Полиноми на една променлива.
Най-голям общ делител на полиноми – тъждество на Безу и алгоритъм на Евклид.
Корени на полиномите, кратни корени.
Зависимост между корени и коефициенти (формули на Виет).

❖ Полиноми с коефициенти над поле, степен на полиноми и делимост на полиноми.

(((Полиноми с коефициенти над поле)))

Нека A е комутативен пръстен с единица, а B е множеството от всички безкрайни редици $(a_0, a_1, a_2,\dots)$, в които краен брой членове са различни от 0. В множеството B въвеждаме операциите събиране $(+)$ и умножение $(.)$ по следния начин:

ако $f = (a_0, a_1, a_2, \dots)$, $g = (b_0, b_1, b_2, \dots) \in B$ полагаме $f + g = (a_0 + b_0, a_1 + b_1, \dots)$ и $f.g = (c_0, c_1, c_2 \dots)$, където $c_n = \sum_{i+j=n} a_i.b_i$, $n = 0, 1, 2, \dots$ (напр. $c_0 = a_0.b_0$, $c_1 = a_0.b_1+a_1.b_0$, $c_2 = a_0.b_2+a_1.b_1+a_2.b_0$ и т.н). С така въведените операции множеството B се превръща в комутативен пръстен с единица $(1, 0, 0, \dots)$. За да го докажем нека си въведем $h = (e_0, e_1, e_2, \dots)$ и $g.h = (d_0, d_1, d_2, \dots)$, където $d_s = \sum_{j+k=s} b_j.e_k$.
За всяко $f, g, h \in B$, са налице следните очевидни свойства:

1. $f + g = g + f$
2. $(f + g)+h=f+(g + h)$
3. съществува нулев елемент $0 = (0, 0, 0, \dots) \in B$: $f + 0 = 0 + f = f$
4. съществува противоположен елемент $-f$: $-f = (-a_0, -a_1, -a_2, \dots) \in B$

Така, за да докажем, че B е комутативен пръстен, трябва да покажем асоциативността, комутативността и двата дистрибутивни закона за умножение, както и съществуването на единичен елемент.

5. Асоциативност на умножението:

Нека $(f.g).h = (p_0, p_1, p_2, \dots)$, $f.(g.h) = (p_0', p_1', p_2' \dots)$

$$p_m = \sum_{n+k=m} c_n.e_k = \sum_{n+k=m} (\sum_{i+j=n} a_i.b_j)\, e_k = \sum_{i+j+k=m} a_i.b_j.e_k$$

$$p_m' = \sum_{i+s=m} a_i.d_s = \sum_{i+s=m} a_i .(\sum_{j+k=s} b_j.e_k) = \sum_{i+j+k=m} a_i.b_j.e_k$$

Следователно $p_m = p_m'$ за всяко $m = 0, 1, 2 \dots$ т.е. $(f.g).h = f.(g.h)$

6. Дистрибутивни закони:

Нека $g + h = v$, $v = (b_0 + e_0, b_1 + e_1, \dots)$, $f.v = w$,

$$w = f.(g + h) \Rightarrow w_q = \Sigma_{i+k=q}\, a_i.v_k = \Sigma_{i+k=q}\, a_i.\,(b_k + e_k) = \Sigma_{i+k=q}\,(a_i.b_k + a_i.e_k) =$$

$$= \Sigma_{i+k=q}\, a_i.b_k + \Sigma_{i+k=q}\, a_i.e_k = f.g + f.h$$

Аналогично и за другия дистрибутивен закон: $(f + g).h = f.\,h + g.\,h$

7. Комутативност на умножението:
Нека $f.g = v$, $g.f = l$, тогава

$$f.g = v \Rightarrow v_n = \Sigma_{i+j=n}\, a_i.b_j$$

$$g.f = l \Rightarrow l_n = \Sigma_{i+j=n}\, b_j.a_i$$

$$\Rightarrow v = l \Rightarrow f.g = g.f$$

8. За единичен елемент на пръстена B си избираме $e = (1, 0, 0, \dots)$. От дефиницията за единичен елемент то $f.e = e.f = f \in B$, което лесно се вижда, че е вярно.

От всичко до тук => B е комутативен пръстен с единица.

