Глава 1

Комплексни числа. Полета - числови полета и примери за нечислови полета.

Уравнението $x^2+1=0$ няма решение в реални числа, както и всички квадратни тричлени с реални коефициенти и отрицателна дискриминанта.

> Определение 1.1. *Имагинерната единица $i=\sqrt{-1}$ е един от корените на уравнението $x^2+1=0$.*

Другият корен на $x^2+1=0$ е $-i$. Непосредствено пресмятаме, че

$$i^2=-1, \quad i^3=i^2.i=-i, \quad i^4=(i^2)^2=(-1)^2=1.$$

Следователно, за произволно естествено число k е в сила

$$i^{4k}=(i^4)^k=1^k=1, \quad i^{4k+1}=i^{4k}.i=i, \quad i^{4k+2}=i^{4k}.i^2=-1, \quad i^{4k+3}=i^{4k}.i^3=-i.$$

С други думи, всички мономи на имагинерната единица i се изчерпват от $\pm i$ и ± 1. Произволен полином на i с реални коефициенти има вида

$$\begin{aligned} a_0+a_1i+a_2i^2+a_3i^3+a_4i^4+a_5i^5+a_6i^6+a_7i^7+a_8i^8+\ldots+a_ni^n= \\ =a_0+a_1i-a_2-a_3i+a_4+a_5i-a_6-a_7i+a_8+\ldots+a_ni^n= \\ =(a_0-a_2+\ldots+a_{4k}-a_{4k+2}+\ldots)+i(a_1-a_3+\ldots+a_{4k+1}-a_{4k+3}+\ldots) \end{aligned}$$

и се представя като полином на i от степен, ненадминаваща 1. Например,

$$5i^6+3i^5-2i^3+3i^2-4i+1=-5+3i+2i-3-4i+1=-7+i.$$

> Определение 1.2. *Множеството*
> $$\mathbb{C}:=\{a+bi\,|\,a,b\in\mathbb{R}\}$$
> *на полиномите на имагинерната единица i с реални коефициенти се нарича множество на комплексните числа.*

Означението $X:=Y$ се използва, когато определяме математически обект X като известен преди това обект Y. В случая, определяме множеството $\mathbb{C}$ на комплексните числа като полиномите на i с реални коефициенти.
Навсякъде по-нататък ще бележим с

$$\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}$$

множествата на естествените, целите, рационалните и реалните числа. Ако някакво свойство е изпълнено за всички елементи $x\in M$ на множество M, записваме съкратено $\forall x\in M$. Когато съществува $x_o\in M$ с някакво свойство, пишем $\exists x_o\in M$.
Ако $z=a+bi\in\mathbb{C}$ е комплексно число, представено като полином на имагинерната единица i от степен ≤ 1, то свободният член $\mathrm{Re}(z):=a$ се нарича реална част на z, а коефициентът $\mathrm{Im}(z):=b$ на i се нарича имагинерна част на z. Например, $\mathrm{Re}(2-i)=2$, $\mathrm{Im}(2-i)=-1$.

Ако $a_1 + ib_1 = a_2 + ib_2$ с $a_1, b_1, a_2, b_2 \in \mathbb{R}$ са равни комплексни числа, то

$$i(b_1 - b_2) = a_2 - a_1.$$

Допускането $b_1 \neq b_2$ води до

$$i = \frac{a_2 - a_1}{b_1 - b_2} \in \mathbb{R},$$

което е противоречие. Следователно $b_1 = b_2$, откъдето $0 = a_2 - a_1$ и $a_1 = a_2$. С това доказахме, че комплексните числа a_1+ib_1 и a_2+ib_2 са равни тогава и само тогава, когато реалните им части $a_1 = a_2$ и имагинерните им части $b_1 = b_2$ са равни.

Оттук следва, че комплексните числа $z = a+ib \in \mathbb{C}$ са във взаимно еднозначно съответствие с точките от равнината $\mathbb{R}^2$ с координати (a, b). Реалната част a на $z = a+ib$ е абсцисата на съответната точка, а имагинерната част b на $z = a+ib$ е ординатата на съответната точка. Затова казваме, че абсцисната ос е реалната ос на комплексната равнина, а ординатната ос е имагинерната ос.

Определение 1.3. *Ако $z = a+ib$ е комплексно число, то комплексното число $\overline{z} := a - ib$ със същата реална част a като z и противоположна имагинерна част $-b$ се нарича комплексно спрегнато на z.*

Точката $(a, -b) \in \mathbb{R}$, отговаряща на $\overline{z}$ е симетрична на съответната точка (a, b) на $z = a + ib$ относно абсцисната или реалната ос. Комплексно число $z = \overline{z}$ съвпада с комплексно спрегнатото си точно когато $z = a \in \mathbb{R}$ е реално.

