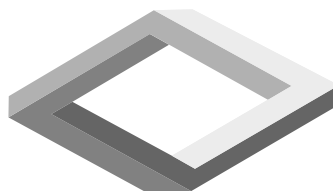


MATEMATYKA  
OLIMPIJSKA



***Algebra i Teoria Liczb***

*Adam Neugebauer*



CZERWIEC 2018

Opracowanie graficzne: *Autorzy*

Wydanie I

ISBN: 978-83-7267-710-5

Wydawnictwo Szkolne OMEGA, 30-552 Kraków, ul. Wielicka 44 C  
tel. 12 4 256 256; +48 662 152 899  
[www.ws-omega.com.pl](http://www.ws-omega.com.pl) e-mail: [biuro@ws-omega.com.pl](mailto:biuro@ws-omega.com.pl)

# Przedmowa

Przedstawiamy pierwsze całościowe chociaż nieostateczne<sup>1</sup> wydanie serii podręczników pod wspólnym tytułem MATEMATYKA OLIMPIJSKA. Mamy tu na myśli matematykę elementarną w zakresie wyznaczonym przez zadania OM (krajowe i międzynarodowe). Matematyka ta, mimo niewielkiego obciążenia definicyjnego, jest bliższa matematyce *akademickiej* niż matematyce *szkolnej*. Proponowany sposób wykładu (definicja, twierdzenie, przykłady, zadania i ćwiczenia<sup>2</sup>) jest więc bliższy akademickiemu niż szkolnemu. Szczegółowy spis treści powinien dawać dostatecznie dobre wyobrażenie o terytorium zajmowanym przez Matematykę Olimpijską w królestwie matematyki. Każdy tom kończy się krótką bibliografią, w której pokazujemy kilka źródeł dających możliwość rozszerzenia i pogłębienia przedmiotowej wiedzy. W indeksie zamieszczamy również terminy zaledwie wspomniane w tekście. Powinno to rozbudzać ciekawość Czytelników i zachęcać do samodzielnych poszukiwań w literaturze. Znak  $\diamond$  oznacza koniec rozwiązania zadania lub koniec przykładu, a znak  $\square$  – koniec dowodu (lub tylko sformułowania) twierdzenia. Czasami zamiast *wtedy i tylko wtedy, gdy* piszemy *iff* (ang. *if and only if*), a zamiast *bez straty ogólności* piszemy *b.s.o.* Napis  $\xi := \zeta$  oznacza:  $\xi$  jest z definicji (z określenia) równe  $\zeta$ .

Poszczególne części *żółtego, zielonego i czerwonego* skryptów były wielokrotnie w latach 2007-2017 wydawane jako preprinty w niewielkich nakładach. Znalazły one pewne uznanie w oczach niektórych nauczycieli zajmujących się kształceniem uczniów-olimpijczyków. W szczególności, dr Jacek Dymel (Kraków), opiekun naukowy i wychowawca licznych laureatów OM i MOM, zachęcił nas do przygotowania niniejszego wydania.

Serdeczne podziękowania składamy profesorowi Andrzejowi Schinzlowi za aprobatę naszej wizji teorioliczbowej części przedsięwzięcia (pozostałe części wzorują się na niej) i wskazanie błędów. Kolega Wojtek Wawrów wskazał nam niepoliczalny zbiór usterek i błędów w poprzednich wersjach trzech części, a także kilka propozycji ulepszenia tych części. Zasłużył tym na naszą bezgraniczną wdzięczność. Nasi uczniowie (i koledzy jednego z nas) Marcin Michorzewski, Paweł Poczobut i Krzysztof Małyśa w różnych okresach powstawania serii byli bardzo pomocni. Dziękujemy im za to.

A P E L. Mimo licznych wysiłków, w książkach z pewnością pozostało jeszcze sporo do poprawienia. Wobec tego zwracamy się do Was, drodzy Czytelnicy, z gorącym apelem o krytyczne czytanie i informowanie o zauważonych błędach i innych niedostatkach zarówno merytorycznych jak i dydaktycznych (adres: **koloroweskrypty @ gmail.com**). Bylibyśmy bardzo wdzięczni za wzięcie sobie do serca tego apelu. Nasze reakcje na Wasze uwagi zamieszczamy na stronie [sites.google.com/site/koloroweskrypty](https://sites.google.com/site/koloroweskrypty).

A u t o r z y

<sup>1</sup>Mamy nadzieję na napisanie *Kolorowego suplementu*, w którym znajdą się brakujące na razie fragmenty.

<sup>2</sup>Użyte przykłady, zadania i ćwiczenia, poza trywialnymi, nie są oryginalne. Pochodzą z rozmaitych źródeł, głównie z zawodów i olimpiad matematycznych. Wyjątkowo tylko wskazujemy z jakich.

# Słowo wstępne do tomu

*Mathematik ist die Königin der Wissenschaften und  
die Zahlentheorie die Königin der Mathematik.*<sup>3</sup>

(Carl Friedrich Gauss)

Tom pierwszy (ATL – *żółty*) przedstawia podstawowe pojęcia i metody elementarnej *Algebry i Teorii Liczb*. Jest w zasadzie samowystarczalny: zaczyna się od **liczb naturalnych**. Dążąc do **krzywych eliptycznych**, po drodze mówi o jednoznaczności rozkładu na **czynniki nierozkładalne** w **pierścieniu** liczb całkowitych i **pierścieniu wielomianów**, **kongruencjach**, **ułamkach łańcuchowych**, **formach kwadratowych**, **ciągach rekurencyjnych**, **pierścieniach kwadratowych**, i o **równaniach diofantycznych**, w szczególności o **równaniu indyjskim**. Centralnym rozdziałem skryptu jest rozdział 5: badanie reszt z dzielenia liczb całkowitych przez ustaloną liczbę  $m$  – **moduł** – dostarcza mocnego narzędzia teorioliczbowego – **arytmetyki modulo  $m$**  – z którym powinni oswajać się już gimnazjaliści.

Motta podajemy w ich oryginalnych językach.<sup>4</sup>

Książkę należy zacząć czytać od *Elementarza* (rozdział 2) następnie przejść do *Arytmetyki Modularnej* (rozdział 5), stopniowo, gdy pojawia się potrzeba, zapoznając się z materiałem rozdziałów 1, 3 i 4. Kolejność czytania dalszych rozdziałów jest w zasadzie dowolna.

Rozdziały 2, 3 i 4 kończą się zestawami zadań treningowych i wskazówkami/rozwiązaniami. Proponowana kolejność działań:

- (0) dobrze zrozum matematyczną treść zadania i wykonaj eksperymenty rachunkowe,
- (1) szukaj rozwiązania (nie rezygnuj przed upływem jednej godziny!),
- (2) czytaj (z ołówkiem w ręce) pokazaną wskazówkę/rozwiązanie uzupełniając wszystkie szczegóły, i porównaj z rozwiązaniem własnym (jeżeli takowe masz),
- (3) spróbuj znaleźć uogólnienie,
- (4) zreferuj kolegom.

Życzymy owocnej lektury.

---

<sup>3</sup>Matematyka jest królową nauki, a teoria liczb – królową matematyki.