Нека с A_0 означим подмножеството на B състоящо се от всички редици от вида $(a, 0, 0 \dots)$, $a \in B$. От тук следва, че A_0 е подпръстен на B. Да разгледаме изображението $\varphi : A \to A_0$, дефинирано с равенството $\varphi(a) = (a, 0, 0, \dots)$. Очевидно φ е биекция и освен това $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(a.b) = \varphi(a)\varphi(b)$. Следователно φ е изоморфизъм между $A \to A_0$. Благодарение на този изоморфизъм можем да отъждествяваме A с A_0 и да считаме, че A е подпръстен на B. По-нататък вместо **(a, 0, 0 …)** ще пишем само **a.**

Нека с **x** означим редицата $(0, 1, 0, 0, \dots)$. От правилата за умножение в пръстена B следва, че $x^2 = (0, 0, 1, 0, \dots)$, $x^3 = (0, 0, 0, 1, \dots)$ и изобщо $x^n = (0, \dots 0, 1, 0, \dots)$ като 1 стой на $(n + 1)$-вото място. Освен това, ако $a \in A$, то $a.x^n = (0, \dots 0, a, 0, \dots)$, като a стой на $(n + 1)$-во място.

Нека $f = (a_0, a_1, a_2, \dots a_n \dots)$ и a_n е последният ненулев член в тази редица. Тогава

$$f = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0 \dots 0, a_n, 0 \dots) = a_0 + a_1.x + \dots + a_n.x^n$$

Така стигнахме до познатия вид на полиномите. Пръстенът B означаваме с $A[x]$ и ще наричаме пръстен на полиномите на една променлива x с коефициенти от A, или по-просто полиномиален пръстен над A, а елементите му ще наричаме полиноми. С горната формула всеки полином се записва по единствен начин и познатите ни операции събиране и умножение се извършват също по познатия начин.

Без изменение се пренасят познатите понятия като:

- коефициент - това са a_0 , a_1 , a_2 и т.н.;

- свободен член - това е a_0;

- едночлен от ***i***-та степен – $a_i.x^i$

(((Степен на полиноми и делимост на полиноми)))

Числото ***n*** се нарича степен на полинома ***f*** и се бележи с ***deg f***. Така всеки ненулев полином има степен, която е естествено число или ***0***. Полиномите от степен ***0*** ще наричаме константи и ще считаме, че нулевият полином (т.е. нулевият елемент на ***A***) има степен $-\infty$.

За всеки два полинома $f, g \in B = A[x]$ са в сила следните свойства:

1. $deg\ (f+g) \leq max\{deg\ f, deg\ g\}$
2. $deg\ (f.g) \leq deg\ f + deg\ g$

Ако събираме полиноми съответно от ***m***-та и ***n***-та степен. не можем да получим полином със степен, по-голяма от по-голямата от двете степени. Но пък ако $m = n$ и коефициентите пред най-високата степен са противоположни елементи, съответно ще получим по-малка степен на резултата.

(((Пример:

$f = 2.x^3 + 105x^2 + 1$

$g = -2.x^3 + 10x^1 + 13$

$f + g = 105x^2 + 10x^1 + 14$, т.е $\deg (f + g) = 2 < 3 = \max \{\deg f, \deg g\}$)))

Второто свойство не е толкова ясно. Степента на произведението на два полинома е сума от степените им. При произведение на полиноми с коефициенти от Z_n може да се получат делители на ***0*** и да се получи полином с по-малка степен.

(((Пример:

$f = 3.x^2 + 1$

$g = 2.x^3$

$f.g = 6x^5 + 2x^3$, т.е $\deg (f.g) = 5 = 2 + 3 = \deg f + \deg g$

Z_6 - комутативен пръстен с единица:

$f = \overline{2}x + 1 \in Z_6[x]$
$g = \overline{3}x \in Z_6[x]$
$fg = \overline{2}.\overline{3}x^2 + \overline{3}x = \overline{6}x^2 + \overline{3}x = \overline{3}x$

$\deg\ fg = 1 < 2 = \deg\ f + \deg\ g$)))

<u>Теорема - За делене с частно и остатък:</u>

Нека F е поле и $f, g \in F[x]$, $g \neq 0$. Тогава съществува единствена двойка полиноми $q, r \in F[x]$, такива че $f = g.q + r$ и $\deg r < \deg g$ (прието е да се казва, че сме разделили f на g с частно q и остатък r).

