Полиноми на няколко променливи. Симетрични полиноми.

Нека A е комутативен пръстен с единичен елемнт 1. При построяването на пръстена от полиноми $B = A[x]$ над A се оказа, че B също е комутативен пръстен с единица, който съдържа A като подпръстен. За всеки елемент $f \in B, f \neq 0$ съществува единствено представяне $f = \sum_{i \geq 0} a_i x^i$, където $a_i \in A$ и само краен брой от тях са различни от нула. Елементът, означен с x наричаме *независима/неизвестна променлива*.

Използвайки абсолютно същата процедура, този път от B получаваме пръстен $C = B[y]$, който също е комутативен и притежава единичен елемент. В допълнение C съдържа B като подпръстен, а y е нова независима променлива. Отново е сила, че всеки ненулев елемент $g \in C$ се записва еднозначно с $g = \sum_{j \geq 0} f_j y^j$ за елементи $f_j \in B$. От представянето на елементите f_j достигаме до $g = \sum_{j \geq 0} \left(\sum_{i \geq 0} a_{ij} x^i \right) y^j = \sum_{i \geq 0, j \geq 0} a_{ij} x^i y^j$ за елементи $a_{ij} \in A$ само краен брой от които са различни от нула. От представянето на всеки елемент $g \in C$ се вижда, че $C = B[y] = A[x][y] = A[x, y]$

Ако положим $x_1 = x, x_2 = y$ и продължим по същата процедура, след общо n на брой стъпки получааме комутативният пръстен с единица $A[x_1, x_2, \ldots, x_n]$, който съдържа A като подпръстен. Всеки елемент $f \in A[x_1, x_2, \ldots, x_n]$ има вида

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1 \geq 0, i_2 \geq 0, \ldots, i_n \geq 0} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

само с краен брой ненулеви елементи $a_{i_1 i_2 \ldots i_n} \in A$, като този запис може да се опрости значително, ако се въведе мултииндекса $i = (i_1, i_2, \ldots, i_n) \in$

$\mathbb{N}^n$ и се запише

$$f = \sum_{|i| \geq 0} a_i \mathbf{x}^i,$$

където $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Полученият пръстен $A[x_1, x_2, \ldots, x_n]$ се нарича *пръстен на полиномите на n променливи с коефициенти от A*.

Елемент $f(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n]$ се нарича *полином на променливите* $x_1, x_2, \ldots, x_n$ *с коефициентиот* A и ако $f \neq 0$, то той се записва като сума на краен брой едночлени от вида $ax_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$, където $a \in A$ и $a \neq 0$, а $i_1, i_2, \ldots, i_n$ са цели неотрицателни числа. Нека друг едночлен на f има вида $bx_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}$ за елемент $b \in A, b \neq 0$ и цели неотрицателни числа $j_1, j_2, \ldots, j_n$. Тези два едночлена се наричат *подобни*, ако $i_1 = j_1, i_2 = j_2, \ldots, i_n = j_n$. Щесчитаме че в f, евентуално след извършване на приведение, няма подобни едночлени. Тогава f се представя еднозначно като сума на едночлени, които не са подобни.

Ако имаме едночлена $ax_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$, то неговата *степен* е числото $i_1 + i_2 + \cdots + i_n \geq 0$. Степента $\deg f$ на самият полином f е най-високата степен на едночлен от f. Отново, ако $f = 0$, дефинираме $\deg f = -\infty$.

<u>Пример:</u>

Да разгледаме полиномът на четири променливи

$$f = \underbrace{x_1^5x_3}_{\text{степен } 6} + \underbrace{x_1^2x_3x_4}_{\text{степен } 4} + \underbrace{x_1^5x_2}_{\text{степен } 6} + \underbrace{x_2x_4}_{\text{степен } 2} + \underbrace{x_2x_4^2}_{\text{степен } 3} + \underbrace{x_1^5}_{\text{степен } 5}.$$

Очевидно най-голямата степен на едночлен е 6 и следователно $\deg f = 6$.