<sup>4</sup>Na życzenie niektórych Czytelników poprzednich (preprintowych) wydań dodajemy teraz ich tłumaczenia.

# Tabliczka chronologiczna

<b>Euklides</b> z Aleksandrii	(ok. 365 p.n.e. - ok. 300 p.n.e.)
<b>Eratostenes</b> z Cyreny	(275 p.n.e. - 194 p.n.e.)
<b>Diofantos</b> z Aleksandrii	(III - IV wiek n.e.)
<b>Brahmagupta</b>	(598 - 660)
<b>Bhaskara</b>	(1114 - 1185)
Leonardo Pisano Bigollo zw. <b>Fibonacci</b>	(ok. 1170 - ok. 1240)
Niccolò Fontana zw. <b>Tartaglia</b>	(ok. 1499 - 1557)
François <b>Viète</b>	(1540 - 1603)
Claude Gaspard <b>Bachet de Méziriac</b>	(1581 - 1638)
Pierre de <b>Fermat</b>	(1601 - 1665)
Isaac <b>Newton</b>	(1643 - 1727)
Jakob <b>Bernoulli</b>	(1654 - 1705)
Leonhard <b>Euler</b>	(1707 - 1783)
Étienne <b>Bézout</b>	(1730 - 1783)
Joseph-Louis <b>Lagrange</b>	(1736 - 1813)
Adrien Marie <b>Legendre</b>	(1752 - 1833)
Sophie <b>Germain</b>	(1776 - 1831)
Carl Friedrich <b>Gauss</b>	(1777 - 1855)
August Ferdinand <b>Möbius</b>	(1790 - 1868)
Peter Gustav <b>Lejeune-Dirichlet</b>	(1805 - 1859)
Joseph <b>Liouville</b>	(1809 - 1882)
Évariste <b>Galois</b>	(1811 - 1832)
James Joseph <b>Sylvester</b>	(1814 - 1897)
Pafnucy <b>Czebyszew</b>	(1821 - 1894)
Charles <b>Hermite</b>	(1822 - 1901)
Gotthold <b>Eisenstein</b>	(1823 - 1852)
Richard <b>Dedekind</b>	(1831 - 1916)
François Édouard <b>Lucas</b>	(1842 - 1891)
Georg <b>Frobenius</b>	(1849 - 1917)
Adolf <b>Hurwitz</b>	(1859 - 1919)
Kurt <b>Hensel</b>	(1861 - 1941)
David <b>Hilbert</b>	(1862 - 1943)
Hermann <b>Minkowski</b>	(1864 - 1909)
Jacques <b>Hadamard</b>	(1865 - 1963)
Charles de la Vallée <b>Poussin</b>	(1866 - 1962)
Srinivasa <b>Ramanujan</b>	(1887 - 1920)

# Liczby pierwsze $3 \leq p \leq 2011$ i ich pierwiastki pierwotne

$p$	$g$	$g'$	$p$	$g$	$p$	$g$	$p$	$g$	$p$	$g$	$p$	$g$	$p$	$g$	$p$	$g$
3	2	-1	173	2	397	5	641	3	887	5	1163	5	1451	2	1721	3
5	2	-2	179	2	401	3	643	11	907	2	1171	2	1453	2	1723	3
7	3	-2	181	2	409	21	647	5	911	17	1181	7	1459	5	1733	2
11	2	-3	191	19	419	2	653	2	919	7	1187	2	1471	6	1741	2
13	2	-2	193	5	421	2	659	2	929	3	1193	3	1481	3	1747	2
17	3	-3	197	2	431	7	661	2	937	5	1201	11	1483	2	1753	7
19	2	-4	199	3	433	5	673	5	941	2	1213	2	1487	5	1759	6
23	5	-2	211	2	439	15	677	2	947	2	1217	3	1489	14	1777	5
29	2	-2	223	3	443	2	683	5	953	3	1223	5	1493	2	1783	10
31	3	-7	227	2	449	3	691	3	967	5	1229	2	1499	2	1787	2
37	2	-2	229	6	457	13	701	2	971	6	1231	3	1511	11	1789	6
41	6	-6	233	3	461	2	709	2	977	3	1237	2	1523	2	1801	11
43	3	-9	239	7	463	3	719	11	983	5	1249	7	1531	2	1811	6
47	5	-2	241	7	467	2	727	5	991	6	1259	2	1543	5	1823	5
53	2	-2	251	6	479	13	733	6	997	7	1277	2	1549	2	1831	3
59	2	-3	257	3	487	3	739	3	1009	11	1279	3	1553	3	1847	5
61	2	-2	263	5	491	2	743	5	1013	3	1283	2	1559	19	1861	2
67	2	-4	269	2	499	7	751	3	1019	2	1289	6	1567	3	1867	2
71	7	-2	271	6	503	5	757	2	1021	10	1291	2	1571	2	1871	14
73	5	-5	277	5	509	2	761	6	1031	14	1297	10	1579	3	1873	10
79	3	-2	281	3	521	3	769	11	1033	5	1301	2	1583	5	1877	2
83	2	-3	283	3	523	2	773	2	1039	3	1303	6	1597	11	1879	6
89	3	-3	293	2	541	2	787	2	1049	3	1307	2	1601	3	1889	3
97	5	-5	307	5	547	2	797	2	1051	7	1319	13	1607	5	1901	2
101	2	-2	311	17	557	2	809	3	1061	2	1321	13	1609	7	1907	2
103	5	-2	313	10	563	2	811	3	1063	3	1327	3	1613	3	1913	3
107	2	-3	317	2	569	3	821	2	1069	6	1361	3	1619	2	1931	2
109	6	-6	331	3	571	3	823	3	1087	3	1367	5	1621	2	1933	5
113	3	-3	337	10	577	5	827	2	1091	2	1373	2	1627	3	1949	2
127	3	-9	347	2	587	2	829	2	1093	5	1381	2	1637	2	1951	3
131	2	-3	349	2	593	7	839	11	1097	3	1399	13	1657	11	1973	2
137	3	-3	353	3	599	7	853	2	1103	5	1409	3	1663	3	1979	2
139	2	-4	359	7	601	7	857	3	1109	2	1423	3	1667	2	1987	2
149	2	-2	367	6	607	3	859	2	1117	2	1427	2	1669	2	1993	5
151	6	-5	373	2	613	2	863	5	1123	2	1429	6	1693	2	1997	2
157	5	-5	379	2	617	3	877	2	1129	11	1433	3	1697	3	1999	3
163	2	-4	383	5	619	2	881	3	1151	17	1439	7	1699	3	2003	5
167	5	-2	389	2	631	3	883	2	1153	5	1447	3	1709	3	2011	3

