

Лекция 0

§0. Комплексни числа и полиноми

1. Определение и аритметични операции. Комплексно число се нарича наредената двойка (x, y) от реални числа x и y . Две комплексни числа (x_1, y_1) и (x_2, y_2) са равни когато $x_1 = x_2$ и $y_1 = y_2$. Между комплексните числа са определени аритметичните действия събиране и умножение,

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
$$(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

Комплексното число от вида $(x, 0)$ може да бъде отъждествено с реалното число x , понеже има съгласуваност между аритметичните операции, $(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0)$ и $(x_1, 0)(x_2, 0) = (x_1x_2, 0)$. Комплексното число $(0, 1)$ се нарича **имагинерна единица** и се бележи с i , $i = (0, 1)$. По формулата за умножение имаме

$$i^2 = ii = (0, 1)(0, 1) = (-1, 0) = -1.$$

Освен това $(0, y) = (0, 1)(y, 0) = iy$, следователно всяко комплексно число може да се запише във вида

$$(x, y) = (x, 0) + (0, y) = x + iy,$$

или $z = x + iy$, където z е означение за комплексното число. Записът $z = x + iy$ се нарича **алгебрична форма** на запис на комплексното число z . Ако е дадено комплексното число $z = x + iy$, то реалното число x се нарича **реална част** на z , а реалното число y се нарича **имагинерна част** на z , при което използваме следните означения $x = \operatorname{Re} z$ и $y = \operatorname{Im} z$. Комплексното число $x - iy$ се нарича **комплексно спрегнато** на $z = x + iy$ и се бележи със \bar{z} , $\bar{z} = x - iy$. Очевидно $\bar{\bar{z}} = z$ и освен това $\bar{z} = z$ тогава и само тогава, когато z е реално число ($\operatorname{Im} z = 0$).

Величината $|z| = \sqrt{x^2 + y^2}$ се нарича **модул** на комплексното число z . Лесно се вижда, че $z\bar{z} = |z|^2$, т.е. $|z| = \sqrt{z\bar{z}}$. Да отбележим равенството $|z| = |\bar{z}|$.

Ако $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$, то в алгебричен запис събирането и умножението имат вида $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$ и $z_1z_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2)$.

Аритметичните операции имат свойства, напълно аналогични на тези при реалните числа,

$$z_1 + z_2 = z_2 + z_1 \text{ и } z_1z_2 = z_2z_1 \text{ (комутативност),}$$
$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3) \text{ и } (z_1z_2)z_3 = z_1(z_2z_3) \text{ (асоциативност),}$$
$$z_1(z_2 + z_3) = z_1z_2 + z_1z_3 \text{ (дистрибутивност).}$$

Аритметичните действия между комплексни числа извършваме следвайки познатите правила за работа с реалните числа и факта, че $i^2 = -1$. Например за умножението имаме

$$(x_1 + iy_1)(x_2 + iy_2) = x_1x_2 + ix_1y_2 + iy_1x_2 + i^2y_1y_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).$$

Нулата в множеството на комплексните числа е комплексното число $(0, 0) = 0 + i0$, а единицата е комплексното число $(1, 0) = 1 + i0$ и те играят същата роля както нулата и единицата в множеството на реалните числа.

Множеството на комплексните числа ще означаваме с \mathbb{C} (множеството на реалните числа се означава с \mathbb{R}).

В множеството \mathbb{C} е определена и аритметичната операция деление, при което може да се дели на всяко комплексно число, различно от нула. Определяме $\frac{z_1}{z_2}$ като

единственото комплексно число z , за което $z_2 z = z_1$. След умножаване последното равенство с \bar{z}_2 получаваме $(\bar{z}_2 z_2)z = z_2 z_1$, откъдето намираме

$$z = \frac{z_1}{z_2} = \frac{z_1 \bar{z}_2}{z_2 \bar{z}_2} = \frac{z_1 \bar{z}_2}{|z_2|^2} = \frac{(x_1 + iy_1)(x_2 - iy_2)}{x_2^2 + y_2^2} = \frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2} + i \frac{-x_1 y_2 + y_1 x_2}{x_2^2 + y_2^2}.$$

Множеството на комплексните числа \mathbb{C} е **числово поле**, понеже в него са определени двете аритметични операции събиране(изваждане) и умножение(деление) с указаните свойства на комутативност, асоциативност и дистрибутивност, при което може да се дели на всяко различно от нула число. Множеството на реалните числа \mathbb{R} и на рационалните числа \mathbb{Q} също са числови полета. Съществуват и числови полета с краен брой елементи.