<u>Д-во:</u>

Съществуване: Провеждаме индукция по $n = \deg f$

I. 1) Ако $f = 0$, т.е това е случаят $n = -\infty$, то тогава $f = 0 = 0.g + 0$, от където следва, че $q = 0, r = 0$

2) Ако $\deg f < \deg g$, то тогава $f = 0.g + f$, т.е. $q = 0, r = f$

3) Ако $\deg f = 0 = \deg g$, тогава $f = g.(f.g^{-1}) + 0$ и $q = f.g^{-1}, r = 0$

Базата е доказана/показана.

II. Нека е доказано за всички полиноми f: $\deg f < n$

III. Нека $\deg f = n$

1) Ако $\deg f < \deg g \rightarrow$ точка I.2.
2) Ако $\deg f \geq \deg g$

$f = a_0 + a_1.x^1 + \ldots + a_n.x^n$

$g = b_0 + b_1.x^1 + \ldots + b_m.x^m$, $n \geq m$
Тук си харесваме следния полином:

$h = a_n.b_m^{-1}.x^{n-m}.g$
Като заместим g в записа на h получаваме следното:

$h = a_n.b_m^{-1}x^{n-m}b_0 + a_n.b_m^{-1}x^{n-m}b_1.x + \ldots + a_n.b_m^{-1}x^{n-m}b_m.x^m$
последният едночлен е $a_n.x^n$, т.е. степента на h е n и освен това старшият коефициент е a_n. Затова си образуваме разликата:
$\mathbf{s = f - h = f - a_n.b_m^{-1}x^{n-m}.g}$

Тъй като коефициентите пред най-високите степени на f и на h са противоположни елементи на полето $F[x]$, следва че $deg\ s < deg\ f = n$.

От индукционното допускане (II.), следва че

съществуват q_1, r_1: $s = q_1.g + r_1, deg\ r_1 < deg\ g$

$s = f - h = f - a_n.b_m^{-1}.x^{n-m}.g = q_1.g + r_1 \Rightarrow f = (a_n.b_m^{-1}.x^{n-m} + q_1).g + r_1, \quad deg\ r_1 < deg\ g$

Получихме, че наистина съществуват полиномите q, r такива, че $f = q.g + r$ и

$deg\ r < deg\ g$

Единственост: Допускаме, че

$f = g.\ q_1 + r_1, deg\ r_1 < deg\ g$

$f = g.\ q_2 + r_2, deg\ r_2 < deg\ g$

Като извадим двете равенства получаваме:

$0 = g.(q_1 - q_2) + r_1 - r_2 \Leftrightarrow g.(q_1 - q_2) = r_2 - r_1$ *(1)*

$deg\ (r_2 - r_1) \leq max\{deg\ r_1, deg\ r_2\} < deg\ g$ *(2)*

Ако $q_1 - q_2 \neq 0 \Rightarrow deg\ (g(q_1 - q_2)) = deg\ g + deg\ (q_1 - q_2) \geq deg\ g$ *(3)*

От (1) получаваме, че (2) = (3), които всъщност не са равни и се получава противоречие.

$\Rightarrow q_1 - q_2 = 0 \Leftrightarrow q_1 = q_2 \Rightarrow r_1 = r_2,$

т.е. частното и остатъкът са единствени.

❖ **Определение на най-голям общ делител на два полинома НОД(h(x), g(x)) = (h(x), g(x)), теорема за съществуване на най-голям общ делител на два полинома с коефициенти над поле, изразяване на НОД (h(x), g(x)) чрез полиномите h(x) и g(x) (тъждество на Безу), алгоритъм на Евклид.**

<u>Опр. – Делимост на полиноми :</u>

Нека $f, g \in F[x]$ и F е поле. Казаме, че полиномът g дели полинома **f**, когато $f = g.h$, като $h \in F[x]$. Записваме $g \mid f$.

Следващите няколко свойства следват директно от определението .

