Глава 9

Пръстени на нормиране. Теорема за продължение.

Лема-Определение 10. *Ако S е R-алгебра, то множеството $\overline{R}$ на целите над R елементи на S е подпръстен на S, наречен цяла обвивка на R в S.*

Доказателство: Трябва да установим, че ако $x, y \in S$ са цели над R, то $x - y$ и xy са цели над R. За целта да отбележим, че R-алгебрата $R[x]$ е крайнопороден R-модул и $R[x]$-алгебрата $R[x, y] = R[x][y]$ е крайнопороден $R[x]$-модул, доколкото y е цял над $R[x]$. Следователно $R[x, y]$ е крайнопороден R-модул. Достатъчно е да докажем, че всеки елемент $\alpha \in R[x, y]$ е цял над R, за да получим, че $x - y, xy \in R[x, y]$ са цели над R. Ако $R[x, y] = Rt_1 + \ldots + Rt_k$ за подходящи $t_j \in R[x, y]$, $1 \leq j \leq k$, то $\alpha t_j = \sum\limits_{i=1}^{k} r_{ij} t_i$ за някакви $r_{ij} \in R$, $\forall 1 \leq j \leq k$. Умножението $\mu_\alpha : R[x, y] \to R[x, y]$ с α е хомоморфизъм на R-модули с матрица $r = (r_{ij})_{i,j=1}^{k} \in R_{k \times k}$ спрямо пораждащите $t_1, \ldots, t_k$ на R-модула $R[x, y]$ Ако $E_k \in R_{k \times k}$ е единичната матрица, а $t = (t_1, \ldots, t_k)$, то $t(\alpha E_k) = tr$, откъдето $t(r - \alpha E_k) = (0, \ldots, 0)$. Умножавайки отдясно с адюнгираната матрица на $r - \alpha E_k \in R_{k \times k}$, получаваме $\det(r - \alpha E_k) t_j = 0$ за $\forall 1 \leq j \leq k$. Характеристичният полином $f_r(\alpha) = \det(r - \alpha E_k)$ е полином на α от степен k със старши коефициент $(-1)^k$, така че съществуват $\rho_1, \ldots, \rho_{k-1} \in R$ с

$$(\alpha^k + \rho_{k-1}\alpha^{k-1} + \ldots + \rho_1 \alpha + \rho_0) t_j = 0 \text{ за } \forall 1 \leq j \leq k.$$

Оттук следва, че

$$(\alpha^k + \rho_{k-1}\alpha^{k-1} + \ldots + \rho_1 \alpha + \rho_0) \beta = 0 \text{ за } \forall \beta \in R[x, y].$$

В частност, за $\beta = 1$ получаваме цяла зависимост

$$\alpha^k + \rho_{k-1}\alpha^{k-1} + \ldots + \rho_1 \alpha + \rho_0 = 0$$

на α над R, Q.E.D.

Определение 9.1. *Областта на цялост R с поле от частни F се нарича целозатворена, ако съвпада с цялата си обвивка, $\overline{R} = R$.*

Определение 9.2. *Нека R е област на цялост с поле от частни F. Ако за всеки ненулев елемент $x \in F \setminus \{0\}$ е в сила $x \in R$ или $x^{-1} \in R$ (възможно и двете), то R се нарича пръстен на нормиране.*

Нека R е пръстен на нормиране с поле от частни F. Тогава мултипликативната група R^* е подгрупа на мултипликативната група $F^* = F \setminus \{0\}$. Групата F^* е абелева, така че подгрупата R^* е нормална и можем да образуваме фактор-групата $V = F^*/R^*$. Групата V се нарича група от стойности на R (value group). Наследената от F^* групова операция във V се записва адитивно. Въвеждаме линейна наредба във V по правилото $xR^* \geq yR^*$ тогава и само тогава, когато $xy^{-1} \in R$. Проверяваме съгласуваност на тази линейна наредба с груповата операция във V, т.е. от $x_1R^* \geq y_1R^*$ и $x_2R^* \geq y_2R^*$ следва

$x_1x_2R^* \geq y_1y_2R^*$. Естественият хомоморфизъм

$$\pi_{R^*} : F^* \longrightarrow V = F^*/R^*,$$

$$\pi_{R^*}(x) = xR^* \text{ за } \forall x \in F^*$$

с ядро $Ker(\pi_{R^*}) = R^*$ и образ $Im(\pi_{R^*}) = V$ изпълнява условията

$$\pi_{R^*}(xy) = \pi_{R^*}(x) + \pi_{R^*}(y) \text{ и } \pi_{R^*}(x+y) \geq \min(\pi_{R^*}(x), \pi_{R^*}(y)) \text{ за } \forall x, y \in F^*.$$

По-точно, ако $\min(\pi_{R^*}(x), \pi_{R^*}(y)) = \pi_{R^*}(y)$ или $xy^{-1} \in R$, то $x+y = (xy^{-1}+1)y$ с $(x+y)y^{-1} = xy^{-1} + 1 \in R$ има образ $\pi_{R^*}(x+y) \geq \pi_{R^*}(y)$. Продължаваме изображението $\pi_{R^*} : F^* \to V$ до $\pi_{R^*} : F \to V$, полагайки $\pi_{R^*}(0) = \infty$. По този начин получаваме нормиране на F.

Определение 9.3. *Нормиране на поле F е изображение $\nu : F \to V \cup \{\infty\}$ върху обединението на линейно наредената група V и ∞, което изпълнява следните три свойства:*
(i) $\nu(x) = \infty$ тогава и само тогава, когато $x = 0$;
(ii) $\nu(xy) = \nu(x) + \nu(y)$ за $\forall x, y \in F$;
(iii) $\nu(x+y) \geq \min(\nu(x), \nu(y))$ за $\forall x, y \in F$.

Да предположим, че групата от стойности V на нормирането $\nu : F \to V \cup \{\infty\}$ няма ненулеви нилпотентни елементи. Даколкото ν се ограничава до хомоморфизъм $\nu : (F^*, .) \to (V, +)$, единицата $1 \in F^*$ се трансформира в $\nu(1) = 0$. Следователно $\nu(-1) = 0$, съгласно $(-1)^2 = 1$ и $0 = \nu(1) = 2\nu(-1)$. Твърдим, че подмножеството

$$R = \{x \in F \,|\, \nu(x) \geq 0\}$$

е подпръстен на F. Наистина, за произволни $x, y \in R$ следва $\nu(xy) = \nu(x) + \nu(y) \geq 0$, така че $xy \in R$. От друга страна, $\nu(-y) = \nu(y) + \nu(-1) = \nu(y)$ дава $\nu(x-y) = \nu(x + (-y)) \geq \min(\nu(x), \nu(-y)) = \min(\nu(x), \nu(y)) \geq 0$, откъдето $x - y \in R$. Мултипликативната група

$$R^* = \{x \in F \,|\, \nu(x) = 0\}.$$

По-точно, ако $x, x^{-1} \in R$, то от $xx^{-1} = 1$ получаваме $0 = \nu(1) = \nu(x) + \nu(x^{-1})$ с $\nu(x) \geq 0$. Следователно $\nu(x) = \nu(x^{-1}) = 0$. Обратно, ако $\nu(x) = 0$, то $x \neq 0$ и от $xx^{-1} = 1$ следва $0 = \nu(1) = \nu(x) + \nu(x^{-1}) = \nu(x^{-1})$, така че $x^{-1} \in R$ и $x \in R^*$. Множеството

$$\mathfrak{M} = \{x \in F \,|\, \nu(x) > 0\}$$

на необратимите в R елементи на R е идеал, защото за $\forall x, y \in \mathfrak{M}$ е в сила $\nu(x-y) \geq \min(\nu(x), \nu(y)) > 0$, а за произволни $x \in \mathfrak{M}$ и $z \in R$ е изпълнено $\nu(xz) = \nu(x) + \nu(z) \geq \nu(x) > 0$. Следователно R е локален пръстен с максимален идеал $\mathfrak{M}$. Още повече, $R = \{x \in F \,|\, \nu(x) \geq 0\}$ е пръстен на нормиране, защото за $\forall 0 \neq x \in F$ имаме $\nu(x) \geq 0$ или $\nu(x) \leq 0$. Ако $\nu(x) \geq 0$, то $x \in R$. Ако $\nu(x) \leq 0$, то $\nu(x^{-1}) = \nu(1) - \nu(x) = -\nu(x) \geq 0$ и $x^{-1} \in R$.

