UMOWY:

0. $\square$ oznacza koniec rozumowania (czasem pustego); jeśli pewne jego fragmenty należy uzupełnić, to zamiast $\square$ używam $\boxminus$.

1. „Zadanie” oznacza prosty lemat do samodzielnego uzasadnienia, na ogół później wykorzystywany. By ułatwić powołanie się na tezę, polecenia („dowieść” itp.) są w sformułowaniu pominięte.

2. „Ćwiczenie” nie wymaga specjalnej inwencji, lecz umożliwia sprawdzenie, czy wcześniej przeczytana część jest zrozumiała.

3. „Zadania uzupełniające” to zadania nieco trudniejsze, niekiedy trudne lub przemycające dodatkowe wiadomości. Brak tu więc szerszego wyboru zadań – należy szukać ich w podanej lieraturze. Zadania ze zbioru Kostrykina dotykające bieżącego materiału nierzadko wymieniam (numeracja wg. pierwszego polskiego wydania, z 1995r).

4. Gwiazdka $*$ wskazuje materiał uzupełniający, nie wykorzystywany poza materiałem też oznaczonym gwiazdką; zaznacza też zadania trudniejsze lub dalej nie wykorzystywane. W przypadku zadań ze zbioru Kostrykina oznaczam tak zadania trudniejsze.

5. „p.x” oznacza punkt (część paragrafu) o numerze x w bieżącym paragrafie, §a.x oznacza punkt x w paragrafie a, §I.a.x oznacza to samo, ale w rozdziale I. (Może być stosowane np. w rozdziale IV, jeśli tak będzie.) Podobne są odniesienia do literatury.

I LICZBOWY ZESPOLONE I WSTĘPNE WIADOMOŚCI O WIELOMIANACH

§ 1. Liczby zespolone.

1. Liczby zespolone i działania na nich

Niech $\mathbb{C}$ oznacza zbiór wszystkich wyrażeń (napisów) postaci $x \boxplus yi$, gdzie $x, y \in \mathbb{R}$, zaś i jest ustalonym symbolem. Przykładem takich wyrażeń są $1 \boxplus (-5)i$, $\sqrt{3} \boxplus \pi i$, itp. (Użycie litery i ma za sobą długą tradycję, lecz matematycznie nie jest w żaden sposób wyróżnione. Tak i, jak $\boxplus$ traktujemy jako symbole, nie nadając im obecnie żadnego znaczenia matematycznego.)

Wyrażenia $z = x \boxplus yi$ oraz $z' = x' \boxplus y'i$ uważamy za równe tylko wtedy, gdy $x = x'$ oraz $y = y'$. Dwa wyrażenia dodajemy i mnożymy stosując wzory

$$(x \boxplus yi) + (x' \boxplus y'i) := (x + x') \boxplus (y + y')i$$

$$(x \boxplus yi)(x' \boxplus y'i) := (xx' - yy') \boxplus (yx' + xy')i$$

gdzie w nawiasach po prawej stronie wykonywane są działania arytmetyczne w $\mathbb{R}$. Wzory te łatwo zapamiętać: odpowiadają one dodawaniu i mnożeniu wyrażeń algebraicznych przy założeniu, że $i^2 = -1$.

Zadanie 1. Mają miejsce równości:
a) $(x \boxplus 0i) + (x' \boxplus 0i) = (x + x') \boxplus 0i$ oraz $(x \boxplus 0i)(x' \boxplus 0i) = xx' \boxplus 0i$.
b) $x \boxplus yi = (x \boxplus 0i) + (y \boxplus 0i)(0 \boxplus 1i)$.

Dla krótkości $x \boxplus 0i$ zapisujemy jako x, zaś $0 \boxplus i$ jako i. Te uproszczenia oznaczeń prowadzą do utożsamienia zbioru $\mathbb{R}' := \{x \boxplus 0i : \ x \in \mathbb{R}\} \subset \mathbb{C}$ ze zbiorem $\mathbb{R}$ liczb rzeczywistych, i w ten sposób do spojrzenia na $\mathbb{C}$ jako na zbiór zawierający $\mathbb{R}$. Nie jest to źródłem nieporozumień, ponieważ działania algebraiczne w $\mathbb{R}$ i $\mathbb{R}'$ odpowiadają sobie, jak pokazuje część a) zadania. Zaś na podstawie części b) możemy też zamiast $x \boxplus yi$ pisać $x + yi$; będziemy tak odtąd zawsze czynić.

Elementy zbioru $\mathbb{C}$ nazywamy **liczbami zespolonymi.** Tak więc jeśli z jest liczbą zespoloną, to $z = x + yi$ dla pewnych jednoznacznie wyznaczonych $x, y \in \mathbb{R}$; liczbę x nazywamy **częścią rzeczywistą** z i oznaczamy $\mathrm{Re}(z)$, a y **częścią urojoną** z i oznaczamy $\mathrm{Im}(z)$. (Oznaczenia te odpowiadają nazwom angielskim „Real part of z" i „Imaginary part of z" i podobnym nazwom niemieckim, z których się wywodzą.) Z definicji,

$$\mathrm{Re}(z), \mathrm{Im}(z) \in \mathbb{R} \text{ oraz } \ z = \mathrm{Re}(z) + \mathrm{Im}(z)i \quad \forall z \in \mathbb{C}. \tag{0}$$

Zbiór $\mathbb{R}' = \{z \in \mathbb{C} : \mathrm{Im}(z) = 0\}$ nazywamy **osią rzeczywistą**, a $\{z \in \mathbb{C} : \mathrm{Re}(z) = 0\}$ –**osią urojoną**. Liczby do tych osi należące nazywamy rzeczywistymi lub czysto urojonymi, odpowiednio.

Twierdzenie 1. *i) Działanie dodawania w $\mathbb{C}$ jest przemienne i łączne (tzn. $a + b = b + a$ oraz $a + (b + c) = (a + b) + c$ dla każdych $a, b, c \in \mathbb{C}$). Działanie mnożenia też jest przemienne i łączne.*

ii) 0 jest elementem neutralnym dla dodawania (tzn. $a + 0 = a$ dla każdego $a \in \mathbb{C}$), zaś 1 dla mnożenia (tzn. $a \cdot 1 = a$ dla każdego $a \in \mathbb{C}$).

iii) Mnożenie jest rozdzielne względem dodawania, tzn. $a \cdot (b + c) = a \cdot b + a \cdot c$ dla wszystkich $a, b, c \in \mathbb{C}$.

iv) W $\mathbb{C}$ wykonywalne jest dzielenie przez elementy różne od zera, tzn. dla każdych $a, b \in \mathbb{C}, b \neq 0$, istnieje dokładnie jeden element $z \in \mathbb{C}$ taki, że $zb = a$. Podobnie, w $\mathbb{C}$ wykonywalne jest odejmowanie, tzn. dla każdych $a, b \in \mathbb{C}$ istnieje jedyny element $z' \in \mathbb{C}$ taki, że $z' + b = a$.

Element z z części iv) oznaczać będziemy przez a/b lub $\frac{a}{b}$ lub ab^{-1}, zaś element z' z tej części – przez $a - b$.

Wykonywalność odejmowania w $\mathbb{C}$ i teza ii) wynikają wprost z przyjętych definicji i własności liczb rzeczywistych. Podobnie jest z łącznością dodawania i z przemiennością obu działań. Teza iii) oraz łączność mnożenia są bardziej zawiłe jeśli wyrazić je przez liczby rzeczywiste (będzie ich sześć), stanowiące części rzeczywiste i urojone liczb a, b i c; nietrudno jednak dowieść otrzymanych tożsamości. (Nieco inny dowód proponuje poniższe zadanie.) Natomiast wykonalność dzielenia będzie udowodniona w p.3.

Zadanie 2. a) Dowieść równości $a(b + c) = ab + ac$ gdy liczba b jest rzeczywista, a liczba c czysto urojona, a także gdy liczba a jest rzeczywista lub czysto urojona. W oparciu o to dowieść tezy iii).

b) Podobnie, dowieść równości $a(bc) = (ab)c$ gdy liczba a jest rzeczywista lub czysto urojona, i w oparciu o to i o iii) dowieść łączności mnożenia.

Zadanie 3. * Dowieść w oparciu o równość $i^2 = -1$, że w zbiorze $\mathbb{C}$ <u>nie</u> można określić relacji $<$ takiej, że
a) dla każdych $z, z' \in \mathbb{C}$ zachodzi $z < z'$ lub $z = z'$ lub $z > z'$, i możliwości te wykluczają się wzajemnie, oraz
b) jeśli $z > 0$ i $z' > 0$, to $zz' > 0$ i $z + z' > 0$, zaś jeśli $z < 0$ i $z' < 0$, to $z + z' < 0$.

