Wykład 8
Zasadnicze twierdzenie algebry. Pojęcie pierścienia

1 Zasadnicze twierdzenie algebry i jego dowód

Definicja 8.1. Wielomianem o współczynnikach zespolonych nazywamy funkcję $f\colon \mathbb{C} \to \mathbb{C}$ postaci

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

gdzie $a_0, a_1, \ldots, a_n$ są ustalonymi liczbami zespolonymi oraz $n = 0, 1, \ldots$ Ponadto dla $a_n \neq 0$ mówimy, że n jest stopniem wielomianu f.

Lemat 8.2. *Niech f będzie wielomianem o współczynnikach zespolonych. Wówczas dla każdego $r > 0$ istnieje stała $K > 0$ taka, że*

$$|f(z_1) - f(z_2)| \leqslant K \cdot |z_1 - z_2|$$

dla wszystkich $z_1, z_2 \in \mathbb{C}$ takich, że $|z_1|, |z_2| < r$.

Dowód. Jeżeli $f(x) = a_0$ dla $x \in \mathbb{C}$, to wystarczy wziąć $K = 1$. Załóżmy więc, że $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, gdzie $n \geqslant 1$ i $a_n \neq 0$. Weźmy dowolne $z_1, z_2 \in \mathbb{C}$ takie, że $|z_1|, |z_2| < r$. Wtedy dla $k = 1, 2, \ldots, n$ mamy, że

$$z_1^k - z_2^k = (z_1 - z_2) \cdot (z_1^{k-1} + z_1^{k-2}z_2 + \ldots + z_1 z_2^{k-2} + z_2^{k-1})$$

oraz z nierówności trójkąta:

$$\begin{gathered} |z_1^{k-1} + z_1^{k-2}z_2 + \ldots + z_1 z_2^{k-2} + z_2^{k-1}| \leqslant \\ \leqslant |z_1|^{k-1} + |z_1|^{k-2}|z_2| + \ldots + |z_1||z_2|^{k-2} + |z_2|^{k-1} \leqslant k r^{k-1}. \end{gathered}$$

Stąd

$$\begin{gathered} |f(z_1) - f(z_2)| = |a_n(z_1^n - z_2^n) + a_{n-1}(z_1^{n-1} - z_2^{n-1}) + \ldots + a_1(z_1 - z_2)| \leqslant \\ \leqslant |a_n||z_1^n - z_2^n| + |a_{n-1}||z_1^{n-1} - z_2^{n-1}| + \ldots + |a_1||z_1 - z_2| \leqslant \\ \leqslant |a_n||z_1 - z_2| n r^{n-1} + |a_{n-1}||z_1 - z_2|(n-1)r^{n-2} + \ldots + |a_1||z_1 - z_2| = \\ = |z_1 - z_2|(|a_n| n r^{n-1} + |a_{n-1}|(n-1)r^{n-2} + \ldots + |a_2|2r + |a_1|), \end{gathered}$$

więc wystarczy wziąć $K = |a_n| n r^{n-1} + |a_{n-1}|(n-1)r^{n-2} + \ldots + |a_2|2r + |a_1|$. $\square$

Definicja 8.3. Powiemy, że liczba zespolona z_0 jest granicą ciągu (z_n) liczb zespolonych, jeżeli

$$\forall_{\varepsilon>0}\exists_{n_0\in\mathbb{N}}\forall_{n\geqslant n_0}|z_n - z_0| < \varepsilon.$$

Piszemy wtedy $\lim\limits_{n\to\infty} z_n = z_0$.

