1}^{p} \left(\sum_{j=1}^{m} Rf_j \right) g_s = \sum_{s=1}^{p} \sum_{j=1}^{m} R(f_j g_s)$$

се поражда като R-модул от pm полиноми $f_j g_s$, $1 \leq j \leq m$, $1 \leq s \leq p$. В частност, $A_n = R[s_1, \ldots, s_n]$ е крайно породен R-модул, Q.E.D.

Следствие 2.29. *Нека R е комутативен подпръстен с единица на комутативен пръстен с единица S. Тогава множеството $\mathcal{O}_S$ на целите над R елементи на S е подпръстен на S, съдържащ R.*

Доказателство: Ако $s, t \in S$ са цели над R, то подпръстенът $R[s, t]$ на S е крайно породен R-модул по Следствие 2.28. Тогава съглесно Твърдение 2.27, елементите $s - t, st \in R[s, t]$ са цели над R, така че $\mathcal{O}_S$ е подпръстен на S.
Всеки елемент $r \in R$ е цял над R като корен на полинома $x - r \in R[x]$ със старши коефициент 1, Q.E.D.

4. Теорема на Hilbert за базиса

Да напомним, че пръстенът на полиномите $k[x_1, \ldots, x_n]$ с коефициенти от поле k няма делители на нулата. По-точно:

Определение 2.30. *Ненулевият елечент a на пръстен R е делител на нулата, ако съществува $b \in R \setminus \{0\}$ с $ab = 0$.*

Определение 2.31. *Пръстенът R се нарича област или област на цялост, ако няма делители на нулата.*

Лема 2.32. *Ако R е комутативна област с единица, то пръстенът $R[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от R е комутативна област с единица.*
В частност, за произволно поле k пръстенът $k[x_1, \ldots, x_n]$ е комутативна област с единица.

Доказателство: Преди всичко, ако R е комутативен пръстен с единица, то пръстенът $R[x]$ на полиномите на една променливя x с коефициенти от R е комутативна област с единица. Наистина, ако $f(x) = \sum_{i=0}^{n} a_i x^i$ с $a_n \neq 0$ и $g(x) = \sum_{j=0}^{m} b_j x^j$ с $b_m \neq 0$ са нетъждествено нулеви полиноми с коефициенти от R, то коефициентът на x^{n+m} в произведението

$$f(x)g(x) = \sum_{i=0}^{n+m} \left(\sum_{s=0}^{i} a_s b_{i-s} \right) x^i$$

е равен на $a_n b_m \neq 0$, защото пръстенът R няма делители на нулата.
С индукция по броя на променливите n, ако $R[x_1, \ldots, x_{n-1}$ е комутативна област с единица, то $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ е комутативна област с единица.
Всяко поле k е комутативна област с единица, така че $k[x_1, \ldots, x_n]$ е комутативна област с единица, Q.E.D.

Твърдение 2.33. *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 $I \triangleleft R[x]$, 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 $f_1, \ldots, f_j, \ldots$.
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 2.2, 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 $LC(f_{m+1}) = \sum_{i=1}^{m} LC(f_i) r_i$ за някои $r_i \in R$.
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. 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, $f_{m+1} = f'_{m+1} + \sum_{i=1}^{m} x^{\deg(f_{m+1}) - \deg(f_i)} f_i r_i \in \langle f_1, \ldots, f_m \rangle$, което противоречи на избора на f_{m+1} и доказва нътеровостта на $R[x]$, Q.E.D.
Като непосредствено следствие от Твърдение 2.33 получаваме следното

Следствие 2.34. *Ако R е нътеров 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 нътеров комутативен пръстен с единица.*

Доказателство: С индукция по брой на променливите n, ако $R[x_1, \ldots, x_{n-1}]$ е нътеров комутативен пръстен с единица, то $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ е нътеров комутативен пръстен с единица, Q.E.D.
Комбинирайки Лема 2.32 и Следствие 2.34 получаваме следната

Теорема 1. **(Теорема на Hilbert за базиса)** *Пръстенът на полиномите $k[x_1, \ldots, x_n]$ на няколко променливи с коефициенти от поле k е нътерова комутативна област с единица.*

Следствие 2.35. *Всяко афинно алгебрично множество $V \subset k^n$ е множество на нулите $V = V(f_1, \ldots, f_m)$ 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 $V = V(S) \subseteq \overline{k}^n$ е афинното алгебрично множество на нулите на S. По Лема 1.12 (iii), $V = V(\langle S \rangle)$ съвпада с множеството на нулите на идеала $\langle S \rangle \lhd \overline{k}[x_1, \ldots, x_n]$, породен от S. Съгласно Теорема 1 и Твърдение 2.2, съществува крайна пораждаща система $\{f_1, \ldots f_m\} \subseteq S$ на идеала $\langle S \rangle$, така че $V(\langle S \rangle) = V(\langle f_1, \ldots, f_m \rangle) = V(f_1, \ldots, f_m)$, Q.E.D.