Да означим с $\mathbb{R}^{\geq 0}$ множеството на неотрицателните реални числа, а с $\mathbb{R}^{>0}$ - множеството на положителните реални числа. Произведението

$$z\overline{z} = (a + ib)(a - ib) = a^2 - i^2b^2 = a^2 + b^2 \in \mathbb{R}^{\geq 0}$$

на комплексно число z и неговото комплексно спрегнато $\overline{z}$ е неотрицателно реално число, което се анулира тогава и само тогава, когато $a = b = 0$ и $z = 0$ е началото на комплексната равнина.

Определение 1.4. *Неотрицателният корен квадратен*

$$|z| := \sqrt{z\overline{z}} = \sqrt{a^2 + b^2} \in \mathbb{R}^{\geq 0}$$

от произведението на z и $\overline{z}$ се нарича модул на z.

Геометрично, модулът $|z|$ на комплексно число $z \in \mathbb{C}$ е разстоянието от началото 0 на комплексната равнина до точката, която отговаря на комплексното число z.

Аритметичните действия на комплексни числа $z_1 = a_1 + ib_1$ и $z_2 = a_2 + ib_2$ са като на полиноми на имагинерната единица i. По-точно, събирането

$$z_1 + z_2 = (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$$

и изваждането

$$z_1 - z_2 = (a_1 + ib_1) - (a_2 + ib_2) = (a_1 - a_2) + i(b_1 - b_2)$$

на комплексни числа се свежда до събиране, съответно, изваждане на техните реални и имагинерни части. Умножението на комплексни числа

$$z_1z_2 = (a_1 + ib_1)(a_2 + ib_2) =$$
$$= (a_1a_2 + i^2b_1b_2) + i(a_1b_2 + a_2b_1) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$$

е като умножение на полиноми на i със свойството $i^2 = -1$. За да разделим комплексно число $z_1 = a_1 + ib_1$ на ненулево комплексно число $z_2 = a_2 + ib_2$ различно от 0, умножаваме дробта $\frac{z_1}{z_2}$ с $1 = \frac{\overline{z_2}}{\overline{z_2}}$ и получаваме

$$\frac{z_1}{z_2} = \frac{z_1}{z_2}.1 = \frac{z_1}{z_2}\frac{\overline{z_2}}{\overline{z_2}} = \frac{(a_1+ib_1)(a_2-ib_2)}{(a_2+ib_2)(a_2-ib_2)} = \left(\frac{a_1a_2+b_1b_2}{a_2^2+b_2^2}\right) + i\left(\frac{b_1a_2-a_1b_2}{a_2^2+b_2^2}\right),$$

използвайки че делението с положителното реално число $z_2\overline{z_2} = a_2^2 + b_2^2$ е равносилно на умножение на полинома $z_1\overline{z_2} = (a_1a_2 + b_1b_2) + i(b_1a_2 - a_1b_2)$ на i с положителното реално число $\frac{1}{a_2^2+b_2^2} \in \mathbb{R}^{>0}$. Например,

$$\frac{(1-2i)(3+i)}{(1-i)(2+i)} = \frac{3-2i^2-6i+i}{2-i^2-2i+i} = \frac{5-5i}{3-i} =$$
$$= \frac{5(1-i)}{3-i}.\frac{3+i}{3+i} = \frac{5(3-i^2-3i+i)}{9-i^2} = \frac{5(4-2i)}{10} = 2-i.$$

Твърдение 1.5. *Комплексното спрягане е съгласувано с аритметичните операции с комплексни числа, т.е. за произволни комплексни числа $z_1, z_2 \in \mathbb{C}$ е в сила*

$$\overline{z_1+z_2} = \overline{z_1} + \overline{z_2}, \quad \overline{z_1-z_2} = \overline{z_1} - \overline{z_2};$$
$$\overline{z_1z_2} = \overline{z_1}\ \ \overline{z_2} \quad \text{и} \quad \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}} \quad \text{в случая на } z_2 \neq 0.$$

Доказателство. Ако $z_j = a_j + ib_j$ за $1 \leq j \leq 2$ и $a_j, b_j \in \mathbb{R}$, то

$$\overline{z_1+z_2} = \overline{(a_1+a_2)+i(b_1+b_2)} = (a_1+a_2) - i(b_1+b_2) =$$
$$= (a_1-ib_1) + (a_2-ib_2) = \overline{z_1} + \overline{z_2}.$$

Действието изваждане е обратно на събирането, така че прилагайки съгласуваността на събирането на комплексни числа с комплексното спрягане към $z_1 = (z_1 - z_2) + z_2$ получаваме, че

$$\overline{z_1} = \overline{(z_1-z_2)+z_2} = \overline{z_1-z_2} + \overline{z_2},$$

откъдето

$$\overline{z_1} - \overline{z_2} = \overline{z_1-z_2}.$$

Пресмятаме непосредствено, че

$$\overline{z_1z_2} = \overline{(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)} =$$
$$= (a_1a_2-b_1b_2) - i(a_1b_2+a_2b_1) = (a_1-ib_1)(a_2-ib_2) = \overline{z_1}\ \ \overline{z_2}$$