Множеството на комплексните числа \mathbb{C} може да се отъждестви с точките в една равнина (**комплексна равнина**) снабдена с декартова координатна система с оси x и y с начало точката $O(0,0)$ (Рис. 0.1), при което на комплексно спрегнатото $\bar{z} = x - iy$ съответства точка, която е симетрична на $z = x + iy$ относно абсцисната ос, която се нарича още **реална ос** на комплексната равнина \mathbb{C} .

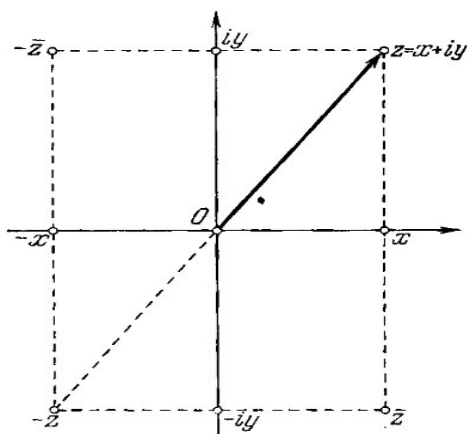


Рис. 0.1.

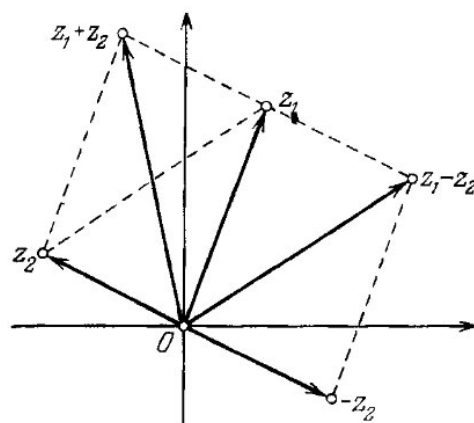


Рис. 0.2.

Ординатната ос се нарича **имагинерна ос**. Комплексното число z се отъждествява още и с неговия радиус вектор, с начало в точката O и край в точката z , при което дължината на този вектор е точно $|z|$. Аритметичните действия събиране и изваждане на двете числа z_1 и z_2 се съгласуват със събирането и изваждането на съответните вектори по **правилото на успоредника** (Рис. 0.2).

Разстоянието между точките z_1 и z_2 е равно на дължината на вектора $z_1 - z_2$, т.е. на $|z_1 - z_2|$, при което е изпълнено неравенството на триъгълника

$$\left| |z_1| - |z_2| \right| \leq |z_1 + z_2| \leq |z_1| + |z_2|.$$

Прилагайки последното неравенство последователно, получаваме по-общото неравенство

$$|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|.$$

Ако комплексното число z е реално ($\text{Im } z = 0$), то неговият комплексен модул съвпада с реалния (поради което и не възниква необходимост да ги различаваме чрез отделни означения).

Положението на точката $z = x + iy$ в комплексната равнина се определя по единствен начин и от нейните **полярни координати** r и φ (Рис. 0.3)

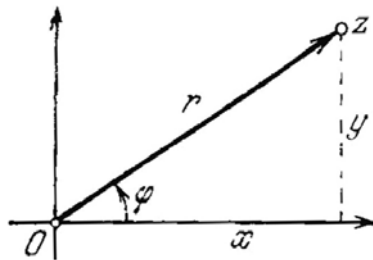


Рис. 0.3.