Определение 9.4. *Нормирането $\nu : F \to V \cup \{\infty\}$ на поле F е дискретно, ако групата от стойности V е изоморфна на адитивната група $(\mathbb{Z}, +)$ на целите числа.*

Например, ако $p \in k$ е точка от афинната права, то всяка рационална функция върху k може да се представи във вида $(x-p)^n \frac{f_o(x)}{g_o(x)}$ за някакво цяло n и полиноми $f_o(x), g_o(x) \in k[x]$ с $f_o(p) \neq 0$, $g_o(x) \neq 0$. Изображението

$$\nu_p : k(X) \longrightarrow \mathbb{Z} \cup \{\infty\},$$

$$\nu_p\left((x-p)^n \frac{f_o(x)}{g_o(x)}\right) = n$$

е дискретно нормиране, чийто пръстен съвпада с локалния пръстен $\mathcal{O}_p, k$ на точката $p \in k$.

Твърдение 9.5. *Нека R е пръстен на нормиране с поле от частни F. Тогава:*
(i) R е локален пръстен;
(ii) всеки подпръстен S на F, съдържащ R е също пръстен на нормиране;
(iii) R е целозатворена област.

Доказателство: (i) Нека $\mathfrak{M}$ е множеството на необратимите елементи на R. Съгласно Лема 7.8, достатъчно е да проверим, че $\mathfrak{M}$ е идеал в R, за да твърдим, че пръстенът R е локален. Ако $x \in \mathfrak{M}$ и $a \in R$, то $ax \in \mathfrak{M}$, защото ако $ax \in R$ е обратим и $y = (ax)^{-1} \in R$, то $axy = 1_R$. Оттук следва $x^{-1} = ay \in R$, което противоречи на $x \in \mathfrak{M}$. Нека $x, y \in \mathfrak{M}$. Ако $x = 0_R$ или $y = 0_R$, то е ясно, че $x + y \in \mathfrak{M}$. Остава да докажем, че $x + y \in \mathfrak{M}$ за произволни $x, y \in \mathfrak{M} \setminus \{0_R\}$. В полето от частни F на R, ненулевите елементи $x, y \in F$ имат обратни $x^{-1}, y^{-1} \in F$. По определението за пръстен на нормиране, за ненулевия елемент $xy^{-1} \in F$ е в сила $xy^{-1} \in R$ или $yx^{-1} = (xy^{-1})^{-1} \in R$. След евентуална размяна на x с y можем да считаме, че $xy^{-1} \in R$. Следователно $1_R + xy^{-1} \in R$, а оттам и $x+y = (1_R + xy^{-1})y \in \mathfrak{M}$, доколкото $y \in \mathfrak{M}$ принадлежи на $\mathfrak{M}$ заедно с всички свои кратни с елементи на R. Това доказва, че множеството $\mathfrak{M}$ на необратимите елементи на R образува идеал в R, така че пръстенът R е локален.
(ii) По определение, за $\forall 0 \neq x \in F$ поне едното от x или x^{-1} принадлежи на пръстена на нормиране R. Вземайки предвид, че R се съдържа в S, поне едното от x или x^{-1} попада в S и S е пръстен на нормиране.
(iii) Нека елементът $x \in F$ е цял над R. Това означава съществуване на $r_1, \dots, r_n \in R$, така че

$$x^n + r_1 x^{n-1} + r_2 x^{n-2} + \dots + r_{n-1} x + r_n = 0. \tag{9.1}$$

Ако $x \in R$, то няма какво да се доказва. Ако $x \notin R$, то $x^{-1} \in R$, доколкото R е пръстен на нормиране. Умножаваме (9.1) с x^{1-n} и получаваме

$$x + r_1 + r_2 x^{-1} + \dots + r_{n-1} x^{2-n} + r_n x^{1-n} = 0.$$

Следователно $x = -r_1 - r_2 x^{-1} - r_3 (x^{-1})^2 - \dots - r_{n-1}(x^{-1})^{n-2} - r_n (x^{-1})^{n-1} \in R$, противно на допускането $x \notin R$. Оттук $x \in R$ и всеки пръстен на нормиране R е целозатворена област, Q.E.D.
За доказателството на следващата Теорема за продължение ни е нужна следната

Лема 9.6. *Нека R е комутативен пръстен с единица, I е идеал в R, а*

$$\pi_I : R \longrightarrow R/I,$$

$$\pi_I(r) = r + I$$

е естественият хомоморфизъм с ядро $Ker(\pi_I) = I$ и образ $Im(\pi_I) = R/I$. Тогава редукцията на коефициентите

$$\Pi_I : R[x] \longrightarrow R/I[x],$$

$$\Pi_I \left(\sum_{i=0}^{m} r_i x^i \right) = \sum_{i=0}^{m} (r_i + I) x^i$$

по модул I е хомоморфизъм на пръстени с ядро $Ker(\Pi_I) = I[x]$ и образ $Im(\Pi_I) = R/I[x]$.

Доказателство: Непосредствено проверяваме, че Π_I е съгласувано със събирането на полиноми,

$$\Pi_I\left(\sum_{i=0}^{m} r_i x^i + \sum_{j=0}^{n} s_j x^j\right) = \Pi_I\left(\sum_{i=0}^{\max(m,n)} (r_i+s_i)x^i\right) = \sum_{i=0}^{\max(m,n)} (r_i+s_i+I)x^i =$$

$$\sum_{i=0}^{m}(r_i+I)x^i + \sum_{j=0}^{n}(s_j+I)x^j = \Pi_I\left(\sum_{i=0}^{m} r_i x^i\right) + \Pi_I\left(\sum_{j=0}^{n} s_j x^j\right)$$

и Π_I е съгласувано с умножението на полиноми

$$\Pi_I\left(\left(\sum_{i=0}^{m} r_i x^i\right)\left(\sum_{j=0}^{n} s_j x^j\right)\right) = \Pi_I\left(\sum_{i=0}^{m+n}\left(\sum_{l=0}^{i} r_l s_{i-l}\right)x^i\right) =$$

$$\sum_{i=0}^{m+n}\left[\left(\sum_{l=0}^{i} r_l s_{i-l}\right)+I\right]x^i = \sum_{i=0}^{m+n}\left[\sum_{l=0}^{i}(r_l+I)(s_{i-l}+I)\right]x^i =$$

$$\left(\sum_{i=0}^{m}(r_i+I)x^i\right)\left(\sum_{j=0}^{n}(s_j+I)x^j\right) = \Pi_I\left(\sum_{i=0}^{m} r_i x^i\right)\Pi_I\left(\sum_{j=0}^{n} s_j x^j\right).$$

Следователно Π_I е хомоморфизъм на пръстени. Условието $\sum\limits_{i=0}^{m} r_i x^i \in Ker(\Pi_I)$ е еквивалентно на $r_i + I = I$ за всички $0 \leq i \leq m$, така че ядрото $Ker(\Pi_I) = I[x]$ се състои от полиномите на x с коефициенти от I. Всеки полином $\overline{f(x)} = \sum\limits_{i=0}^{m}(s_j+I)x^j \in R/I[x]$ е образ $\overline{f(x)} = \Pi_I\left(\sum\limits_{j=0}^{m} s_j x^j\right)$ на полином $f(x) = \sum\limits_{j=0}^{m} s_j x^j \in R[x]$, така че образът $Im(\Pi_I) = R/I[x]$, Q.E.D.