Лема 2.36. *Ако $\varphi : R \to S$ е хомоморфизъм на комутативни пръстени с единица и R е нътеров пръстен, то образът $Im(\varphi) := \{\varphi(r) \,|\, r \in R\}$ на φ е нътеров 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 нътеров, идеалът $\varphi^{-1}(I) \lhd R$ е крайнопороден, т.е. съществуват $r_1, \ldots, r_n \in \varphi^{-1}(I)$, така че

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

Твърдим, че

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

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 нътеров, Q.E.D.

Следствие 2.37. *Ако R е нътеров комутативен пръстен с единица, то всяка крайнопородена R-алгебра $S = R[a_1, \ldots, a_n]$ е също нътеров 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 2.34, полиномиалният пръстен $R[x_1, \ldots, x_n]$ е нътеров комутативен пръстен с единица. Прилагайки Лема 2.36 получаваме, че $Im(\pi_A) = R[a_1, \ldots, a_n] = S$ е нътеров комутативен пръстен с единица, Q.E.D.

Задача 2.38. *Да се докаже, че ако R е комутативен пръстен с единица и пръстенът на полиномите $R[x]$ на x с коефициенти от R е нътеров, то R е нътеров 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.

5. Ньотеровост на топологията на Зариски

Определение 2.39. *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 2.40. *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 $X = U_{\beta_1} \cup \ldots \cup_{\beta_n}$. 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

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

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 2.41. *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 нарастяща 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 1 и Твърдение 2.2, редицата от идеали $I(Z_m) = I(Z_{m+1}) = \ldots$ се стабилизира след краен брой стъпки. Оттук и редицата от афинни многообразия $Z_m = VI(Z_m)$ 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.

6. Факториалност на ньотерови области

Ненулевият елемент a на комутативен пръстен с единица R дели елемента $b \in R$, ако съществува $c \in R$, така че $b = ac$.

Определение 2.42. *Ненулевият елемент r на комутативен пръстен с единица R се нарича неразложим, ако $r \notin R^*$ не е обратим и във всяко разлагане $r = st$ в произведение на $s, t \in R$ поне единият от множителите s или t е обратим в R.*

Определение 2.43. *Комутативният пръстен с единица R се нарича факториален, ако $\forall r \in R \setminus (R^* \cup \{0\})$ има единствено с точност до множители от R^* разлагане $r = r_1 \ldots r_k$ в крайно произведение на неразложими r_i.*

Лема 2.44. (Достатъчни условия за факториалност)
(i) В ньотерова комутативна област R с единица, всеки ненулев елемент $r \in R \setminus (R^* \cup \{0\})$ има необезателно единствено с точност до множители от R^* разлагане в крайно произведение $r = r_1 \ldots r_k$ на неразложими $r_i \in R$.
(ii) Ньотеровата област R е факториална тогава и само тогава, когато всеки неразложим $s \in R$ поражда прост идеал $\langle s \rangle = sR \lhd R$.

Доказателство: (i) Да допуснем противното. Ако $r \in R$ е необратим елемент без крайно разлагане в произведение от неразложими, то $r = r_1$ не е неразложим и съществува разлагане $r_1 = r_2 r_2'$ в произведение на $r_2, r_2' \in R \setminus R^*$. Поне единият от множителите, например r_2, не се разлага в крайно произведение от неразложими. Продължавайки по същия начин получаваме безкрайна редица $\{r_n\}_{n=1}^{\infty}$ от необратими елементи, които не се разлагат в крайно произведение от неразложими и r_{n+1} дели r_n за $\forall n \in \mathbb{N}$. Съответните главни идеали $r_n R$ образуват безкрайна ненамаляваща редица

$$r_1 R \subseteq r_2 R \subseteq \ldots \subseteq r_n R \subseteq r_{n+1} R \subseteq \ldots.$$

Твърдим, че тази редица е строго растяща. Наистина, от равенството $r_n R = r_{n+1} R$ следва $r_{n+1} = r_n s$ за някое $s \in R$. Заместваики в $r_n = r_{n+1} r_{n+1}'$ получаваме, че $r_n - r_n s r_{n+1}' = r_n(1 - s r_{n+1}') = 0$. Доколкото R е област и $r_n \neq 0$, последното е равносилно на $1 = s r_{n+1}'$. Това означава, че $r_{n+1}' \in R^*$, противно на избора на $r_{n+1}' \in R \setminus R^*$. Наличието на безкрайна строго растяща редица от идеали

$$r_1 R \subsetneq r_2 R \subsetneq \ldots \subsetneq r_n R \subsetneq r_{n+1} R \subsetneq \ldots$$

противоречи на ньотеровостта на R и доказва съществуването на крайно разлагане на всяко $r \in R$ в произведение от неразложими.
(ii) Нека ньотеровата област R е факториална, $s \in R$ е неразложим елемент, а $uv \in sR$. Тогава съществува $r \in R$, така че $uv = sr$ и s (с точност до множител