където $r = |z|$, а φ е ъгълът между реалната ос и вектора z , отчитан в положителна посока (обратна на въртенето на часовниковата стрелка). Този ъгъл се нарича още **аргумент** на комплексното число z и се бележи с $\arg z$, $\varphi = \arg z$. Когато $z = 0$, аргументът не е определен. От рис. 0.3 се вижда, че $x = r \cos \varphi$ и $y = r \sin \varphi$, следователно можем да запишем

$$(0.1) \quad z = r(\cos \varphi + i \sin \varphi),$$

което се нарича **тригонометрична форма** на запис на комплексното число z . От формулата (0.1) следва, че аргументът на z не се определя еднозначно, а с точност до събираеми от вида $2k\pi$, $k \in \mathbb{Z}$. По този начин се въвежда **многозначната функция** $\arg z$, която приема безбройно много стойности

$$\arg_k z = \arg_0 z + 2k\pi, \quad k \in \mathbb{Z},$$

където $\arg_0 z$ обикновено се определя да приема стойности от интервала $(-\pi, \pi]$ ($-\pi < \arg_0 z \leq \pi$). Ако обстоятелствата изискват, стойностите на $\arg_0 z$ могат да се определят в произволен полуотворен интервал с дължина 2π , например $[0, 2\pi)$ ($0 \leq \arg_0 z < 2\pi$). Когато пишем $z = r(\cos \varphi + i \sin \varphi)$, обикновено се има предвид, че φ е някоя от стойностите на $\arg z$, например $\varphi = \arg_0 z$, но равенството (0.1) всъщност е изпълнено за всяка стойност на аргумента. Две комплексни числа $z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$ и $z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2)$ са равни, когато са равни техните модули, $r_1 = r_2$ и $\varphi_1 = \varphi_2 + 2k\pi$, за някое $k \in \mathbb{Z}$. Последното означава равенство на техните аргументи, $\arg z_1 = \arg z_2$, при което последното равенство трябва да се схваща като равенство на две множества (две множества са равни, когато всеки елемент на едното принадлежи на другото и обратно).

Комплексното число $\cos \varphi + i \sin \varphi$ се означава с $e^{i\varphi}$,

$$(0.2) \quad e^{i\varphi} = \cos \varphi + i \sin \varphi,$$

следователно $z = r e^{i\varphi}$, което се нарича **експоненциална (показателна) форма** на запис на z . Заменяйки φ с $-\varphi$ в (0.2) получаваме $e^{-i\varphi} = \cos \varphi - i \sin \varphi$, следователно

$$\cos \varphi = \frac{e^{i\varphi} + e^{-i\varphi}}{2}, \quad \sin \varphi = \frac{e^{i\varphi} - e^{-i\varphi}}{2i},$$

които се наричат **формули на Ойлер**. Лесно се проверява, че функцията $e^{i\varphi}$ притежава обичайните свойства на експонентата

$$e^{i\varphi_1} e^{i\varphi_2} = e^{i(\varphi_1 + \varphi_2)}, \quad \frac{e^{i\varphi_1}}{e^{i\varphi_2}} = e^{i(\varphi_1 - \varphi_2)}, \quad (e^{i\varphi})^n = e^{in\varphi}, \quad n \in \mathbf{N},$$

откъдето следва, че ако $z_1 = r_1 e^{i\varphi_1}$ и $z_2 = r_2 e^{i\varphi_2}$, то

$$z_1 z_2 = r_1 r_2 e^{i(\varphi_1 + \varphi_2)}, \quad \frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\varphi_1 - \varphi_2)},$$

а също така следва и **формулата на Моавър**

$$(\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi.$$

Твърдение 0.1. Аритметичните операции, комплексното спрягане и модулет притежават следните основни свойства.

1) $\overline{z_1 \pm z_2} = \bar{z}_1 \pm \bar{z}_2.$

2) $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2, \quad \overline{\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}} = \begin{pmatrix} \bar{z}_1 \\ \bar{z}_2 \end{pmatrix}.$

3) $|z_1 z_2| = |z_1| |z_2|, \quad \left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|}. \blacksquare$

Доказателството на твърдение 0.1 се свежда до непосредствена проверка.