Разглеждайки горния пример, който съдържа два едночлена от най-висока степен, възниква въпросът кой е старшият член на f. Отговор е възможно да се даде след въвеждането на *лексикографска наредба*. Нека $K = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}, a \neq 0$ и $L = bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}, b \neq 0$ са два едночлена на полином $f \neq 0$. Ако съществува число $i (1 \leq i \leq n)$, такова че $k_1 = l_1, \ldots, k_{i-1} = l_{i-1}$, но $k_i > l_i$, казваме, че K е по-висок от L и записваме $K > L$ (ясно е, че ако $l_i > k_i$, то $L > K$). Това е добра наредба в множеството на всички едночлени, защото за всеки два едночлена K и L е изпълнено или $K > L$, или $L > K$ и също за всеки три едночлена K, L, M от $K > L$ и $L > M$ следва $K > M$. Това означава, че всички едночлени на даден полином f могат да се наредят в низходящ ред относно релацията $>$ на едночлени (т.е. във верига). В такъв случай най-високият едночлен ще наричаме старши едночлен на f.

В примера от по-горе едночлените подреждаме в низходящ ред едночлените

$$f = x_1^5 x_2 + x_1^5 x_3 + x_1^5 + x_1^2 x_3 x_4 + x_2 x_4^2 + x_2 x_4$$

и виждаме, че старшият едночлен е $x_1^5 x_2$.

Ако A е област и $f, g \in A[x_1, x_2, \ldots, x_n]$ са ненулеви полиноми, то $\deg(fg) = \deg f + \deg g$. Така в частност от $f \neq 0, g \neq 0$ следва, че $fg \neq 0$ и $A[x_1, x_2, \ldots, x_n]$ също е област.

Лема (за старшия едночлен). *Нека A е област и $f, g \in A[x_1, x_2, \ldots, x_n]$. Тогава старшият едночлен на fg е равен на произведението на старшите едночлени на f и g.*

Доказателство. Нека имаме

$$f = \underbrace{ax_1^{k_1} \ldots x_n^{k_n}}_{\text{старши едночлен } =K} + \cdots + \underbrace{cx_1^{r_1} \ldots x_n^{r_n}}_{\text{произволен едночлен } =R} + \ldots$$

и

$$g = \underbrace{bx_1^{l_1} \ldots x_n^{l_n}}_{\text{старши едночлен } =L} + \cdots + \underbrace{dx_1^{s_1} \ldots x_n^{s_n}}_{\text{произволен едночлен } =S} + \ldots.$$

Произволен едночлен на полинома fg е $RS = cdx_1^{r_1+s_1} \ldots x_n^{r_n+s_n}$, а за едночлена KL имаме $KL = abx_1 k_1 + l_1 \ldots x_n^{k_n+l_n}$. Тъй като A е област, при предположение, че $a, b, c, d \neq 0$ получаваме, че $ab \neq 0$ и $cd \neq 0$. Твърдим, че ако $R \neq K$ или $S \neq L$, то $KL > RS$.

1 случай: $R \neq K$ и $S \neq L$. Тогава $\exists i (1 \leq i \leq n) : k_1 = r_1, \ldots, k_{i-1} = r_{i-1}$, но $k_1 > r_i$ и $\exists j (1 \leq j \leq n) : l_1 = s_1, \ldots, l_{j-1} = s_{j-1}$, но $l_j > s_j$. Нека без ограничение на общността считаме, че $i \leq j$. Тогава $l_1 = s_1, \ldots, l_{i-1} = s_{i-1}$ и или $l_i = s_i$ при $i < j$, или $l_i > s_i$ при $i = j$. Така $l_i \geq s_i$. Тогава за едночлените KL и RS имаме $k_1 + l_1 = r_1 + s_1, \ldots, k_{i-1} + l_{i-1} = r_{i-1} + s_{i-1}$, но $k_i + l_i > r_i + s_i$. Следователно $KL > RS$.