Lemat 8.4. *Niech f będzie wielomianem o współczynnikach zespolonych. Wówczas z $\lim\limits_{n\to\infty} z_n = z_0$ wynika, że $\lim\limits_{n\to\infty} |f(z_n)| = |f(z_0)|$.*

Dowód. Weźmy dowolne $\varepsilon > 0$. Z Lematu 8.2 dla $r = 1 + |z_0|$ istnieje stała $K > 0$ taka, że $|f(z) - f(z_0)| \leq K|z - z_0|$ dla wszystkich $z \in \mathbb{C}$ takich, że $|z| < 1 + |z_0|$, gdyż $|z_0| < 1 + |z_0|$. Ale $\lim\limits_{n\to\infty} z_n = z_0$, więc dla $\delta = \min\{\frac{\varepsilon}{2K}, 1\}$ istnieje $n_0 \in \mathbb{N}$ takie, że dla wszystkich $n \geqslant n_0$ jest $|z_n - z_0| < \delta$, czyli $|z_n - z_0| < 1$, a więc $|z_n| = |(z_n - z_0) + z_0| \leqslant$ $\leqslant |z_n - z_0| + |z_0| < 1 + |z_0|$, skąd $|f(z_n) - f(z_0)| \leqslant K\frac{\varepsilon}{2K} = \frac{\varepsilon}{2} < \varepsilon$ dla $n \geqslant n_0$. Oznacza to, że $\lim\limits_{n\to\infty} |f(z_n)| = |f(z_0)|$. □

Definicja 8.5. Powiemy, że ciąg (z_n) liczb zespolonych jest *ograniczony*, jeżeli istnieje stała $A > 0$ taka, że $|z_n| \leqslant A$ dla wszystkich $n \in \mathbb{N}$.

Lemat 8.6. *Z każdego ciągu ograniczonego liczb zespolonych można wybrać podciąg zbieżny do pewnej liczby zespolonej.*

Dowód. Niech (z_n) będzie ograniczonym ciągiem liczb zespolonych. Wtedy istnieje stała $A > 0$ taka, że $|z_n| \leqslant A$ dla wszystkich $n \in \mathbb{N}$. Ponadto dla $n = 1, 2, \ldots$ istnieją $a_n, b_n \in \mathbb{R}$ takie, że $z_n = a_n + b_n i$, więc $|a_n| \leqslant \sqrt{a_n^2 + b_n^2} = |z_n| \leqslant A$ i podobnie $|b_n| \leqslant A$ dla $n = 1, 2, \ldots$ Zatem (a_n) i (b_n) są ograniczonymi ciągami liczb rzeczywistych. Stąd z twierdzenia Weierstrassa istnieje podciąg (a_{k_n}) ciągu (a_n), który jest zbieżny do pewnej liczby rzeczywistej a_0. Zatem z twierdzenia Weierstrassa istnieje podciąg $(b_{l_{k_n}})$ ciągu (b_{k_n}) zbieżny do pewnej liczby rzeczywistej b_0. Stąd także podciąg $(a_{l_{k_n}})$ jest zbieżny do a_0. Weźmy dowolne $\varepsilon > 0$. Wtedy istnieje $n_0 \in \mathbb{N}$ takie, że dla wszystkich $n \geqslant n_0$ jest $|a_{l_{k_n}} - a_0| < \frac{\varepsilon}{\sqrt{2}}$ i $|b_{l_{k_n}} - b_0| < \frac{\varepsilon}{\sqrt{2}}$. Zatem dla $z_0 = a_0 + b_0 i$ oraz dla $n \geqslant n_0$ mamy $|z_{l_{k_n}} - z_0| = \sqrt{|a_{l_{k_n}} - a_0|^2 + |b_{l_{k_n}} - b_0|^2} < \sqrt{\frac{\varepsilon^2}{2} + \frac{\varepsilon^2}{2}} = \varepsilon$. Oznacza to, że $\lim\limits_{n\to\infty} z_{l_{k_n}} = z_0$. □

ZASADNICZE TWIERDZENIE ALGEBRY. *Każdy wielomian dodatniego stopnia o współczynnikach zespolonych posiada pierwiastek zespolony.*

Dla wielomianów stopnia 1 nasze twierdzenie zachodzi, bo mają one postać $f(x) = ax + b$, gdzie $a, b \in \mathbb{C}$ i $a \neq 0$ oraz wtedy $f(-\frac{b}{a}) = 0$.