Mimo to, piszemy $x + 0i < x' + 0i$ jeśli $x, x' \in \mathbb{R}$ oraz $x < x'$. Należy jednak pamiętać o tym, że wyłączywszy przypadek gdy z i z' leżą na osi rzeczywistej, nie została dla $z, z' \in \mathbb{C}$ określona żadna nierówność pomiędzy nimi.

<u>Zadania ze zbioru Kostrykina:</u> w §I.6.1: 1a),b),c), od 2 do 5, 11.

2. Ujęcie Hamiltona liczb zespolonych.

Podane ujęcie ma tę słabą stronę, że terminy „wyrażenie” czy „napis” nie są jasno zdefiniowane. W. R. Hamilton wskazał w pierwszej połowie 19 w., jak temu zaradzić. Ponieważ wyrażenie $x \boxplus yi$ jest jednoznacznie wyznaczone przez parę (x, y) liczb rzeczywistych, więc można o „wyrażeniach” wcale nie wspominać, a $\mathbb{C}$ zdefiniować jako zbiór uporządkowanych par (x, y) liczb rzeczywistych, w którym wprowadzono działania dodawania i mnożenia przy pomocy wzorów: $(x, y) + (x', y') := (x + x', y + y')$ oraz $(x, y)(x', y') := (xx' - yy', xy' + x'y)$. Oznaczając $(0, 1)$ przez i, a także parę postaci $(x, 0)$ przez x, odtwarzamy „wyrażeniowy” sposób zapisywania liczb zespolonych: mamy bowiem $(x, y) = x + yi$ zgodnie z przyjętymi działaniami w $\mathbb{C}$. Pdejście takie jest już całkiem ścisłe, gdyż pary uporządkowane definiuje się łatwo przy pomocy najprostszych pojęć teorii mnogości. Ceną, jaką się płaci za tę „matematyczną poprawność” jest to, że definicja mnożenia, a także cały sposób postępowania, wydają się wyciągnięte z kapelusza: podać je może dopiero ktoś, kto bardziej naiwny sposób definiowania $\mathbb{C}$ już przemyślał. Dlatego w dalszej części nie zawsze będziemy się na podobną ścisłość silić, i gdzie to wygodne (np. przy omawianiu wielomianów) będziemy mówić o „wyrażeniach", których sposób dodawania czy mnożenia podamy.

3. Geometryczna interpetacja i wykonalność dzielenia.

Liczbę zespoloną $x+yi$ przedstawiać będziemy jako punkt płaszczyzny $\mathbb{R}\times\mathbb{R}$ o odciętej x i rzędnej y. Ustala to wzajemnie jednoznaczną odpowiedniość pomiędzy zbiorem $\mathbb{C}$ a zbiorem punktów tej płaszczyzny. Dzięki temu, możemy w dalszej części myśleć o $\mathbb{C}$ jako o płaszczyźnie, w której ustalono prostokątny układ współrzędnych i którą rozważamy z opisanymi powyżej działaniami. Płaszczyzna $\mathbb{R}\times\mathbb{R}$, której każdy punkt (x, y) interpretowany jest jako liczba zespolona $x + yi$, nazywana jest **płaszczyzną liczb zespolonych** lub **płaszczyzną Gaussa-Arganda** (choć pierwszy użył jej C.Wessel, a Gauss –ostatni.). Prosta $y = 0$ tej płaszczyzny nazywana jest jej **osią rzeczywistą**, a prosta $x = 0$ **osią urojoną**. Punktem przecięcia tych osi jest liczba $0 \in \mathbb{C}$. Liczby osi urojonej nazywamy czysto urojonymi, a osi rzeczywistej -rzeczywistymi; ostatnia nazwa pieczętuje dokonane już wcześniej utożsamienie $\mathbb{R}$ z $\mathbb{R}' = \{x + 0i : x \in \mathbb{R}\}$.

W dalszej części nie będziemy odróżniać liczby $x+yi$ od odpowiadającego jej punktu płaszczyzny Gaussa-Arganda, a tę oznaczać bedziemy przez $\mathbb{C}$, tak samo jak zbiór liczb zespolonych. Identyfikacja taka ułatwia wykorzystanie pojęć geometrycznych do badania liczb zespolonych i do opisu ich własności.W szczególności, dla $z = x+yi \in \mathbb{C}$ określamy:

$|z| := \sqrt{x^2 + y^2}$ = odległość od 0 do z,

$\overline{z} := x - yi = \mathrm{Re}(z) - \mathrm{Im}(z)i$ = obraz z przy symetrii prostopadłej względem osi rzeczywistej,

$\mathrm{Arg}_{[0,2\pi)}(z)$:=jedyna liczba z przedziału $[0, 2\pi)$, będąca łukową miarą zorientowanego kąta o wierzchołku w 0 i pierwszym ramieniu przechodzącym przez 1, a drugim przez z. (Tu zakładamy $z \neq 0$.) W dalszej części, $\mathrm{Arg}_{[0,2\pi)}$ często skracamy do Arg.[1]

Wielkości te nazywamy, odpowiednio, **modułem, sprzężeniem** i **argumentem głównym** liczby zespolonej z.

RYSUNEK

Uwaga 1. a) Rysunki takie, jak powyższy, są pomocne, lecz mogą prowokować do następującego błędu. Rzut prostokątny na oś urojoną zaznaczonego na rysunku punktu

[1] W wielu podręcznikach, $\mathrm{Arg}(z)$ oznacza liczbę, otrzymaną przez dwukrotne zastąpienie w tej definicji przedziału $[0, 2\pi)$ przez $(-\pi, \pi]$.

$z = -4 + 2i$ jest równy, jako punkt płaszczyzny Gaussa-Arganda, liczbie $2i$. Nie jest to jednak część urojona z, gdyż ta jest równa 2. Podobnie, częścią urojoną czysto urojonej liczby i nie jest i, lecz 1, itp. (Jest tak za sprawą przyjętej przez nas definicji, która jednak jest powszechnie stosowana i wygodna.)

b) Dla $x \in \mathbb{R}$, moduł liczby zespolonej $x + 0i$ jest równy wartości bezwzględnej x, rozumianej jako niemniejsza z liczb x oraz $-x$. Dla liczb zespolonych taka definicja wartości bezwzględnej traci sens (bo nie jest w $\mathbb{C}$ określona relacja $<$, patrz zadanie 3 w p.1), a **wartością bezwzględną** liczby zespolonej niekiedy nazywa się jej moduł.

c) Moduł, sprzężenie i części rzeczywista i urojona liczby z określiliśmy jednoznacznie dla każdego $z \in \mathbb{C}$, zaś $\mathrm{Arg}(z)$ tylko dla $z \neq 0$. Przyjmiemy więc ponadto, że równość $\varphi = \mathrm{Arg}(0)$ zachodzi dla każdej liczby rzeczywistej φ.

Z definicji łatwo wynikają dla $z, z' \in \mathbb{C}$ zależności:

$$\overline{\overline{z}} = z, \quad \overline{z + z'} = \overline{z} + \overline{z'}, \quad \overline{zz'} = \overline{z}\,\overline{z'}; \tag{1}$$

$$\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z}), \quad \mathrm{Im}(z) = \frac{i}{2}(\overline{z} - z), \tag{2}$$

$$|z|^2 = (\mathrm{Re}(z))^2 + (\mathrm{Im}(z))^2, \text{ w szczeglnoci } |\mathrm{Re}(z)| \leq |z| \text{ oraz } |\mathrm{Im}(z)| \leq |z|, \tag{3}$$

$$|z| = |\overline{z}| = |-z| \text{ oraz } |z| = \sqrt{z\overline{z}} \text{ (nieujemny pierwiastek z liczby rzeczywistej } z\overline{z}). \tag{4}$$

Na koniec, ponieważ odległość pomiędzy punktami płaszczyzny o współrzędnych (x, y) i (x', y'), odpowiednio, wynosi $\sqrt{(x - x')^2 + (y - y')^2}$, więc z definicji modułu

$$|z - z'| = \text{ odległość pomiędzy punktami } \quad z, z' \in \mathbb{C}. \tag{5}$$

Podamy teraz (brakujący dotąd) dowód wykonalności dzielenia w $\mathbb{C}$, oparty na tożsamości $z\overline{z} = |z|^2$ z (4). Jeśli $zb = a$ i $b \neq 0$, to także $zb\overline{b} = a\overline{b}$, co mnożąc stronami przez odwrotność $\frac{1}{|b|^2}$ liczby rzeczywistej $|b|^2 = b\overline{b}$ daje $z = \frac{1}{|b|^2}a\overline{b}$. Przeciwnie, liczba $\frac{1}{|b|^2}a\overline{b}$ spełnia nałożony na $a : b$, bo

$$(\frac{1}{|b|^2}a\overline{b})b = \frac{1}{|b|^2}a(b\overline{b}) = \frac{1}{|b|^2}a|b|^2 = a$$

(W rozumowaniu tym kilkukrotnie korzystaliśmy z łączności i przemienności mnożenia).□

Zadanie 1. W oparciu o tożsamość $|z|^2 = z\overline{z}$ dowieść dla $u, v \in \mathbb{C}$:
a) $|u + v|^2 = |u|^2 + |v|^2 + 2\mathrm{Re}(u\overline{v})$.
b) $|u + v|^2 + |u - v|^2 = 2(|u|^2 + |v|^2)$.