# Spis treści

<b>1</b>	<b>Pojęcia podstawowe</b>	<b>1</b>
1.1	Liczby naturalne . . . . .	1
1.1.1	Kilka zasad podstawowych . . . . .	1
1.1.2	Zasada Indukcji Matematycznej . . . . .	3
1.2	Działania algebraiczne . . . . .	6
1.3	Grupa . . . . .	8
1.4	Pierścień przemienny. Ciało . . . . .	9
1.5	Liczby zespolone . . . . .	11
<b>2</b>	<b>Elementarz</b>	<b>18</b>
2.1	Największy wspólny dzielnik w pierścieniu $\mathbb{Z}$ . . . . .	18
2.1.1	Podzielność i dzielenie z resztą w $\mathbb{Z}$ . . . . .	18
2.1.2	Ideały w pierścieniu $\mathbb{Z}$ . . . . .	20
2.1.3	Największy wspólny dzielnik . . . . .	22
2.1.4	Zasadnicze Twierdzenie Arytmetyki . . . . .	24
2.1.5	Najmniejsza wspólna wielokrotność . . . . .	25
2.1.6	Algorytm Euklidesa . . . . .	26
2.2	Równanie $ax + by = n$ . . . . .	28
2.2.1	Twierdzenie Brahmagupty-Bacheta . . . . .	28
2.2.2	Twierdzenie Sylwestera . . . . .	29
2.3	Liczby pierwsze . . . . .	31
2.3.1	Istnienie i jednoznaczność rozkładu na czynniki pierwsze . . . . .	31
2.3.2	Sito Eratostenesa. Twierdzenie Euklidesa . . . . .	32
2.3.3	Kilka pytań dotyczących liczb pierwszych . . . . .	34
2.4	Wykładniki $p$ -adyczne . . . . .	36
2.4.1	Definicje. Formuła Legendre'a . . . . .	36
2.4.2	Lemat o zwiększaniu wykładnika $p$ -adycznego . . . . .	38
2.5	Trójki pitagorejskie . . . . .	42
2.5.1	Trik . . . . .	42
2.5.2	Trójki pitagorejskie . . . . .	43
2.6	Zadania dodatkowe . . . . .	44
2.6.1	Treści zadań . . . . .	44
2.6.2	Wskazówki i rozwiązania . . . . .	48
<b>3</b>	<b>Wielomiany</b>	<b>64</b>
3.1	Pierścień wielomianów . . . . .	64
3.2	Siedem idei szkolnych . . . . .	66
3.2.1	Pierwsza idea: twierdzenie Bézouta . . . . .	66
3.2.2	Druga idea: algorytm dzielenia z resztą . . . . .	68

3.2.3	Trzecia idea: twierdzenie Lagrange'a i o jednoznaczności . . . . .	70
3.2.4	Czwarta idea: pierwiastki wymierne . . . . .	72
3.2.5	Piąta idea: postać kanoniczna trójmianu kwadratowego . . . . .	73
3.2.6	Szósta idea: Wielomian jako funkcja rzeczywista . . . . .	75
3.2.7	Siódma idea: wzory Viète'a . . . . .	77
3.3	Jednoznaczność rozkładu w pierścieniu wielomianów . . . . .	81
3.3.1	Podzielność w pierścieniu wielomianów . . . . .	82
3.3.2	Ideał. Największy wspólny dzielnik . . . . .	83
3.3.3	Zasadnicze twierdzenie arytmetyki wielomianów . . . . .	84
3.3.4	Wielomiany nierozkładalne . . . . .	85
3.3.5	Jednoznaczność rozkładu . . . . .	85
3.4	Dalsze twierdzenia o wielomianach . . . . .	86
3.4.1	Zawartość wielomianu . . . . .	86
3.4.2	Wielomiany nierozkładalne w $\mathbb{Q}[X]$ . . . . .	89
3.4.3	Zasadnicze Twierdzenie Algebry . . . . .	92
3.4.4	Rozkłady w pierścieniu $\mathbb{C}[X]$ i $\mathbb{R}[X]$ . . . . .	94
3.4.5	Pierwiastki wielomianu $X^n - 1$ . . . . .	95
3.4.6	Wielomiany cyklotomiczne . . . . .	97
3.4.7	Rozwiązywanie równań stopnia 3 i 4 . . . . .	98
3.4.8	Wzory Viète'a . . . . .	101
3.4.9	Wielomiany palindromiczne . . . . .	104
3.4.10	Wielomian interpolacyjny Lagrange'a . . . . .	105
3.4.11	Funkcje wymierne. Ułamki proste . . . . .	106
3.4.12	Funkcje wymierne jako funkcje . . . . .	108
3.5	Wielomiany wielu zmiennych . . . . .	108
3.5.1	Definicje . . . . .	108
3.5.2	Tożsamość Sophie Germain . . . . .	110
3.5.3	Jeszcze dwie faktoryzacje . . . . .	111
3.6	Zadania dodatkowe . . . . .	112
3.6.1	Treści zadań . . . . .	112
3.6.2	Wskazówki/rozwiązania . . . . .	118
<b>4</b>	<b>Funkcje arytmetyczne</b> . . . . .	<b>143</b>
4.1	Sumy potęg dzielników . . . . .	143
4.1.1	Funkcja $\tau$ . . . . .	144
4.1.2	Funkcja $\sigma$ . . . . .	145
4.2	Funkcja $\varphi$ Eulera . . . . .	146
4.3	Splot Dirichleta i odwracanie Möbiusa . . . . .	147
4.3.1	Splot Dirichleta . . . . .	147
4.3.2	Twierdzenie Möbiusa o odwracaniu . . . . .	148
4.4	Piętnaście zadań dodatkowych . . . . .	150
4.4.1	Treści zadań . . . . .	150
4.4.2	Rozwiązania wybranych ćwiczeń i zadań dodatkowych . . . . .	151
<b>5</b>	<b>Arytmetyka modularna</b> . . . . .	<b>157</b>
5.1	Wstęp do teorii kongruencji . . . . .	157
5.1.1	Definicja i cechy podzielności . . . . .	157
5.1.2	Motywacja: równania diofantyczne . . . . .	160
5.1.3	Twierdzenie Schura . . . . .	161