Wystarczy zatem udowodnić to twierdzenie dla wielomianw stopni $\geqslant 2$. Ale jeżeli $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, gdzie $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$ i $n \geqslant 2$, to $f(x) = a_n \cdot g(x)$, gdzie $g(x) = x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \ldots + \frac{a_1}{a_n}x + \frac{a_0}{a_n}$ i wielomiany f i g mają takie same zbiory pierwiastków. Stąd wystarczy wykazać, że dla każdego $n \geq 2$ i dla

dowolnych $a_0, a_1, \ldots, a_{n-1} \in \mathbb{C}$ wielomian

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \tag{1}$$

posiada pierwiastek zespolony.

Lemat 8.7. *Dla wielomianu f postaci* (1) *i dla każdego $z \in \mathbb{C}$ takiego, że $|z| > 1 + |a_{n-1}| + \ldots + |a_0|$ mamy, że $|f(z)| > 1 + |a_0|$.*

Dowód. Załóżmy, że $z \in \mathbb{C}$ i $|z| > 1 + |a_{n-1}| + \ldots + |a_0|$. Wtedy $|z| > 1$, więc $|z|^k > 1$ dla $k = 1, 2, \ldots$ Stąd dla takich z mamy

$$|f(z)| = |z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0| \geqslant$$
$$\geqslant |z^n| - |a_{n-1}z^{n-1} + \ldots + a_1 z + a_0| \geq |z|^n - |a_{n-1}||z|^{n-1} - \ldots - |a_1||z| - |a_0|.$$

Ale $|z|^k \leqslant |z|^{n-1}$ dla $k = 0, 1, \ldots, n-1$, bo $|z| > 1$ i $n \geqslant 2$, więc

$$|f(z)| \geqslant |z|^n - |z|^{n-1} \cdot (|a_{n-1}| + \ldots + |a_1| + |a_0|) =$$
$$|z|^{n-1} \cdot (|z| - |a_{n-1}| - \ldots - |a_1| - |a_0|) \geqslant |z|^{n-1} \geq |z|,$$

bo $n \geq 2$ i $|z| > 1 + |a_{n-1}| + \ldots + |a_0|$. Stąd

$$|f(z)| > 1 + |a_{n-1}| + \ldots + |a_1| + |a_0| \geqslant 1 + |a_0|,$$

czyli $|f(z)| > 1 + |a_0|$ dla $|z| > 1 + |a_{n-1}| + \ldots + |a_1| + |a_0|$. □

Lemat 8.8. *Dla wielomianu f postaci* (1) *istnieje $z_0 \in \mathbb{C}$ takie, że*

$$|f(z)| \geqslant |f(z_0)|$$

dla każdego $z \in \mathbb{C}$.

Dowód. Ponieważ dla każdego $z \in \mathbb{C}$ jest $|f(z)| \geq 0$, więc zbiór $\{|f(z)| : z \in \mathbb{C}\}$ jest ograniczony z dołu. Posiada on zatem kres dolny q. Wtedy $|f(z)| \geq q$ dla każdego $z \in \mathbb{C}$ oraz dla dowolnego $m \in \mathbb{N}$ istnieje $z_m \in \mathbb{C}$ takie, że $|f(z_m)| < q + \frac{1}{m}$. Gdyby dla pewnego m było $|z_m| > 1 + |a_{n-1}| + \ldots + |a_1| + |a_0|$, to z Lematu 8.7,

$$|f(z_m)| > 1 + |a_0| = |f(0)| + 1 \geqslant q + 1 \geqslant q + \tfrac{1}{m},$$