Zadania uzupełniające. (Nadal, u, v, w itp. to ustalone liczby zespolone.)

1. Dowieść, że jeśli $|u| = |v|$ i $u \neq v$, to istnieją dokładnie 2 liczby zespolone z takie, że $|z - u| = |z - v|$ i $|z| = 1$. Podać interpretację geometryczną i sposób wyznaczenia.

2. Dowieść **tożsamości Apolloniusza**: $|v-u|^2+|v-w|^2 = \frac{1}{2}|u-w|^2+2|v-\frac{1}{2}(u+w)|^2$.

3. a) Dowieść tożsamości $(|u_1|^2+|u_2|^2)(|v_1|^2+|v_2|^2) = |u_1v_1-u_2\overline{v_2}|^2+|u_1v_2+u_2\overline{v_1}|^2$.
b) Wywnioskować, że jeśli każda z liczb naturalnych k, l jest sumą 4 kwadratów liczb całkowitych, to i kl jest taką sumą.

Tożsamość z a), wyrażona przez części rzeczywiste i urojone liczb u, u_1, v, v_1, wiąże 8 liczb rzeczywistych i nazywana jest **tożsamością Eulera**.

4. Udowodnić, że jeśli $|u| < 1$ i $|v| < 1$, to $|u+v| < |1+u\overline{v}|$. (Wskazówka: obliczyć kwadrat obu stron.)

5. Udowodnić, że jeśli $|w| = 1$ i $w \neq 1$, to liczba $\frac{w+1}{w-1}$ jest czysto urojona, oraz że implikacja przeciwna też ma miejsce.

6. Dla $\lambda \in \mathbb{C}$ rozwiązać równanie $\overline{z} = \lambda z$ w liczbach zespolonych $z \neq 0$.

7. Udowodnić, że jeśli $z \neq 1$ jest liczbą zespoloną o module 1, to równanie istnieje dokładnie jedna liczba rzeczywista $t \in \mathbb{R}$ taka, że $z = (1+ti)/(1-ti)$.

8. Rozpatrzmy równanie $a|z|^2 + \mathrm{Re}(uz) + b = 0$, gdzie $a, b \in \mathbb{R}$ i $u \in \mathbb{C}$ są dane.
a) Dowieść, że opisuje ono prostą gdy $a = 0$ i $u \neq 0$, zaś okrąg, punkt lub $\emptyset$ gdy $a \neq 0$.
b) Dowieść, że każdą prostą i każdy okrąg można opisać równaniem takiej postaci.

9. * Niech $z_k \in \mathbb{C} \setminus \{0\}$ dla $k = 1, 2, 3, 4$. Dowieść równoważności warunków
a) $z_1z_2z_3z_4$ jest rombem, którego przekątne przecinają się w zerze;
b) $\sum_k z_k = 0$,
c) dla każdego $k \leq 4$ istnieje $l \leq 4$ takie, że $z_k + z_l = 0$.

Zadania ze zbioru Kostrykina: od 6 do 9 w w §I.6.1 i 1,2,5,10 w §I.6.6.

4. Nierówności trójkąta

Z (5) wynika, że trójkąt o wierzchołkach $0, z_1$ i $z_1 + z_2$ ma boki długości $|z_1|, |z_2|$ i $|z_1 + z_2|$. Ponieważ długość każdego boku jest niewiększa niż suma długości pozostałych dwóch boków, a niemniejsza niż różnica tychże, więc otrzymujemy następujące **nierówności trójkąta:**

$$||z_1| - |z_2|| \leq |z_1 + z_2| \leq |z_1| + |z_2|, \text{ dla każdych } z_1, z_2 \in \mathbb{C}. \tag{6}$$

Ze względu na wagę tych nierówności podamy też samodzielny (nie odwołujący się do geometrii szkolnej) dowód drugiej z nich. Mamy mianowicie

$$|z_1 + z_2|^2 = |z_1|^2 + |z_2|^2 + 2\mathrm{Re}(z_1\overline{z_2}) \leq |z_1|^2 + |z_2|^2 + 2|z_1||\overline{z_2}| = (|z_1| + |z_2|)^2$$

przy czym pierwsza równość wynika z zadania 1a) w p.3, a nierówność – z (3). □

Odnotujmy, że w (6) można zastąpić $|z_1+z_2|$ przez $|z_1-z_2|$ (dla dowodu wystarcza zastosować (6) do z_1 i $-z_2$).

Ćwiczenie. Otrzymać pierwszą nierówność w (6), opierając się na drugiej.

Ćwiczenie. Interpretując $\mathbb{C}$ jako płaszczyznę naszkicować zbiory
a) $\{z \in \mathbb{C}: \ |z-1|=1\}$, c) $\{z \in \mathbb{C}: \ \mathrm{Re}(z)=|z|\}$,
b) $\{z \in \mathbb{C}: \ 1 \leq |z-i| < 2\}$, d)$\{z \in \mathbb{C}: \ \mathrm{Arg}(z)=\pi/4\}$.

Zadanie 1. Jeśli $|z_1+z_2|=|z_1|+|z_2|$ i $z_1 \neq 0$, to $z_2 = tz_1$ dla pewnej nieujemnej liczby rzeczywistej t.

Zadania ze zbioru Kostrykina: 5 w §I.6.2.

5. Zapis biegunowy i wzory de Moivre'a.

Lemat 1. *a) Gdy $r=|z|$ i $\varphi = \mathrm{Arg}(z)$, to $z = r(\cos\varphi + i\sin\varphi)$.*

b) Przeciwnie, jeśli zachodzi równość $z = r(\cos\varphi + i\sin\varphi)$, gdzie $r \geq 0$ i $\varphi \in \mathbb{R}$, to $r=|z|$ i φ różni się od $\alpha := Arg(z)$ o całkowitą wielokrotność liczby 2π.

Dowód. a) wynika z definicji funkcji trygonometrycznych i przyjętych definicji.

b) Niech $z = r(\cos\varphi + i\sin\varphi)$, gdzie $r \geq 0$. Ponieważ $\sqrt{r^2\cos^2\varphi + r^2\sin^2\varphi} = r$, więc $|z|=r$. Z a) wynika więc, że $\cos\varphi + i\sin\varphi = \cos\alpha + i\sin\alpha$. Zatem $\cos\varphi = \cos\alpha$ i $\sin\varphi = \sin\alpha$, wobec czego $\varphi - \alpha$ jest całkowitą wielokrotnością liczby 2π.□

Definicja. a) Dowolną liczbę rzeczywistą φ, różniącą się od $\mathrm{Arg}(z)$ o całkowitą wielokrotność 2π, nazywamy **argumentem** liczby z; piszemy wówczas $\varphi = \arg(z)$.

b) Przedstawienie $z \in \mathbb{C}$ w postaci $z = r(\cos\varphi + i\sin\varphi)$, gdzie $r \geq 0$, nazywamy **trygonometrycznym** lub **biegunowym.**

Zauważmy jeszcze, że jeśli $\overline{z} \neq z$, to $\mathrm{Arg}(\overline{z}) = 2\pi - \mathrm{Arg}(z)$. Rezygnując z argumentów głównych mamy prostszy wzór, prawdziwy dla każdego $z \in \mathbb{C}$:

$$\arg(\overline{z}) = -\arg(z). \tag{7}$$

Oznacza on: jesli φ jest dowolnym argumentem jednej z liczb $z, \overline{z}$, to $-\varphi$ jest argumentem drugiej.

Zadanie 1. Jeśli $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ oraz $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, to $z_1z_2 = r_1r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2))$. (Potrzebne tu tożsamości dotyczące funkcji cos i sin powinny być znane ze szkoły; por. też dalej zadanie 1 z §II.1.3.)