5.1.4	Kongruencje liniowe . . . . .	162
5.1.5	Odwracanie modulo $m$ . . . . .	163
5.2	Twierdzenie Eulera, Fermata i Wilsona . . . . .	164
5.2.1	Zupełne i zredukowane układy reszt . . . . .	164
5.2.2	Twierdzenie Eulera . . . . .	165
5.2.3	Małe twierdzenie Fermata . . . . .	166
5.2.4	Twierdzenie Wilsona . . . . .	167
5.3	Układy kongruencji liniowych . . . . .	168
5.3.1	Twierdzenie chińskie o resztach . . . . .	169
5.3.2	Zadanie o długiej igle . . . . .	171
5.3.3	Uogólnione twierdzenie chińskie o resztach . . . . .	172
5.4	Pierścień klas reszt modulo $m$ . . . . .	175
5.4.1	Działania na warstwach modulo $m$ . . . . .	176
5.4.2	Grupa $(\mathbb{Z}/m)^*$ warstw odwracalnych . . . . .	177
5.4.3	Ciało $\mathbb{Z}/p$ . . . . .	178
5.4.4	Pierwiastki kongruencji wielomianowych . . . . .	178
5.4.5	Kongruencje wielomianowe modulo $p$ . . . . .	181
5.4.6	Ważne zastosowanie twierdzenia chińskiego . . . . .	181
5.5	Rząd elementu grupy w teorii liczb . . . . .	183
5.5.1	Podgrupy i twierdzenie Lagrange'a . . . . .	183
5.5.2	Podstawowe własności rzędu elementu . . . . .	184
5.5.3	Rząd elementu w grupie $(\mathbb{Z}/m, +)$ . . . . .	186
5.5.4	Rząd elementu w grupie $((\mathbb{Z}/m)^*, \cdot)$ . . . . .	186
5.5.5	O liczbach pierwszych w ciągach arytmetycznych . . . . .	189
5.5.6	Twierdzenie Zsigmondy'ego . . . . .	191
5.6	Pierwiastki pierwotne . . . . .	195
5.6.1	Definicja i uwagi wstępne . . . . .	195
5.6.2	Twierdzenie o istnieniu pierwiastków pierwotnych . . . . .	197
5.6.3	Jeszcze kilka przykładów . . . . .	199
5.6.4	Indeks . . . . .	201
5.6.5	Dwa słowa o liczbach Carmichaela . . . . .	202
5.7	Reszty kwadratowe i prawo wzajemności . . . . .	203
5.7.1	Reszty i niereszty kwadratowe modulo $p$ . . . . .	203
5.7.2	Symbol Legendre'a . . . . .	204
5.7.3	Kryterium Eulera . . . . .	204
5.7.4	Kryterium Gaussa . . . . .	206
5.7.5	Prawo wzajemności reszt kwadratowych . . . . .	208
5.7.6	Prawo wzajemności a ciągi arytmetyczne . . . . .	211
5.7.7	Trójmian kwadratowy modulo $p$ . . . . .	213
5.7.8	Kilka zadań . . . . .	214
5.7.9	Liczba lokalnie kwadratowa jest kwadratem (globalnym) . . . . .	217
5.8	Kongruencje modulo $p^n$ . Liczby $p$ -adyczne . . . . .	218
5.8.1	Reszty kwadratowe modulo $p^n$ . . . . .	219
5.8.2	Lemat Hensela . . . . .	220
5.8.3	Jedno interesujące zadanie . . . . .	221
5.8.4	Dwa słowa o liczbach $p$ -adycznych . . . . .	222

<b>6</b>	<b>Dodatkowe wiadomości o wielomianach</b>	<b>224</b>
6.1	Pochodna wielomianu . . . . .	224
6.1.1	Funkcja wielomianowa . . . . .	224
6.1.2	Definicja pochodnej . . . . .	225
6.1.3	Twierdzenia Rolle'a i Lagrange'a . . . . .	225
6.1.4	Wzór Maclaurina i wzór Taylora . . . . .	226
6.1.5	Pochodna a pierwiastki wielokrotne . . . . .	227
6.2	Wielomiany symetryczne . . . . .	227
6.2.1	Definicja . . . . .	228
6.2.2	Twierdzenie Newtona . . . . .	229
6.2.3	Wyróżnik . . . . .	230
6.2.4	Funkcje tworzące . . . . .	230
6.3	Liczby algebraiczne i przestępne . . . . .	232
6.3.1	Wielomian minimalny liczby algebraicznej . . . . .	232
6.3.2	Uwalnianie się od niewymierności w mianowniku . . . . .	233
6.3.3	Pierścień liczb algebraicznych całkowitych . . . . .	234
6.3.4	Nierozkładalność wielomianów cyklotomicznych . . . . .	236
6.3.5	Liczby przestępne . . . . .	238
6.3.6	Twierdzenie Liouville'a . . . . .	238
6.4	O zerach wielomianów wielu zmiennych . . . . .	240
6.4.1	Combinatorial Nullstellensatz . . . . .	241
6.4.2	Kilka zastosowań . . . . .	244
6.4.3	Twierdzenia Chevalley'a i Warninga . . . . .	245
6.5	Wielomiany i liczby Bernoulliego . . . . .	248
6.5.1	Sumowanie potęg . . . . .	248
6.5.2	Wielomiany i liczby Bernoulliego . . . . .	248
<b>7</b>	<b>Aproksymacje diofantyczne</b>	<b>250</b>
7.1	Twierdzenie Dirichleta . . . . .	250
7.2	Ciągi Farey'a . . . . .	251
7.3	Ułamki łańcuchowe . . . . .	253
7.3.1	Kanoniczne rozwinięcia. Reguła Eulera . . . . .	253
7.3.2	Nieskończone ułamki łańcuchowe . . . . .	256
7.3.3	Złota liczba. Twierdzenie Hurwitza . . . . .	259
7.3.4	Grupa $\mathbf{GL}_2(\mathbb{Z})$ . . . . .	261
7.3.5	Równoważność liczb . . . . .	262
7.3.6	Niewymierności kwadratowe . . . . .	263
7.3.7	Okresowe ułamki łańcuchowe . . . . .	265
7.3.8	Twierdzenia Lagrange'a i Galois . . . . .	267
<b>8</b>	<b>Sumy kwadratów</b>	<b>270</b>
8.1	Jedna ważna tożsamość . . . . .	270
8.2	Sumy dwóch kwadratów . . . . .	272
8.2.1	Twierdzenie Fermata-Eulera . . . . .	272
8.2.2	Drugi dowód twierdzenia Fermata-Eulera . . . . .	274
8.2.3	Twierdzenie o przedstawieniu . . . . .	275
8.3	Jeszcze trochę geometrii w teorii liczb . . . . .	277
8.3.1	Kraty w płaszczyźnie . . . . .	277
8.3.2	Dyskretne podgrupy płaszczyzny . . . . .	278