Нека X е неприводимо афинно многообразие над алгебрично затворено поле k, а p е точка от X. Тогава афинният координатен пръстен $k[X]$ на X е подпръстен на полето $K(X)$ на рационалните функции върху X и остойностяващото изображение

$$\varepsilon_p : k[X] \longrightarrow k,$$

$$\varepsilon(\overline{f}) = f(p)$$

е хомоморфизъм на пръстени с ядро $Ker(\varepsilon_p) = \mathfrak{M}_p \triangleleft k[X]$ и образ $Im(\varepsilon_p) = k$. Да допуснем, че съществува $f_o \in \mathfrak{M}_{p,X}$, така че всеки идеал в $\mathcal{O}_{p,X}$ е от вида $\langle f_o^\nu \rangle \mathcal{O}_{p,X} = f_o^\nu \mathcal{O}_{p,X}$ за някакво цяло неотрицателно ν. Ще видим, че тази ситуация отговаря на гладка точка p върху неприводима афинна крива X. Тогава всеки елемнт на $\mathcal{O}_{p,X}$ е от вида $f = f_o^\nu g$ за подходящо $g \in \mathcal{O}_{p,X}^*$. По-точно, от $\langle f \rangle_{\mathcal{O}_{p,X}} = \langle f_o^\nu \rangle_{\mathcal{O}_{p,X}}$ следва $f = f_o^\nu g$ и $f_o^\nu = fh$ за някакви $g, h \in \mathcal{O}_{p,X}$. Оттук $f = fgh$ в областта на цялост $\mathcal{O}_{p,X}$ дава $gh = 1$ или $g, h \in \mathcal{O}_{p,X}^*$. В резултат получаваме дискретно нормиране

$$\nu_p : \mathcal{O}_{p,X} \longrightarrow \mathbb{Z} \cup \{\infty\},$$

$$\nu_p(f) = \nu_p(f_o^\nu g) = \nu \text{ за } \forall f = f_o^\nu g \in \mathcal{O}_{p,X} \setminus \{0\} \text{ с } \nu \in \mathbb{N} \cup \{0\},\ g \in \mathcal{O}_{p,X}^*,$$

$$\nu_p(0) = \infty.$$

Остойностяващото изображение $\varepsilon_p : k[X] \to k$ се продължава до хомоморфизъм $\mathcal{E}_p : \mathcal{O}_{p,X} \to k$ с ядро $Ker(\mathcal{E}) = \mathfrak{M}_{p,X}$. Още повече, пръстенът на дискретно нормиране $\mathcal{O}_{p,X}$ е максималният подпръстен на $k(x)$, съдържащ $k[X]$, до който можем да продължим остойностяващото изображение в точка p.

ТЕОРЕМА 11. (**Теорема за продължение**) *Нека F е поле, A е подпръстен на F, k е алгебрично затворено поле и $\varphi : A \to k$ е нетъждествено нулев хомоморфизъм на пръстени. Тогава съществува пръстен на нормиране $A \subseteq R \subset F$ и хомоморфизъм на пръстени $\Phi : R \to k$, продължаващ ϕ, така че ядрото $Ker(\Phi)$ е максималният идеал на R.*

Доказателство: Да разгледаме множеството

$$\Sigma = \{(R, \Phi) \,|\, A \subseteq R \subseteq F,\, \Phi : R \to k,\, \Phi|_A = \varphi\}$$

на наредените двойки (R, Φ) от подпръстени R на F, съдържащи A и хомоморфизми на пръстени $\Phi : R \to k$, продължаващи $\varphi : A \to k$. За два елемента $(R_1, \Phi_1), (R_2, \Phi_2) \in \Sigma$ ще казваме, че $(R_1, \Phi_1) \geq (R_2, \Phi_2)$, ако R_2 е подпръстен на R_1 и Φ_1 продължава Φ_2. Така въведената релация е частична наредба в Σ. Всяко линейно наредено подмножество $\{(R_\alpha, \Phi_\alpha)\}_{\alpha \in I}$ на Σ има точна горна граница $\left(R_\infty = \cup_{\alpha \in I}^{\infty} R_\alpha, \Phi_\infty\right)$, където $\Phi_\infty(r) = \Phi_\alpha(r)$ за някои $\alpha \in I$ с $r \in R_\alpha$. Доколкото Φ_β продължава Φ_α за $\forall \beta > \alpha$ от I, това определение е коректно и задава хомоморфизъм $\Phi_\infty : R_\infty \to k$, продължаващ всички Φ_α. По Лемата на Цорн, съществува максимален елемент $(R, \Phi) \in \Sigma$. Ще докажем, че R е пръстен на нормиране с максимален идеал $\mathfrak{M} = Ker(\Phi)$.

Първо, ще проверим, че R е локален пръстен с максимален идеал $\mathfrak{M} = Ker(\Phi)$. За целта е достатъчно да установим, че ядрото $Ker(\Phi)$ на хомоморфизма $\Phi : R \to k$ съвпада с множеството на необратимите в R елементи на R или, еквивалентно, $R \setminus Ker(\Phi)$ съвпада с множеството на обратимите в R елементи на R. Ако $r \in R$ е обратим в R, то $r \notin Ker(\Phi)$, защото в противен случай $1 \in Ker(\Phi)$, $R = Ker(\Phi)$ и хомоморфизмът $\varphi : A \to k$ е тъждествено нулев. За произволен елемент $x \in R \setminus Ker(\Phi)$ твърдим, че $x^{-1} \in R$. Необходимо и достатъчно условие за това е $R[x^{-1}] = R$. Равенството на пръстени $R[x^{-1}] = R$, ще бъде изведено от съществуването на продължение $\Phi : R[x^{-1}] \longrightarrow k$ на $\Phi : R \to k$, така че $(R[x^{-1}], \Phi) \in \Sigma$ и максималността на $(R, \Phi) \in \Sigma$ да води до $R[x^{-1}] = R$. Преди всичко, $x \notin Ker(\Phi)$ дава $\Phi(x) \neq 0$ в полето k, така че съществува $\Phi(x^{-1}) := \Phi(x)^{-1} \in k$. Ще положим

$$\Phi(r_0 + r_1 x^{-1} + \ldots + r_n x^{-n}) = \Phi(r_0) + \Phi(r_1)\Phi(x)^{-1} + \ldots + \Phi(r_n)\Phi(x)^{-n}.$$

Коректността на това определение изисква да проверим, че ако $\sum\limits_{i=0}^{m} s_i x^{-i} = 0$ в $R[x^{-1}]$, то и $\Phi\left(\sum\limits_{i=0}^{m} s_i x^{-i}\right) = \sum\limits_{i=0}^{m} \Phi(s_i)\Phi(x)^{-i} = 0$. За целта да отбележим, че $0 = \left(\sum\limits_{i=0}^{m} s_i x^{-i}\right) x^m = \sum\limits_{i=0}^{m} s_i x^{m-i} \in R[x] = R$ има нулев образ $0 = \sum\limits_{i=0}^{m} \Phi(s_i)\Phi(x)^{m-i}$ под действие на хомоморфизма $\Phi : R \to k$. Умножавайки последното равенство с $\Phi(x)^{-m}$ получаваме $\sum\limits_{i=0}^{m} \Phi(s_i)\Phi(x)^{-i} = 0$. Непосредствено се проверява, че така определеното изображение $\Phi : R[x^{-1}] \to k$ е хомоморфизъм на пръстени. По-точно,

$$\Phi\left(\sum_{i=0}^{m} r_i x^{-i} + \sum_{j=0}^{n} t_j x^{-j}\right) = \Phi\left(\sum_{i=0}^{\max(m,n)} (r_i + t_i)\Phi(x)^{-i}\right) =$$

$$\sum_{i=0}^{\max(m,n)} \Phi(r_i + t_i)\Phi(x)^{-i} = \left(\sum_{i=0}^{m} \Phi(r_i)\Phi(x)^{-i}\right) + \left(\sum_{j=0}^{n} \Phi(t_j)\Phi(x)^{-j}\right) =$$

$$\Phi\left(\sum_{i=0}^{m} r_i x^{-i}\right) + \Phi\left(\sum_{j=0}^{n} t_j x^{-j}\right) \quad \text{и}$$

$$\Phi\left(\left(\sum_{i=0}^{m} r_i x^{-i}\right)\left(\sum_{j=0}^{n} t_j x^{-j}\right)\right) = \Phi\left(\sum_{i=0}^{m+n}\left(\sum_{s=0}^{i} r_s t_{i-s}\right) x^{-i}\right) =$$

$$\sum_{i=0}^{m+n}\Phi\left(\sum_{s=0}^{i} r_s t_{i-s}\right)\Phi(x)^{-i} = \sum_{i=0}^{m+n}\left(\sum_{s=0}^{i}\Phi(r_s)\Phi(t_{i-s})\right)\Phi(x)^{-i} =$$

$$\left(\sum_{i=0}^{m}\Phi(r_i)\Phi(x)^{-i}\right)\left(\sum_{j=0}^{n}\Phi(t_j)\Phi(x)^{-j}\right) = \Phi\left(\sum_{i=0}^{m} r_i x^{-i}\right)\Phi\left(\sum_{j=0}^{n} t_j x^{-j}\right).$$

С това доказахме, че всеки елемент на $R \setminus Ker(\Phi)$ е обратим в R и R е локален пръстен с максимален идеал $\mathfrak{M} = Ker(\Phi)$.