Twierdzenie 1. *Dla każdych $z_1, z_2 \in \mathbb{C}$ prawdziwe są wzory*

$$|z_1z_2| = |z_1||z_2| \text{ oraz } \arg(z_1z_2) = \arg(z_1) + \arg(z_2), \tag{8}$$

przy czym druga równość oznacza: jeśli φ_1 jest dowolnym argumentem z_1, a φ_2 dowolnym argumentem z_2, to $\varphi_1 + \varphi_2$ jest argumentem $z_1 z_2$.

Dowód. Mamy $z_k = |z_k|(\cos\varphi_k + i\sin\varphi_k)$ dla $k = 1, 2$. Wykorzystosując kolejno lemat i zadanie otrzymujemy tezę.

Zadanie 2. Jeśli $z_2 \neq 0$, to

$$\arg(z_1/z_2) = \arg(z_1) - \arg(z_2), \qquad |z_1/z_2| = \frac{|z_1|}{|z_2|}, \qquad \overline{z_1/z_2} = \frac{\overline{z_1}}{\overline{z_2}} \tag{9}$$

Stosując indukcję matematyczną otrzymujemy analogiczne tezy dla iloczynu skończenie wielu liczb zespolonych. W szczególności,

$$\arg(z^n) = n \cdot \arg(z) \quad \text{oraz} \quad |z^n| = |z|^n \quad \text{dla} \quad n \in \mathbb{Z} \text{ i } z \in \mathbb{C}. \tag{10}$$

Dla liczby zespolonej $z = \cos\varphi + i\sin\varphi$ otrzymujemy równości:

$$(\cos\varphi + i\sin\varphi)^n = \cos(n\varphi) + i\sin(n\varphi) \text{ dla } n = 0, \pm1, \pm2, \ldots \text{ i } \varphi \in \mathbb{R}. \tag{11}$$

Wzory (10) i (11) noszą nazwę **wzorów de Moivre'a.**

Wskażmy jeszcze, jak wzory de Moivre'a pozwalają na wyznaczenie wartości funkcji trygonometrycznych wielokrotności zadanego kąta φ. W tm celu wystarczy wyliczyć lewą stronę (5) na drodze bezpośredniego potęgowania. Porównując otrzymane wielkości znajdujemy wzory wyrażające $\cos(n\varphi)$ oraz $\sin(n\varphi)$ poprzez $\cos\varphi$ i $\sin\varphi$.

Przykład 1. Niech $n = 3$. Wówczas

$$(\cos\varphi + i\sin\varphi)^3 = \cos^3\varphi + 3i\cos^2\varphi\sin\varphi - 3\cos\varphi\sin^2\varphi - i\sin^3\varphi.$$

Zatem:

$$\cos(3\varphi) = \cos^3\varphi - 3\cos\varphi\sin^2\varphi \qquad \text{oraz} \qquad \sin(3\varphi) = 3\cos^2\varphi\sin\varphi - \sin^3\varphi.$$

Ćwiczenie. Wyrazić $\cos(4\varphi)$ oraz $\sin(4\varphi)$ poprzez $\cos(\varphi)$ i $\sin(\varphi)$.

Korzystając z równości $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ można otrzymać analogiczne wzory i dla $n > 4$.

Zadania uzupełniające.

1. Podać tożsamości otrzymane przez porównanie części rzeczywistych wzorów Newtona i de Moivre'a na z^n, gdy:
   a) $z = 1 + i$, n jest liczbą parzystą;
   b) $z = -1 + i\sqrt{3}$, n jest liczbą parzystą;

c) Te same wartości z, lecz bez założenia parzystości n i przy prównaniu także części urojonych.

2. Dowieść, że $\sum_{k=0}^{n} \cos(k\varphi) = \frac{1}{2} + \frac{\sin((n+\frac{1}{2})\varphi)}{2\sin(\frac{1}{2}\varphi)}$. (Wskazówka: $\sum_{k=0}^{n} z^k = \frac{z^{n+1}-1}{z-1}$.)

Zadania ze zbioru Kostrykina: większość z §I.6.2 (ostatnie dwa są trudne).

6. Interpretacja działań w $\mathbb{C}$ i przekształceń afinicznych $\mathbb{C} \to \mathbb{C}$.

Dodawanie liczb zespolonych można łatwo interpretować geometrycznie: $z_1 + z_2$ jest czwartym wierzchołkiem równoległoboku, którego pozostałymi (kolejnymi) wierzchołkami są $z_1, 0, z_2$. Stąd $z_1 - z_2$ jest czwartym wierzchołkiem równoległoboku, którego pozostałymi (kolejnymi) wierzchołkami są $z_1, 0, -z_2$.

Ćwiczenie. Uzasadnić, dlaczego równość z zadania 1b) w p.3 nazywana jest „regułą równoległoboku". Dać też interpretację tożsamości Apolloniusza z p.3.

Natomiast dla opisu mnożenia w $\mathbb{C}$ zajmijmy się ogólniej funkcja $f : \mathbb{C} \to \mathbb{C}$, zadaną wzorem $f(z) = az + b$, dla pewnych $a, b \in \mathbb{C}$. Funkcję taką nazwiemy **afiniczną**. Interesuje nas przypadek, gdy jest ona różnowartościowa (równoważnie: gdy $a \neq 0$), a wtedy nazywamy ją **nieosobliwą**. Rozpatrzmy wpierw przypadki szczególne.

i) $b = 0$ i $|a| = 1$. Wówczas z (8) wynika dla $z \in \mathbb{C}$, że $|f(z)| = |z|$ i $\arg(f(z)) = \arg(z) + \alpha$, gdzie $\alpha := \arg(a)$. Obraz $f(z)$ punktu $z \in \mathbb{C}$ leży więc w tej samej, co z odległości od 0, a $\arg(f(z))$ różni się o stałą (niezależną od z) wielkość α od $\arg(z)$.

RYSUNEK

Gdy $b = 0$ i $|a| = 1$, to f jest **obrotem płaszczyzny wokół** 0 o kąt $\alpha = \arg(a)$.

ii) $b = 0$, zaś a jest dodatnią liczbą rzeczywistą. Wtedy $\arg(a) = 0$, skąd $\arg(az) = \arg(z)$. Obraz $f(z)$ punktu z leży więc na półprostej $0z$, przy czym $|f(z)| = a|z|$.

RYSUNEK

Gdy $b = 0$ i $a \in \mathbb{R}^+$, to f jest **jednokładnością o środku** 0 **i skali** a.

iii) $a = 1$. Wówczas f jest zadane wzorem $f(z) = z + b$. Obraz każdego punktu $z \in \mathbb{C}$ otrzymujemy przesuwając z o wektor $\overrightarrow{0b}$

RYSUNEK

Gdy $a = 1$, to f jest **przesunięciem** o $\overrightarrow{0b}$.

iv) Przypadek ogólny ($a \neq 0$). Napiszmy

$$f(z) = b + |a|(\frac{a}{|a|}z) = f_3(f_2(f_1(z))),$$

gdzie $f_1(z) = \frac{a}{|a|}z$, $f_2(z) = |a|z$, $f_3(z) = z + b$ dla $z \in \mathbb{C}$. Zatem $f = f_3 \circ f_2 \circ f_1$ jest złożeniem wymienionych trzech przekształceń, przy czym:

f_1 jest obrotem o środku 0 o kąt $\arg(\frac{a}{|a|}) = \arg(a)$,

f_2 jest jednokładnością o środku 0 i skali $|a|$,

f_3 jest przesunięciem o wektor $\overrightarrow{0b}$.

Dla $b = 0$ wynika stąd, że przekształcenie $z \mapsto az$ jest złożeniem obrotu i jednokładności, mających środki w 0 i opisanych wyżej. Umożliwia to wyznaczenie iloczynu az przy zadanych a i z (nawet przy pomocy cyrkla i linijki, co tu nie jest istotne).

Zadanie 1. Niech $f : \mathbb{C} \to \mathbb{C}$ będzie zadane wzorem $f(z) = p + a(z - p)$, gdzie $a, p \in \mathbb{C}$ są dane. Dowieść, że:

a) Gdy $|a| = 1$, to f jest obrotem wokół p o kąt $\arg(a)$.

b) Gdy $a \in \mathbb{R}$, to f jest jednokładnością o środku p i skali a.

c) Jeśli $a \neq 0$, to f jest złożeniem przekszałceń $z \mapsto p + \frac{a}{|a|}(z-p)$ i $z \mapsto p + |a|(z-p)$.

Zadanie 2. Dowieść, że gdy $a \neq 1$ i $a \neq 0$, to przekształcenie afiniczne $f(z) = az + b$ można dla pewnego $p \in \mathbb{C}$ przedstawić w postaci złożenia obrotu wokół p o kąt $\arg(a)$ i jednokładności o środku w p i skali $|a|$. (Wskazówka: obrać za p **punkt stały** przekształcenia f, tzn. taki, że $f(p) = p$.)