съгласно $(-i)^2 = i^2 = -1$. Прилагаме доказаното тъждество към произведението на $\frac{z_1}{z_2}$ с z_2 и получаваме

$$\overline{z_1} = \overline{\left(\frac{z_1}{z_2}\right)z_2} = \overline{\left(\frac{z_1}{z_2}\right)}\,\overline{z_2},$$

откъдето

$$\frac{\overline{z_1}}{\overline{z_2}} = \overline{\left(\frac{z_1}{z_2}\right)}.$$

□

Нека $z = a+ib \in \mathbb{C}\setminus\{0\}$ е ненулево комплексно число. Тогава $|z| = \sqrt{a^2+b^2} \neq 0$ и $t := \frac{z}{|z|} \in \mathbb{C}$. Комплексното число

$$t := \frac{z}{|z|} = \frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}}$$

има квадрат на модула

$$|t|^2 = t\bar{t} = \left(\frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}}\right)\left(\frac{a}{\sqrt{a^2+b^2}} - i\frac{b}{\sqrt{a^2+b^2}}\right) =$$
$$= \left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1$$

и t принадлежи на единичната окръжност $S^1 := \{t \in \mathbb{C} \mid |t| = 1\}$ в комплексната равнина $\mathbb{C}$. Да означим с φ ориентирания ъгъл от положителната реална ос до радиус-вектора на точката t. От точката t спускаме перпендикуляр към реалната ос и получаваме правоъгълен триъгълник с хипотенуза 1. Катетът срещу ъгъла φ е равен на $\sin\varphi$ и на имагинерната част на t, така че

$$\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}.$$

Прилежащият катет на φ е равен на $\cos\varphi$ и на реалната част на t, т.е.

$$\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}.$$

Следователно

$$t = \frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}} = \cos\varphi + i\sin\varphi.$$

Това дава представянето

$$z = |z|(\cos\varphi + i\sin\varphi) \tag{1.1}$$

на комплексното число z. Казваме, че z има аргумент φ. Да забележим, че аргументът на ненулево комплексно число е определен с точност до целочислено кратно на 2π, защото тригонометричните функции $\sin x$ и $\cos x$ са 2π-периодични. Представянето (1.1) на $z \in \mathbb{C}$ се нарича тригонометричен вид на комплексното число z.

Тригонометричният вид на комплексно число е удобен при извършване на действията умножение и деление, както се вижда от следното

Твърдение 1.6. *Нека* $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$ *са ненулеви комплексни числа в тригонометричен вид с модули* $r_1, r_2 \in \mathbb{R}^{>0}$ *и аргументи* $\varphi_1, \varphi_2 \in \mathbb{R}$ *и* $n \in \mathbb{Z}$ *е цяло число. Тогава*

$$z_1 z_2 = r_1 r_2[\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)], \tag{1.2}$$
$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)] \quad \text{и} \tag{1.3}$$
$$z_1^n = r_1^n\left[\cos(n\varphi_1) + i\sin(n\varphi_1)\right]. \tag{1.4}$$

Доказателство. Пресмятаме непосредствено, че

$$(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) =$$
$$= (\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2) =$$
$$= \cos(\varphi_1+\varphi_2) + i(\sin(\varphi_1+\varphi_2)),$$

използвайки тригонометричните формули

$$\sin(\varphi_1+\varphi_2) = \sin\varphi_1\cos\varphi_2 + \sin\varphi_2\cos\varphi_1$$

и

$$\cos(\varphi_1+\varphi_2) = \cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2.$$

Оттук,

$$z_1 z_2 = |z_1|(\cos\varphi_1 + i\sin\varphi_1)|z_2|(\cos\varphi_2 + i\sin\varphi_2) = |z_1||z_2|[\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)]$$

доказва (1.2).
За да установим верността на (1.3), използваме че

$$(\cos\varphi_2+i\sin\varphi_2)[\cos(-\varphi_2)+i\sin(-\varphi_2)]=\cos(\varphi_2-\varphi_2)+i\sin(\varphi_2-\varphi_2)=\cos 0+i\sin 0=1,$$

откъдето

$$\frac{1}{\cos\varphi_2+i\sin\varphi_2}=\cos(-\varphi_2)+i\sin(-\varphi_2)\quad \text{и}$$

$$\frac{z_1}{z_2}=\frac{|z_1|(\cos\varphi_1+i\sin\varphi_1)}{|z_2|(\cos\varphi_2+i\sin\varphi_2)}=\frac{|z_1|}{|z_2|}(\cos\varphi_1+i\sin\varphi_1)\frac{1}{\cos\varphi_2+i\sin\varphi_2}=$$

$$=\frac{|z_1|}{|z_2|}(\cos\varphi_1+i\sin\varphi_1)[\cos(-\varphi_2)+i\sin(-\varphi_2)]=\frac{|z_1|}{|z_2|}[\cos(\varphi_1-\varphi_2)+i\sin(\varphi_1-\varphi_2)].$$