Остава да установим, че за $\forall 0 \neq x \in F$ е в сила $x \in R$ или $x^{-1} \in R$. Еквивалентно, за $\forall 0 \neq x \in F$ е изпълнено $R[x] = R$ или $R[x^{-1}] = R$. Съгласно максималността на $(R, \Phi) \in \Sigma$, достатъчно е да проверим, че $\Phi : R \to k$ се продължава до хомоморфизъм на пръстени $\Phi_1 : R[x] \to k$ или хомоморфизъм на пръстени $\Phi_{-1} : R[x^{-1}] \to k$. Преди всичко твърдим, че $\forall 0 \neq y \in F$ е алгебрично над полето от остатъци $R/\mathfrak{M}$ на R. Да допуснем противното и да забележим, че хомоморфизмът $\Phi : R \to k$ с ядро $Ker(\Phi) = \mathfrak{M}$ индуцира влагане $\overline{\Phi} : R/\mathfrak{M} \to k$ на полето от остатъци $R/\mathfrak{M}$ в полето k. Разглеждаме изображението

$$\overline{\Phi_0} : R/\mathfrak{M}[y] \longrightarrow k,$$

$$\overline{\Phi_0}\left(\sum_{i=0}^{m}(r_i + \mathfrak{M})y^i\right) = \overline{\Phi}(r_0 + \mathfrak{M}),$$

трансформиращо y в $\overline{\Phi_0}(y) = 0$. Непосредствено се проверява, че $\overline{\Phi_0}$ е съгласувано със събирането на полиноми от $R/\mathfrak{M}[y]$,

$$\overline{\Phi_0}\left(\sum_{i=0}^{m}(r_i + \mathfrak{M})y^i + \sum_{j=0}^{n}(s_j + \mathfrak{M})y^j\right) = \overline{\Phi_0}\left(\sum_{i=0}^{\max(m,n)}(r_i + s_i + \mathfrak{M})y^i\right) =$$

$$\overline{\Phi}(r_0+s_0+\mathfrak{M}) = \overline{\Phi}(r_0+\mathfrak{M})+\overline{\Phi}(s_0+\mathfrak{M}) = \overline{\Phi_0}\left(\sum_{i=0}^{m}(r_i + \mathfrak{M})y^i\right)+\overline{\Phi_0}\left(\sum_{j=0}^{n}(s_j + \mathfrak{M})y^j\right)$$

и $\overline{\Phi_0}$ е съгласувано с умножението на полиноми

$$\overline{\Phi_0}\left(\left(\sum_{i=0}^{m}(r_i + \mathfrak{M})y^i\right)\left(\sum_{j=0}^{n}(s_j + \mathfrak{M})y^j\right)\right) =$$

$$\overline{\Phi_0}\left(\sum_{i=0}^{m+n}\left(\sum_{l=0}^{i}(r_l + \mathfrak{M})(s_{i-l} + \mathfrak{M})\right)y^i\right) = \overline{\Phi}((r_0 + \mathfrak{M})(s_0 + \mathfrak{M}) =$$

$$\overline{\Phi}(r_0 + \mathfrak{M})\overline{\Phi}(s_0 + \mathfrak{M}) = \overline{\Phi_0}\left(\sum_{i=0}^{m}(r_i + \mathfrak{M})y^i\right)\overline{\Phi_0}\left(\sum_{j=0}^{n}(s_j + \mathfrak{M})y^j\right).$$

Следователно $\overline{\Phi_0}$ е хомоморфизъм на пръстени. Композирайки с редукцията на коефициентите

$$\Pi_{\mathfrak{M}} : R[y] \longrightarrow R/\mathfrak{M}[y]$$

по модул максималния идеал $\mathfrak{M}$, получаваме хомоморфизъм на пръстени

$$\Phi_0 = \overline{\Phi_0} \circ \Pi_{\mathfrak{M}} : R[y] \longrightarrow k$$

с $\Phi_0(y) = 0$, продължаващ $\Phi : R \to k$. Следователно $(R[y], \Phi_0) \in \Sigma$ и съгласно максималността на $(R, \Phi) \in \Sigma$, оттук следва, че $R[y] = R$. В резултат, $y \in R$,

откъдето $y \in R \cap Ker(\Phi_0) = Ker(\Phi) = \mathfrak{M}$. С други думи, $y + \mathfrak{M} = \mathfrak{M}$ е нулевият елемент на $R/\mathfrak{M}$, което противоречи на трансцендентността на y над $R/\mathfrak{M}$.
Да обърнем внимание, че произволно нетривиално алгебрично разширение $R/\mathfrak{M}[y]$ на $R/\mathfrak{M} \subset k$ се съдържа в алгебрично затвореното поле k. С други думи, влагането $\overline{\Phi} : R/\mathfrak{M} \to k$ се продължава до влагане на полета $\overline{\Phi_o} : R/\mathfrak{M}[y] \to k$. Условието $0 \neq R/\mathfrak{M}[y] = Im(\Pi_{\mathfrak{M}})$ е еквивалентно на $\mathfrak{M}[y] = Ker(\Pi_{\mathfrak{M}}) \neq R[y]$. Ако $\mathfrak{M}[y] \subsetneqq R[y]$ и $\overline{\Phi_0} : R/\mathfrak{M}[y] \to k$ продължава $\overline{\Phi} : R/\mathfrak{M} \to k$, то $\Phi_0 = \overline{\Phi_0} \circ \Pi_{\mathfrak{M}} : R[y] \to k$ продължава $\Phi : R \to k$ и $R[y] = R$, $y \in R$. По този начин, остава да се провери, че за $\forall 0 \neq x \in F$ е в сила $\mathfrak{M}[x] \subsetneqq R[x]$ или $\mathfrak{M}[x^{-1}] \subsetneqq R[x^{-1}]$. Да допуснем, че $\mathfrak{M}[x] = R[x]$ и $\mathfrak{M}[x^{-1}] = R[x^{-1}]$. Тогава съществуват $m_0, m_1, \ldots, m_k, m'_0, m'_1, \ldots, m'_l \in \mathfrak{M}$, така че

$$1 = m_0 + m_1 x + \ldots + m_k x^k = m'_0 + m'_1 x^{-1} + \ldots + m'_l x^{-l}. \tag{9.2}$$

Без ограничение на общността можем да считаме, че степените k, съответно l на полиномите на x, съответно x^{-1} с коефициенти от $\mathfrak{M}$ са минималните възможни за представяне на $1 \in \mathfrak{M}[x] = \mathfrak{M}[x^{-1}]$. След евентуална размяна между x и x^{-1} имаме $k \geq l$. Тогава

$$1 - m'_0 = m'_1 x^{-1} + \ldots + m'_l x^{-l}$$

е обратим в R елемент на R и умножавайки почленно с $(1 - m'_0)^{-1} m_k x^k$ получаваме

$$m_k x^k = \mu_{k-1} x^{k-1} + \ldots + \mu_{k-l} x^{k-l} \tag{9.3}$$

за подходящи $\mu_{k-1}, \ldots, \mu_{k-l} \in \mathfrak{M}$. Заместването на (9.3) в (9.2) дава

$$1 = \mu'_0 + \mu'_1 x + \ldots + \mu'_{k-1} x^{k-1}$$

с $\mu'_0, \mu'_1, \ldots, \mu'_{k-1} \in \mathfrak{M}$. Това противоречи на минималността на k и доказва, че поне единият от идеалите $\mathfrak{M}[x] \triangleleft R[x]$ или $\mathfrak{M}[x^{-1}] \triangleleft R[x^{-1}]$ е собствен в съответния полиномиален пръстен, Q.E.D.
За следващите разглеждания ни е необходимо понятието алгебрична обвивка на поле. Необходимите сведения са събрани в Приложението.

Следствие 9.7. *Ако A е подпръстен на поле F, то цялата обвивка*

$$\overline{A} = \cap_{R \supseteq A} R$$

на A в F съвпада със сечението на пръстените на нормиране R на F, съдържащи A.