Да разгледаме уравнението ($n \in \mathbf{N}$)

$$z^n = w,$$

където $w \neq 0$ е някакво комплексно число. За да намерим неговите решения, полагаме $z = r(\cos \varphi + i \sin \varphi)$. Нека $w = \rho(\cos \theta + i \sin \theta)$, където $\theta = \arg_0 w$. Тогава

$$z^n = r^n (\cos n\varphi + i \sin n\varphi)$$

следователно $r^n = \rho$ и $n\varphi = \theta + 2k\pi$, $k \in \mathbf{Z}$, откъдето получаваме следните решения

$$z_k = \sqrt[n]{\rho} \left(\cos \frac{\theta + 2k\pi}{n} + i \sin \frac{\theta + 2k\pi}{n} \right), \quad k \in \mathbf{Z},$$

които са безбройно много, но между тях само n на брой са различни по между си, тъй като техните стойности се повтарят с период n . Веднага се вижда, че $z_{k+n} = z_k$, понеже

$$\frac{\theta + 2(k+n)\pi}{n} - \frac{\theta + 2k\pi}{n} = 2\pi,$$

а функциите $\sin \varphi$ и $\cos \varphi$ са периодични с период 2π . Една поредица от различни стойности се получава за $k = 0, 1, \dots, n-1$. Така доказахме следното

Твърдение 0.2. Всичките решения на уравнението $z^n = w$, $w \neq 0$, се дават по формулата

$$(0.3) \quad z_k = \sqrt[n]{|w|} \left(\cos \frac{\theta + 2k\pi}{n} + i \sin \frac{\theta + 2k\pi}{n} \right), \quad k = 0, 1, \dots, n-1,$$

където θ е някаква стойност на аргумента на w . \blacksquare

За генериране различните решения на $z^n = w$ по формулата (0.3), може да се използва всяка поредица от n на брой цели числа k . В комплексната равнина корените са разположени по окръжност с център в началото и радиус $\sqrt[n]{\rho}$, $\rho = |w|$, и равно нарастване на аргумента с $\frac{2\pi}{n}$, образувайки правилен n -ъгълник (Рис. 0.4).

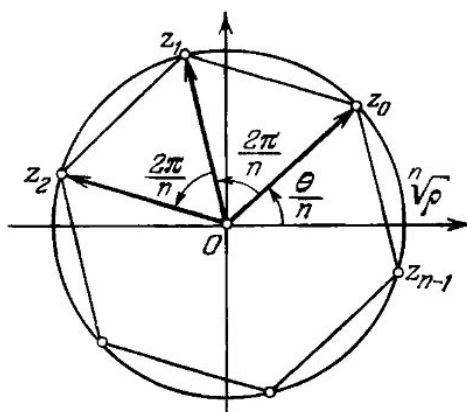


Рис. 0.4.

2. Полиноми. Полином на една променлива x се определя като функция, образувана посредством краен брой последователни операции събиране и умножение. Един полином $f(x)$ има вида

$$(0.4) \quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

където числата $a_0, a_1, \dots, a_{n-1}, a_n$ се наричат **коэффициенти** на полинома. Най-високата степен на променливата, която участва в запис на полинома $f(x)$, се нарича **степен** на полинома и се бележи с $\deg f(x)$. В запис (0.4) имаме $\deg f(x) \leq n$ и $\deg f(x) = n$, точно когато $a_n \neq 0$. Полиномите от степен нула и само те са константи. Числото α се нарича **корен (нула)** на полинома $f(x)$, когато $f(\alpha) = 0$. Полиномите могат да се събират и умножават, при което отново се получават полиноми.

Два полинома са равни тогава и само тогава, когато са от една и съща степен и коефициентите пред съответните степени на променливата са равни.

Между полиномите може да се определи операция на **деление с остатък**.

Теорема 0.1. Нека $f(x)$ и $g(x)$ са полиноми, при което $\deg g(x) \geq 1$. Тогава съществуват единствени полиноми $q(x)$ и $r(x)$, за които

$$(0.5) \quad f(x) = g(x)q(x) + r(x),$$

при което $\deg r(x) < \deg g(x)$. Полиномът $q(x)$ се нарича **частно**, а полиномът $r(x)$ се нарича **остатък** от делението на полинома $f(x)$ на полинома $g(x)$.