С това проверихме (1.3).
Ако $n\in\mathbb{N}$ е естествено число, то за

$$t_1:=\frac{z_1}{|z_1|}=\cos\varphi_1+i\sin\varphi_1$$

е в сила

$$t_1^n=\underbrace{t_1\dots t_1}_{n}=\underbrace{(\cos\varphi_1+i\sin\varphi_1)\dots(\cos\varphi_1+i\sin\varphi_1)}_{n}=\cos(n\varphi_1)+i\sin(n\varphi_1),$$

съгласно правилото за умножение на комплексни числа в тригонометричен вид. За $n=0$ имаме $z_1^0=1$. В случая на отрицателно цяло n, пресмятаме че

$$t_1^n=t_1^{(-1)(-n)}=(t_1^{-1})^{-n}=\left(\frac{1}{t_1}\right)^{-n}=[\cos(-\varphi_1)+i\sin(-\varphi_1)]^{-n}=$$
$$=\cos((-n)(-\varphi_1))+i\sin((-n)(-\varphi_1))=\cos(n\varphi_1)+i\sin(n\varphi_1),$$

използвайки $1=\cos(0)+i\sin(0)$, правилото за деление на комплексни числа в тригонометричен вид и правилото за повдигане на комплексно число в естествена степен. Това доказва (1.4) и завършва доказателството на твърдението. □

Лема 1.7. *Нека $z_1=r_1(\cos\varphi_1+i\sin\varphi_1)$ и $z_2=r_2(\cos\varphi_2+i\sin\varphi_2)$ са ненулеви комплексни числа в тригонометричен вид. В такъв случай, z_1 и z_2 са равни тогава и само тогава, когато модулите им $r_1=r_2$ са равни и аргументите им $\varphi_2-\varphi_1=2k\pi$, $k\in\mathbb{Z}$ се различават с цяло кратно на 2π.*

Доказателство. Ако $r_1=r_2$ и $\varphi_2=\varphi_1+2k\pi$, то

$$z_2=r_2(\cos\varphi_2+i\sin\varphi_2)=r_1[\cos(\varphi_1+2k\pi)+i\sin(\varphi_1+2k\pi)]=$$
$$=r_1(\cos\varphi_1+i\sin\varphi_1)=z_1$$

поради 2π-периодичността на $\cos x$ и $\sin x$.
Да допуснем, че комплексните числа $a_1+ib_1=z_1=z_2=a_2+ib_2$ са равни. Тогава $a_1=a_2$, $b_1=b_2$, откъдето

$$|z_1|=r_1=\sqrt{a_1^2+b_1^2}^{\,>0}=\sqrt{a_2^2+b_2^2}^{\,>0}=r_2=|z_2|$$

и точките

$$cos\varphi_1+i\sin\varphi_1=\frac{z_1}{|z_1|}=\frac{z_2}{|z_2|}=cos\varphi_2+i\sin\varphi_2\in S^1=\{t\in\mathbb{C}\,|\,|t|=1\}$$

от единичната окръжност съвпадат. Оттук, реалните и имагинерните части на тези комплексни числа са равни и

$$\cos\varphi_2 - \cos\varphi_1 = -2\sin\frac{\varphi_2-\varphi_1}{2}\sin\frac{\varphi_2+\varphi_1}{2} = 0,$$

$$\sin\varphi_2 - \sin\varphi_1 = 2\sin\frac{\varphi_2-\varphi_1}{2}\cos\frac{\varphi_2+\varphi_1}{2} = 0.$$

Ако допуснем, че $\sin\frac{\varphi_2-\varphi_1}{2} \neq 0$, то $\sin\frac{\varphi_2+\varphi_1}{2} = 0 = \cos\frac{\varphi_2+\varphi_1}{2}$ противоречи на $\cos\left(\frac{\varphi_2+\varphi_1}{2}\right)^2 + \sin\left(\frac{\varphi_2+\varphi_1}{2}\right)^2 = 1$. Следователно $\sin\frac{\varphi_2-\varphi_1}{2} = 0$, откъдето

$$\frac{\varphi_2-\varphi_1}{2} = k\pi$$

за някакво цяло число $k \in \mathbb{Z}$ и $\varphi_2 - \varphi_1 = 2k\pi \in 2\pi\mathbb{Z}$.

□

Теорема 1.8. (Формула на Моавър:) *Ако $z = r(\cos\varphi + i sin\varphi) \in \mathbb{C}\setminus\{0\}$ е ненулево комплексно число в тригонометричен вид, то множеството $\sqrt[n]{z}$ на n-тите корени на z съвпада с множеството*

$$M = \left\{ \sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2k\pi}{n}\right) + i\sin\left(\frac{\varphi+2k\pi}{n}\right)\right] \middle| 0 \leq k \leq n-1 \right\}$$

и се състои от n ненулеви комплексни числа. (С $\sqrt[n]{r}^{>0}$ означаваме положителния реален n-ти корен от $r \in \mathbb{R}^{>0}$.)