от R^*) участва в разлагането на u или v. Ако $u = st$, то $u \in sR$ и идеалът sR е прост.
Нека всеки неразложим в R елемент поражда прост идеал и

$$r = r_1 r_2 \dots r_m = s_1 s_2 \dots s_n \quad \text{за } m \geq n$$

са две крайни разлагания на $r \in R \setminus R^*$ в произведение на неразложими r_i, s_j. От $r_1 \dots r_m \in s_1 R$ и простотата на $s_1 R \lhd R$ следва, че след евентуално преномериране $r_1 \in s_1 R$. Ако $r_1 = s_1 t_1$ за $t_1 \in R$, неразложимостта на r_1 и $s_1 \notin R^*$ изискват $t_1 \in R^*$. Следователно

$$r_1 r_2 \dots r_m - s_1 s_2 \dots s_n = s_1(t_1 r_2 \dots r_m - s_2 \dots s_n) = 0,$$

където неразложимият елемент $s_1 \neq 0$. Следователно $(t_1 r_2) \dots r_m = s_2 \dots s_n$. Продължаваме по същия начин докато получим съвпадение на r_i и s_i с точност до обратим елемент на R и $m = n$, Q.E.D.

7. Области на главни идеали

Твърдение 2.45. *Всяка комутативна област от главни идеали с единица R е факториална нътерова област.*

Доказателство: Всяка комутативна област на главни идеали с единица R е нътерова комутативна област с единица. Съгласно Лема 2.44(ii), достатъчно е да проверим, че произволен неразложим елемент $s \in R$ поражда прост идеал $\langle s \rangle$, за да твърдим, че областта R е факториална. Да предположим, че $ab \in \langle s \rangle$ за $a, b \in R$ и $a \notin \langle s \rangle$. Тогава идеалът $\langle s \rangle$ се съдържа строго в идеала $\langle s, a \rangle$. Нека $t \in R$ е пораждащ на $\langle s, a \rangle$. Тогава $s \in \langle s, a \rangle = \langle t \rangle$ се представя във вида $s = tr$ за някое $r \in R$. Съгласно неразложимостта на s имаме $r \in R^*$ или $t \in R^*$. Ако $r \in R^*$, то $t = sR^{-1} \in \langle s \rangle$, откъдето $\langle s, a \rangle = \langle t \rangle \subseteq \langle s \rangle \subsetneq \langle s, a \rangle$, което е невъзможно. Следователно $t \in R^*$ и $\langle s, a \rangle = R$. За единицата $1 \in R = \langle s, a \rangle$ на пръстена R съществуват $u, v \in R$, така че $1 = su + av$ (тъждество на Bezout). В резултат, $b = sub + abv \in \langle s \rangle$, защото $ab \in \langle s \rangle$. Това доказва простотата на идеал $\langle s \rangle$, Q.E.D.

Лема 2.46. *Пръстенът $k[x]$ на полиномите на една променлива x с коефициенти от поле k е област на главни идеали.*

Доказателство: Ако $I = \{0\}$ е нулевият идеал в $k[x]$, то $I = \langle 0 \rangle$ е главен. За произволен ненулев идеал $0 \neq I \lhd k[x]$ твърдим, че всеки ненулев полином $f(x) \in I \setminus \{0\}$ от минимална степен $\deg(f) \geq 0$ поражда I. Включването $\langle f \rangle \subseteq I$ следва от затвореността на I относно умножение с елементи на $k[x]$. За обратното включване $I \subseteq \langle f \rangle$ делим произволен полином $g(x) \in I$ на $f(x)$ с частно $q(x) \in k[x]$ и остатък $r(x) \in k[x]$, така че $g(x) = f(x)q(x) + r(x)$ и $\deg(r) < \deg(f)$. Полиномът $r(x) = g(x) - f(x)q(x) \in I$, защото $g, f \in I$. Допускането $r(x) \not\equiv 0$ води до противоречие с избора на $f(x) \in I \setminus \{0\}$ от минимална степен, така че $r(x) \equiv 0$ и $g(x) = f(x)q(x) \in \langle f \rangle$. Оттук $I \subseteq \langle f \rangle$ и $I = \langle f \rangle$, Q.E.D.

Задача 2.47. *Нека k е поле, а $S = k[a]$ е 1-породена k-алгебра. Да се докаже, че всеки идеал в S е главен.*

Ще докажем, че пръстенът $k[x_1, \dots, x_n]$ на полиномите на няколко променливи с коефициенти от поле k е факториална комутативна нътерова област с единица. За $n \geq 2$ пръстенът $k[x_1, \dots, x_n]$ не е област на главни идеали. За да докажем този факт ще използваме следната

Лема 2.48. *Ако $f(x_1,\ldots,x_n)\in R[x_1,\ldots,x_n]$ е хомогенен полином от степен $d\in\mathbb{N}$ с коефициенти от комутативна област с единица R, то във всяко разлагане*

$$f(x_1,\ldots,x_n)=g(x_1,\ldots,x_n)h(x_1,\ldots,x_n)$$

в произведение на полиноми $g(x_1,\ldots,x_n),h(x_1,\ldots,x_n)\in R[x_1,\ldots,x_n]$, множителите $g(x_1,\ldots,x_n)$ и $h(x_1,\ldots,x_n)$ са хомогенни.