Доказателство. Да положим $\deg f(x) = n$ и $\deg g(x) = m \geq 1$. Съществуването ще докажем чрез индукция по степента n . Ако $n < m$, то можем да положим $q(x) \equiv 0$ и $r(x) = f(x)$, при което полагане очевидно е валидно равенството (0.5), както и изискването степента на остатъка $r(x)$ да бъде строго по-малка от степента на делителя $g(x)$. По този начин индукционната база е налице. Да допуснем че твърдението е вярно за всички степени на делимото $f(x)$ до някакъв ред n и нека $f(x)$ е полином от степен $n+1$. Имаме

$$f(x) = f_{n+1} x^{n+1} + f_n x^n + \dots + f_1 x + f_0, \quad f_{n+1} \neq 0,$$

$$g(x) = g_m x^m + g_{m-1} x^{m-1} + \dots + g_1 x + g_0, \quad g_m \neq 0.$$

Полиномът

$$\hat{f}(x) = f(x) - \frac{f_{n+1}}{g_m} x^{n+1-m} g(x)$$

е от степен по-малка или равна на n . Съгласно индукционното предположение, полиномът $\hat{f}(x)$ може да се запише във вида

$$\hat{f}(x) = g(x)\hat{q}(x) + r(x),$$

където $\deg r(x) < \deg g(x)$. Сега за полинома $f(x)$ получаваме представянето

$$f(x) = \hat{f}(x) + \frac{f_{n+1}}{g_m} x^{n+1-m} g(x) = g(x) \left[\frac{f_{n+1}}{g_m} x^{n+1-m} + \hat{q}(x) \right] + r(x),$$

$$f(x) = g(x)q(x) + r(x),$$

където

$$q(x) = \frac{f_{n+1}}{g_m} x^{n+1-m} + \hat{q}(x), \quad \deg r(x) < \deg g(x),$$

което искахме да докажем. Нека сега имаме две представяния

$$f(x) = g(x)q_1(x) + r_1(x) \quad \text{и} \quad f(x) = g(x)q_2(x) + r_2(x),$$

където $\deg r_1(x) < \deg g(x)$ и $\deg r_2(x) < \deg g(x)$. Тогава след изваждане и групиране получаваме

$$r_2(x) - r_1(x) = g(x)[q_1(x) - q_2(x)].$$

Ако $q_1(x)$ и $q_2(x)$ са различни полиноми, то в дясната страна на последното равенство ще стои полином от степен поне $\deg g(x)$, докато от лявата страна сигурно стои полином от степен строго по малка от $\deg g(x)$, което е противоречие. Следователно $q_1(x) = q_2(x)$, откъдето веднага получаваме $r_1(x) = r_2(x)$. По този начин доказахме единствеността на представянето (0.5). ■

Доказателството на теорема 0.1 съдържа в себе си и правилото за деление на полиноми чрез последователно изключване на най-високите степени в делимото.

Единственото конструктивно изискване към формулата (0.5) е степента на остатъка $r(x)$ да бъде строго по-малка от степента на делителя $g(x)$.

Нека $f(x)$ е полином, $n = \deg f(x) \geq 1$, и a е някакво число. Да положим $g(x) = x - a$. Тогава съгласно теорема 0.2 съществува полином $q(x)$ и константа r , за които

$$(0.6) \quad f(x) = (x - a)q(x) + r,$$

където по необходимост $\deg q(x) = n - 1$ и очевидно $r = f(a)$. От тук в частност следва верността на

Твърдение 0.3. Числото a е корен на полинома $f(x)$, $\deg f(x) \geq 1$, тогава и само тогава, когато $f(x)$ се дели на полинома $x - a$ без остатък, т.е. когато съществува полином $q(x)$, за който е налице равенството $f(x) = (x - a)q(x)$. ■

Да разгледаме отново представянето (0.6). Имаме

$$f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \quad \text{и} \quad q(x) = q_{n-1} x^{n-1} + q_{n-2} x^{n-2} + \dots + q_1 x + q_0.$$

След заместване в (0.6) и приравняване коефициентите пред съответните степени получаваме последователно

$$f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 = (x - a)(q_{n-1} x^{n-1} + q_{n-2} x^{n-2} + \dots + q_1 x + q_0) + r,$$

$$f_n = q_{n-1}, \quad f_{n-1} = q_{n-2} - a q_{n-1}, \quad \dots, \quad f_2 = q_1 - a q_2, \quad f_1 = q_0 - a q_1, \quad f_0 = r - a q_0,$$

които могат да се запишат

$$q_{n-1} = f_n,$$

$$q_{n-2} = f_{n-1} + a q_{n-1},$$

...