Доказателство. Нека

$$M' := \left\{ \sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2m\pi}{n}\right) + i\sin\left(\frac{\varphi+2m\pi}{n}\right)\right] \middle| m \in \mathbb{Z} \right\}.$$

Ще проверим, че

$$M' \subseteq \sqrt[n]{z} \subseteq M' \subseteq M$$

и ще комбинираме с тривиалното включване $M \subseteq M'$, за да получим, че $M = M' = \sqrt[n]{z}$. След това ще докажем, че множеството M се състои от n различни комплексни числа.

За всяко

$$y = \sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2m\pi}{n}\right) + i\sin\left(\frac{\varphi+2m\pi}{n}\right)\right] \in M'$$

е в сила

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

съгласно 2π-периодичността на $\cos x$ и $\sin x$. Това доказва $M' \subseteq \sqrt[n]{z}$.

Ако $x = s(\cos\psi + i\sin\psi) \in \sqrt[n]{z}$, то по определение

$$r(\cos\varphi + i sin\varphi) = z = x^n = s^n[\cos(n\psi) + i\sin(n\psi)].$$

Съгласно Лема 1.7, оттук следва $s^n = r$ за $r, s \in \mathbb{R}^{>0}$ и $n\psi - \varphi = 2m\pi$ за някое $m \in \mathbb{Z}$. Следователно $s = \sqrt[n]{r}$, $\psi = \frac{\varphi+2m\pi}{n}$, $x \in M'$ и $\sqrt[n]{z} \subseteq M'$, откъдето $\sqrt[n]{z} = M'$.

Включването $M \subseteq M'$ е ясно. За обратното включване $M' \subseteq M$ делим произволно цяло число $m \in \mathbb{Z}$ на n с частно $q \in \mathbb{Z}$ и остатък $k \in \mathbb{Z}$, $0 \leq k \leq n-1$, така че $m = nq + k$, Тогава

$$\frac{\varphi+2m\pi}{n} = \frac{\varphi+2nq\pi+2k\pi}{n} = \frac{\varphi+2k\pi}{n} + 2q\pi,$$

откъдето

$$\sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2m\pi}{n}\right)+i\sin\left(\frac{\varphi+2m\pi}{n}\right)\right]=$$
$$=\sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2k\pi}{n}\right)+i\sin\left(\frac{\varphi+2k\pi}{n}\right)\right]\in M,$$

съгласно 2π-периодичността на $\cos x$ и $\sin x$. Това доказва включването $M' \subseteq M$ и съвпадението $\sqrt[n]{z}=M'=M$.

Ако допуснем, че

$$\sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2k\pi}{n}\right)+i\sin\left(\frac{\varphi+2k\pi}{n}\right)\right]=$$
$$=\sqrt[n]{r}^{>0}\left[\cos\left(\frac{\varphi+2l\pi}{n}\right)+i\sin\left(\frac{\varphi+2l\pi}{n}\right)\right]$$

за $0 \leq k, l \leq n-1$, то от Лема 1.7 получаваме, че

$$\left(\frac{\varphi+2l\pi}{n}\right)-\left(\frac{\varphi+2k\pi}{n}\right)=\frac{2(l-k)\pi}{n}=2s\pi$$

за някое $s \in \mathbb{Z}$. Следователно $l-k=ns$ и n дели $l-k$. Съгласно

$$-(n-1)=0-(n-1)\leq l-k\leq (n-1)-0=n-1,$$

оттук следва $l-k=0$. С това установихме, че $\sqrt[n]{z}$ се състои от n различни комплексни числа и завършихме доказателството на теоремата.

$\square$

Определение 1.9. *Непразно множество F е поле, ако в него са определени две операции, събиране*

$$F\times F\longrightarrow F,\quad (a,b)\mapsto a+b$$

и умножение

$$F\times F\longrightarrow F,\quad (a,b)\mapsto ab,$$

изпълняващи следните свойства:
(i) *асоциативност на събирането: $(a+b)+c=a+(b+c)$ за произволни $a,b,c\in F$;*
(ii) *комутативност на събирането: $a+b=b+a$ за произволни $a,b\in F$;*
(iii) *съществуване на нула $0\in F$, така че $a+0=a$ за всяко $a\in F$;*
(iv) *всеки елемент $a\in F$ има противоположен $-a\in F$, така че $a+(-a)=0$;*
(v) *асоциативност на умножението: $(ab)c=a(bc)$ за произволни $a,b,c\in F$;*
(vi) *комутативност на умножението: $ab=ba$ за произволни $a,b\in F$;*
(vii) *съществуване на единица $1\in F$, така че $1.a=a$ за всяко $a\in F$;*
(viii) *всеки ненулев елемент $a\in F\setminus\{0\}$ има обратен $a^{-1}\in F\setminus\{0\}$, така че $aa^{-1}=1$;*
(ix) *дистрибутивни закони за събиране и умножение: $(a+b)c=ac+bc$ и $a(b+c)=ab+ac$ за произволни $a,b,c\in F$.*