skąd $|f(z_m)| > q + \frac{1}{m}$ i mamy sprzeczność. Stąd $|z_m| \leq 1 + |a_{n-1}| + \ldots + |a_0|$ dla $m \in \mathbb{N}$. Zatem z Lematu 8.6 istnieje podciąg (z_{k_n}) ciągu (z_n) taki, że $\lim\limits_{n\to\infty} z_{k_n} = z_0$ dla pewnego $z_0 \in \mathbb{C}$. Wówczas dla każdego $z \in \mathbb{C}$ i dla każdego m mamy, że $|f(z_m)| < |f(z)| + \frac{1}{m}$, skąd

$$|f(z)| > |f(z_{k_n})| - \tfrac{1}{k_n},$$

więc po przejściu do granicy z wykorzystaniem Lematu 8.4 uzyskamy, że $|f(z)| \geq |f(z_0)|$. $\square$

Udowodnimy teraz lemat, który zakończy dowód zasadniczego twierdzenia algebry.

Lemat 8.9. *Dla wielomianu f postaci* (1) *i dla liczby z_0 z Lematu* 8.8 *mamy, że* $f(z_0) = 0$.

Dowód. Niech $h(z) = f(z + z_0) = (z + z_0)^n + a_{n-1}(z + z_0)^{n-1} + \ldots + a_1(z + z_0) + a_0 = z^n + b_{n-1}z^{n-1} + \ldots + b_1 z + b_0$ dla pewnych $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$, $b_n = 1$. Niech k będzie najmniejszą liczbą naturalną taką, że $b_k \neq 0$. Wówczas $h(z) = z^n + b_{n-1}z^{n-1} + \ldots + b_k z^k + b_0$. Z Lematu 8.8 mamy, że dla każdego $z \in \mathbb{C}$

$$|z^n + b_{n-1}z^{n-1} + \ldots + b_k z^k + b_0| \geq |f(z_0)|$$

oraz $b_0 = h(0) = f(z_0)$, więc dla $z \in \mathbb{C}$ mamy

$$|z^n + b_{n-1}z^{n-1} + \ldots + b_k z^k + b_0| \geqslant |b_0|. \tag{2}$$

Dla $c \in (0, 1)$ podstawmy w nierówności (2): $z = c \cdot \sqrt[k]{-\frac{b_0}{b_k}}$. Otrzymamy wówczas

$$|c^n \left(\sqrt[k]{-\frac{b_0}{b_k}}\right)^n + b_{n-1}c^{n-1}\left(\sqrt[k]{-\frac{b_0}{b_k}}\right)^{n-1} + \ldots + b_k c^k \left(\sqrt[k]{-\frac{b_0}{b_k}}\right)^k + b_0| \geqslant |b_0|, \tag{3}$$

więc z (3) po uproszczeniach i podstawieniu

$$d_n = \left(\sqrt[k]{-\tfrac{b_0}{b_k}}\right)^n, d_{n-1} = b_{n-1}\left(\sqrt[k]{-\tfrac{b_0}{b_k}}\right)^{n-1}, \ldots, d_{k+1} = b_{k+1}\left(\sqrt[k]{-\tfrac{b_0}{b_k}}\right)^{k+1}$$

uzyskamy

$$|d_n c^n + d_{n-1}c^{n-1} + \ldots + d_{k+1}c^{k+1} - b_0 c^k + b_0| \geqslant |b_0| \text{ dla } c \in (0, 1). \tag{4}$$

Oznaczmy $g(x) = d_n x^{n-k-1} + d_{n-1}x^{n-k-2} + \ldots + d_{k+1}$. Wtedy z (4) mamy

$$|c^{k+1}g(c) + b_0(1 - c^k)| \geqslant |b_0| \text{ dla } c \in (0, 1). \tag{5}$$