<u>Ćwiczenie.</u> Obrót płaszczyzny $\mathbb{C}$ wokół $p = 2$ przeprowadza $2 + 5i$ na $5 + 4i$. Na co obrót ten przeprowadza $9 + i$?

<u>Ćwiczenie.</u> Niech $f : \mathbb{C} \to \mathbb{C}$ będzie nieosobliwym przekształceniem afinicznym.
a) Udowodnić, że jeśli L jest prostą w $\mathbb{C}$, to $f(L)$ też nią jest.
b) Udowodnić, że dla każdych $z_1, p, z_2 \in \mathbb{C}$ takich, że $z_1, z_2 \neq p$, kąty z_1pz_2 i $f(z_1)f(p)f(z_2)$ są przystające.

(Wskazówka: Obie tezy są oczywiste, gdy f jest jednokładnością, obrotem czy przesunieciem.)

<u>Ćwiczenie.</u> a) Dowieść, że jeśli $f, g : \mathbb{C} \to \mathbb{C}$ są nieosobliwymi przekształceniami afinicznymi, to $f \circ g$ i f^{-1} też.

b) Czy składanie nieosobliwych przekształceń afinicznych $\mathbb{C} \to \mathbb{C}$ jest przemienne?

<u>Zastosowanie: liczby zespolone a miara kąta zorientowanego.</u>

Przypuśćmy, że z_1, z_2, p są różnymi punktami $\mathbb{C}$ i rozważmy zorientowany kąt z_1pz_2 (tzn. taki, którego pierwszym ramieniem jest półprosta pz_1, a drugim– półprosta pz_2, obie wychodzące z p; kolejność ramion jest istotna). [2]

[2] Istotna jest też umowa, że kąt mierzymy „idąc od pierwszego ramienia do drugiego w kierunku przeciwnym do

Dla zmierzenia tego kąta rozpatrzmy wpierw przypadek $p = 0$. Wówczas za szukaną miarę φ przyjmujemy każdą liczbę postaci $\arg(z_2) - \arg(z_1)$; jest więc ona wyznaczona z dokładnością do wielokrotności 2π. Ze wzoru (9) w p.5 wynika, że $\varphi = \arg(\frac{z_2}{z_1})$.

Gdy $p \neq 0$ rozważamy przekształcenie przesunięcia o wektor $-\overrightarrow{0p}$. Ponieważ nie zmienia ono kątów i przeprowadza z_1, z_2 i p na $z_1 - p, z_2 - p$ i 0, odpowiednio, to z powyższego przypadku szczególnego wynika, że

$$\arg(\frac{z_2 - p}{z_1 - p}) \text{ jest miarą zorientowanego kąta } z_1 p z_2 \tag{12}$$

Zadanie 3. Przy $p = 0$ wykazać, że

$$\varphi = \arg(\frac{\overline{z_1} z_2}{|z_1||z_2|}) \text{ oraz } \cos\varphi = \mathrm{Re}\frac{\overline{z_1} z_2}{|z_1||z_2|} = \mathrm{Re}\frac{z_1 \overline{z_2}}{|z_1||z_2|}.$$

Zadania uzupełniające.

1. Dowieść, że jeśli $|u| = |v| \neq 0$, to istnieją dokładnie 2 liczby zespolone λ takie, że $\lambda u = \overline{\lambda v}$ i $|\lambda| = 1$. Podać interpretację geometryczną i sposób wyznaczenia λ.

2. Dowieść, że $|z_1 - z_2| \leq ||z_1| - |z_2|| + |\arg(z_1/z_2)| \cdot \min(|z_1|, |z_2|)$ dla $z_1, z_2 \neq 0$. Dać interpretację geometryczną.

3. Obrót płaszczyzny złożono z symetrią prostopadłą względem prostej przechodzącej przez środek obrotu. Czym jest zbiór punktów stałych tego złożenia?

4. Dowieść, że (odcinek $[a, b]$ jest prostopadły do odcinka $[c, d]$)$\Leftrightarrow (b - a)(\overline{d} - \overline{c}) + (d - c)(\overline{b} - \overline{a}) = 0$.

5. Niech dane będą kąty zorientowane uvw oraz $u'v'w'$ na płaszczyźnie $\mathbb{C}$. Dowieść, że:

   a) Kąty $u'v'w'$ i uvw są równe $\Leftrightarrow \frac{u-v}{w-v} : \frac{u'-v'}{w'-v'}$ jest liczbą rzeczywistą dodatnią.

   b) Kąty uvw i $u'v'w'$ dopełniają się $\Leftrightarrow \frac{u-v}{w-v} : \frac{u'-v'}{w'-v'}$ jest liczbą rzeczywistą ujemną.

Zadania ze zbioru Kostrykina: 7,8,9 w §I.6.6.

§ 2. Wstępne informacje o ciałach i o pierścieniu wielomianów.

1. Ciała i pierścienie

Wygodnie jest wyróżnić pewne wspólne własności liczb zespolonych, liczb rzeczywistych i liczb wymiernych.

wskazówek zegara". Patrz też dalej w rozdziale IV.

Definicja. Niech $\mathbb{F}$ będzie dowolnym zbiorem, w którym określone są dwa działania (czyli funkcje $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$). Jedno z nich nazwijmy dodawaniem, a jego wartość na parze (a, b) oznaczmy przez $a + b$, zaś drugie nazwijmy mnożeniem, a jego wartość na parze (a, b) oznaczmy przez $a \cdot b$ lub przez ab. Powiemy, że zbiór $\mathbb{F}$ z tymi działaniami jest ciałem, jeśli spełnione są wszystkie poniższe warunki:

i) oba działania są przemienne i łączne;

ii) istnieje element $0_{\mathbb{F}} \in \mathbb{F}$, który jest neutralny dla dodawania, i istnieje różny od $0_{\mathbb{F}}$ element $1_{\mathbb{F}} \in \mathbb{F}$, neutralny dla mnożenia;

iii) mnożenie jest rozdzielne względem dodawania;

iv) dla każdego elementu $a \in \mathbb{F}$ istnieje w $\mathbb{F}$ rozwiązanie równania $a + x = 0_{\mathbb{F}}$, oraz każdy element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ posiada odwrotność w $\mathbb{F}$ (tzn. istnieje w $\mathbb{F}$ rozwiązanie równania $a \cdot x = 1_{\mathbb{F}}$).

Zadanie 1. Gdy warunki od i) do iv) są spełnione, to

a) W $\mathbb{F}$ wykonywalne jest odejmowanie, tzn. dla $a, b \in \mathbb{F}$ istnieje w $\mathbb{F}$ dokładnie jedno rozwiązanie równania $a+x = b$. (Oznaczamy je $b-a$ i przyjmujemy $-a := 0-a$.)

b) W $\mathbb{F}$ wykonywalne jest dzielenie przez elementy niezerowe, tzn. gdy $a, b \in \mathbb{F}$ i $a \neq 0$, to w $\mathbb{F}$ istnieje dokładnie jedno rozwiązanie równania $a \cdot x = b$. (Oznaczamy je $b : a$ lub b/a i piszemy $a^{-1} := 1/a$.)

c) Istnieje tylko jeden element neutralny względem dodawania i tylko jeden element neutralny względem mnożenia.

Ze szkoły i wykładu Analizy wiadomo, że zbiór $\mathbb{R}$ liczb rzeczywistych, rozpatrywany ze „zwykłymi” działaniami dodawania i mnożenia, jest ciałem. Tak samo jest ze zbiorem $\mathbb{Q}$ liczb wymiernych. Wreszcie twierdzenie z p.1 orzeka, że *zbiór $\mathbb{C}$ liczb zespolonych, rozpatrywany ze zdefiniowanymi w p.1 działaniami, jest ciałem.*

Ćwiczenie. Dowieść, że dodawanie i mnożenie wyznaczają działania w $\mathbb{F} := \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, i że zbiór $\mathbb{F}$ rozpatrywany z tymi działaniami jest ciałem.