8.3.3	Twierdzenie Minkowskiego o figurze wypukłej . . . . .	280
8.3.4	Dwa zastosowania . . . . .	281
8.3.5	Liczby naturalne postaci $x^2 + 2y^2$ i $x^2 + 3y^2$ . . . . .	283
8.3.6	Liczby pierwsze postaci $x^2 + 5y^2$ . . . . .	285
8.4	Binarne formy kwadratowe . . . . .	287
8.4.1	Wyróżnik formy . . . . .	288
8.4.2	Równoważność form . . . . .	288
8.4.3	Lemat Lagrange'a . . . . .	290
8.4.4	Redukcja form dodatnio-określonych . . . . .	291
8.5	Sumy więcej niż dwóch kwadratów . . . . .	293
8.5.1	Twierdzenie o sumach czterech kwadratów . . . . .	294
8.5.2	Uwagi o sumach trzech kwadratów . . . . .	296
8.6	Dodatek. Piąty dowód TFE . . . . .	297
<b>9</b>	<b>Arytmetyka ciągów rekurencyjnych</b> . . . . .	<b>301</b>
9.1	Klasyczny ciąg Fibonacciego . . . . .	301
9.1.1	Wzór Bineta . . . . .	302
9.1.2	Kilka tożsamości . . . . .	302
9.1.3	Dwie interpretacje ciągu $(f_n)$ . . . . .	304
9.1.4	Ciąg $(f_n)$ jest NWD-ciągiem . . . . .	304
9.2	Metoda Eulera i metoda funkcji tworzących . . . . .	305
9.2.1	Metoda Eulera . . . . .	305
9.2.2	Pierścień formalnych szeregów potęgowych . . . . .	308
9.2.3	Metoda funkcji tworzących . . . . .	309
9.3	Ciągi Lucasa . . . . .	309
9.3.1	Przestrzeń $\mathcal{R}ek(P, Q)$ . . . . .	310
9.3.2	Definicja ciągów Lucasa . . . . .	310
9.3.3	Kilka tożsamości . . . . .	311
9.3.4	Podzielność wyrazów ciągów Lucasa . . . . .	312
9.4	Ilustracja geometryczna . . . . .	313
9.4.1	Macierze odwzorowań liniowych . . . . .	313
9.4.2	Wyznacznik odwzorowania liniowego . . . . .	315
9.4.3	Pola trójkątów . . . . .	315
9.4.4	Ogólny wzór Cassini'ego . . . . .	316
9.5	Ciągi rekurencyjne modulo $p$ . . . . .	317
9.5.1	Warstwy zespolone modulo $p$ . . . . .	317
9.5.2	$\mathbb{F}_p(\iota)$ jest ciałem . . . . .	319
9.5.3	Dwa słowa o grupie moltiplicatywnej $\mathbb{F}_p(\iota)^*$ . . . . .	320
9.5.4	Wzory Eulera-Bineta modulo $p$ . . . . .	321
9.5.5	Okresowość ciągów rekurencyjnych modulo $p$ . . . . .	322
<b>10</b>	<b>Pierścienie kwadratowe</b> . . . . .	<b>325</b>
10.1	Pierścień liczb całkowitych Gaussa . . . . .	326
10.1.1	Definicja i podstawowe własności . . . . .	326
10.1.2	Dzielenie z resztą i podzielność w $\mathbb{Z}[i]$ . . . . .	327
10.1.3	Algorytm Euklidesa w $\mathbb{Z}[i]$ . . . . .	330
10.1.4	Liczby pierwsze w $\mathbb{Z}[i]$ . . . . .	330
10.1.5	Twierdzenie o jednoznaczności rozkładu w $\mathbb{Z}[i]$ . . . . .	332
10.1.6	Rozkład liczb pierwszych wymiernych w $\mathbb{Z}[i]$ . . . . .	334

10.1.7	Wzór na wartość $r(n)$ . . . . .	335
10.2	Pierścienie kwadratowe . . . . .	336
10.2.1	Jedności w $\mathbb{Z}[\tau_D]$ . . . . .	337
10.2.2	Dzielenie z resztą w $\mathbb{Z}[\tau_D]$ . . . . .	337
10.2.3	Podzielność, NWD i ideały w $\mathbb{Z}[\tau_D]$ . . . . .	340
10.2.4	Dig'owość pierścieni kwadratowych . . . . .	342
10.2.5	Wnioski z dig'owości . . . . .	342
10.2.6	Związek z formami kwadratowymi . . . . .	344
10.2.7	Jednoznaczność rozkładu . . . . .	347
10.2.8	Pierścienie $\mathbb{Z}[\tau_{-2}]$ , $\mathbb{Z}[\tau_{-3}]$ i $\mathbb{Z}[\tau_{-5}]$ . . . . .	349
10.3	Teoria podzielności w digach . . . . .	354
10.3.1	Dziedziny całkowitości . . . . .	354
10.3.2	Relacja podzielności. Relacja stowarzyszenia . . . . .	355
10.3.3	Ideał. Dziedzina ideałów głównych . . . . .	356
10.3.4	Największy wspólny dzielnik . . . . .	357
10.3.5	Elementy nierozkładalne i pierwsze w $\mathcal{R}$ . . . . .	357
10.3.6	Jednoznaczność rozkładu w digach . . . . .	358
10.4	Jedności rzeczywiste . . . . .	360
10.4.1	Lemat o równaniu $x^2 - Dy^2 = 1$ . . . . .	360
10.4.2	Jedności fundamentalne . . . . .	361
10.4.3	Pierścienie typu $(-1)$ i $(+1)$ . . . . .	364
<b>11</b>	<b>Równania diofantyczne</b> . . . . .	<b>365</b>
11.1	Metody podstawowe . . . . .	365
11.1.1	Wykorzystanie nierówności . . . . .	365
11.1.2	Metoda zstępowania . . . . .	366
11.1.3	Wykorzystanie kongruencji . . . . .	367
11.1.4	Wykorzystanie jednoznaczności rozkładu . . . . .	369
11.2	Wielkie Twierdzenie Fermata . . . . .	371
11.2.1	Metoda Fermata dowodu WTF(4) . . . . .	372
11.2.2	Twierdzenie Sophie Germain . . . . .	374
11.2.3	Metoda Eulera dowodu WTF(3) . . . . .	375
11.2.4	Równanie $x^3 + y^3 + z^3 = w^3$ . . . . .	377
11.3	Równanie Ramanujana . . . . .	378
11.4	Równanie indyjskie . . . . .	383
11.4.1	Twierdzenie podstawowe . . . . .	383
11.4.2	Interpretacje . . . . .	386
11.4.3	Równanie <i>anty</i> -indyjskie . . . . .	388
11.4.4	Ogólne równanie indyjskie . . . . .	389
11.4.5	Kilka zadań . . . . .	390
11.5	Punkty wymierne na prostych i na stożkowych . . . . .	391
11.6	Krzywe sześciennic . . . . .	398
11.6.1	Postać normalna. Przykłady . . . . .	398
11.6.2	Krzywe eliptyczne . . . . .	402
11.6.3	Metoda siecznych-stycznych . . . . .	403
11.6.4	Równania $y^2 = x^3 + 1$ i $y^2 = x^3 - 1$ . . . . .	406
11.6.5	Dodawanie punktów krzywej eliptycznej . . . . .	409

<b>12 Kilka wiadomości dodatkowych</b>	<b>412</b>
12.1 Część całkowita i ułamkowa liczby rzeczywistej . . . . .	412
12.1.1 Podstawowe własności . . . . .	412
12.1.2 Twierdzenie Beatty'ego . . . . .	414
12.1.3 Zadania z częścią ułamkową . . . . .	415
12.2 Zapis pozycyjny liczb . . . . .	417
12.2.1 Zapis pozycyjny liczb naturalnych . . . . .	417
12.2.2 Zapis pozycyjny liczb rzeczywistych . . . . .	419
12.3 Ułamki egipskie . . . . .	421
12.3.1 Skończone sumy ułamków egipskich . . . . .	421
12.3.2 Szeregi harmoniczne . . . . .	425
12.3.3 Liczby harmoniczne. Twierdzenie Wolstenholme'a . . . . .	429
12.4 Współczynniki dwumienne . . . . .	431
12.4.1 Wielomiany Newtona . . . . .	432
12.4.2 Twierdzenie Lucasa . . . . .	432
12.4.3 Twierdzenie Wolstenholme'a-Glaishera . . . . .	434
12.5 Rozmieszczenie liczb pierwszych . . . . .	436
12.5.1 Dwa twierdzenia Czebyszewa . . . . .	436
12.5.2 Twierdzenie o liczbach pierwszych . . . . .	440
<b>Literatura</b>	<b>441</b>
<b>Indeks</b>	<b>442</b>



# Rozdział 1

## Pojęcia podstawowe

*Les nombres (entiers) me semblent constituer comme un monde de réalités qui existent en dehors de nous avec la même caractère d'absolue nécessité que les réalités de la nature dont la connaissance nous est donnée par nos sens.*<sup>1</sup>

(Charles Hermite w liście do Georga Cantora)

W rozdziale tym przypominamy podstawowe fakty dotyczące liczb naturalnych oraz poznajemy definicje najważniejszych struktur algebraicznych takich jak grupa, pierścień i ciało. W końcu rozdziału poznajemy nowy rodzaj liczb: liczby zespolone.