Ponadto $|c^{k+1}g(c) + b_0(1 - c^k)| \leqslant |c^{k+1}g(c)| + |b_0||1 - c^k| = c^{k+1}|g(c)| + |b_0|(1 - c^k)$, bo $0 < c < 1$. Zatem z (5):

$$c^{k+1}|g(c)| + |b_0| - |b_0|c^k \geqslant |b_0| \text{ dla } c \in (0, 1),$$

a więc

$$c|g(c)| \geqslant |b_0| \text{ dla } c \in (0, 1).$$

Ponadto

$$|g(c)| = |d_n c^{n-k-1} + d_{n-1}c^{n-k-2} + \ldots + d_{k+1}| \leqslant$$
$$\leqslant |d_n|c^{n-k-1} + |d_{n-1}|c^{n-k-2} + \ldots + |d_{k+1}| \leqslant$$
$$|d_n| + |d_{n-1}| + \ldots + |d_{k+1}|,$$

bo $0 < c < 1$. Zatem

$$c(|d_n| + |d_{n-1}| + \ldots + |d_{k+1}|) \geqslant |b_0| \text{ dla } c \in (0,1).$$

Stąd po przejściu do granicy względem $c \to 0$ otrzymamy, że $0 \geq |b_0|$, czyli $|b_0| = 0$. Ale $f(z_0) = b_0$, więc $f(z_0) = 0$. $\square$

2 Pojęcie pierścienia

Definicja 8.10. *Pierścieniem* nazywamy system algebraiczny $(P, +, \cdot, 0, 1)$ taki, że
P1. $(P, +, 0)$ jest grupą abelową;
P2. $\forall_{a,b,c\in P}\ a \cdot (b + c) = a \cdot b + a \cdot c$;
P3. $\forall_{a,b,c\in P}\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
P4. $\forall_{a\in P}\ a \cdot 1 = a$;
P5. $\forall_{a,b\in P}\ a \cdot b = b \cdot a$.

Działanie oznaczane przez $+$ nazywamy *dodawaniem*, zaś działanie oznaczane przez $\cdot$ nazywamy *mnożeniem*, natomiast element oznaczony symbolem 1 nazywamy *jedynką pierścienia* P. Grupę abelową $(P, +, 0)$ nazywamy *grupą addytywną pierścienia* P i oznaczamy przez P^+. *Odejmowanie* w pierścieniu $(P, +, \cdot, 0, 1)$ definiujemy za pomocą wzoru:

$$a - b = a + (-b) \text{ dla dowolnych } a, b \in P. \tag{6}$$

Następujące stwierdzenie grupuje podstawowe własności działań w pierścieniu.

Stwierdzenie 8.11. *Niech $(P, +, \cdot, 0, 1)$ będzie pierścieniem. Wówczas:*
(i) $\forall_{a\in P}\ a \cdot 0 = 0 \cdot a = 0$,
(ii) $\forall_{a,b\in P}\ -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$ i $(-a) \cdot (-b) = a \cdot b$,
(iii) $\forall_{a,b,c\in P}\ (a + b) \cdot c = a \cdot c + b \cdot c$,
(iv) $\forall_{a\in P}\ (-1) \cdot a = a \cdot (-1) = -a$,
(v) $\forall_{a,a_1,\ldots,a_n\in P}\ a \cdot (a_1 + \ldots + a_n) = a \cdot a_1 + \ldots + a \cdot a_n$,
(vi) **6.** $\forall_{a,b,c\in P}\ a \cdot (b - c) = a \cdot b - a \cdot c$.

Dowód. (i). Ponieważ $0 = 0 + 0$, więc na mocy **P2**: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, czyli $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$, skąd z prawa skracania w grupach mamy, że $a \cdot 0 = 0$. Zatem na mocy **P5** także $0 \cdot a = 0$.

(ii). Na mocy **P2** i (i) mamy, że $a \cdot b + a \cdot (-b) = a \cdot [b + (-b)] = a \cdot 0 = 0$, skąd $a \cdot (-b) = -(a \cdot b)$. Stąd na mocy **P5**: $-(a \cdot b) = -(b \cdot a) = b \cdot (-a) = (-a) \cdot b$. Ponadto, $(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b$.