Доказателство: Ако R е пръстен на нормиране на F, съдържащ A, то $R \supseteq \overline{A}$, защото $\overline{R} = R$ е целозатворен. Следователно $\cap_{R \supseteq A} R \supseteq \overline{A}$.
Обратно, $\cap_{R \supseteq A} R \subseteq \overline{A}$ е еквивалентно на

$$\cup_{R \supseteq A}(F \setminus R) = F \setminus (\cap_{R \supseteq A} R) \supseteq (F \setminus \overline{A}).$$

Затова е достатъчно да проверим, че за всяко $x \in F \setminus \overline{A}$ има пръстен на нормиране $R_o \supseteq A$, който не съдържа x. Ако $x \in A[x^{-1}]$, то съществуват $a_0, a_1, \ldots, a_m \in A$, така че

$$x = a_0 + a_1 x^{-1} + \ldots + a_m x^{-m}.$$

Умножавайки с x^m получаваме цяла зависимост

$$x^{m+1} - a_0 x^m - a_1 x^{m-1} - \ldots - a_{m-1} x - a_m = 0$$

на x над A, което противоречи на $x \notin \overline{A}$. Следователно $x \notin A[x^{-1}]$ за $x \notin \overline{A}$. По този начин, $x^{-1} \in A[x^{-1}]$ е необратим елемент на $A[x^{-1}]$ и се съдържа в някакъв максимален идеал $\mathfrak{M} \triangleleft A[x^{-1}]$. Нека $\overline{k}$ е алгебричната обвивка на полето $k = A[x^{-1}]/\mathfrak{M}$. Да разгледаме естествения хомоморфизъм

$$\pi_{\mathfrak{M}} : A[x^{-1}] \longrightarrow k \subset \overline{k}|,$$

$$\pi_{\mathfrak{M}}\left(\sum_{j=0}^{n}\alpha_j x^{-j}\right)=\sum_{j=0}^{n}\alpha_j x^{-j}+\mathfrak{M}=\alpha_0+\mathfrak{M}$$

с ядро $Ker(\pi_{\mathfrak{M}}) = \mathfrak{M} \ni x^{-1}$ и образ $Im(\pi_{\mathfrak{M}}) = k$. Съгласно Теоремата за продължение, съществува пръстен на нормиране $R_o \supseteq A[x^{-1}]$ и продължение $\Phi : R_o \to \overline{k}$ на $\pi_{\mathfrak{M}} : A[x^{-1}] \to \overline{k}$, така че $Ker(\Phi) = \mathfrak{M}_o$ е максималният идеал на R_o. Но $x^{-1} \in Ker(\Phi) = \mathfrak{M}_o$ не е обратим в R_o, така че $(x^{-1})^{-1} = x \notin R_o$ и $\overline{A} = \cap_{R\supseteq A} R$, Q.E.D.

Теорема 12. *Нека k е произволно поле, а $L = k[a_1, \dots, a_n]$ е разширение на k, което е крайнопородена k-алгебра. Тогава $a_1, \dots, a_n$ са алгебрични над k.*

Доказателство: Да допуснем, че не всички a_i са алгебрични над k. След евентуална пермутация можем да считаме, че $a_1, \dots, a_m$ са трансцендентни в съвкупност над k, а $a_{m+1}, \dots, a_n$ са поотделно алгебрични над $k[a_1, \dots, a_m]$. Тогава за $\forall m + 1 \le i \le n$ съществуват естествени $d_i \in \mathbb{N}$ и полиноми $g_{i,j}(a_1, \dots, a_m) \in k[a_1, \dots, a_m]$ с $m + 1 \le i \le n$, $0 \le j \le d_i$, така че

$$g_{i,d_i}(a_1,\dots,a_m)a_i^{d_i}+g_{i,d_i-1}(a_1,\dots,a_m)a_i^{d_i-1}+\dots+g_{i,0}(a_1,\dots,a_m)=0 \quad (9.4)$$

и $g_{i,d_i}(a_1, \dots, a_m) \not\equiv 0$ за $\forall m + 1 \le i \le n$.
В качеството си на алгебрично затворено поле, алгебричната обвивка $\overline{k}$ на k е безкрайно поле. Твърдим, че съществуват $\alpha_1, \dots, \alpha_m \in \overline{k}$ с $g_{i,d_i}(\alpha_1, \dots, \alpha_m) \neq 0$ за $\forall m + 1 \le i \le n$. За целта е достатъчно да установим, че нетъждествено нулевият полином $f(a_1, \dots, a_m) = \prod\limits_{i=m+1}^{n} g_{i,d_i}(a_1, \dots, a_m)$ не се анулира в поне една точка $\alpha = (\alpha_1, \dots, \alpha_m) \in k^m$. С индукция по m, $f(a_1) = 0$ има краен брой корени. В общия случай да представим

$$f(a_1,\dots,a_m)=\sum_{j=0}^{d} f_j(a_1,\dots,a_{m-1})a_m^j$$

като полином на a_m с коефициенти $f_j(a_1, \dots, a_{m-1}) \in k[a_1, \dots, a_{m-1}]$. Съгласно $f(a_1, \dots, a_{m-1}, a_m) \not\equiv 0$ съществува $0 \le j_o \le d$ с $f_{j_o}(a_1, \dots, a_{m-1}) \not\equiv 0$. По индукционно предположение, съществува $\alpha' = (\alpha_1, \dots, \alpha_{m-1}) \in \overline{k}^{m-1}$ с $f_{j_o}(\alpha') \neq 0$. Тогава $f(\alpha', a_m) = \sum\limits_{j=0}^{d} f_j(\alpha')a_m^j \not\equiv 0$ е нетъждествено нулев полином на a_m и има краен брой корени. Това доказва съществуването на $\alpha = (\alpha', \alpha_m) \in \overline{k}^m$ с $f(\alpha) \neq 0$.
Съгласно Теоремата за разширение, Теорема 11, хомоморфизмът на пръстени $\varphi : k[a_1, \dots, a_m] \to \overline{k}$, който се ограничава до $\varphi|_k = \mathrm{Id}_k$ и трансформира a_i в $\Phi(a_i) = \alpha_i$ се продължава до хомоморфизъм $\Phi : R \to \overline{k}$ на пръстен на нормиране $k[a_1, \dots, a_m] \subseteq R \subseteq L$. Твърдим, че $a_{m+1}, \dots, a_n \in R$. Ако допуснем, че $a_i \notin R$ за някое $m+1 \le i \le n$, то $a_i^{-1} \in R$, защото $0 \neq a_i \in L$, а R е пръстен на нормиране. Още повече, a_i^{-1} принадлежи на максималния идеал $\mathfrak{M} = Ker(\Phi)$ на R, защото $a_i^{-1} \in R$ не е обратимо в R. Умножавайки (9.4) с $a_i^{-d_i}$ получаваме

$$g_{i,d_i}(a_1,\dots,a_m)+g_{i,d_i-1}(a_1,\dots,a_m)a_i^{-1}+\dots+g_{i,0}(a_1,\dots,a_m)a_i^{-d_i}=0. \quad (9.5)$$

Прилагайки Φ към (9.5) получаваме $g_{i,d_i}(\alpha_1, \dots, \alpha_m) = 0$, което е противоречие. Следователно $a_{m+1}, \dots, a_n \in R$, откъдето $L = k[a_1, \dots, a_m, a_{m+1}, \dots, a_n] \subseteq R \subseteq L$, т.е. $R = L = k[a_1, \dots, a_n]$. Но L е поле, така че ядрото на хомоморфизма $\Phi : L \to \overline{k}$ е тривиално, $\mathfrak{M} = Ker(\Phi) = \{0\}$. С други думи, $\Phi : L \to \overline{k}$ е влагане на L в $\overline{k}$, което се ограничава до $\Phi|_k \equiv \varphi|_k \equiv \mathrm{Id}_k$. Сега от алгебричността на $\overline{k}$ нас k следва алгебричността на L нас k, Q.E.D.

Приложение:

Алгебрична обвивка на поле

Ако $\sigma : K \to E$ е хомоморфизъм на полета, то или σ е влагане или $\sigma|_K \equiv 0$. Причината е в това, че ядрото $Ker(\sigma) := \{a \in K \mid \sigma(a) = 0\}$ е идеал в K, а единствените идеали на полето K са $\{0\}$ и K.
Ако $\sigma : K \to E$ е влагане на полета и $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ е полином с коефициенти от K, то образът на f под действие на σ е полиномът

$$f^{\sigma}(x) := \sum_{i=0}^{n} \sigma(c_i) x^i \in E[x]$$

с коефициенти от E.
Ще казваме, че полиномът $f(x) \in K[x]$ е нетъждествен, ако $\deg(f(x)) \geq 1$, т.е. f не принадлежи на полето от коефициенти K.