<u>С-ва:</u>

1. $f \mid f, \quad f \mid \alpha.f, \quad f \mid g.f$
2. $g \mid f, \quad f \mid g \Rightarrow g = \alpha . f \; (\alpha \in F, \alpha \neq 0)$
3. $f \mid g, g \mid h \Rightarrow f \mid h$
4. $f \mid g_1, f \mid g_2 \Rightarrow f \mid (u_1 g_1 + u_2 g_2)$
5. $f \mid 0$
6. $f \mid g$ *и* $g \neq 0 \Rightarrow \deg f \leq \deg g$

<u>(((Доказателство – Св. 2:</u>

$f \mid g \Rightarrow g = f.h; \quad g \mid f \Rightarrow f = g.t \Rightarrow g = (g.t).h = g(t.h) \Rightarrow g(1 - t.h) = 0$

$\Rightarrow 1 = t.h \Rightarrow \deg t = \deg h = 0, \quad g = \alpha . f, \alpha \in F)))$

<u>Опр. – Най-голям общ делител:</u>

Нека F е поле и $f, g \in F[x]$, като $f(x) \neq 0$ или $g(x) \neq 0$. Най-големият общ делител на f и g е $d \in F[x]$, ако:

1. $d \mid f$ и $d \mid g$
2. и при $d_1 \mid f$ и $d_1 \mid g$, то $d_1 \mid d$

Записваме - $НОД\,(f, g) = (f, g) = d$

<u>Теорема – За съществуване на НОД на два полинома с коефиценти над поле</u>

Нека $F[x]$ е поле. Всеки два полинома $f, g \in F[x]$ притежават най-голям общ делител във $F[x]$.

Д-во:

Ако $f(x) = g(x) = 0$, тогава НОД е нулевият полином – така всеки полином от F е общ делител на f и g, но единствено нулевият полином удовлетвотява второто условие за НОД.

Поради това предполагаме, че поне единият от f и g е ненулев *(*)*.

Дефинираме си подмножеството $M =\{u.f + v.g \mid u, v \in F[x]\}$

Като положим $u = 1$ и $v = 0$, получаваме че $f \in M$, а при $u = 0$ и $v = 1$ $\Rightarrow g \in M$. Слевователно и 2-та полинома са от M. От *(*)* става ясно, че в M има ненулеви полиноми. Измежду тях избираме такъв ненулев полином d, който има най-ниска възможна степен.

$deg(d) \leq deg(h)$, за всеки ненулев полином $h \in M$ *(**)*.

От $d \in M$ следва, че $d = u_1.f + v_1.g$ *(***)*

Ще докажем, че d е НОД на f и g. Тъй като M е подмножество се съдържа в $F[x]$, то $d \in F[x]$.

1. Защо d е общ делител на f и g

   Допускаме, че d не дели f $\Rightarrow f = d.q + r$, където $r \neq 0$ и $deg(r) < deg(d)$. Като използваме *(***)* получаваме

   $r = f - d.q = f - (u_1.f + v_1.g).q = (1 - u_1.q).f + v_1.q.g$

   $\Rightarrow r = u.f + v.g$

   $\Rightarrow r \in M$, т.е. полиномът принадлежи на множеството **M** и има по-малка степен от d, което противоречи на *(**)*. От тук следва, че d дели f. По същият начин се доказва, че d дели g.

2. Нека d_1 дели f и g. От *(***)* следва, че d_1 дели d.

   (И теоремата е доказана.)

   От доказателството се вижда, че ако $(f, g) = d$ съществуват полиноми u и v, такива че $u.f + v.g = d$. Прието е това равенство да се нарича ***<u>Тъждество на Безу</u>***

<u>Опр. - Взаимно прости полиноми:</u>

Два полинома f и g се наричат взаимно прости, ако $НОД(f, g) = 1$

Твърдения:

Нека F е поле и $f, g \in F[x]$, като $НОД(f, g) = 1$. Тогава

1) $f \mid h, g \mid h \Rightarrow f.g \mid h$
2) $f \mid g.t \Rightarrow f \mid t$

Алгоритъм на Евклид за намиране на НОД (f, g):

Дадено: $f, g \in F[x], g \neq 0$

Резултат: $d \in F[x], d = (f, g)$

Процедура: $f = q_1.g + r_1, \deg r_1 < \deg g,$

$НОД (f, g) = НОД (g, r_1)$

Д-во:

От горе се вижда, че $r_1 = f - q_1.g$
Нека $d_1 = (f, g)$ и $d_2 = (g, r_1)$. Тогава

$d_1 \mid f \quad \& \quad d_1 \mid g \Rightarrow d_1 \mid u_1 f + u_2 g \Rightarrow d_1 \mid 1.f - q_1 g \Rightarrow d_1 \mid r_1$