(iii). Na mocy **P5**, **P2** i znowu **P5** mamy, że $(a+b)\cdot c = c\cdot(a+b) = c\cdot a+c\cdot b = a\cdot c+b\cdot c$.

(iv). Na mocy **P4** i **P5** mamy, że $a = a \cdot 1 = 1 \cdot a$, więc z (ii) i **P5**, $-a = -(a \cdot 1) = a \cdot (-1) = (-1) \cdot a$.

(v). Indukcja względem n. Dla $n = 2$ teza wynika z **P2**. Załóżmy, że teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ i niech $a_1, \ldots, a_n, a_{n+1} \in P$. Wtedy na mocy **P2** i założenia indukcyjnego: $a\cdot(a_1+\ldots+a_n+a_{n+1}) = a\cdot[(a_1+\ldots+a_n)+a_{n+1}] = a\cdot(a_1+\ldots+a_n)+$ $+a \cdot a_{n+1} = a \cdot a_1 + \ldots + a \cdot a_n + a \cdot a_{n+1}$, czyli teza zachodzi dla liczby $n + 1$. □

(vi). Z określenia odejmowania, z **P2**, z (ii) i znowu z określenia odejmowania mamy, że $a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$. □

Ponieważ $(P,+,0)$ jest grupą abelową, więc ma sens *całkowita wielokrotność* $k \cdot a$ elementu $a \in P$ przez liczbę całkowitą k. Przypomnijmy jej określenie:

$0 \cdot a = 0$, $1 \cdot a = a$ oraz dla $n \in \mathbb{N}$: $n \cdot a = \underbrace{a + \ldots + a}_{n}$ i $(-n) \cdot a = (-a) + \ldots + (-a)$.

Z twierdzeń 1.13 i 1.14 wynika od razu następujące

Stwierdzenie 8.12. *Niech $(P, +, \cdot, 0, 1)$ będzie pierścieniem. Wówczas:*
(i) $\forall_{a\in P}\forall_{n,m\in\mathbb{Z}}\ n \cdot (m \cdot a) = (nm) \cdot a$,
(ii) $\forall_{a\in P}\forall_{n,m\in\mathbb{Z}}\ (n + m) \cdot a = n \cdot a + m \cdot a$,
(iii) $\forall_{a,b\in P}\forall_{n\in\mathbb{Z}}\ n \cdot (a + b) = n \cdot a + n \cdot b$.

Stwierdzenie 8.13. Dla dowolnych elementów a, b pierścienia P i dla każdego $k \in \mathbb{Z}$ zachodzi wzór:

$$k \cdot (a \cdot b) = (k \cdot a) \cdot b = a \cdot (k \cdot b). \tag{7}$$

Dowód. Ponieważ $0 \cdot (a \cdot b) = 0$, $(0 \cdot a) \cdot b = 0 \cdot b = 0$ i $a \cdot (0 \cdot b) = a \cdot 0 = 0$ na podstawie definicji mnożenia elementu pierścienia przez liczbę całkowitą 0 oraz na mocy Stwierdzenia 8.11 (i), więc dla $k = 0$ wzór (7) zachodzi. Załóżmy, że wzór (7) zachodzi dla pewnego $k \in \mathbb{N}_0$. Wtedy $(k+1)\cdot(a\cdot b) = k\cdot(a\cdot b)+a\cdot b = (k\cdot a)\cdot b+a\cdot b = (k\cdot a+a)\cdot b = [(k+1)\cdot a]\cdot b$ oraz $(k+1)\cdot(a\cdot b) = k\cdot(a\cdot b)+a\cdot b = a\cdot(k\cdot b)+a\cdot b = a\cdot(k\cdot b+b) = a\cdot[(k+1)\cdot b]$, więc wzór (7) zachodzi wówczas także dla liczby $k + 1$. Wobec tego na mocy zasady indukcji wzór (7) zachodzi dla każdego $k \in \mathbb{N}_0$.