Лема 9.8. *За всеки нетъждествен полином $f(x) \in K[x]$ с коефициенти от поле K съществува разширение E на K, в което $f(x)$ има корен $\alpha \in E$.*

Доказателство: Нека $p(x)$ е неразложим над K делител на $f(x)$. Твърдим, че фактор-пръстенът $F := K[x]/\langle p \rangle$ е поле. От това, че $K[x]$ е комутативен пръстен с единица следва, че и F е комутативен пръстен с единица. Остава да докажем, че всеки ненулев елемент $g + \langle p \rangle \neq \langle p \rangle$, $g \in K[x]$ на F е обратим. Ако $g \notin \langle p \rangle$ или p не дели g, то най-големият общ делител $(p, g) = 1$, съгласно неразложимостта на $p(x)$ над K. Тъждеството на Безу $p(x)u(x) + g(x)v(x) = 1$ за подходящи полиноми $u(x), v(x) \in K[x]$ дава обратния $(g + \langle p \rangle)^{-1} = v + \langle p \rangle \in F$.
Да разгледаме естествения хомоморфизъм

$$\pi : K[x] \longrightarrow K[x]/\langle p \rangle = F.$$

Понеже $\pi(1_K) = 1 + \langle p \rangle = 1_F \neq 0_F$, ограничението $\pi : K \to (K + \langle p \rangle)/\langle p \rangle = \pi(K)$ не се анулира тъждествено. Следователно идеалът $Ker(\pi) \cap K$ на K е нулев и по теоремата за хомоморфизмите $\pi : K = K/(Ker(\pi) \cap K) \to (K + \langle p \rangle)/\langle p \rangle = \pi(K)$ е изоморфизъм.
Нека S е множество, изоморфно на $F - \pi(K)$ и непресичащо се с K. Разглеждаме множеството $E := K \cup S$ и взаимно-еднозначно изображение

$$\Phi : E = K \cup S \longrightarrow \pi(K) \cup [F - \pi(K)] = F$$

с $\Phi|_K = \pi|_K$. Определяме структура на поле върху E по такъв начин, че Φ да е изоморфизъм на полета. Това изисква $\Phi(x + y) = \Phi(x) + \Phi(y)$ и $\Phi(xy) = \Phi(x)\Phi(y)$. Затова въвеждаме събиране и умножение в E по правилата

$$x + y := \Phi^{-1}(\Phi(x) + \Phi(y)), \qquad xy := \Phi^{-1}(\Phi(x)\Phi(y)).$$

За $* = +$ или $* = .$ непосредствено следва асоциативността

$$(x * y) * z = \Phi^{-1}[\Phi(x) * \Phi(y)] * z = \Phi^{-1}\{[\Phi(x) * \Phi(y)] * \Phi(z)\} =$$
$$\Phi^{-1}\{\Phi(x) * [\Phi(y) * \Phi(z)]\} = \Phi^{-1}[\Phi(x) * \Phi(y * z)] = x * (y * z)$$

и комутативността

$$x * y = \Phi^{-1}(\Phi(x) * \Phi(y)) = \Phi^{-1}(\Phi(y) * \Phi(x)) = y * x.$$

Нулата $0_E = 0_K$ и единицата $1_E = 1_K$, доколкото

$$x + 0_K = \Phi^{-1}(\Phi(x) + \Phi(0_K)) = \Phi^{-1}(\Phi(x) + \pi(0_K)) =$$
$$\Phi^{-1}(\Phi(x) + 0_F) = \Phi^{-1}\Phi(x) = x \quad \text{и}$$
$$x1_K = \Phi^{-1}(\Phi(x)\Phi(1_K)) = \Phi^{-1}(\Phi(x)\pi(1_K)) =$$
$$\Phi^{-1}(\Phi(x)1_F) = \Phi^{-1}\Phi(x) = x.$$

Противоположният $-x = \Phi^{-1}[-\Phi(x)]$, а обратният $x^{-1} = \Phi^{-1}[\Phi(x)^{-1}]$ за $x \neq 0$, съгласно

$$x + \Phi^{-1}[-\Phi(x)] = \Phi^{-1}\{\Phi(x) + [-\Phi(x)]\} = \Phi^{-1}(0_F) = 0_E,$$

$$x\Phi^{-1}[\Phi(x)^{-1}] = \Phi^{-1}[\Phi(x)\Phi(x)^{-1}] = \Phi^{-1}(1_F) = 1_E.$$

(Тук използваме взаимната-еднозначност на Φ това, че $\Phi(0_E) = 0_F$, $\Phi(1_E) = 1_F$.) Съгласно комутативността на умножението в E десният дистрибутивен закон $x(y+z) = xy + xz$ следва от левия дистрибутивен закон

$$(x+y)z = \Phi^{-1}[\Phi(x+y)\Phi(z)] = \Phi^{-1}\{[\Phi(x) + \Phi(y)]\Phi(z)\} =$$

$$\Phi^{-1}[\Phi(x)\Phi(z) + \Phi(y)\Phi(z)] = \Phi^{-1}[\Phi(xz)] + \Phi^{-1}[\Phi(yz)] = xz + yz.$$

Следователно E е поле, а $\Phi : E \rightarrow F$ е изоморфизъм на полета.
Твърдим, че подмножеството $K \subset E$ е подполе. Изобщо, образът $\sigma(L)$ на поле L под действие на влагане $\sigma : L \hookrightarrow L_1$ е подполе, защото $\sigma(x) - \sigma(y) = \sigma(x-y) \in \sigma(L)$ за $\forall x, y \in L$ и $\sigma(x)\sigma(y)^{-1} = \sigma(xy^{-1}) \in \sigma(L)$ за $\forall x, y \in L$, $y \neq 0$. Прилагайки този факт към $\pi : K \hookrightarrow F$ получаваме, че $\pi(K)$ е подполе на F. После $\Phi^{-1} : \pi(K) \hookrightarrow E$ влага $\pi(K)$ като подполе $\Phi^{-1}\pi(K) = \Phi^{-1}\Phi(K) = K$ на E.
За да намерим корен на $f(x)$ в E, достатъчно е да намерим корен $\alpha \in E$ на $p(x)$. По определение, полиномът $p(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ принадлежи на ядрото на $\pi : K[x] \rightarrow K[x]/\langle p \rangle = F$. Следователно

$$0_F = \pi(p(x)) = \pi\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} \pi(c_i)(x + \langle p \rangle)^i = p^{\pi}(x + \langle p \rangle).$$

Това означава, че $x + \langle p \rangle \in F$ е корен на $p^{\pi}(z) \in F[z]$. Чрез изоморфизма на полета $\Phi^{-1} : F \rightarrow E$ получаваме корен $\alpha := \Phi^{-1}(x + \langle p \rangle) \in E$ на $p^{\Phi^{-1}\pi}(z) = p^{\Phi^{-1}\Phi}(z) = p(z)$. По-подробно,

$$0_E = \Phi^{-1}(0_F) = \Phi^{-1}\left(p^{\pi}(x + \langle p \rangle)\right) = \Phi^{-1}\left(\sum_{i=0}^{n} \pi(c_i)(x + \langle p \rangle)^i\right) =$$

$$\sum_{i=0}^{n} \Phi^{-1}\pi(c_i)\left[\Phi^{-1}(x + \langle p \rangle)\right]^i = \sum_{i=0}^{n} \Phi^{-1}\Phi(c_i)\alpha^i = \sum_{i=0}^{n} c_i\alpha^i = p(\alpha), \quad \text{Q.E.D.}$$

СЛЕДСТВИЕ 9.9. *За произволни нетъждествени полиноми $f_1, \ldots, f_n \in K[x]$ с коефициенти от поле K съществува разширение E на K, в което всяко f_i има корен α_i.*

Доказателство: С индукция по $1 \leq i \leq n$ ще установим съществуването на поле E_i, в което $f_1, \ldots, f_i$ имат корени $\alpha_1, \ldots, \alpha_i$. За $i = 1$ по Лема 9.8 съществува разширение E_1 на K, в което $f_1(x) \in K[x]$ има корен α_1. Да допуснем, че сме построили разширение $E_i \supset K$, в което $f_1, \ldots, f_i$ имат корени $\alpha_1, \ldots, \alpha_i$. Избираме E_{i+1} като разширение на E_i, в което $f_{i+1}(x)$ има корен α_{i+1}. Тогава $f_1, \ldots, f_i, f_{i+1}$ имат корени $\alpha_1, \ldots, \alpha_i, \alpha_{i+1} \in E_{i+1}$, Q.E.D.