Definicja. a) Jeśli spełnione są wszystkie warunki definicji ciała poza istnieniem rozwiązania równania $ax = 1_{\mathbb{F}}$ to powiemy, że zbiór $\mathbb{F}$ z rozważanymi działaniami tworzy **pierścień przemienny z jedynką**. Przykładem takiego pierścienia, nie będącego ciałem, jest zbiór $\mathbb{Z}$ liczb całkowitych ze „zwykłymi” działaniami.

b) Gdy w definicji ciała (odp. pierścienia przemiennego z jedynką) pominiemy przemienność mnożenia, to zdefiniujemy **ciało nieprzemienne** (odp. **pierścień z jedynką**). Wtedy jednak rozdzielność mnożenia względem dodawania rozumiemy tak:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{oraz} \quad (b + c) \cdot a = b \cdot a + c \cdot a \quad \text{dla wszystkich } a, b, c \in \mathbb{F}$$

a definicję odwrotności i elementu neutralnego względem mnożenia tak: $1_{\mathbb{F}}$ jest elementem neutralnym względem mnożenia, jeśli $a \cdot 1_{\mathbb{F}} = 1_{\mathbb{F}} \cdot a = a$ dla każdego $a \in \mathbb{F}$, zaś b jest odwrotnością a, jeśli $a \cdot b = b \cdot a = 1_{\mathbb{F}}$.

W danym zbiorze określić możemy różne działania, tak więc by wskazać o jakie ciało czy o jaki pierścień chodzi, należy podać nie tylko zbiór jego elementów, ale i wyróżnione w nim działania. Tym niemniej, często wymieniamy tylko zbiór elementów, zwłaszcza gdy działania w nim bądź są znane skądinąd, badź też jedynymi istotnymi dla nas ich własnościami są te, które wynikają z warunków i)–iv). Gdy nie powiedziano inaczej, w zbiorach $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ rozpatrujemy tylko znane nam już działania.

Definicja. Podzbiór $\mathbb{G}$ ciała $\mathbb{F}$ nazywamy jego **podciałem**, jeśli (niżej, działania wykonujemy w $\mathbb{F}$)

a) w $\mathbb{G}$ istnieje element, różny od $0_{\mathbb{F}}$, oraz

b) dla wszystkich $x, y \in \mathbb{G}$ takich, że $y \neq 0_{\mathbb{F}}$, zachodzi $x : y \in \mathbb{G}$ i $x - y \in \mathbb{G}$.

Zadanie 2. Gdy $\mathbb{G}$ jest podciałem ciała $\mathbb{F}$, to:

a) $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathbb{G}$, a także $xy \in \mathbb{G}$ i $x + y \in \mathbb{G}$ dla wszystkich $x, y \in \mathbb{G}$.

b) $\mathbb{G}$ można traktować jako ciało, w którym suma nie zależy od tego, czy wyliczamy ją zgodnie z działaniem określonym w $\mathbb{G}$, czy określonym w $\mathbb{F}$, i tak samo jest dla iloczynu.

Ciałem liczbowym nazywamy każde podciało ciała liczb zespolonych. Liczby rzeczywiste traktujemy przy tym jako elementy $\mathbb{C}$, tak więc $\mathbb{Q}$ i $\mathbb{R}$ są ciałami liczbowymi, podobnie jak i ciało rozpatrywane w ćwiczeniu 1.

Zadanie 3. Każde ciało liczbowe zawiera zbiór $\mathbb{Q}$, więc jest nieskończone.

Nie każde ciało jednak jest nieskończone. I tak niech $\mathbb{Z}_n := \{0, 1, ..., n-1\}$, gdzie $n \geq 2$, i dla $a, b \in \mathbb{Z}_n$ przyjmujemy

$$a + b = \text{ reszta z dzielenia liczby sumy liczb } a \text{ i } b \text{ przez } n$$
$$a \bullet b = \text{ reszta z dzielenia iloczynu liczb } a \text{ i } b \text{ przez } n$$

Nietrudno dowieść (co nastąpi na wykładzie Algebry 1), że z działaniami tymi zbiór $\mathbb{Z}_n$ jest pierścieniem, i że jest on ciałem wtedy i tylko wtedy, gdy n jest liczbą pierwszą. (Patrz też [BM] i ....) Na ćwiczeniach omówiony zostanie przypadek $n = 2$ i przykład ciała o 4 elementach, a więc różnego od każdego z pierścieni $\mathbb{Z}_n$. Ogólnie, liczebności ciał skończonych przebiegają wszystkie (dodatnie) potęgi liczb pierwszych.

Uwaga 1. Sumę k jedynek $1_{\mathbb{F}}$ ciała $\mathbb{F}$ oznaczać będziemy $k_{\mathbb{F}}$. Dla przykładu, mamy $p_{\mathbb{F}} = 0_{\mathbb{F}}$ w ciele $\mathbb{Z}_p$, zaś $3_{\mathbb{F}} = 1_{\mathbb{F}}$ w ciele o 4 elementach (co nie jest oczywiste).

Zadania uzupełniające.

1. Dla elementów x, y pierścienia P przyjmijmy $[x, y] := xy - yx$. Dowieść **tożsamości Jacobiego**: $[[x, y], z] + [y, z], x] + [[z, x], y] = 0$.

2. Bijekcję (przekształcenie różnowartościowe i „na”) $f : \mathbb{F} \to \mathbb{G}$ pomiędzy dwoma ciałami nazywamy **izomorfizmem**, jeśli $f(a+b) = f(a)+f(b)$ i $f(ab) = f(a)f(b)$ dla

wszystkich $a, b \in \mathbb{F}$. Izomorfizm nazywamy **automorfizmem ciała** $\mathbb{F}$, jeśli $\mathbb{F} = \mathbb{G}$. Dowieść, że jedynym automorfizmem ciała $\mathbb{Q}$ jest identyczność, i tak samo jest dla ciała $\mathbb{R}$.

Problem 1. (Wymaga samodzielnej lektury.) Z §2.3 wiemy, że sprzężenie jest automorfizmem ciała $\mathbb{C}$. Czy prócz sprzężenia i identyczności istnieją inne jeszcze jego automorfizmy?

2. Ogólne wiadomości o wielomianach

Definicja. **Wielomianem** zmiennej x, o współczynnikach w zadanym ciele $\mathbb{F}$, nazywamy każde wyrażenie

$$f = \sum_{j=0}^{\infty} a_j x^j, \tag{12}$$

gdzie $a_0, a_1, \ldots$ są elementami $\mathbb{F}$ takimi, że $a_j \neq 0_{\mathbb{F}}$ tylko dla skończonej liczby wskaźników j. Wyrazy a_j nazywamy **współczynnikami** wielomianu f. O wielomianach o współczynnikach w $\mathbb{F}$ mówimy też, że są **nad** $\mathbb{F}$. Ich zbiór oznaczamy przez $\mathbb{F}[x]$.

Umawiamy się, że w przedstawieniu (12) możemy pomijać wyrażenia postaci $0x^j$. Np. jeśli$f = 1 + 0x + 3x^2 + 0x^3 - x^4 + \sum_{j=5}^{\infty} 0x^j$, to piszemy naogół $f = 1 + 3x^2 - x^4$. Nie rozróżniamy też elementu $a \in \mathbb{F}$ i wielomianu $f = a + \sum_{j=1}^{\infty} 0x^j$.

W $\mathbb{F}[x]$ określamy działania dodawania i mnożenia przyjmując dla $f = \sum_{i=0}^{\infty} a_j x^j$ i $g = \sum_{j=0}^{\infty} b_j x^j$:

$$f + g := \sum_{i=0}^{\infty} (a_j + b_j) x^j \quad \text{oraz} \qquad fg := \sum_{j=0}^{\infty} \Big(\sum_{k+l=j} a_k b_l \Big) x^j \tag{13}$$

Dla $c \in \mathbb{F}$ i $f \in \mathbb{F}[x]$ możemy więc też mówić o iloczynie cf (bo c jest wielomianem.)

Twierdzenie 1. $\mathbb{F}[x]$ *ze zdefiniowanymi wyżej działaniami jest pierścieniem przemiennym z jedynką.* $\boxminus$

Dla $f = \sum_{i=0}^{\infty} a_i x^i \neq 0$ określamy

$$\deg(f) := \max\{i : a_i \neq 0\}$$

liczbę tę nazywamy **stopniem** wielomianu f. Wspólczynnik $a_{\deg(f)}$ nazywamy **prowadzącym**. Definicje te mogą budzić wątpliwości, gdy $f = 0$; przyjmujemy zatem $\underline{\deg(0) = -\infty}$ i za wspólczynnik prowadzący wielomianu 0 przyjmujemy 0.