Niech teraz $k = -n$, gdzie $n \in \mathbb{N}$. Wtedy $k \cdot (a \cdot b) = n \cdot [-(a \cdot b)] = n \cdot [(-a) \cdot b] = [n\cdot(-a))]\cdot b = (k\cdot a)\cdot b$ oraz $k\cdot(a\cdot b) = n\cdot[-(a\cdot b)] = n\cdot[a\cdot(-b)] = a\cdot[n\cdot(-b)] = a\cdot(k\cdot b)$, na mocy pierwszej części rozwiązania i własności całkowitej wielokrotności elementu grupy addytywnej pierścienia P. Wobec tego wzór (7) zachodzi także dla dowolnej ujemnej liczby całkowitej k, co kończy dowód. □

W pierścieniu P możemy też określić nieujemną całkowitą potęgę dowolnego elementu $a \in P$ przyjmując, że:
$a^0 = 1$, $a^1 = a$ oraz dla $n \in \mathbb{N}$: $a^{n+1} = a^n \cdot a$ (czyli $a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$).

Z Wniosku 1.4 wynika natychmiast następujące

Stwierdzenie 8.14. *Niech $(P, +, \cdot, 0, 1)$ będzie pierścieniem. Wówczas:*
(i) $\forall_{a\in P}\forall_{n,m\in\mathbb{N}_0}\ a^n \cdot a^m = a^{n+m}$.
(ii) $\forall_{a\in P}\forall_{n,m\in\mathbb{N}_0}\ (a^n)^m = a^{nm}$.

Stwierdzenie 8.15. Dla dowolnych elementów a, b pierścienia P i dla dowolnego $n \in \mathbb{N}$, $n \geq 2$ zachodzi wzór:

$$a^n - b^n = (a-b) \cdot \left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right). \tag{8}$$

Dowód. Po opuszczeniu nawiasów otrzymamy, że
$(a-b) \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-1} + b^{n-1}) = a^n + a^{n-1}b + \ldots + a^2b^{n-2} + ab^{n-1} +$
$-a^{n-1}b - a^{n-2}b - \ldots - ab^{n-1} - b^n = a^n - b^n$, co kończy dowód wzoru (8). $\square$

Podstawiając we wzorze (8) w miejsce b element $-b$ i uwzględniając to, że dla $k \in \mathbb{N}_0$, $(-b)^{2k} = b^{2k}$ oraz $(-b)^{2k+1} = -b^{2k+1}$ uzyskamy następujące

Stwierdzenie 8.16. Dla dowolnych elementów a, b pierścienia P i dla dowolnego $n \in \mathbb{N}$ zachodzi wzór:

$$a^{2n+1} + b^{2n+1} = (a+b) \cdot \left(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - \ldots + a^2b^{2n-2} - ab^{2n-1} + b^{2n}\right). \tag{9}$$

Stwierdzenie 8.17. Dla dowolnych elementów a, b pierścienia P i dla dowolnego $n \in \mathbb{N}$ zachodzi wzór:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k. \tag{10}$$

Dowód. Stosujemy indukcję względem n. Dla $n = 1$, $L = (a+b)^1 = a + b$, $P = \sum_{k=0}^{1} \binom{1}{k} a^{1-k}b^k = \binom{1}{0} a^1b^0 + \binom{1}{1} a^0b^1 = a \cdot 1 + 1 \cdot b = a + b$, czyli $L = P$ i teza zachodzi dla $n = 1$. Załóżmy, że wzór (10) zachodzi dla pewnej liczby naturalnej n. Wtedy $(a+b)^{n+1} = (a+b) \cdot (a+b)^n = a \cdot (a+b)^n + b \cdot (a+b)^n = a \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k + b \cdot$ $\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k}b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1} = a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k}b^k +$ $b^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^{k+1} = a^{n+1} + b^{n+1} + \sum_{j=0}^{n-1} \binom{n}{j+1} a^{n-j}b^{j+1} + \sum_{j=0}^{n-1} \binom{n}{j} a^{n-j}b^{j+1}$. Ale $\binom{n}{j+1} + \binom{n}{j} = \binom{n+1}{j+1}$ dla $j = 0, 1, \ldots, n-1$, więc uzyskujemy stąd, że $(a+b)^{n+1} = a^{n+1} +$

$$b^{n+1}+\sum_{j=0}^{n-1}\binom{n+1}{j+1}a^{n-j}b^{j+1} = a^{n+1}+b^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^{n+1-k}b^k = \sum_{j=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k.$$