### 1.1 Liczby naturalne

Zakładamy, że Czytelnik jest dobrze zaznajomiony z pojęciem **liczby całkowitej**. Zbiór wszystkich liczb  $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  oznaczamy przez  $\mathbb{Z}$ . Dodatnie elementy tego zbioru nazywamy **liczbami naturalnymi**. Zbiór liczb naturalnych oznaczamy symbolem  $\mathbb{N}$ . W niektórych podręcznikach zero uważa się za liczbę naturalną. Nam będzie wygodniej zaczynać liczby naturalne od 1.

#### 1.1.1 Kilka zasad podstawowych

Najważniejszym faktem dotyczącym liczb naturalnych jest Zasada Minimum. Jest ona w istocie aksjوماتem (czyli twierdzeniem przyjmowanym bez dowodu).

**ZASADA MINIMUM** *Każdy niepusty podzbiór zbioru liczb naturalnych zawiera (dokładnie jedną) liczbę najmniejszą.*

Standardowe zastosowania Zasady Minimum w rozumowaniach teoriolichbowych zobaczymy w dowodach twierdzeń T2.14 i T2.16. Teraz pokażemy na prostym przykładzie, jak to działa. Wybieramy w tym celu *dowód niewymierności*  $\sqrt{n}$ , gdzie  $n \in \mathbb{N}$  nie jest kwadratem:

**ZADANIE 1.1** Udowodnić, że jeżeli liczba naturalna  $n$  nie jest kwadratem żadnej liczby całkowitej, to nie jest też kwadratem żadnej liczby wymiernej.

---

<sup>1</sup>Liczby (naturalne) zdają mi się stanowić coś w rodzaju świata bytów obiektywnie istniejących z taką samą cechą absolutnej konieczności jaką ma, poznawany za pomocą zmysłów, świat realny.

ROZWIĄZANIE. Załóżmy, nie wprost, że istnieją takie ułamki  $\frac{a}{b}$ , że  $a, b \in \mathbb{N}$ , i dla których zachodzi równość  $\sqrt{n} = \frac{a}{b}$ , czyli równość  $nb^2 = a^2$ . Rozważmy więc (niepusty!) zbiór mianowników wszystkich takich ułamków  $\frac{a}{b}$ . Niech  $b_0$  będzie najmniejszą liczbą w tym zbiorze. Wówczas

$$\frac{nab_0}{ab_0} = n = \frac{ka^2}{kb_0^2}$$

dla pewnego  $a \in \mathbb{N}$  i dowolnej liczby  $k \in \mathbb{N}$ . Stąd

$$n = \frac{nab_0 - ka^2}{ab_0 - kb_0^2} = \frac{a}{b_0} \cdot \frac{nb_0 - ka}{a - kb_0} = \sqrt{n} \cdot \frac{nb_0 - ka}{a - kb_0} \quad (1.1)$$

na mocy zasady **odejmowania proporcji stronami** i założenia  $\sqrt{n} = a/b_0$ . Podnosząc równość (1.1) obustronnie do kwadratu i upraszczając przez  $n$ , dostajemy

$$n = \left( \frac{nb_0 - ka}{a - kb_0} \right)^2.$$

Położmy w tej równości  $k$  wyznaczone (jednoznacznie) z nierówności  $k^2 < n < (k+1)^2$ . Wówczas  $kb_0 < a < kb_0 + b_0$ , skąd  $0 < a - kb_0 < b_0$  i widzimy, że dodatni mianownik  $a - kb_0$  ułamka  $\frac{nb_0 - ka}{a - kb_0}$  jest mniejszy niż  $b_0$ . Sprzeczność.  $\diamond$

Przykład. Dowodzimy: *Liczba 1 jest najmniejszą liczbą naturalną*. Rzeczywiście, jeżeli istnieją liczby naturalne mniejsze niż 1, to niech (Zasada Minimum!)  $n_0$  będzie najmniejszą liczbą naturalną mniejszą niż 1. Wówczas  $n_0^2 < n_0 < 1$ . Sprzeczność. Q.e.d.  $\diamond$

Czytelnik zechce z pewnością udowodnić prawdziwość kolejnej zasady:

**ZASADA SKWANTOWANIA** *Jeżeli liczby całkowite  $a, b$  spełniają warunek  $a > b$ , to  $a \geq b + 1$ . W szczególności: jeżeli  $c \in \mathbb{Z}$  i  $c > 0$ , to  $c \geq 1$ .*

Przykładowe zastosowanie Zasady Skwantowania widzimy w rozwiązaniu takiego zadania:

**ZADANIE 1.2** Udowodnić, że jeżeli dla liczb naturalnych  $a, b, c, d, k, l$  zachodzi równość  $bc - ad = 1$  i nierówności  $\frac{a}{b} < \frac{k}{l} < \frac{c}{d}$ , to  $k \geq a + c$  i  $l \geq b + d$ .

ROZWIĄZANIE. Nierówność  $\frac{a}{b} < \frac{k}{l}$  daje  $0 < bk - al$ . Stąd, ponieważ mamy do czynienia z liczbą całkowitą, dostajemy  $1 \leq bk - al$ . Mnożąc tę nierówność przez  $c$ , znajdujemy

$$c \leq c(bk - al) = bck - acl = (1 + ad)k - acl,$$

skąd  $a(cl - dk) + c \leq k$ , czyli  $a + c \leq k$  (bo  $cl - dk > 0$ , więc  $cl - dk \geq 1$ ). Podobnie, mnożąc nierówność  $cl - dk \geq 1$  przez  $b$ , dostaniemy nierówność  $b + d \leq l$ .  $\diamond$

Często stosujemy również Zasadę Maksimum:

**ZASADA MAKSIMUM** *Każdy niepusty i ograniczony (od góry) zbiór liczb naturalnych zawiera dokładnie jeden element największy.*

**ZADANIE 1.3** Udowodnić Zasadę Maksimum korzystając z Zasady Minimum.



ROZWIĄZANIE. Niech  $X$  będzie niepustym i ograniczonym podzbiorem zbioru liczb naturalnych. To znaczy, że istnieje takie  $a \in \mathbb{N}$ , że dla każdego  $x \in X$  mamy  $x \leq a$ . Niech  $Y = \{y \in \mathbb{N} : \forall x \in X y \geq x\}$  będzie zbiorem wszystkich ograniczeń górnych zbioru  $X$ . Zbiór  $Y$  jest niepusty, bo  $a \in Y$ . Zawiera zatem element najmniejszy. Oznaczmy go  $m$ . Wówczas

$$m \geq x$$

dla każdego  $x \in X$ , bo  $m \in Y$ . Twierdzimy, że  $m$  należy do  $X$  i jest, wobec tego, największym elementem zbioru  $X$ . Gdyby  $m \notin X$ , to wszystkie nierówności  $m \geq x$  byłyby ostre i wtedy (na mocy Zasady Skwantowania) mielibyśmy  $m - 1 \geq x$  dla każdego  $x \in X$ . To jednakże jest niemożliwe, bo  $m$  jest najmniejszym elementem zbioru  $Y$ .  $\diamond$