Wielomiany stopnia 1 nazywamy **liniowymi,** a stopnia 0 i $-\infty$ **stałymi.**

Twierdzenie 2. *Jeśli* $f, g \in \mathbb{F}[x]$, *to*

a) $\deg(f+g) \leq \max(\deg(f), \deg(g))$, *przy czym* $\deg(f+g) = \deg(f)$ *jeśli* $\deg(g) < \deg(f)$,

b) $\deg(fg) = \deg(f) + \deg(g)$. *(Przyjmujemy* $c + d := -\infty$ *gdy* $-\infty \in \{c, d\}$.*)* ⊟

Wniosek 1. *a)* $\mathbb{F}[x]$ *nie jest ciałem; co więcej, żaden element* $f \in \mathbb{F}[x]$ *stopnia dodatniego nie jest odwracalny względem mnożenia.*

b) (Prawo skracania w $\mathbb{F}[x]$.*) Gdy* $fg = fh$ *i* $f, g, h \in \mathbb{F}[x]$, *to* $f = 0$ *lub* $g = h$.

Dowód. a) jest oczywiste, a dla dowodu b) zauważmy, że jeśli $f(g-h) = 0$, to $\deg(f) < 0$ lub $\deg(g-h) < 0$; patrz twierdzenie 2b).□

Definicja. **Wartość wielomianu** $f = \sum_{j=0}^{\infty} c_j x^j \in \mathbb{F}[x]$ **w punkcie** $a \in \mathbb{F}$ określamy wzorem $f(a) := \sum_{j=0}^{\infty} c_j a^j$.

Znane ze szkoły dla $\mathbb{R}[x]$ twierdzenie Bezout pozostaje słuszne, wraz z dowodem, przy $\mathbb{R}$ zastąpionym przez dowolne ciało $\mathbb{F}$. Wykorzystamy tylko taką jego konsekwencję: *gdy* $a \in \mathbb{F}$ *jest* **pierwiastkiem wielomianu** $f \in \mathbb{F}[x]$, *tzn.* $f(a) = 0$, *to* $f = (x-a)g$ *dla pewnego wielomianu* $g \in \mathbb{F}[x]$.

Definicja. Powiemy, że liczba $k \in \mathbb{N} \cup \{0\}$ jest **krotnością elementu** $a \in \mathbb{F}$ **jako pierwiastka wielomianu** $f \in \mathbb{F}[x]$, $f \neq 0$, jeśli $f = (x-a)^k g$ dla pewnego wielomianu $g \in \mathbb{F}[x]$ takiego, że $g(a) \neq 0$. (Dopuszczamy możliwość, że $k = 0$ i $f(a) \neq 0$!)

Lemat 1. *Powyższa krotność jest jednoznacznie wyznaczona.*

Dowód. a) Wpierw przez indukcję względem $\deg(f)$ dowiedziemy istnienia żądanego rozkładu. Gdy $f(a) \neq 0$, jest nim $f = (x-a)^0 f$; w szczególności rozkład istnieje gdy $\deg(f) = 0$. Gdy zaś $f(a) = 0$, to $f = (x-a)h$ dla pewnego wielomianu h, przy czym z założenia indukcyjnego $h = (x-a)^k g$ dla pewnych $k \in \mathbb{N} \cup \{0\}$ i $g \in \mathbb{F}[x]$ takich, że $g(a) \neq 0$. Daje to szukany rozkład $f = (x-a)^{k+1} g$.

b) Dla dowodu jednoznaczności przypuśćmy, że $f = (x-a)^k g = (x-a)^l h$, gdzie $g(a) \neq 0 \neq h(a)$. Przyjmując $k \leq l$ wnosimy z prawa skracania, że $g = (x-a)^{l-k} h$. A że $g(a) \neq 0$, to $l - k = 0$. □

Twierdzenie 3. *a) Krotność a jako pierwiastka wielomianu* $f_1 f_2$ *jest sumą jego krotności jako pierwiastka wielomianów* f_1 *i* f_2, *odp. (Podobnie dla iloczynu większej liczby wielomianów.)*

b) Jeśli $a_1, a_2, ..., a_s$ $(s \geq 1)$ *są różnymi pierwiastkami wielomianu* $f \neq 0$, *krotności* $k_1, k_2, ..., k_s$ *odpowiednio, to* $f = (x-a_1)^{k_1}(x-a_2)^{k_2}...(x-a_s)^{k_s} h$ *dla pewnego wielomianu* $h \in \mathbb{F}[x]$ *takiego, że* $h(a_i) \neq 0$ *dla każdego* i.

Dowód. a) wynika z przyjętej definicji, a b) przez indukcję względem s wynika z a). ⊟

Wniosek 2. *Przy założeniach części b) twierdzenia 3, zachodzi* $k_1 + ... + k_s \leq \deg(f)$*, a jeśli* $s = \deg(f)$*, to* $k_1 = ... = k_s = 1$ *i* h *jest stałą. Wielomian stopnia* $n \geq 0$ *ma więc nie więcej, niż* n *różnych pierwiastków.*

Dowód. Zachodzi $s \leq k_1 + ... + k_s + \deg(h) = \deg(f)$. (Równość wynika z części a) twierdzenia 3, a nierówność stąd, że $k_i \geq 1$ $\forall i$.) $\boxminus$

Wniosek 3. *Niech* $f, g \in \mathbb{F}[x]$ *mają tę własność, że* $f(a) = g(a)$ *dla nieskończenie wielu* $a \in \mathbb{F}$*. Wówczas* $f = g$*.*

Dowód. $f - g$ ma nieskończenie wiele pierwiastków.$\square$

Zadanie 1. Gdy ciało $\mathbb{F}$ jest skończone, to istnieje niezerowy wielomian $f \in \mathbb{F}[x]$ taki, że $f(a) = 0$ dla wszystkich $a \in \mathbb{F}$.

Zadania ze zbioru Kostrykina: w §I.7.1: 1,2, 4,5,6; zadanie 3 w §I.7.2 i 1,2,3 w §I.7.3.

3. Rozkład wielomianu zespolonego bądź rzeczywistego na czynniki nierozkładalne.

Twierdzenie 1 („Zasadnicze Twierdzenie Algebry”)**.** *Wielomian zespolony dodatniego stopnia ma pierwiastek.*

Będzie to udowodnione na wykładach Topologii i Funkcji Analitycznych; por. [BM].

Twierdzenie 2. *Gdy* $f \in \mathbb{C}[x]$ *i* $\deg(f) > 0$*, to*

$$f = (x - a_1)^{k_1} ... (x - a_s)^{k_s} h \text{ dla pewnych } a_1, ..., a_s, h \in \mathbb{C} \text{ i } k_1, ..., k_s \in \mathbb{N}. \tag{14}$$

Dowód. Zastosujmy twierdzenie 3 z p.2 przy $(a_1, ..., a_s)$ będącym ciągiem wszystkich pierwiastków f. Wielomian h nie ma wtedy pierwiastków, więc jest stopnia 0, patrz powyżej. $\square$

Uwaga 1. Gdy zachodzi równość (14), to

a) $a_1, ..., a_s$ i $k_1, ..., k_s$ są z dokładnością do kolejności wyznaczone tym, że $a_1, ..., a_s$ jest zbiorem wszystkich pierwiastków f, a k_i jest krotnością pierwiastka a_i. Ponadto, stała h jest współczynnikiem prowadzącym wielomianu f (wystarcza wykonać mnożenie współczynników prowadzących), co też wyznacza ją jednoznacznie.

b) $\sum_{i=1}^{s} k_i = \deg(f)$ na podstawie twierdzenia 2a) z p.2. Zespolony wielomian $f \neq 0$ ma więc $n = \deg(f)$ pierwiastków zespolonych, gdy każdy liczyć tylekroć, ile wynosi jego krotność.

Twierdzenie 3. *Gdy* f *jest niezerowym wielomianem o współczynnikach rzeczywistych, to*

a) Zespolone pierwiastki wielomianu f *są parami sprzężone: jeśli* $a \in \mathbb{C}$ *i* $f(a) = 0$*, to* $f(\overline{a}) = 0$*.*

b) Wielomian f *jest iloczynem wielomianów rzeczywistych stopni 1 i 2.*

Dowód. Teza a) wynika bezpośrednio z własności sprzężenia. Dowód b) przeprowadzimy przez indukcję względem stopnia wielomianu. Na podstawie Zasadniczego Twierdzenia Algebry, f ma pewien pierwiastek $a \in \mathbb{C}$. Jeśli $a \in \mathbb{R}$, to $f = (x-a)g$ dla pewnego $g \in \mathbb{R}[x]$, przy czym $\deg(g) < \deg(f)$. Z założenia indukcyjnego, zastosowanego do g, wynika prawdziwość tezy b) dla f.