$$q_1 = f_2 + a q_2,$$

$$q_0 = f_1 + aq_1,$$

$$r = f_0 + aq_0.$$

Горните формули се използват практически за последователно намиране на коефициентите на частното $q(x)$ и на остатъка r , при което изчисленията могат да се подредят в таблица (**правило на Хорнер**)

	f_n	f_{n-1}	...	f_2	f_1	f_0
a	$q_{n-1} = f_n$	$q_{n-2} = f_{n-1} + aq_{n-1}$...	$q_1 = f_2 + aq_2$	$q_0 = f_1 + aq_1$	$r = f_0 + aq_0$

Например да разделим полинома $f(x) = x^4 - 2x^3 - 3x^2 + 2x + 5$ на полинома $g(x) = x - 2$. За да изпълним правилото на Хорнер, съставяме таблица пресмятаме последователно търсените коефициенти на частното и остатъка.

	1	-2	-3	2	5
2	1	0	-3	-4	-3

Следователно $q(x) = x^3 - 3x - 4$, а $r = -3$, което означава равенството

$$x^4 - 2x^3 - 3x^2 + 2x + 5 = (x - 2)(x^3 - 3x - 4) - 3.$$

Едно от големите предимства на полето на комплексните числа се състои във възможността да намираме корените на алгебрични уравнения, които корени в общия случай могат да не са реални числа, например решенията на уравнението $z^2 + 1 = 0$ са двойката комплексно спрегнати числа $z_{1,2} = \pm i$. Следната теорема носи името **основна теорема на алгебрата**.

Теорема 0.2. Нека $f(z)$ е полином с реални или комплексни коефициенти и $\deg f(z) \geq 1$. Тогава съществува поне едно комплексно число z_0 , което е корен на полинома, т.е. $f(z_0) = 0$. ■

От теорема 0.2 и твърдение 0.3 следва, че всеки полином $f(z)$, за който $n = \deg f(z) \geq 1$, може да се запише във вида

$$f(z) = f_1(z)(z - z_1),$$

където z_1 е някой негов комплексен корен, а $f_1(z)$ е полином, за който $\deg f_1(z) = n - 1$. Продължавайки разсъждението по същия начин за $f_1(z)$ и т.н. до изчерпване степента на $f(z)$, ще получим верността на следната

Теорема 0.3. Нека $f(z)$ е полином с реални или комплексни коефициенти и $n = \deg f(z) \geq 1$. Тогава $f(z)$ може да се запише във вида

$$(0.7) \quad f(z) = A(z - z_1)(z - z_2) \cdots (z - z_n),$$

където z_1, z_2, \dots, z_n са корените на полинома $f(z)$, а числото A е старшият коефициент на $f(z)$. ■

Равенството (0.7) показва, че всеки полином от степен $n \geq 1$ с реални или комплексни коефициенти има точно n на брой комплексни (или реални) корени.

В качеството на пример да вземем уравнението $z^n - 1 = 0$. Решенията на това уравнение се наричат n -ти корени на единицата, които съгласно (0.3) се дават по формулата

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad k = 0, 1, \dots, n-1.$$

Сега теорема 0.3 указва, че за полинома $z^n - 1$ е в сила следното разлагане на линейни множители

$$z^n - 1 = (z - z_0)(z - z_1) \cdots (z - z_{n-1}) = \prod_{k=0}^{n-1} \left[z - \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \right) \right].$$

3. Числови полета. Числовите полета са множества, в които са определени двете операции събиране и умножение, при което са налице познатите свойства на тези операции от числовото поле на рационалните числа \mathbb{Q} , полето на реалните числа \mathbb{R} и полето на комплексните числа \mathbb{C} . Събирането и умножението са комутативни и асоциативни, а умножението се разпределя върху събираемите. Съществуват два специални елемента – нула и единица, които са неутрални съответно на събирането и умножението. Всяко число притежава обратно число относно събирането, което в сбор с него дава нула. Най-важното свойство на едно числово поле обаче се състои във възможността да делим на число, което е различно от нула, което означава, че всяко ненулево число притежава обратно относно умножението.

Разгледаните дотук числови полета съдържат безбройно много числа. Освен тях съществуват и **крайни полета**, които съдържат краен брой числа. Една таква поле например е $GF(q)$ – полето на остатъците по модул q , където q е някакво **просто число**. Естественото число $q > 1$ се нарича просто, когато няма други делители освен себе си и числото 1. Прости са например числата 2, 3, 5, 7, 11 и т.н. Простите числа са безбройно много.