**Ćwiczenie 1.1** Udowodnić Zasadę Minimum korzystając z Zasady Maksimum.

### 1.1.2 Zasada Indukcji Matematycznej

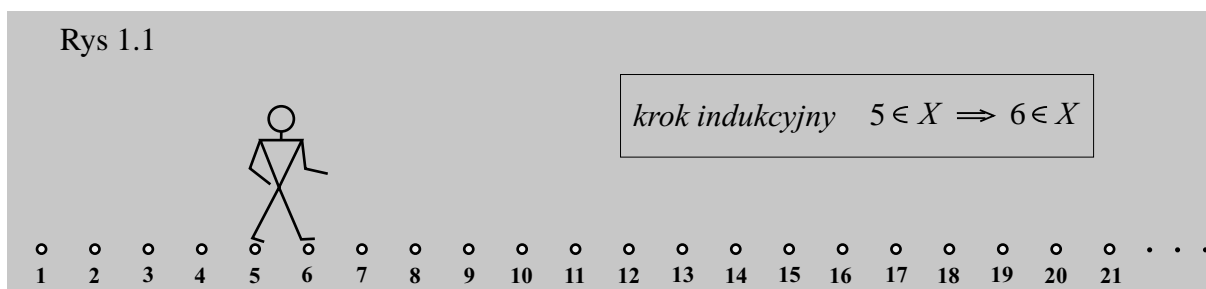
Zasada Indukcji Matematycznej jest (logicznie) równoważna Zasadzie Minimum, ale często bywa wygodniejsza w stosowaniu.

**ZASADA INDUKCJI MATEMATYCZNEJ** Niech  $X \subseteq \mathbb{N}$  będzie podzbiorem zbioru liczb naturalnych. Załóżmy, że spełnione są warunki:

$$(B) \quad \boxed{1 \in X}, \quad (I) \quad \boxed{k \in X \Rightarrow k + 1 \in X}.$$

Wówczas  $X = \mathbb{N}$ .

Podzbiór  $X$  zbioru liczb naturalnych nazwiemy **podzbiorem induktywnym**, gdy spełnia warunek (I). Zasada Indukcji Matematycznej mówi po prostu, że zawierający liczbę 1 podzbiór induktywny zbioru liczb naturalnych jest całym zbiorem liczb naturalnych  $\mathbb{N}$ .



Przykład. Udowodnimy, że suma wszystkich liczb naturalnych nie większych niż  $n$  wynosi  $\frac{n(n+1)}{2}$ . Oznaczmy tę sumę przez  $S_n$ . Mamy udowodnić, że zbiór

$$X = \left\{ k \in \mathbb{N} : S_k = \frac{k(k+1)}{2} \right\}$$

jest całym zbiorem liczb naturalnych. W pierwszym kroku sprawdzamy, czy zbiór  $X$  spełnia warunek (B) (zwany **warunkiem bazowym**). Tę część rozumowania nazywamy **bazą** rozumowania indukcyjnego. W aktualnym przypadku warunek bazowy jest spełniony (bowiem

$1 = \frac{1 \cdot 2}{2}$ ). Sprawdzenie zachodzenia warunku (I), czyli induktywności zbioru  $X$ , nazywa się **krokiem indukcyjnym** rozumowania indukcyjnego. Załóżmy więc, że liczba naturalna  $k$  należy do  $X$ . Wówczas, w aktualnym przypadku,

$$S_{k+1} = S_k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2},$$

więc  $k+1 \in X$ . Dzięki ZIM (Zasadzie Indukcji Matematycznej) widzimy, że  $X = \mathbb{N}$ .  $\diamond$

Podobnie dowodzimy też poniższego ćwiczenia:

**Ćwiczenie 1.2** Udowodnić, że dla każdej liczby naturalnej  $n > 1$ :

1.  $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ ,
2.  $1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{n(4n^2-1)}{3}$ ,
3.  $\frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{2 \cdot 4 \cdot 6 \cdot \dots \cdot 2n} < \frac{1}{\sqrt{3n+1}}$ ,
4.  $\sqrt{2 + \sqrt{2 + \dots + \sqrt{2}}} = 2 \cos \frac{\pi}{2^{n+1}}$  ( $n$  pierwiastków),
5.  $\frac{1}{1+x} + \frac{2}{1+x^2} + \frac{4}{1+x^4} + \dots + \frac{2^n}{1+x^{2^n}} = \frac{2^{n+1}}{1-x^{2^{n+1}}} - \frac{1}{1-x}$  dla  $|x| \neq 1$ .

**Ćwiczenie 1.3** Udowodnić poniższe wersje ZIM:

(1) Jeżeli podzbiór  $X \subseteq \mathbb{N}$  spełnia warunki

$$(B) \quad \boxed{1 \in X}, \quad (IU) \quad \boxed{\{1, \dots, k\} \subseteq X \Rightarrow k+1 \in X},$$

to  $X = \mathbb{N}$ .

(2) Jeżeli podzbiór  $X \subseteq \mathbb{N}$  spełnia warunki

$$(B1-2) \quad \boxed{1, 2 \in X}, \quad (I2) \quad \boxed{k \in X \Rightarrow k+2 \in X},$$

to  $X = \mathbb{N}$ .

**ZADANIE 1.4** Udowodnić, że zbiór  $\mathcal{G} = \{0, 1, \dots, 1023\}$  da się rozbić na sumę takich dwóch rozłącznych równolicznych podzbiorów  $\mathcal{A}, \mathcal{B}$ , że dla każdego  $k = 1, 2, \dots, 9$  suma  $k$ -tych potęg liczb zbioru  $\mathcal{A}$  równa jest sumie  $k$ -tych potęg liczb zbioru  $\mathcal{B}$ .

**ROZWIĄZANIE.** Po pierwsze dobrze jest się domyślić, że jest to zadanie dające się rozwiązać za pomocą indukcji. Mianowicie oznaczmy przez  $X$  zbiór takich liczb naturalnych  $n$ , dla których zbiór  $\mathcal{G}(n) = \{0, 1, \dots, 2^{n+1} - 1\}$  można przedstawić w postaci sumy takich dwóch równolicznych podzbiorów  $\mathcal{A}(n)$  i  $\mathcal{B}(n)$ , że dla każdego  $k = 1, 2, \dots, n$  suma  $k$ -tych potęg liczb zbioru  $\mathcal{A}(n)$  równa jest sumie  $k$ -tych potęg liczb zbioru  $\mathcal{B}(n)$ . Nasze zadanie polega na udowodnieniu, że  $9 \in X$ . Wykażemy przez indukcję nierównie więcej:  $X = \mathbb{N}$ .