Доказателство: Да допуснем, че поне един от множителите, например, g се разлага в сума $g=g^{(k_1)}+\ldots+g^{(k_s)}$ от $s\geq 2$ хомогенни компоненти $g^{(k_i)}\not\equiv 0$ от степен k_i. Без ограничение на общността, $k_1>\ldots>k_s$. Нека $h=h^{(m_1)}+\ldots+h^{(m_t)}$ е разлагането на h в сума на $t\geq 1$ хомогенни компоненти $h^{(m_j)}\not\equiv 0$ от степен m_j и $m_1>\ldots>m_t$. Произведението

$$f=gh=(g^{(k_1)}+\ldots+g^{(k_s)})(h^{(m_1)}+\ldots+h^{(m_t)})$$

има хомогенна компонента $g^{(k_1)}h^{(m_1)}$ от максимална степен k_1+m_1 и хомогенна компонента $g^{(k_s)}h^{(m_t)}$ от минимална степен k_s+m_t. Пръстенът $R[x_1,\ldots,x_n]$ на полиномите на $x_1,\ldots,x_n$ с коефициенти от комутативна област с единица R е комутативна област с единица, съгласно Лема 2.32. Следователно произведенията $g^{(k_1)}h^{(m_1)}$ и $g^{(k_s)}h^{(m_t)}$ на нетъждествено нулеви хомогенни полиноми са нетъждествено нулеви хомогенни полиноми. По предположение, $s\geq 2$, откъдето $k_1<k_s$. От друга страна, $m_1\geq m_t$ с равенство точно когато $t=1$. Следователно $k_1+m_1>k_s+m_t$ и полиномът $f=gh$ има поне две ненулеви хомогенни компоненти. Това противоречи на хомогенността на f и доказва хомогенността на $g(x_1,\ldots,x_n)$ и $h(x_1,\ldots,x_n)$, Q.E.D.

Лема 2.49. *Пръстенът $k[x_1,\ldots,x_n]$ на полиномите на $n\geq 2$ променливи с коефициенти от поле k не е област на главни идеали.*

Доказателство: Да допуснем, че $k[x_1,\ldots,x_n]$ е област на главни идеали. Тогава съществува полином $f(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$, който поражда идеала $\mathfrak{M}=\langle x_1,\ldots,x_n\rangle$ на полиномите с нулев свободен член. От $x_i\in\langle f\rangle=\mathfrak{M}$ за $\forall 1\leq i\leq n$ следва съществуването на полиноми $g_i(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$, така че

$$x_i=f(x_1,\ldots,x_n)g_i(x_1,\ldots,x_n). \tag{2.4}$$

Полиномите x_i са хомогенни от степен 1. Съгласно Лема 2.48, множителите им $f(x_1,\ldots,x_n)$ и $g_i(x_1,\ldots,x_n)$ са хомогенни и $\deg(g_i)=1-\deg(f)$ за $\forall 1\leq i\leq n$. От (2.4) е ясно, че $f(x_1,\ldots,x_n)\not\equiv 0$ и $g_i(x_1,\ldots,x_n)\not\equiv 0$ за $\forall 1\leq i\leq n$. Следователно $f,g_1,\ldots,g_n$ имат неотрицателни общи степени и $f(x_1,\ldots,x_n)$ е хомогенен полином от обща степен 0 или 1.

Ако $\deg(f)=0$ и $f\in k^*$, то идеалът $\mathfrak{M}=\langle f\rangle=k[x_1,\ldots,x_n]$ съвпада с целия полиномиален пръстен. Но афинното алгебрично множество

$$V(\mathfrak{M})=V(x_1,\ldots,x_n)=\{(0,\ldots,0)\}$$

се състои от една точка, докато $V(k[x_1,\ldots,x_n])=\emptyset$ е празното афинно алгебрично множество. Това изключва случая $\deg(f)=0$.

Ако $\deg(f)=1$, то $f(x_1,\ldots,x_n)=\sum\limits_{i=1}^{n}c_ix_i\in k[x_1,\ldots,x_n]$ с поне едно $c_i\neq 0$. От равенството $\mathfrak{M}=\langle f\rangle$ на идеали следва равенството

$$\{(0,\ldots,0)\}=V(\mathfrak{M})=V(\langle f\rangle)=V(f)\subset k^n$$

на съответните афинни алгебрични множества. Но за $n\geq 2$, хиперповърхнината $V(f)$ през началото е линейно пространство над k с размерност $n-1\geq 1$, докато $V(\mathfrak{M})=\{(0,\ldots,0)\}$ е точка. Противоречието доказва, че идеалът $\mathfrak{M}=\langle x_1,\ldots,x_n\rangle\lhd k[x_1,\ldots,x_n]$ не е главен и пръстенът $k[x_1,\ldots,x_n]$ не е област на главни идеали, Q.E.D.