При целите числа е валидно правилото за деление с остатък. Ако n е някакво цяло число и m е някакво естествено число, то съществува единствено цяло число n' и единствено цяло неотрицателно число r , $0 \leq r < m$, за които е валидно равенството $n = n'm + r$. В този случай числото n' се нарича **частно**, а числото r се нарича **остатък** от делението на цялото число n на естественото число m . Записът $n_1 = n_2 \pmod{m}$ означава, че разликата $n_1 - n_2$ се дели на m , т.е. n_1 и n_2 имат равни остатъци при делението на m .

Полето $GF(q)$ се състои от остатъците, които се получават при делението на q , т.е. от целите неотрицателни числа $0, 1, 2, \dots, q-1$, които са по-малки от самото просто число q . Полето $GF(q)$ съдържа точно q на брой елемента. Операциите събиране и умножение са същите както при целите числа, само че за резултат се взема остатъкът на сбора или произведението по $\text{mod } q$.

Например в $GF(5)$ имаме $3+4=2$, понеже остатъкът на сбора $3+4=7$ при деление на 5 е равен на 2. Аналогично $2*4=3$, понеже остатъкът на произведението $2*4=8$ при деление на 5 е равен на 3.

Комутативността и асоциативността на така определеното събиране и умножение в $GF(q)$ се проверяват непосредствено. Не е трудно да се съобрази, че двете операции са свързани с обичайния дистрибутивен закон. Нулата в $GF(q)$ е остатъкът 0, а единицата е остатъкът 1. Обратният елемент относно събирането на остатъкът k , $0 < k < q$ е остатъкът $q-k$, понеже $k+(q-k)=q=0 \pmod{q}$. Малко по-трудно е да се провери, че всеки ненулев елемент на $GF(q)$ има обратен относно умножението. Това свойство означава, че уравнението $ax = b$, $a, b \in GF(q)$, $a \neq 0$, има единствено решение в полето $GF(q)$. Ако запишем това единствено решение по аналогия във вида $x = \frac{b}{a}$, то фактически по този начин задаваме операцията **деление**, като обратна на операцията умножение.

Нека $a \in GF(q)$, $a \neq 0$. Да разгледаме остатъците $r_0, r_1, r_2, \dots, r_{q-1}$ по $\text{mod } q$ на произведенията на числото a с числата $0, 1, 2, \dots, q-1$, които представляват

елементите на $GF(q)$. Да допуснем, че между тези остатъци има два равни, $r_i = r_j$, $0 \leq i < j \leq q-1$. Тогава разликата $ai - aj = a(i - j)$ ще се дели на q , следователно простото число q дели произведението $a(i - j)$, което е невъзможно, понеже нито един от множителите a и $i - j$ на се дели на q . Тези остатъци са q на брой и както вече установихме са различни по между си, следователно те представляват евентуално в някакъв друг ред елементите на $GF(q)$. По този начин всеки остатък от $GF(q)$, ще се срещне точно на едно място някъде в редицата $r_0, r_1, r_2, \dots, r_{q-1}$, откъдето веднага заключаваме, че уравнението $ax = b$ има решение, което освен това е единствено.

Например да разгледаме полето на остатъците $GF(5)$. Правилата за събиране и умножение в $GF(5)$ са приведени в следните таблици.

Таблица за събиране в $GF(5)$

\oplus	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таблица за умножение в $GF(5)$

\otimes	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Освен линейни уравнения, в $GF(q)$ могат да се решават и линейни системи отново по обичайния начин. Например да решим в $GF(5)$ системата

$$\begin{cases} 2x - 3y = 1 \\ 3x + 2y = 2 \end{cases}$$

След умножаване на второто уравнение с 4 получаваме

$$\begin{cases} 2x - 3y = 1 \\ 2x + 3y = 3 \end{cases}$$

Изваждаме първото уравнение от второто,

$$\begin{cases} 2x - 3y = 1 \\ y = 2 \end{cases}$$

Сега замествайки намереното значение $y = 2$ в първото уравнение, за x получаваме $2x = 2$, т.е. $x = 1$. Системата има единствено решение $x = 1$ и $y = 2$.