Определение 1.10. *Подмножество $F\subseteq\mathbb{C}$ с поне два елемента е числово поле, ако за произволни $a,b\in F$, $b\neq 0$ е в сила*

$$a+b,a-b,ab,\frac{a}{b}\in F.$$

Твърдение 1.11. *(i) Всяко числово поле F е поле. В частност, множеството $\mathbb{C}$ на комплексните числа е поле.*
(ii) Множеството $\mathbb{Q}$ на рационалните числа е минималното числово поле, т.е. $\mathbb{Q}$ е числово поле, което се съдържа във всяко числово поле F.
(iii) Естествените числа $\mathbb{N}$ и целите числа $\mathbb{Z}$ не образуват числови полета.

Доказателство. (i) Събирането и умножението на комплексни числа се ограничава до събиране и умножение във F, защото F е затворено относно тези операции, съгласно Определение 1.10 за числово поле. Остава да проверим аксиомите (i)-(ix) за поле. Наистина, за произволни комплексни числа

$$a = a_0 + ia_1, \quad b = b_0 + ib_1, \quad c = c_0 + ic_1 \in \mathbb{C}$$

с $a_0, a_1, b_0, b_1, c_0, c_1 \in \mathbb{R}$ е в сила асоциативният закон за събиране

$$\begin{aligned} (a+b)+c &= [(a_0+b_0)+i(a_1+b_1)] + (c_0+ic_1) = \\ = [(a_0+b_0)+c_0] + i[(a_1+b_1)+c_1] &= [a_0+(b_0+c_0)] + i[a_1+(b_1+c_1)] = \\ &= (a_0+ia_1) + [(b_0+c_0)+i(b_1+c_1)] = a+(b+c), \end{aligned}$$

съгласно асоциативността на събирането на реални числа и правилото за събиране на комплексни числа. В частност, събирането на $a, b, c \in F$ е асоциативно. Комутативността на събирането

$$\begin{aligned} a+b &= (a_0+ia_1)+(b_0+ib_1) = (a_0+b_0)+i(a_1+b_1) = \\ &= (b_0+a_0)+i(b_1+a_1) = (b_0+ib_1)+(a_0+ia_1) = b+a \end{aligned}$$

на комплексни числа (а оттам и на числа от F) е следствие от комутативността на събирането на реални числа и правилото за събиране на комплексни числа. За произволен елемент $a \in F$ имаме $0 = a - a \in F$. Числото 0 изпълнява равенствата $a + 0 = a$ за всяко $a \in \mathbb{C}$, откъдето и за всяко $a \in F$. Всяко $a \in F$ има противоположно $-a = 0 - a \in F$, така че $a + (-a) = 0$. В сила е асоциативност на умножението на комплексни числа

$$\begin{aligned} (ab)c &= [(a_0+ia_1)(b_0+ib_1)]c = [(a_0b_0-a_1b_1)+i(a_0b_1+a_1b_0)](c_0+ic_1) = \\ &= [(a_0b_0-a_1b_1)c_0-(a_0b_1+a_1b_0)c_1] + i[(a_0b_0-a_1b_1)c_1+(a_0b_1+a_1b_0)c_0] = \\ &= [a_0(b_0c_0-b_1c_1)-a_1(b_0c_1+b_1c_0)] + i[a_0(b_0c_1+b_1c_0)+a_1(b_0c_0-b_1c_1)] = \\ &= (a_0+ia_1)[(b_0c_0-b_1c_1)+i(b_0c_1+b_1c_0)] = a[(b_0+ib_1)(c_0+ic_1)] = a(bc), \end{aligned}$$

благодарение на асоциативността на умножението на реални числа, комутативността на събирането на реални числа, дистрибутивността на събирането и умножението на реални числа, дистрибутивността на изваждането и умножението на реални числа, както и правилото за умножение на комплексни числа. Умножението на комплексни числа, а оттам и на елементи на F е комутативно, т.е.

$$\begin{aligned} ab &= (a_0+ia_1)(b_0+ib_1) = (a_0b_0-a_1b_1)+i(a_0b_1+a_1b_0) = \\ &= (b_0a_0-b_1a_1)+i(b_0a_1+b_1a_0) = (b_0+ib_1)(a_0+ia_1) = ba, \end{aligned}$$