8. Най-голям общ делител. Примитивни полиноми с факториални коефициенти

ОПРЕДЕЛЕНИЕ 2.50. *Ако $a_0, \ldots, a_n$ са неедновременно нулеви елементи от комутативна област с единица R, то най-големият общ делител $d(a_0, \ldots, a_n)$ е такъв общ делител на $a_0, \ldots, a_n$, който се дели на всеки общ делител δ на $a_0, \ldots, a_n$.*
В случая $d(a_0, a_1, \ldots, a_n) \in R^*$ казваме, че $a_0, a_1, \ldots, a_n$ са взаимно прости.

Ако съществува, най-големият общ делител $d(a_0, \ldots, a_n)$ е единствен с точност до множител от R^*. По-точно, ако d и d' са най-големи общи делители на $a_0, \ldots, a_n$, то $d' = dr_1$ за някое $r_1 \in R$, защото d е общ делител, а d' е най-голям общ делител на $a_0, \ldots, a_n$. Аналогично, $d = d'r_2$ за някое $r_2 \in R$, откъдето $d = dr_1r_2$. Съществуването на $a_i \neq 0$ гарантира $d \neq 0$. Сега от $d(r_1r_2 - 1) = 0$ с $d \neq 0$ в областта R следва, че $r_1r_2 = 1$ или $r_1, r_2 \in R^*$.

ЛЕМА 2.51. *Ако R е факториална нътерова комутативна област с единица, то за произволни неедновременно нулеви $a_0, \ldots, a_n \in R$ съществуав най-голям общ делител $d(a_0, \ldots, a_n) \in R$.*

Доказателство: Нека $b_1, \ldots, b_k$ са различните ненулеви елементи на множеството $\{a_0, \ldots, a_n\}$. Тогава $d(a_0, \ldots, a_n) = d(b_1, \ldots, b_k)$. Ако съществува $b_j \in R^*$, то $d(b_1, \ldots, b_k) = 1$ и $a_0, \ldots, a_n$ са взаимно прости.
Нека $b_1, \ldots, b_k \in R \setminus (R^* \cup \{0\})$. Ще казваме, че елементите r_1, r_2 на комутативен пръстен с единица R са асоцирани, ако съществува $u \in R^*$, така че $r_2 = r_1u$. Всяко b_i има разлагане в произведение на краен брой неразложими множители. Означаваме с $\{p_1, \ldots, p_m\}$ обединението на неасоциираните помежду си неразложимите делители на $b_1, \ldots, b_k$ и представяме $b_i = \prod_{j=1}^{m} p_j^{s_{ij}}$ за някои цели $s_{ij} \geq 0$, $1 \leq i \leq k$. Твърдим, че

$$d := \prod_{j=1}^{m} p_j^{\min(s_{1j}, s_{2j}, \ldots, s_{kj})}$$

е най-голям общ делител на $b_1, \ldots, b_k$. Преди всичко, d дели всяко b_i, защото

$$\frac{b_i}{d} = \prod_{j=1}^{m} p_j^{s_{ij} - \min(s_{1j}, \ldots, s_{kj})} \in R$$

като произведение на неотрицателни степени на $p_j \in R$.
Ако δ е общ делител на $b_1, \ldots, b_k$, то неразложимите делители на δ са неразложими делители на b_i за всяко $1 \leq i \leq k$. В частност, неразложимите делители на δ принадлежат на множеството $\{p_1, \ldots, p_k\}$ и можем да представим $\delta = \prod_{j=1}^{m} p_j^{n_j}$ за някои цели $n_j \geq 0$. Твърдим, че от

$$\frac{b_i}{\delta} = \prod_{j=1}^{m} p_j^{s_{ij} - n_j} \in R$$

следва $s_{ij} \geq n_j$ за $\forall 1 \leq j \leq m$. Да допуснем съществуването на $1 \leq j_o \leq m$ с $s_{ij_o} < n_{j_o}$ и да означим с $p_1, \ldots, p_l$, $l \in \mathbb{N}$ онези елементи на $\{p_1, \ldots, p_m\}$, за които $s_{ij} < n_j$, $\forall 1 \leq j \leq l$. Тогава

$$r = \frac{b_i}{\delta} = \frac{\prod_{j=l+1}^{m} p_j^{s_{ij} - n_j}}{\prod_{j=1}^{l} p_j^{n_j - s_{ij}}} = \frac{\lambda}{\mu} \in R$$