2 случай: без ограничение считаме, че $R = K$, но $S \neq L$. Тогава $k_1 = r_1, \ldots, k_n = r_n$; $l_1 = s_1, \ldots, l_{j-1} = s_{j-1}$, но $l_j > s_j$. Тогава за KL и $RS = KS$ имаме, че $k_1 + l_1 = r_1 + s_1, \ldots, k_{j-1} + lj - 1 = r_{j-1} + s_{j-1}$, но $k_j + l_j > r_j + s_j$, което означава, че отново $KL > RS$. $\square$

Казваме, че полиномът $f(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n]$ е *симетричен*, ако $f(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) = f(x_1, x_2, \ldots, x_n)$ за всяка пермутация $i_1, i_2, \ldots, i_n$ на числата от 1 до n.

За $n \in \mathbb{N}$ полиномите на n променливи

$$\begin{aligned}
&\sigma_1 = x_1 + x_2 + \dots + x_n,\\
&\sigma_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n,\\
&\dots\\
&\sigma_n = x_1x_2\dots x_n
\end{aligned}$$

се наричат *елементарни симетрични полиноми.*

Забележка 1: Ако $f(x_1, x_2, \dots, x_n)$ е симетричен полином и $K = ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ е едночлен на f, то за всяка пермутация $i_1, i_2, \dots, i_n$ на $1, 2, \dots, n$ $K' = ax_{i_1}^{k_1}x_{i_2}^{k_2}\dots x_{i_n}^{k_n}$ също е едночлен на f. Наистина, K' е едночлен на $f(x_{i_1}, x_{i_2}, \dots, x_{i_n})$, но f е симетричен и $f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = f(x_1, x_2, \dots, x_n)$. Следователно K' е едночлен и на $f(x_1, x_2, \dots, x_n)$.

Забележка 2: Ако $f(x_1, x_2, \dots, x_n)$ е симетричен и $K = ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ е старшият едночлен на f, то $k_1 \geq k_2 \geq \dots \geq k_n$. Да допуснем противното, т.е. че съществува $i(1 \leq i \leq n-1)$, такова че $k_{i+1} > k_i$. Извършваме пермутацията, състояща се в транспозицията $i \leftrightarrow i+1$ и получаваме едночлена $K' = ax_1^{k_1}\dots x_{i-1}^{k_{i-1}}x_{i+1}^{k_i}x_i^{k_{i+1}}\dots x_n^{k_n}$. Според Забележка 1 едночленът $K'' = ax_1^{k_1}\dots x_{i-1}^{k_{i-1}}x_i^{k_{i+1}}x_{i+1}^{k_i}\dots x_n^{k_n}$ също е едночлен на полинома f, но $k_{i+1} > k_i$ и следователно $K'' > K$, което противоречи на факта, че K е старшият едночлен. Следователно остава да е вярно, че $k_1 \geq k_2 \geq \dots \geq k_n$.

Лесно се съобразява, че ако g е полином на n променливи с коефициенти от A, то $g(\sigma_1, \sigma_2, \dots, \sigma_n)$ е симетричен полином на $x_1, x_2, \dots, x_n$ с коефициенти пак от A. Обратното твърдение се доказва в

Основна теорема за симетричните полиноми.. *Нека A е област и $f(x_1, x_2, \dots, x_n) \in A[x_1, x_2, \dots, x_n]$ е симетричен полином. Тогава съществува, при това единствен полином $g \in A[x_1, x_2, \dots, x_n]$, такъв че $f(x_1, x_2, \dots, x_n) = g(\sigma_1, \sigma_2, \dots, \sigma_n)$.*

Доказателство. Ще докажем само съществуването, което едновременно дава и алгоритъм за намирането на полинома g. Нека $K = ax_1^{k_1}x_2^{k_2}\dots x_{n-1}^{k_{n-1}}x_n^{k_n}$ е старши едночлен на $f = f(x_1, x_2, \dots, x_n)$ с (както видяхме) $k_1 \geq k_2 \geq \dots \geq k_{n-1} \geq k_n (\geq 0)$. Разглеждаме $\varphi_1 = a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\dots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}$