вземайнки предвид комутативността на умножението на реални числа и правилото за умножение на комплексни числа. Ако $a \in F \setminus \{0\}$ е ненулев елемент на F, то $1 = \frac{a}{a} \in F$. Числото 1 изпълнява равенствата $1.a = a$ за всяко $a \in F$. Освен това, всяко $a \in F \setminus \{0\}$ има обратен относно умножението елемент $\frac{1}{a} \in F$, така че $a.\frac{1}{a} = 1$. В сила са и дистрибутивни закони за събиране и умножение. По-точно,

$$\begin{aligned}(a+b)c = [(a_0+ia_1)+(b_0+ib_1)]c = [(a_0+b_0)+i(a_1+b_1)](c_0+ic_1) = \\ = [(a_0+b_0)c_0-(a_1+b_1)c_1]+i[(a_0+b_0)c_1+(a_1+b_1)c_o] = \\ = (a_0c_0+b_0c_0-a_1c_1-b_1c_1)+i(a_0c_1+b_0c_1+a_1c_0+b_1c_0) = \\ = [(a_0c_0-a_1c_1)+i(a_0c_1+a_1c_0)]+[(b_0c_0-b_1c_1)+i(b_0c_1+b_1c_0)] = \\ = (a_0+ia_1)(c_0+ic_1)+(b_0+ib_1)(c_0+ic_1) = ac+bc,\end{aligned}$$

съгласно дистрибутивните закони за събиране и умножение на реални числа, комутативността на събирането на реални числа, както и правилата за събиране и умноженине на комплексни числа. Комбинирайки с изведената вече комутативност на умножението на комплексни числа, получаваме и другия дистрибутивен закон

$$a(b+c) = (b+c)a = ba+ca = ab+ac, \quad \forall a,b,c \in \mathbb{C}.$$

(ii) Да забележим, че множеството $\mathbb{Q}$ на рационалните числа е числово поле, защото съществуват поне две различни рационални числа и сума, разлика, произведение и частно на рационални числа е рационално число
Ако F е числово поле, то за произволен елемент $a \in F$ е в сила

$$0 = a - a \in F.$$

По определение, F има поне два елемента, така че F има ненулев елемент $a \in F \setminus \{0\}$. Следователно

$$1 = \frac{a}{a} \in F.$$

Оттук, за всяко естествено n е изпълнено

$$n = \underbrace{1+\ldots+1}_{n} \in F$$

и множеството $\mathbb{N}$ на естествените числа се съдържа в F. За всяко естествено n е в сила

$$-n = 0 - n \in F,$$

така че и отрицателните цели числа се съдържат в F. С това установихме, че множеството $\mathbb{Z}$ на целите числа се съдържа във всяко числово поле F. За произволни $a, b \in \mathbb{Z} \subset F$, $b \neq 0$ имаме

$$\frac{a}{b} = a : b \in F,$$

откъдето $\mathbb{Q} \subseteq F$ за полето $\mathbb{Q}$ на рационалните числа.
(iii) Множеството $\mathbb{N}$ на естествените числа е затворено относно събиране и умножение, но не и спрямо изваждане и деление. Например, $1, 2 \in \mathbb{N}$, но $1-2 = -1 \notin \mathbb{N}$ и $\frac{1}{2} \notin \mathbb{N}$.
Множеството $\mathbb{Z}$ на целите числа е затворено относно събиране, изваждане и умножение, но не и спрямо деление. Например, за $1, 2 \in \mathbb{Z}$ е в сила $\frac{1}{2} \notin \mathbb{Z}$.

□

Пример 1.12. *За произволно просто число p, множеството $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$ на остатъците при деление на p е нечислово поле относно събирането*

$$+ : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p, \quad \overline{a} + \overline{b} := \overline{a+b}, \quad \forall a, b \in \mathbb{Z}$$

и умножението

$$. : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p, \quad \overline{a}.\overline{b} := \overline{a.b}, \quad \forall a, b \in \mathbb{Z}.$$

Доказателство. Първо ще проверим коректността на събирането и умножението в $\mathbb{Z}_p$, т.е. независимостта на тези операции от избора на целочислени представители на съответните остатъци. За целта да забележим, че $\overline{x} = \overline{y}$ за $x, y \in \mathbb{Z}$ тогава и само тогава, когато x и y имат един и същи остатък при деление на p. Причина за това е, че ако $x = pq_1 + r_1$ и $y = pq_2 + r_2$ са деленията на $x, y \in \mathbb{Z}$ на p с частни $q_1, q_2 \in \mathbb{Z}$ и остатъци $r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1, r_2 \leq p-1$, то $x - y = p(q_1 - q_2) + (r_1 - r_2)$ има нулев остатък при деление на p точно когато съществува цяло число $s \in \mathbb{Z}$, така че $r_1 - r_2 = ps$. Вземайки предвид $-(p-1) = 0 - (p-1) \leq r_1 - r_2 \leq (p-1) - 0 = p - 1$, стигаме до извода, че $r_1 - r_2 = 9$ и $r_1 = r_2$. Ако $\overline{a} = \overline{a_1}$ и $\overline{b} = \overline{b_1}$, то $a_1 - a, b_1 - b \in p\mathbb{Z}$, откъдето

$$(a_1 + b_1) - (a + b) = (a_1 - a) + (b_1 - b) \in p\mathbb{Z} \quad \text{и}$$

$$a_1 b_1 - ab = (a_1 b_1 - a_1 b) + (a_1 b - ab) = a_1(b_1 - b) + (a_1 - a)b \in p\mathbb{Z}.$$