с $\lambda := \prod_{j=l+1}^{m} p_j^{s_{ij}-n_j} \in R$, съгласно $s_{ij} \geq n_j$ за $\forall l+1 \leq j \leq m$ и $\mu := \prod_{j=1}^{l} p_j^{n_j-s_{ij}} \in R\backslash R^*$ съгласно $n_j > s_{ij}$ за $\forall 1 \leq j \leq l$. От равенството $\lambda = \mu r$ следва, че всеки от неразложимите делители $p_1, \ldots, p_l$ на μ е асоциран с някой от неразложимите делители на λ. Неразложимите делители на λ се съдържат в множеството $\{p_{l+1}, \ldots, p_m\}$, така че $\lambda = \mu r$ противоречи на избора на неасоцирани помежду си $p_1, \ldots, p_m$. Следователно $s_{ij} \geq n_j$ за $\forall 1 \leq i \leq k$, $\forall 1 \leq j \leq m$, откъдето $\min(s_{1j}, \ldots, s_{kj}) \geq n_j$ и

$$\frac{d}{\delta} = \prod_{j=1}^{m} p_j^{\min(s_{1j},\ldots,s_{kj})-n_j} \in R.$$

Това доказва, че δ дели d и d е най-голям общ делител на $a_0, \ldots, a_n$, Q.E.D.

Определение 2.52. *Нека $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$ е полином с коефициенти от факториална нътерова комутативна област с единица R. Бележим с*

$$d(f) = d(a_0, a_1, \ldots, a_n)$$

най-големия общ делител на коефициентите на $f(x)$.
Ако $d(f) \in R^*$, то полиномът $f(x)$ се нарича примитивен.

Лема 2.53. (Gauss) *Ако R е факториална нътерова комутативна област с единица и $f(x), g(x) \in R[x]$, то*

$$d(fg) = d(f)d(g).$$

В частност, произведението на примитивни полиноми $f(x), g(x) \in R[x]$ е примитивен полином $fg \in R[x]$.

Доказателство: Достатъчно е да докажем твърдението за примитивни полиноми. Наистина, произволни полиноми $f(x), g(x) \in R[x]$ се представят във вида $f(x) = d(f)f_1(x)$, $g(x) = d(g)g_1(x)$ чрез най-големите общи делители $d(f), d(g) \in R$ на коефициентите им и примитивни $f_1(x), g_1(x) \in R[x]$. Ако сме установили, че $f_1(x)g_1(x)$ е примитивен, то най-големият общ делител $d(fg)$ на коефициентите на $f(x)g(x) = d(f)d(g)f_1(x)g_1(x)$ е точно $d(fg) = d(f)d(g)$.
Да допуснем, че полиномите $f(x) = a_m x^m + \ldots + a_1 x + a_0 \in R[x]$ и $g(x) = b_n x^n + \ldots + b_1 x + b_0 \in R[x]$ са примитивни, но $f(x)g(x) \in R[x]$ не е примитивен. За произволен неразложим общ делител p на коефициентите на $f(x)g(x)$ да означим с i минималното неотрицателно цяло число, за което p не дели a_i. Аналогично, нека j е минималното неотрицателно цяло число, за което p не дели b_j. Съществуването на i и j се осигурява от примитивността на $f(x)$, съответно, $g(x)$. Коефициентът c_{i+j} на x^{i+j} в $f(x)g(x)$ е равен на

$$c_{i+j} = a_i b_j + \sum_{s=1}^{\min(i,n-j)} a_{i-s}b_{j+s} + \sum_{s=1}^{\min(j,m-i)} a_{i+s}b_{j-s}$$

и се дели на p. Съгласно избора на i, коефициентите a_{i-s} с $s \geq 1$ се делят на p. Аналогично, b_{j-s} с $s \geq 1$ се делят на p, откъдето p дели и $a_i b_j$. С други думи, $a_i b_j$ попада в простия идеал pR на факториалната област R, породен от неразложимия елемент $p \in R$. Оттук следва, че $a_i \in pR$ или $b_j \in pR$, което противоречи на избора на a_i и b_j. По този начин получаваме, че произведението на примитивни полиноми $f(x), g(x) \in R[x]$ е примитивен полином $f(x)g(x) \in R[x]$, Q.E.D.

Лема 2.54. *Нека R е факториална нътерова комутативна област с единица, $f(x)$ и $g(x) \not\equiv 0$ са полиноми с коефициенти от R, а $0 \neq r \in R$. Ако $f(x)$ е примитивен полином, делящ $rg(x)$, то $f(x)$ дели $g(x)$.*

Доказателство: Ако $rg(x) = f(x)h(x)$ за някакъв полином $h(x)$, то по Лема 2.53 (Gauss),

$$rd(g) = d(rg) = d(fh) = d(f)d(h) = d(h)$$

с точност до обратим елемент на R. След представяне на $g(x) = d(g)g_1(x)$ и $h(x) = d(h)h_1(x)$ чрез примитивни полиноми $g_1(x), h_1(x) \in R[x]$ получаваме, че $rd(g)[g_1(x) - f(x)h_1(x)] = 0$. Но R, а оттам и $R[x]$ са области, така че $g_1(x) = f(x)h_1(x)$. В резултат, $g(x) = f(x)d(g)h_1(x)$ и $f(x)$ дели $g(x)$, Q.E.D.