Тъй като $d_1 \mid g \quad \& \quad d_1 \mid r_1 \Rightarrow d_1 \mid d_2$

Аналогично $d_2 \mid g \quad \& \quad d_2 \mid r_1 \Rightarrow d_2 \mid u_1 g + u_2 r_1 \Rightarrow d_2 \mid q_1 g + 1.r_1 \Rightarrow d_2 \mid f$
и от $d_2 \mid f \quad \& \quad d_2 \mid g \Rightarrow d_2 \mid d_1$

$d_1 \mid d_2 \quad \& \quad d_2 \mid d_1 \Rightarrow d_1 = \alpha.d_2$

Ако $r_1 = 0$, то $НОД(f, g) = g$
Иначе, ако $r_1 \neq 0$, то $g = q_2.r_1 + r_2$, като $\deg r_2 < \deg r_1$
$НОД(g, r_1) = НОД (r_1, r_2)$

Ако $r_2 = 0 \Rightarrow d = r_1$ и т.н. процесът се повтаря.

Имаме краен брой стъпки, т.е на някоя стъпка ще получим нулев остатък. Най-големият общ делител ще е последният ненулев остатък.

❖ **Корени на полиномите – правило на Хорнер, кратни корени критерий за определяне на кратност на корен чрез производните на полинома. Формули на Виет.**

Опр. - Корен на полином

Нека $f(x) \in F[x]$ е произволен полином. $\alpha \in F$ се нарича корен на полинома $f(x)$**,** ако е изпълнено, че $f(\alpha) = 0$.

Твърдение:

Ако α е корен на полинома $f(x)$ то е в сила $x - \alpha \mid f(x)$. (проверява се тривиално с теоремата за делене с частно и остатък).

Д-во:

Нека положим $g(x) = x - \alpha$. Тогава $f(x) = g(x) . q(x) + r(x)$, от където следва

$deg(r) < deg (g) = 1$

$\Rightarrow deg(r) = 0 \Rightarrow f(x) = (x - \alpha).q(x) + r$ и при $x = \alpha$ получаваме

$f(\alpha) = 0 = (\alpha - \alpha).q(x) + r = 0.q(x) + r \Rightarrow r = 0 \Rightarrow (x - \alpha) \mid f(x)$

***Опр. - к-кратен корен*:**

Нека $f(x) \in F[x]$ е произволен полином. Казваме, че $\alpha \in F$ е k-кратен корен на полинома $f(x)$, ако е изпълнено, че:

$(x - \alpha)^k \mid f(x)$ и $(x - \alpha)^{k+1} \nmid f(x)$

Опр. - Производна:

Нека $f(x) = a_0.x_n + a_1x_{n-1} + \ldots + a_n$ е произволен полином над $F[x]$. Тогава

$f'(x) = a_0nx^{n-1} + a_1(n-1)x^{n-2} + \ldots + a_{n-1}$ се нарича производна на полинома $f(x)$.
Под a_0n разбираме n-кратното на a_0, т.е. сбора n пъти a_0.

С-ва:

- $(c.f(x))' = c.f'(x)$
- $(f + g)' = f' + g'$
- $(f.g)' = f'.g + f.g'$

Твърдение:

Нека $char\ F = 0$, $f(x) \in F[x]$ е произволен полином и K е разширение на F като $\alpha \in K$.

α е k-кратен корен тогава и само тогава, когато ($\Leftrightarrow$) $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ и $f^{(k)}(\alpha) \neq 0$

Д-во:

($\Rightarrow$) Нека α е k-кратен корен на f. Искаме да докажем, че

$f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ и $f^{(k)}(\alpha) \neq 0$.

Ще проведем индукция по k.

Ако $k = 1$, то $f = (x - \alpha).g$, $g \in K$ и $g(\alpha) \neq 0$. Тогава

$f' = g + (x - \alpha).g'$, $f'(\alpha) = g(\alpha) \neq 0 \quad \Rightarrow f(\alpha) = 0,\ f'(\alpha) \neq 0$

Нека $k > 1$ и твърдението е вярно за числа по-малки от k. Имаме

$f = (x - \alpha)^k.g$, $g \in K$ и $g(\alpha) \neq 0 \quad \Rightarrow$

$f' = k.(x - \alpha)^{k-1} g + (x - \alpha)^k.g' = (x - \alpha)^{k-1}(k.g + (x - \alpha)g') = (x - \alpha)^{k-1}.g_1$,

$g_1 = k.g + (x - \alpha)g' \Rightarrow g_1(\alpha) = k.g(\alpha) \neq 0$ (използваме, че $char\ F = 0$)

Следователно α е $(k-1)$-кратен корен на полинома f'. Сега твърдението следва от индукционното предположение.