Следователно $\overline{a_1 + b_1} = \overline{a+b}$, $\overline{a_1 b_1} = \overline{ab}$ и действията събиране и умножение на остатъци не зависят от избора на целочислени представители.
Асоциативността и комутативността на събирането и умножението на остатъци, както и дистрибутивните закони за тези операции следват от свойствата на съответните операции с цели числа. По-точно,

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c})$$

за произволни $a, b, c \in \mathbb{Z}$, съгласно определението за събиране на остатъци и асоциативността на събирането на цели числа. Аналогично,

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}, \quad \forall \overline{a}, \overline{b} \in \mathbb{Z}_p$$

въз основа на определението за събиране на остатъци и комутативността на събирането на цели числа. Определението за умножение на остатъци и асоциативността на умножението на цели числа дават

$$(\overline{a}.\overline{b}).\overline{c} = \overline{ab}.\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}.\overline{bc} = \overline{a}(\overline{b}.\overline{c})$$

за всички $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_p$. От комутативността на умножението на цели числа и определението за умножение на остатъци получаваме

$$\overline{a}.\overline{b} = \overline{ab} = \overline{ba} = \overline{b}.\overline{a} \quad \text{за всички} \quad \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_p.$$

Левият дистрибутивен закон за събиране и умножение на цели числа, както и определенията за събиране и умножение на остатъци дават

$$(\overline{a} + \overline{b})\overline{c} = \overline{a+b}.\overline{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac} + \overline{bc} = \overline{ac} + \overline{b}.\overline{c}$$

за всички $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_p$. Комбинирайки с вече доказаната комутативност на умножението на остатъци, получаваме десния дистрибутивен закон за събиране и умножени

$$\overline{a}(\overline{b} + \overline{c}) = (\overline{b} + \overline{c})\overline{a} = \overline{b}.\overline{a} + \overline{ca} = \overline{a}.\overline{b} + \overline{a}.\overline{c}$$

за произволни $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_p$. За $0, 1 \in \mathbb{Z}$ и всеки остатък $\overline{a} \in \mathbb{Z}_p$ е изпълнено $\overline{0} + \overline{a} = \overline{a}$ и $\overline{1}.\overline{a} = \overline{a}$. Произволен остатък $\overline{a} \in \mathbb{Z}_p$ има противоположен $\overline{(-a)} \in \mathbb{Z}_p$, така че $\overline{a} + \overline{(-a)} = \overline{a + (-a)} = \overline{0}$. Ако $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$ е ненулев остатък, то произволен представител $a \in \mathbb{Z}$ е взаимно прост с p и съществуват цели числа $u, v \in \mathbb{Z}$, изпълняващи тъждеството на Безу $au + pv = 1$. Остатъкът $(\overline{a})^{-1} := \overline{u} \in \mathbb{Z}_p$ е обратен на $\overline{a}$ относно умножението, съгласно

$$\overline{1} = \overline{au + pv} = \overline{au} + \overline{pv} = \overline{a}.\overline{u} + \overline{p}.\overline{v} = \overline{a}.\overline{u} + \overline{0}.\overline{v} = \overline{a}.\overline{u} + \overline{0} = \overline{a}.\overline{u}.$$

Следователно множеството $\mathbb{Z}_p$ на остатъците при деление на просто число p е поле.
Полето $\mathbb{Z}_p$ не е числово. В противен случай, от Твърдение 1.11 (ii) следва, че полето $\mathbb{Z}_p$ с p елемента съдържа безкрайното поле $\mathbb{Q}$ на рационалните числа, което не е възможно.

□

Пример 1.13. *Множеството* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ *е числово поле.*

Доказателство. Множеството $\mathbb{Q}(\sqrt{2})$ съдържа поне две различни комплексни числа, например 0 и 1. За произволни $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ е изпълнено

$$(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Ако $c + d\sqrt{2} \neq 0$, то

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}}.\frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

защото $c^2 \neq 2d^2$ за $c, d \in \mathbb{Q}$, $(c, d) \neq (0, 0)$. По-точно, ако разложим числителите и знаменателите на c и d в прости множители и извършим съкращение, то целият степенен показател на 2 в дясната страна на $c^2 = 2d^2$ е нечетен, докато степенният показател на 2 в c^2 е четен. Това доказва $c^2 \neq 2d^2$ за $c, d \in \mathbb{Q}$. След като проверихме, че $\mathbb{Q}(\sqrt{2})$ е затворено относно действията събиране, изваждане, умножение и деление с ненулев елемент, получаваме, че $\mathbb{Q}(\sqrt{2})$ е числово поле.

□