– едночлен на елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$. Ясно е че в качестото си на такъв едночлен, самият φ_1 е симетричен полином на $x_1, x_2, \ldots, x_n$. Съгласно лемата и лексикографската наредба съобразяваме, че старшият едночлен на $\varphi(x_1, x_2, \ldots, x_n)$ е едночленът $a(x_1)^{k_1-k_2}(x_1x_2)^{k_2-k_3}(x_1x_2x_3)^{k_3-k_4}\ldots(x_1x_2\ldots x_n)^{k_n}$ и в него за кое да е $1 \leq i \leq n$ степенният показател на x_i е равен на $(k_i - k_{i+1}) + (k_{i+1} - ki + 1) + \cdots + (k_{n-1} - k_n) + k_n = k_i$. С други думи видяхме, че старшият едночлен на φ_1 е $K = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$. Нека означим $f_1 = f - \varphi_1$. f_1 също е симетричен полином на $x_1, x_2, \ldots, x_n$ с коефициенти от A и старшият едночлен на f_1 е по-нисък от K. По аналогичен начин (ако $f_1 \neq 0$), ако $L = bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ е старшият едночлен на f_1, образуваме полинома $\varphi_2 = b\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\ldots\sigma_n^{l_n}$. Тогава $f_2 = f_1 - \varphi_2$ е симетричен полином на $x_1, x_2, \ldots, x_n$ с коефициенти от A и старши едночлен по-нисък от L. И така нататък, след общо s на брой стъпки получаваме поредицата от полиноми $f_1 = f - \varphi_1, f_2 = f_1 - \varphi_2, \ldots, f_{s-1} = f_{s-2} - \varphi_{s-1}, f_s = f_{s-1} - \varphi_s, \ldots$. Ако за кой да е f_i старшият му едночлен е $M = cx_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$, то $>$ и следователно $k_1 \geq m_1 \geq m_2 \geq \cdots \geq m_n$. По този начин за n-торката $m_1, m_2, \ldots, m_n$ има краен брой възможности, а именно $(k_1+1)^n$, защото всеки показател m_i може да бъде равен на кое да е от числата от 0 до k_1 за $i = 1, \ldots, n$. И така, старшите членове на полиномите f_i стават все по-ниски и има краен брой възможности за тях, т.е. редицата от тях е ограничена и $\exists s \in \mathbb{N} : f_s = 0$. Сега получаваме, че $f = \varphi_1 + \varphi_2 + \cdots + \varphi_{s-1} + \varphi_s$, което е сума на едночлени на $\sigma_1, \ldots, \sigma_n$ с коефициенти от A, което означава, че $f = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$ за някакъв полином $g \in A[x_1, x_2, \ldots, x_n]$. □

Следствие 1. *Нека F е поле, $f(x) \in F[x_1, x_2, \ldots, x_n]$ и $\alpha_1, \alpha_2, \ldots, \alpha_n$ са корените на f, лежащи в някакво разширение $K \geq F$. Ако $h(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ е симетричен полином, то $h(\alpha_1, \alpha_2, \ldots, \alpha_n) \in F$.*

Доказателство. Нека $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ за $a_i \in F, n \geq 1, a_0 \neq 0$. От теоремата следва, че съществува полином $g(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$, такъв че $g(\sigma_1, \sigma_2, \ldots, \sigma_n)$. При $x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_n = \alpha_n$ формулите на Виет дават, че $\sigma_1 = -\dfrac{a_1}{a_0}, \sigma_2 = \dfrac{a_2}{a_0}, \ldots, \sigma_n = (-1)^n\dfrac{a_n}{a_0}$. По този начин се оказва, че $h(\alpha_1, \alpha_2, \ldots, \alpha_n) = g\left(-\dfrac{a_1}{a_0}, \dfrac{a_2}{a_0}, \ldots, \dfrac{(-1)^n a_n}{a_0}\right) \in F$, понеже g е с коефициенти от F и $\dfrac{(-1)^i a_i}{a_0} \in F$ за $\forall i = 1, 2, \ldots, n$. □