ЛЕМА 9.10. (Артин) *Произволно поле K има разширение E, в което всеки нетъждествен полином $f(x) \in K[x]$ има корен $\alpha_f \in E$.*

Доказателство: За всеки нетъждествен полином $f \in K[x]$ определяме променлива X_f и означаваме с S множеството на тези променливи. Разглеждаме пръстена от полиноми $K[S]$ и идеала

$$I := \langle f(X_f) \mid f \in K[x], \quad \deg f \geq 1 \rangle$$

на $K[S]$. Твърдим, че $I \neq K[S]$. В противен случай $I = K[S]$ съществуват полиноми $f_1 \dots, f_k \in K[x]$ от степен $\deg f_i \geq 1$ и $g_1, \dots, g_k \in K[S]$, така че

$$1 = g_1 f_1(X_{f_1}) + \dots g_k f_k(X_{f_k}). \tag{9.6}$$

Полиномите $g_1, \dots, g_k$ зависят от краен брой променливи. Без ограничение на общността можем да считаме, че $X_{f_1}, \dots X_{f_k}$ са измежду тях и обединението на променливите на $g_1, \dots, g_k$ е $X_{f_1}, \dots X_{f_k}, X_{f_{k+1}}, \dots, X_{f_N}$ за някое естествено $N \geq k$. Съгласно Следствие 9.9 съществува разширение $E_1 \supset K$, така че $f_1 \dots, f_k$ имат корени $\alpha_1, \dots, \alpha_k \in E_1$. Заествайки $X_{f_i} = \alpha_i$ за $1 \leq i \leq k$ и $X_{f_i} = 0$ за $k+1 \leq i \leq N$ в (9.6) получаваме $1 = 0$. Противоречието доказва, че идеалът $I \neq K[S]$ е собствен.

За произволен максимален идеал $\mathfrak{m} \triangleleft K[S]$, съдържащ I, фактор-пръстенът $F := K[S]/\mathfrak{m}$ е поле. Естественият хомоморфизъм

$$\pi : K[S] \longrightarrow K[S]/\mathfrak{m} = F$$

се ограничава до изоморфизъм

$$\pi : K \longrightarrow (K + \mathfrak{m})/\mathfrak{m} = \pi(K),$$

доколкото $1_K \notin Ker(\pi)$ гарантира $Ker(\pi) \cap K = \{0_K\}$.

Нека Σ е множество, изоморфно на $F - \pi(K)$ и непресичащо се с K. Образуваме $E := K \cup \Sigma$ и фиксираме взаимно-еднозначно изображение

$$\Phi : E = K \cup \Sigma \longrightarrow \pi(K) \cup [F - \pi(K)] = F$$

с $\Phi|_K = \pi|_K$. Определяме събиране и умножение в E по такъв начин, че Φ да е хомоморфизъм на пръстени. По-точно,

$$x + y := \Phi^{-1}(\Phi(x) + \Phi(y)) \quad \text{и} \quad xy := \Phi^{-1}(\Phi(x)\Phi(y)) \quad \text{за } \forall x, y \in E.$$

Непосредствено се проверява, че E е поле. Подмножеството $\pi(K) \subset F$ е подполе като образ на полето K под действие на влагането на полета $\pi : K \hookrightarrow F$. Следователно $K \subset E$ е подполе като образ на полето $\pi(K)$ под действие на влагането на полета $\Phi^{-1} : \pi(K) \hookrightarrow E$. По определение, $f(X_f) \in I \subseteq \mathfrak{m} = Ker(\pi)$ за всеки нетъждествен полином $f \in K[x]$. С други думи,

$$0_F = \pi(f(X_f)) = f^{\pi}(\pi(X_f)) = f^{\pi}(X_f + \mathfrak{m})$$

или $X_f + \mathfrak{m}$ е корен на $f^{\pi}(z) \in F[z]$. Действайки с изоморфизма на полета $\Phi^{-1} : F \to E$, оттук получаваме, че

$$0_E = \Phi^{-1}(0_F) = \Phi^{-1}\left(f^{\pi}(X_f + \mathfrak{m})\right) = f^{\Phi^{-1}\pi}\left(\Phi^{-1}(X_f + \mathfrak{m})\right).$$

Полиномът f е с коефициенти от K, така че $f^{\Phi^{-1}\pi}(x) = f^{\Phi^{-1}\Phi}(x) = f(x)$. Следователно $f(x)$ има корен $\alpha := \Phi^{-1}(X_f + \mathfrak{m}) \in E$ за $\forall f \in K[x]$, $\deg f \geq 1$, Q.E.D.

Определение 9.11. *Полето L се нарича алгебрично затворено, ако всеки нетъждествен полином $f(x) \in L[x]$ с коефициенти от L има корен в L.*

Следствие 9.12. *Всяко поле K има алгебрично затворено разширение L.*

Доказателство: Съгласно Лема 9.10 съществува разширение $E_1 \supset K$, така че всеки нетъждествен полином $f(x) \in K[x]$ има корен в E_1. С индукция по $n \in \mathbb{N}$ построяваме безкрайна растяща редица от разширения

$$E_1 \subset E_2 \subset \dots \subset E_n \subset E_{n+1} \subset \dots.$$

Ако E_n е вече определено, то избираме E_{n+1} като разширение на E_n, в което всеки нетъждествен полином $f(x) \in E_n[x]$ има корен. Твърдим, че $L := \cup_{n=1}^{\infty} E_n$ е алгебрично затворено разширение на K. Наистина, за $\forall x, y \in L$ съществуват $p, q \in \mathbb{N}$, така че $x \in E_p$, $y \in E_q$. Ако $m := \max(p, q)$, то $x, y \in E_m$ и можем да определим $x+y, xy \in E_m \subset L$. За произволно $N > m$ полето E_N съдържа x, y и $x+y, xy \in E_N$ съвпадат с вече определените $x+y, xy \in E_m$, защото E_m е подполе на E_N. Множеството L с така зададените събиране и умножение е поле, защото наследява аксиомите за поле от редицата $\{E_n\}_{n=1}^{\infty}$. Всеки нетъждествен полином $f(x)) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in L[x]$, $n \geq 1$, има коефициенти $a_i \in E_{k_i}$. Ако $m := \max(k_0, k_1, \ldots, k_n)$, то $f(x) \in E_m[x]$ и има корен в $E_{m+1} \subset L$. Това установява алгебричната затвореност на L. Твърдим, че K е подполе на L, т.е. ограничението на алгебричните операции на L върху K съвпада с алгебричните операции на K. Това следва от факта, че K е подполе на E_1 и E_1 е подполе на L, Q.E.D.

Определение 9.13. *Разширението $E \supset K$ се нарича алгебрично, ако $\forall \alpha \in E$ е алгебрично над K.*

Определение 9.14. *Разширението $K(\alpha_1, \ldots, \alpha_n)$ на поле K чрез $\alpha_1, \ldots, \alpha_n$ е множеството на рационалните функции*

$$K(\alpha_1, \ldots, \alpha_n) := \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \quad | \quad f, g \in K[x_1, \ldots x_n] \right\}$$

на $\alpha_1, \ldots, \alpha_n$ с коефициенти от K.
Полето F се нарича крайнопородено разширение на своето подполе K, ако съществуват краен брой елементи $\alpha_1, \ldots, \alpha_n \in F$, така че $F = K(\alpha_1, \ldots, \alpha_n)$ е разширение на K чрез $\alpha_1, \ldots, \alpha_n$.

Твърдение 9.15. *Полето F е крайно разширение на полето K тогава и само тогава, когато $F = K(\alpha_1, \ldots, \alpha_n)$ е крайнопородено разширение на K чрез алгебрични над K елементи $\alpha_1, \ldots, \alpha_n \in F$. В такъв случай F е алгебрично разширение на K.*

Доказателство: Ако $[F : K] = d$ и $\xi_1, \ldots, \xi_d$ е базис на F над K, то крайнопороденото разширение $K(\xi_1, \ldots, \xi_d)$ на K е подполе на F, съдържащо $K\xi_1 + \ldots K\xi_d = F$, откъдето $F = K(\xi_1, \ldots, \xi_d)$. За $\forall \xi \in F$ елементите $1, \xi, \ldots, \xi^d$ на F са линейно зависими над K, така че ξ е алгебрично над K. С това установихме, че всяко крайно разширение F на K се поражда от краен брой свои алгебрични над K елементи $\xi_1, \ldots, \xi_d$ и F е алгебрично над K.
Нека $F = K(\xi_1, \ldots, \xi_d)$ се поражда от алгебрични над K елементи $\xi_1, \ldots, \xi_d \in F$. С индукция по $1 < i \leq d$ ще докажем, че $K(\xi_1, \ldots, \xi_i)$ е крайно разширение на K. Разширението $K(\xi_1) \supset K$ е крайно и степента му $[K(\xi_1) : K] = \deg_K(\xi_1) = \deg f_{\xi_1}$ е равна на степента на минималния полином f_{ξ_1} на ξ_1 над K. Да допуснем, че $[K(\xi_1, \ldots, \xi_i) : K] < \infty$ Алгебричността на ξ_{i+1} над K влече алгебричността на този елемент и над $K(\xi_1, \ldots, \xi_i)$. Полето $K(\xi_1, \ldots, \xi_i, \xi_{i+1})$ е крайно разширение на $K(\xi_1, \ldots, \xi_i)$ и степента

$$[K(\xi_1, \ldots, \xi_i, \xi_{i+1}) : K(\xi_1, \ldots, \xi_i)] = \deg_{K(\xi_1, \ldots, \xi_i)}(\xi_{i+1}).$$

Оттук степента

$$[K(\xi_1, \ldots, \xi_i, \xi_{i+1}) : K] = [K(\xi_1, \ldots, \xi_i, \xi_{i+1}) : K(\xi_1, \ldots, \xi_i)][K(\xi_1, \ldots, \xi_i) : K] < \infty$$

е крайна, Q.E.D.