Zatem wzór (10) jest wówczas prawdziwy także dla liczby $n+1$. Stąd na mocy zasady indukcji mamy tezę. □

Zagadka 1. Niech $P_1, \ldots, P_n$ będą pierścieniami. W zbiorze $P_1 \times \ldots \times P_n$ określamy dodawanie i mnożenie następująco:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n),$$

Niech $0 = (0, \ldots, 0)$ oraz $1 = (1, \ldots, 1)$. Udowodnij, że $(P_1 \times \ldots \times P_n, +, \cdot, 0, 1)$ tworzy pierścień.

Zagadka 2. Niech X będzie dowolnym niepustym zbiorem i niech P będzie pierścieniem. W zbiorze P^X wszystkich funkcji ze zbioru X w zbiór P wprowadzamy dodawanie i mnożenie, przyjmując, że dla dowolnych $f, g \in P^X$:

$$(f+g)(x) = f(x) + g(x) \text{ dla każdego } x \in X,$$
$$(f \cdot g)(x) = f(x) \cdot g(x) \text{ dla każdego } x \in X.$$

Udowodnij, że zbiór P^X z tymi działaniami jest pierścieniem.

Zagadka 3. Niech K będzie dowolnym ciałem. Udowodnij, że podzbiór $T_2(K) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in K \right\}$ zbioru 2×2-macierzy nad ciałem K, tworzy pierścień ze względu na zwykłe dodawanie i mnożenie macierzy.

Zagadka 4. Niech P będzie dowolnym pierścieniem. W zbiorze $P \times P$ wprowadzamy dodawanie i mnożenie przyjmując, że dla dowolnych $a, b, c, d \in P$:

$$(a, b) + (c, d) = (a + c, b + d) \text{ oraz } (a, b) \cdot (c, d) = (a \cdot c, a \cdot d + b \cdot c).$$

Udowodnij, że $(P \times P, +, \cdot, (0, 0), (1, 0))$ jest pierścieniem. Będziemy go oznaczali przez $D_2(P)$.

Zagadka 5. Niech T będzie niepustym zbiorem i niech $\{P_t\}_{t \in T}$ będzie rodziną pierścieni oraz $P = \prod_{t \in T} P_t$. W zbiorze P wprowadzamy dodawanie $+$ i mnożenie $\cdot$ przyjmując dla dowolnych $(a_t)_{t \in T}, (b_t)_{t \in T} \in P$, że

$$(a_t)_{t \in T} + (b_t)_{t \in T} = (a_t +_t b_t)_{t \in T}, \tag{11}$$

$$(a_t)_{t \in T} \cdot (b_t)_{t \in T} = (a_t \cdot_t b_t)_{t \in T}. \tag{12}$$

Udowodnij, że jeśli $0 = (0_t)_{t\in T}$ oraz $1 = (1_t)_{t\in T}$, to $(P, +, \cdot, 0, 1)$ jest pierścieniem.

Zagadka 6. Załóżmy, że w pierścieniu P istnieje $a \neq 0$ takie, że $a^n = 0$ dla pewnego naturalnego n. Udowodnij, że wówczas istnieje $c \in P \setminus \{0\}$ takie, że $c^2 = 0$.

Zagadka 7. Załóżmy, że w pierścieniu P istnieje a takie, że $a^n = 0$ dla pewnego naturalnego $n > 1$. Udowodnij, że wówczas $(1 - a) \cdot b = 1$ dla pewnego $b \in P$.