Jeśli zaś a nie leży na osi rzeczywistej, to $\overline{a}$ jest różnym od a pierwiastkiem f, skąd $f = (x-a)(x-\overline{a})h$ dla pewnego $h \in \mathbb{C}[x]$. (Patrz tw. 3 w p.2.) Ponieważ wielomian $f_0 := (x-a)(x-\overline{a})$ ma współczynniki rzeczywiste, to h też ma takie współczynniki, jako wynik dzielenia f przez f_0. Teza znów wynika z założenia indukcyjnego (zastosowanego do h). $\square$

Wniosek 1. *Wielomian $f \in \mathbb{R}[x]$ stopnia nieparzystego ma pierwiastek rzeczywisty.*

Dowód. Gdy f jest nieparzystego stopnia, to nieparzysty jest stopień któregoś z czynników powyższego iloczynu. $\square$

Zadanie uzupełniające 1. Dany jest wielomian $f = x^n + a_1x^{n-1} + ... + a_n \in \mathbb{C}[x]$. Udowodnić, że:

a) Pewien pierwiastek tego wielomianu ma moduł $\leq |a_n|^{1/n}$.

b) Jeśli ponadto $a_1, ..., a_n \in \mathbb{R}$ i $f(0) = -1$, to $f(1) = 0$ lub f ma pierwiastek o module < 1.

Zadania ze zbioru Kostrykina: w §I.7.2: 1 bez e) i f) oraz od 2 do 8.

4. Pierwiastki wielomianu $x^n - u$.

Definicja. Jak w przypadku rzeczywistym, liczbę $z \in \mathbb{C}$ nazwiemy **pierwiastkiem stopnia** n z liczby $u \in \mathbb{C}$, jeśli $z^n = u$.

Twierdzenie 1. *Istnieje dokładnie n pierwiastków stopnia n danej liczby $u \in \mathbb{C} \setminus \{0\}$, i w postaci biegunowej są one zadane wzorami*

$$\mathrm{Arg}(\varepsilon_k) = \frac{1}{n}\mathrm{Arg}(u) + k\frac{2\pi}{n} \quad \text{oraz } |\varepsilon_k| = |u|^{\frac{1}{n}}, \quad \text{dla} \quad k = 0, 1, ..., n-1. \tag{15}$$

Dowód. Na podstawie wzorów de Moivre'a, każda z liczb ε_k jest pierwiastkiem wielomianu $f = x^n - u$. Liczby te są parami różne, bo mają różne Argumenty. Jest ich więc tyle, ile wynosi stopień wielomian f, i teza wynika z wniosku 2 z p.2.$\square$

Uwaga 1. Przy powyższych oznaczeniach mamy $\prod_{i=0}^{n-1}(x - \varepsilon_i) = x^n - u$. (Wynika to z tegoż wniosku i uwagi 1a) z p.3, odniesionych do wielomianu $x^n - u$.)

Zauważmy też, że punkty $\varepsilon_0, ..., \varepsilon_{n-1}$ są wierzchołkami $n-$kąta foremnego wpisanego w okrąg o promieniu $r = |u|^{\frac{1}{n}}$. W szczególnym przypadku, gdy $u = 1$, to $\varepsilon_0 = 1$ oraz $r = 1$. Wszystkie pierwiastki stopnia n z jedynki leżą więc na okręgu jednostkowym i są wierzchołkami wielokąta foremnego, którego 1 jest jednym z wierzchołków.

RYSUNEK

Pierwiastki z jedynki stopni $n = 5$ i $n = 6$

Zadanie 1. Udowodnić, że następujące warunki są równoważne dla $z \in \mathbb{C}$ i $n \in \mathbb{N}$:
a) $z^n = 1$ i $z^l \neq 1$ dla $1 \leq l < n$;
b) $z = \varepsilon_k$ dla liczby k względnie pierwszej z n (stosujemy oznaczenia (4), z $u = 1$);
c) $\{z^l : l = 0, 1, ..., n-1\} = \{\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}\}$.
(Wskazówka: gdy liczby k i n są względnie pierwsze, to dla różnych $l_1, l_2 \in \{0, 1, ..., n-1\}$ liczby $l_1 k$ i $l_2 k$ dają różne reszty z dzielenia przez n.)

Gdy spełniony jest pewien (a więc i wszystkie) z powyższych równoważnych warunków to powiemy, że z jest **pierwotnym** pierwiastkiem z jedynki stopnia n.

Na przykład, wszystkie poza $\varepsilon_0 = 1$ pierwiastki stopnia 5 są pierwotne (tego stopnia), a pierwiastkami pierwotnymi z jedynki stopnia 6 są ε_1 oraz ε_5.

Zadania uzupełniające.

1. Dowieść, że gdy wielomian f ma współczynniki rzeczywiste, to krotności liczb zespolonych a i $\overline{a}$ jako jego pierwiastków są równe.

2. Dowieść, że iloczyn wszystkich pierwiastków z 1 stopnia $n \geq 2$ jest równy $(-1)^{n-1}$, a suma jest równa 0. (Wskazówka: uwaga 1 i wzory Viety.)

3. Obliczyć sumę kwadratów wszystkich pierwiastków z jedynki danego stopnia.

4. a) Wykazać, że $x^n - 1 = g \prod_{2k<n}(x^2 - 2x\cos(\frac{2k\pi}{n}) + 1)$, gdzie $g = x - 1$ gdy n jest liczbą nieparzystą i $g = x^2 - 1$ gdy jest parzystą. (Wskazówka: uwaga 1.)

b) Wywnioskować z a), że $1 + x + ... + x^{n-1} = h \prod_{2k<n}(x^2 - 2x\cos(\frac{2k\pi}{n}) + 1)$, gdzie $h = x + 1$ gdy $2|n$ i $h = 1$ w przeciwnym razie, oraz że $\sqrt{n} = \sqrt{c} \prod_{2k<n}(2\sin(k\pi/n))$, gdzie $c = 2$ gdy $2|n$ i $c = 1$ w przeciwnym razie.

5. Niech liczby naturalne k, l będą względnie pierwsze.

a) Dowieść, że pierwiastek a stopnia kl z jedynki jest iloczynem dwóch pierwiastków z jedynki stopni k i l, odpowiednio, i że przedstawienie takie jest jednoznaczne.

b) Dowieść, że powyżej jeśli a, to i pozostałe dwa pierwiastki są pierwotne wymienionych stopni. Dowieść też implikacji przeciwnej.

6. Niech E oznacza zbiór pierwiastków z jedynki danego stopnia k. Udowodnić, że $\sum_{\varepsilon \in E} \varepsilon^j = 0$ dla $j = 1, 2..., k-1$.

7. Udowodnić następujące **twierdzenie Cotesa**: iloczyn odległości punktu p od wierzchołków n–kąta foremnego, wpisanego w okrąg o promieniu r_0 i środku w q, jest $\geq |r^n - r_0^n|$, gdzie r to długość odcinka pq. Ponadto, równość zachodzi gdy punkt p leży na półprostej wychodzącej z q i przechodzącej przez pewien wierzchołek wielokąta.

8. Niech $a, b, c \in \mathbb{C}$ traktowane będą jako wierzchołki trójkąta. Dowieść, że trójkąt ten wtedy i tylko wtedy jest równoboczny, gdy $(a-b)^2 = (b-c)(c-a) \neq 0$. (Wskazówka: $c = a + (b-a)u$ dla pewnego u.)

9. a) Rozwiązać równanie $\sum_{k=0}^{4} z^k = 0$ dzieląc je przez z^2 i wprowadzając niewiadomą $z + \frac{1}{z}$.

b) Podać opartą o a) konstrukcję pięciokąta foremnego przy pomocy cyrkla i linijki.

§ 3. Możliwe tematy zadań kolokwialnych

„Możliwe” są wszystkie omówione wyżej tematy, lecz szczególnie dobrze jest upewnić się przed kolokwium co do umiejętności rozwiązania zadań dotyczących:

a) wykorzystania wzorów de Moivre'a i pokrewnych;

b) interpretacji geometrycznej przekształceń $\mathbb{C} \to \mathbb{C}$ postaci $z \mapsto az + b$ lub $z \mapsto z^k$ dla pewnych $a, b \in \mathbb{C}$ i $k \in \mathbb{N}$, w tym znajdywania obrazów czy przeciwobrazów zadanych zbiorów przy takich przekształceniach –zarówno danych jawnym wzorem, jak i wtedy, gdy opisano je językiem geometrycznym (np. jako obrót czy przesunięcie czy jednokładność);

c) rozkładu wielomianów na wielomiany najniższych stopni (przypadek rzeczywisty i zespolony), w tym konsekwencji wzorów Viety i sprzężoności pierwiastków zespolonych wielomianów rzeczywistych;

d) wiadomości teoretycznych: mogą pojawić się polecenia sformułowania definicji, twierdzeń czy dowodów (np. przytoczenia dowodu czy jego części).