Следствие 9.16. *Нека полето F е разширение на полето K. Тогава множеството F_o на алгебричните над K елементи на F е подполе на F.*

Доказателство: За $\forall a, b \in F_o$ трябва да докажем, че $a - b \in F_o$ и $ab^{-1} \in F_o$ при $b \neq 0$. Разширението $K(a, b)$ на K чрез алгебричните над K елементи a и b е алгебрично. Следователно $a - b \in K(a, b)$ и $ab^{-1} \in K(a, b)$ за $b \neq 0$ са алгебрични над K и принадлежат на F_o, Q.E.D.

Следствие 9.17. *Всяко поле K има алгебрично затворено, алгебрично над K разширение.*

Доказателство: Нека L е алгебрично затворено разширение на K. Твърдим, че подполето L_o на L, съставено от алгебричните над K елементи на L е алгебрично затворено. Наистина, произволен полином $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 \in L_o[x] \subset L[x]$ има корен $\alpha \in L$ съгласно алгебричната затвореност на L. Понеже $c_0, c_1, \ldots, c_n$ са алгебрични над K, разширението $K(c_0, c_1, \ldots, c_n) \supset K$ е крайно. От друга страна, α е алгебрично над $K(c_0, c_1, \ldots, c_n)$, така че $[K(c_0, c_1, \ldots, c_n, \alpha) : K(c_0, c_1, \ldots, c_n)] < \infty$. Оттук

$$[K(c_0, c_1, \ldots, c_n, \alpha) : K] =$$

$$[K(c_0, c_1, \ldots, c_n, \alpha) : K(c_0, c_1, \ldots, c_n)][K(c_0, c_1, \ldots, c_n) : K] < \infty.$$

Това дава алгебричността на α над K. Следователно $\alpha \in L_o$ и L_o е алгебрично затворено, Q.E.D.

Твърдение 9.18. *Нека K е поле, E е алгебрично разширение на K а $\sigma : K \hookrightarrow L$ е влагане в алгебрично затворено поле L. Тогава съществува продължение $\widetilde{\sigma} : E \hookrightarrow L$ на σ до влагане на E.*
Още повече, ако алгебричното разширение $E \supset K$ е алгебрично затворено и алгебрично затвореното поле L е алгебрично над $\sigma(K)$, то всяко влагане $\widetilde{\sigma} : E \hookrightarrow L$ е изоморфизъм.

Доказателство: Нека Σ е множеството на наредените двойки (F, τ), където $K \subseteq F \subseteq E$, а $\tau : F \hookrightarrow L$ е влагане, продължаващо $\sigma : K \hookrightarrow L$. Множеството $\Sigma \neq \emptyset$, защото $(K, \sigma) \in \Sigma$. Въвеждаме частична наредба в Σ, считайки $(F, \tau) \leq (F', \tau')$, ако F е подполе на F' и ограничението $\tau'|_F = \tau$. Ако $\{(F_\alpha, \tau_\alpha)\}_{\alpha \in A}$ е линейно наредено подмножество на Σ, то $F := \cup_{\alpha \in A} F_\alpha$ е поле с влагане $\tau : F \hookrightarrow L$, определено чрез ограниченията $\tau|_{F_\alpha} := \tau_\alpha$. Следователно (F, τ) е горна граница на $\{(F_\alpha, \tau_\alpha)\}_{\alpha \in A}$.
По Лемата на Цорн съществува максимален елемент $(E_o, \sigma_o) \in \Sigma$. Твърдим, че $E_o = E$. Допускането на противното $E_o \neq E$ води до съществуване на $\alpha \in E - E_o$. По предположение, α е алгебрично над K. Нека $f_\alpha(x) \in K[x]$ е минималният полином на α над K, а $\beta \in L$ е корен на $f_\alpha^\sigma(x) \in \sigma(K)[x]$. Тогава

$$\sigma_1 : E_o(\alpha) = E_o[\alpha] \longrightarrow \sigma_o(E_o)(\beta) = \sigma_o(E_o)[\beta],$$

$$\sigma_1\left(\sum_{i=0}^m c_i \alpha^i\right) := \sum_{i=0}^m \sigma_o(c_i)\beta^i \quad \text{за } c_i \in E_o$$

е хомоморфизъм на полета. Наистина,

$$\sigma_1\left(\sum_{i=0}^m a_i\alpha^i + \sum_{j=0}^n b_j\alpha^j\right) = \sigma_1\left(\sum_{i=0}^{\max(m,n)} (a_i + b_i)\alpha^i\right) =$$

$$\sum_{i=0}^{\max(m,n)} [\sigma_o(a_i) + \sigma_o(b_i)]\beta^i = \sigma_1\left(\sum_{i=0}^m a_i\alpha^i\right) + \sigma_1\left(\sum_{j=0}^n b_j\alpha^j\right) \quad \text{и}$$

$$\sigma_1\left(\left(\sum_{i=0}^m a_i\alpha^i\right)\left(\sum_{j=0}^n b_j\alpha^j\right)\right) = \sigma_1\left(\sum_{i=0}^{m+n}\sum_{s=0}^{i} a_s b_{i-s}\alpha^i\right) =$$

$$\sum_{i=0}^{m+n}\sum_{s=0}^{i} \sigma_o(a_s)\sigma_o(b_{i-s})\beta^i = \sigma_1\left(\sum_{i=0}^m a_i\alpha^i\right)\sigma_1\left(\sum_{j=0}^n b_j\alpha^j\right).$$

Още повече, σ_1 е изоморфизъм на полета, защото ядрото $Ker(\sigma_1) \neq E_o(\alpha)$ и образът $Im(\sigma_1) = \sigma_o(E_o)[\beta]$. Съществуването на продължение $\sigma_1 : E_o(\alpha) \hookrightarrow L$ на $\sigma_o : E_o \hookrightarrow L$ противоречи на максималността на (E_o, σ_o) и доказва, че $E_o = E$.

В частност, ако E е алгебрично затворено и L е алгебрично над $\sigma(K)$, то $\widetilde{\sigma}(E)$ е алгебрично затворено. По-точно, за произволен нетъждествен полином $f(x) \in \widetilde{\sigma}(E)[x]$ полиномът $f^{\widetilde{\sigma}^{-1}}(x) \in E[x]$ има корен $\alpha \in E$. Следователно

$$0_L = \widetilde{\sigma}(0_E) = \widetilde{\sigma}(f^{\widetilde{\sigma}^{-1}}(\alpha)) = f^{\widetilde{\sigma}\widetilde{\sigma}^{-1}}(\widetilde{\sigma}(\alpha)) = f(\widetilde{\sigma}(\alpha))$$

или $\widetilde{\sigma}(\alpha) \in L$ е корен на $f(x)$. От друга страна, L е алгебрично над $\widetilde{\sigma}(E)$, щом е алгебрично над $\sigma(K) \subset \widetilde{\sigma}(E)$. Алгебрично затвореното поле $\widetilde{\sigma}(E)$ няма нетривиални алгебрични разширения, така че $\widetilde{\sigma}(E) = L$ и $\widetilde{\sigma} : E \to L$ е изоморфизъм, Q.E.D.

Следствие 9.19. *Нека L_1 и L_2 са алгебрично затворени алгебрични разширения на поле K. Тогава съществува изоморфизъм $\tau : L_1 \to L_2$ над $\tau|_K = Id_K$.*

Определение 9.20. *Единственото с точност до изоморфизъм алгебрично затворено алгебрично разширение на поле K се нарича алгебрична обвивка на K и се бележи с $\overline{K}$.*