($\Leftarrow$) Нека $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ и $f^{(k)}(\alpha) \neq 0$. Нека α е l-кратен корен на f.

Ако $l < k$, то $l \leq k - 1$ и значи $f^{(l)}(\alpha) = 0$ - противоречие с първата част на теоремата. Ако $l > k$, то $l - 1 \geq k$ и от първата част на теоремата следва $f^{(k)}(\alpha) = 0$, отново противоречие.

$\Rightarrow l = k$, т.е α е k-кратен корен на f. Теоремата е доказана

Правило на Хорнер:

Ако $F[x]$ е комутативен пръстен с единица и

$f(x) = a_0.x^n + a_1x^{n-1} + \ldots + a_n$, $g = x - \alpha \in F[x]$. И $f = q.g + r$, където $deg(r) < deg(g)$ и $q(x) = b_0.x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}$, то коефициентите на частното q и остатъка r се получават по формулите:

$b_0 = a_0,$

$b_1 = a_1 + \alpha.b_0,$

$b_2 = a_2 + \alpha.b_1,$

………

$b_{n-1} = a_{n-1} + \alpha.b_{n-2}$

$r = a_n + \alpha.b_{n-1}$

Д-во:

$f(x) = a_0.x^n + a_1x^{n-1} + \ldots + a_n, \ f(\alpha) = a_0.\ \alpha^n + a_1\,\alpha^{n-1} + \ldots + a_n \ \Rightarrow$

$f(x) - f(\alpha) = a_0.\ (x^n - \alpha^n) + a_1\,(x^{n-1} - \alpha^{n-1}) + \ldots + a_{n-1}\,(x - \alpha) = (x - \alpha).\ q(x) \quad \Rightarrow$

$f(x) = (x - \alpha).\ q(x) + f(\alpha) = (x - \alpha)\,(b_0.x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + f(\alpha) \qquad (r = f(\alpha))$

$a_0.x^n + a_1x^{n-1} + \ldots + a_n = (x - \alpha)\,(b_0.x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + f(\alpha) \Rightarrow$

$a_0.x^n + a_1x^{n-1} + \ldots + a_n = b_0.x^n + (b_1 - \alpha.b_0).x^{n-1} \ldots .. + f(\alpha) - \alpha.b_{n-1}$

Като приравним коефициентите от ляво и от дясно получаваме формулите от правилото на Хорнер.

<u>Формули на Виет:</u>

Формулите на Виет свързват корените на даден полином с неговите коефициенти.
Нека $f(x) = a_0.x^n + a_1x^{n-1} + \ldots + a_n$ е произволен полином от $F[x]$.
Нека $\beta_1, \beta_2, \ldots \beta_n$ са всичките му корени в някакво разширение $K \supset F$. Тогава:

$$\begin{array}{lcll}
\sum_i \beta_i & = & \beta_1 + \beta_2 + \cdots + \beta_n & = -\frac{a_1}{a_0} \\
\sum_{i<j} \beta_i\beta_j & = & \beta_1\beta_2 + \beta_1\beta_3 + \cdots + \beta_1\beta_n + \beta_2\beta_3 + \cdots + \beta_{n-1}\beta_n & = \frac{a_2}{a_0} \\
\vdots & & & \\
\prod_i \beta_i & = & \beta_1\beta_2\cdots\beta_n & = (-1)^n\frac{a_n}{a_0}
\end{array}$$

Д-во:

Полиномът $f(x)$ може да бъде разложен по следния начин в разширението $K \supset F$, в което се намират всичките му корени:

$f(x) = a_0.(x - \beta_1)\,(x - \beta_2) \ldots .\,(x - \beta_n)$

Разкриваме скоботе:

$$
\begin{aligned}
f(x) &= a_0.(x-\beta_1)(x-\beta_2)\ldots.(x-\beta_n)\\
&= a_0x^n\\
&+ a_0x^{n-1}(-1).(\beta_1+\beta_2+\ldots+\beta_n)\\
&+ a_0x^{n-2}(+1).(\beta_1.\beta_2+\beta_1.\beta_3\ldots+\beta_{n-1}.\beta_n)\\
&\ldots\ldots\ldots\\
&+ a_0(-1)^n.(\beta_1.\beta_2\ldots.\beta_n)
\end{aligned}
$$

Сега просто използваме, че коефициентите на 2 полинома, които са еднакви (в нашия случай – написани по 2 различни начина) съвпадат, т.е. коефициентът пред дадена степен в едното представяне е равен на кофициента пред същата степен в другото представяне. С това теоремата е доказана.