9. Факториалност на полиноми с факториални коефициенти

Теорема 2. *Ако R е факториална нъотерова комутативна област с единица, то пръстенът $R[x]$ на полиномите на x с коефициенти от R е също факториална нъотерова комутативна област с единица.*

Доказателство: Съгласно критерия за факториалност на нъотерова комутативна област с единица (Лема 2.44 (ii)), достатъчно е да докажем, че всеки неразложим елемент $p(x) \in R[x]$ поражда прост идеал $\langle p(x)\rangle_{R[x]}$ в $R[x]$.
Ако $\deg p(x) = 0$, то $p \in R$ е неразложим и в R. Предположението $f(x)g(x) \in \langle p\rangle_{R[x]}$ е еквивалентно на $f(x)g(x) = ph(x)$ за някакъв полином $h(x) \in R[x]$. Най-големите общи делители на коефициентите

$$d(f)d(g) = d(fg) = d(ph) = pd(h),$$

така че $d(f)d(g) \in \langle p\rangle_R$ е от простия идеал в R, породен от p. Следователно $d(f) \in \langle p\rangle_R$ или $d(g) \in \langle p\rangle_R$, откъдето $f(x) = d(f)f_1(x) \in \langle p\rangle_{R[x]}$ или, съответно, $g(x) = d(g)g_1(x) \in \langle p\rangle_{R[x]}$.
Ако $\deg p(x) \geq 1$, то неразложимият полином $p(x)$ е обезателно примитивен. Наистина, разлагайки $p(x) = d(p)p_1(x)$ в произведение на най-големия общ делител $d(p)$ на коефициентите на $p(x)$ и примитивен полином $p_1(x)$, $\deg p_1(x) = \deg p(x) \geq 1$, забелязваме, че неразложимостта на $p(x)$ изисква обратимост на $d(p)$ в R.
Нека $f(x)g(x) \in \langle p(x)\rangle_{R[x]}$ и $f(x) \notin \langle p(x)\rangle_{R[x]}$. Избираме ненулев полином

$$h(x) \in \langle p(x), f(x)\rangle_{R[x]}$$

от минимална степен. Ако $h(x) = d(h)h_1(x)$ за примитивен полином $h_1(x) \in R[x]$, то твърдим, че

$$\langle p(x), f(x)\rangle_{R[x]} \subseteq \langle h_1(x)\rangle_{R[x]}. \tag{2.5}$$

Тогава $p(x) = c(x)h_1(x)$ за $c(x) \in R[x]$. Неразложимостта на $p(x)$ налага обратимост на $c(x)$ или $h_1(x)$ в $R[x]$.
Ако $c(x)$ е обратим, то $h_1(x) = c^{-1}p(x) \in \langle p(x)\rangle_{R[x]}$, откъдето

$$\langle p(x), f(x)\rangle_{R[x]} \subseteq \langle h_1(x)\rangle_{R[x]} \subseteq \langle p(x)\rangle_{R[x]},$$

противно на предположението $f(x) \notin \langle p(x)\rangle_{R[x]}$.
Ако $h_1(x) \in R[x]^* = R^*$, то $h(x) = d(h)h_1 \in R$. Съгласно $h \in \langle p(x), f(x)\rangle_{R[x]}$, съществуват полиноми $a(x), b(x) \in R[x]$, така че $h = p(x)a(x) + f(x)b(x)$. Оттук

$$g(x)h = p(x)a(x)g(x) + f(x)g(x)b(x) \in \langle p(x)\rangle_{R[x]}$$

и примитивният полином $p(x)$ дели $hg(x) \not\equiv 0$. Съгласно Лема 2.54, оттук следва, че $p(x)$ дели $g(x)$ и $g(x) \in \langle p(x)\rangle_{R[x]}$.
За да докажем включването (2.5), разширяваме коефициентите на полиномите до полето от частни Q на R и делим $p(x)$ на $h(x)$ с частно $\widetilde{q}(x) \in Q[x]$ и остатък $\widetilde{r}(x) \in Q[x]$, $p(x) = h(x)\widetilde{q}(x) + \widetilde{r}(x)$, $\deg \widetilde{r}(x) < \deg h(x)$. Ако

$$h(x) = ax^k + a_{k-1}x^{k-1} + \ldots + a_1x + a_0 \in R[x], \quad a \neq 0$$

и $m := \deg(\widetilde{q}(x) = \deg p(x) - \deg h(x)$, то съгласно алгоритъма за деление на полиноми на една променлива ,

$$\widetilde{q}(x) \in a^{-1}Rx^m + a^{-2}Rx^{m-1} + \ldots + a^{-m}Rx + a^{-(m+1)}R.$$