[--]

<u>Опр. - ГРУПА</u>

*Едно непразно множество **G** с бинарна операция умножение (.) се нарича група, ако:*

*1. Операцията е асоциативна, т.е. за всеки елемент **a, b, c** е изпълнено **(ab)c = a(bc).***

*2. Съществува неутрален елемент относно операцията, т.е. такъв елемент **e** $\in$ **G,** че за всеки елемент **a** $\in$ **G** е изпълнено **a.e = e.a = a.** Нарича се единичен елемент на **G** или единица*

*3. За всеки елемент **a** $\in$ **G** съществува елемент **a'** $\in$ **G,** т.че **a.a' = a'.a = e.** Нарича се обратен елемент на **a** и ще го бележим с a^{-1}.*

<u>Опр. - ПРЪСТЕН:</u>

*Нека **K** е непразно множество, в което са дефинирани следните две операции:*

- ***първата** на всеки два елемента **a, b** $\in$ **K** съпоставя елемент **a + b** $\in$ **K,** който се нарича сума на **a** и **b***
- ***втората** на всеки два елемента **a, b** $\in$ **K** съпоставя елемент **a.b** $\in$ **K**, който се нарича произведение на **a** и **b***

*Казваме, че относно тези операции **K** е пръстен, ако са изпълнени следните условия:*

(1) ***(a + b) + c = a + (b + c)*** *- асоциативност на събирането*
(2) ***a + b = b + a*** *- комутативност на събирането*
(3) *съществува нулев елемент **0** $\in$ **K** такъв, че **a + 0 = a**, за всяко **a** $\in$ **K***
(4) *за всяко **a** $\in$ **K** съществува противоположен елемент **–a** $\in$ **K** такъв, че **a + (-a) = 0***
(5) ***(a.b).c = a.(b.c)*** *- асоциативност на умножението*
(6) ***(a + b).c = ac + bc*** *- дясна дистрибутивност на умножението*
(7) ***c.(a + b) = ca + cb*** *- лява дистрибутивност на умножението*

<u>Опр. – КОМУТАТИВЕН ПРЪСТЕН:</u>

*Нека **M** е пръстен. Ако* $ab = ba, \ \forall a, b \in M \Longrightarrow$ ***M** е комутатативен пръстен.*

<u>Опр. – ПРЪСТЕН С ЕДИНИЦА:</u>

*Нека **M** е пръстен. Ако* $\exists e \in M : \ ae = ea = a, \ \forall a \in M \Longrightarrow M$ *е пръстен с единица.*

<u>Опр. – ПОЛЕ:</u>

Нека К е комутативен пръстен с единица. Казваме, че К е поле, ако всеки ненулев елемент на К е обратим.

Опр. – РАЗШИРЕНИЕ НА ПОЛЕ:

*Ако едно поле **F** се съдържа изцяло в полето **K** ще казваме, че **K** е разширение на полето **F**. **F** е подполе на полето **K**.*

Опр. – ХАРАКТЕРИСТИКА НА ПОЛЕ:

*Нека **F** е поле и **e ϵ F** е единичният му елемент. Казваме, че полето има крайна характеристика, ако за никое естествено чилсло **n** имаме **n.e = 0**. Най-малкото естествено число **n**, за което това е вярно се нарича характеристика на полето и се бележи с **char(F).***

Опр. – ИЗОБРАЖЕНИЕ:

*Ако **f** е изображение (функция) от множеството **X** към (или в) множеството **Y,** **f** е правило, по което на всеки елемент от **X** е съпоставен елемент от **Y.** Означава се **f: X → Y***

- *сюрекция - покрива всички елементи на **Y;***
- *инекция – най-много един съответстващ елемент;*
- *биекция – едновременно сюрекция и инекция;*

Опр. – ИЗОМОРФИЗЪМ:

Биекция, при която връзките между елементите на крайното множество са същите, както тези на съответстващите им елементи в началното множество се нарича изоморфизъм.