Затова $q(x) := a^{m+1}\widetilde{q}(x) \in R[x]$ и от равенството

$$a^{m+1}p(x) = h(x)q(x) + a^{m+1}\widetilde{r}(x)$$

следва, че $r(x) := a^{m+1}\widetilde{r}(x) = a^{m+1}p(x) - h(x)q(x) \in R[x]$. Още повече, $h(x) \in \langle p(x), f(x)\rangle_{R[x]}$, така че $r(x) \in \langle p(x), f(x)\rangle_{R[x]}$ от степен $\deg r(x) = \deg \widetilde{r}(x) < \deg h(x)$. Изборът на $h(x)$ като ненулев полином от $\langle p(x), f(x)\rangle_{R[x]}$ с минимална степен налага тъждественото анулиране на $r(x) \equiv 0$. Следователно полиномът $a^{m+1}p(x) = h(x)q(x)$. Отделяме $d(h)$ като множител и разлагаме $h(x) = d(h)h_1(x)$ чрез примитивен полином $h_1(x) \in R[x]$. Тогава равенството $a^{m+1}p(x) = d(h)h_1(x)q(x)$ показва, че $h_1(x)$ дели $a^{m+1}p(x)$. Прилагаме Следствие 2.54 и получаваме, че $h_1(x)$ дели $p(x)$ или $p(x) \in \langle h_1(x)\rangle_{R[x]}$. Аналогични разсъждения доказват, че $f(x) \in \langle h_1(x)\rangle_{R[x]}$, Q.E.D.

Следствие 2.55. *Ако R е факториална нътерова комутативна област с единица, то $R[x_1, \ldots, x_n]$ е факториална нътерова комутативна област с единица.*

Доказателство: С индукция по броя n на променливите, ако $R[x_1, \ldots, x_{n-1}]$ е факториална нътерова комутативна област с единица, то

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$$

е факториална нътерова комутативна област с единица, съгласно Теорема 2, Q.E.D.

Следствие 2.56. *Пръстенът $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n]$ на $x_1, \ldots, x_n$ с коефициенти от поле k е факториална нътерова комутативна област с единица.*

Доказателство: Пръстенът $k[x_1]$ на полиномите на една променлива с коефициенти от поле k е факториална нътерова област, в качеството си на област на главни идеали. С индукция по броя на променливите n получаваме, че $k[x_1, \ldots, x_{n-1}] = k[x_1, \ldots, x_{n-1}][x_n]$ е факториална нътерова област, Q.E.D.

Задача 2.57. *Да се докаже, че за произволен полином $f(x) \in \mathbb{C}[x]$ от нечетна степен $\deg(f) = 2n+1$, полиномът $g(x, y) = y^2 - f(x) \in \mathbb{C}[x, y]$ е неразложим.*

Упътване: Да допуснем, че $g(x, y) \in \mathbb{C}[x, y] \setminus \mathbb{C}$ се разлага в произведение $g(x, y) = g_1(x, y)g_2(x, y)$ за полиноми $g_j(x, y) \in \mathbb{C}[x, y] = \mathbb{C}[x][y]$ от неотрицателни степени $d_j = \deg_y(g_j) \in \mathbb{Z}$ относно y, които не принадлежат на мултипликативната група $\mathbb{C}[x, y]^* = \mathbb{C}^*$. Условието $d_1 + d_2 = 2$ е в сила за $d_1 = 2$, $d_2 = 0$ или за $d_1 = d_2 = 1$.
Ако $g(x, y) = [a(x)y^2 + b(x)y + c(x)]g_2(x)$ за полиноми $a(x), b(x), c(x), g_2(x) \in \mathbb{C}[x]$, то $g_2(x) \equiv 1$ и $g_2 \in \mathbb{C}^*$, противно на предположението $g_1(x, y), g_2(x, y) \notin \mathbb{C}^*$. Ако $g(x, y) = [a(x)y + b(x)][p(x)y + q(x)]$ с $a(x), b(a), p(x), q(x) \in \mathbb{C}[x]$, то

$$a(x) \equiv p(x) \equiv 1, \quad b(x) + q(x) \equiv 0, \quad b(x)q(x) = -f(x).$$

Следователно $f(x) = b(x)^2$ трябва да е от четна степен.

Задача 2.58. *Да се докаже, че за произволен полином $f(x) \in \mathbb{C}[x]$ от степен $\deg(f) = 3n \pm 1$, взаимно проста с 3, полиномът $g(x, y) = y^3 + f(x) \in \mathbb{C}[x, y]$ е неразложим.*

Упътване: По аналогия със Задача 2.57, допуснете че полиномът $g(x,y) = g_1(x,y)g_2(x,y)$ е разложим в произведение на полиноми $g_j(x,y) \in \mathbb{C}[x][y] \setminus \mathbb{C}^*$ от неотрицателни степени $d_j = \deg_y(g_j) \in \mathbb{Z}$. С точност до пермутация на множителите, сведете разглежданията към $d_1 = 0$, $d_2 = 3$ или $d_1 = 1$, $d_2 = 2$.