Korzystając z Zasady Indukcji zdefiniujemy zbiory  $\mathcal{A}(n)$  i  $\mathcal{B}(n)$  dla każdego  $n \in \mathbb{N}$ . Niech  $\mathcal{A}(1) = \{0, 3\}$  i  $\mathcal{B}(1) = \{1, 2\}$  (to jest **baza definicji indukcyjnej**). Następnie definiujemy

$$\mathcal{A}(n+1) = \mathcal{A}(n) \cup [\mathcal{B}(n) + 2^{n+1}], \quad \mathcal{B}(n+1) = \mathcal{B}(n) \cup [\mathcal{A}(n) + 2^{n+1}]. \quad (1.2)$$

[Używamy tu wygodnego skrótów  $\mathcal{X} + a = \{x + a : x \in \mathcal{X}\}$  dla dowolnego podzbioru  $\mathcal{X} \subseteq \mathbb{N}$  i dowolnej liczby  $a \in \mathbb{N}$ .] To jest **krok indukcyjny definicji indukcyjnej** (= określenie obiektu następnego za pomocą poprzedniego lub poprzednich). Mamy więc na przykład:

$$\mathcal{A}(2) = \mathcal{A}(1) \cup [\mathcal{B}(1) + 4] = \{0, 3\} \cup [\{1, 2\} + 4] = \{0, 3\} \cup \{5, 6\} = \{0, 3, 5, 6\},$$

$$\mathcal{B}(2) = \mathcal{B}(1) \cup [\mathcal{A}(1) + 4] = \{1, 2\} \cup [\{0, 3\} + 4] = \{1, 2\} \cup \{4, 7\} = \{1, 2, 4, 7\}.$$

Łatwo, przez indukcję(!), sprawdzić, że zbiory  $\mathcal{A}(n)$ ,  $\mathcal{B}(n)$  są rozłączne i równoliczne. Czytelnik powinien bezwzględnie to zrobić.

Pozostało nam sprawdzenie, że  $\sum_{x \in \mathcal{A}(n)} x^k = \sum_{x \in \mathcal{B}(n)} x^k$  dla wszystkich  $n \in \mathbb{N}$  i wszystkich  $1 \leq k \leq n$ . Robimy to, oczywiście, za pomocą indukcji matematycznej, której baza jest po prostu równością  $0 + 3 = 1 + 2$ .

Dla wykonania kroku indukcyjnego ustalmy liczby naturalne  $k \leq n + 1$ . Mamy wtedy

$$\begin{aligned} \sum_{x \in \mathcal{A}(n+1)} x^k &= \sum_{x \in \mathcal{A}(n)} x^k + \sum_{x \in \mathcal{B}(n)} (x + 2^{n+1})^k = \sum_{x \in \mathcal{A}(n)} x^k + \sum_{x \in \mathcal{B}(n)} \sum_{s=0}^k \binom{k}{s} x^{k-s} 2^{(n+1)s} = \\ &= \sum_{x \in \mathcal{A}(n)} x^k + \sum_{s=0}^k \binom{k}{s} 2^{(n+1)s} \sum_{x \in \mathcal{B}(n)} x^{k-s} = \sum_{x \in \mathcal{G}(n)} x^k + \sum_{s=1}^k \binom{k}{s} 2^{(n+1)s} \sum_{x \in \mathcal{B}(n)} x^{k-s}. \end{aligned}$$

Pierwsza równość wynika z (1.2), druga z twierdzenia o dwumianie (por. (1.7)), trzecia z przemienności sumy, a czwarta z równości  $\mathcal{G}(n) = \mathcal{A}(n) \sqcup \mathcal{B}(n)$  (suma rozłączna, zob. KOM). Dokładnie tak samo dostaniemy

$$\sum_{x \in \mathcal{B}(n+1)} x^k = \sum_{x \in \mathcal{G}(n)} x^k + \sum_{s=1}^k \binom{k}{s} 2^{(n+1)s} \sum_{x \in \mathcal{A}(n)} x^{k-s}.$$

Założenie indukcyjne, czyli równości  $\sum_{x \in \mathcal{A}(n)} x^{k-s} = \sum_{x \in \mathcal{B}(n)} x^{k-s}$  dla wszystkich  $s = 1, \dots, k$  (przy czym w przypadku  $s = k$  równość ta oznacza, po prostu równość mocy  $|\mathcal{A}(n)| = |\mathcal{B}(n)|$ ) daje więc równość  $\sum_{x \in \mathcal{A}(n+1)} x^k = \sum_{x \in \mathcal{B}(n+1)} x^k$ . W ten sposób zadanie jest rozwiązane.  $\diamond$

Rozwiązując poniższe zadanie również należy postawić tezę ogólną (dla dowolnego  $n$ ), a następnie udowodnić ją za pomocą ZIM.

**ZADANIE HALMOSA.** W pewnym miasteczku mieszka 345 zamężnych matematyczek. Każda z nich wie w każdej chwili czy mąż innej jest wierny czy nie, nic nie wie jednak o swoim mężu. Prawo tego miasteczka wymaga aby każdy, kto jest w stanie przeprowadzić dowód niewierności swojego partnera, zastrzelił go na specjalnym miejscu straceni tego samego dnia o zachodzie słońca. Każda matematyczka jest absolutnie inteligentna i absolutnie prawomyślna. Pewnego dnia pani burmistrz (jedyna niezamężna w miasteczku) ogłosiła, że w miasteczku są niewierni mężowie. Zakazała porozumiewania się paniom matematyczkom w rzeczonyj sprawie,

jednocześnie nakazując przeprowadzanie rozumowań dowodowych. W rzeczywistości w miasteczku było 40 niewiernych mężów. Co się stanie w miasteczku po ogłoszeniu pani burmistrz?

Czasami niezbędne jest stosowne wzmocnienie tezy, która staje się założeniem w kroku indukcyjnym:

**Ćwiczenie 1.4** Udowodnić za pomocą indukcji, że dla dowolnej liczby naturalnej  $n$  zachodzi nierówność

$$h_n(2) := 1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} < 2.$$

*Wskazówka.* Łatwiej dowodzić nierówności mocniejszej:  $h_n(2) \leq 2 - \frac{1}{n}$ .

**ZADANIE 1.5** Udowodnić, że Zasada Minimum jest równoważna Zasadzie Indukcji.

**ROZWIĄZANIE.** (1) Dowodzimy najpierw, że z ZIM wynika ZM. Postępujemy nie wprost. To znaczy, założymy, że zbiór  $Y \subseteq \mathbb{N}$  jest podzbiorem niepustym bez elementu najmniejszego. Zdefiniujemy podzbiór  $X \subseteq \mathbb{N}$ :

$$X = \{n \in \mathbb{N} : \{1, 2, \dots, n\} \cap Y = \emptyset\}.$$

Jasne, że  $1 \in X$  (bo  $\{1\} \cap Y = \emptyset$ , bowiem w przeciwnym przypadku liczba 1 byłaby elementem najmniejszym w  $Y$ ). Zatem  $X$  spełnia warunek bazowy ZIM. Sprawdzimy, że  $X$  jest podzbiorem induktywnym: Niech  $k \in X$ . Wówczas  $\{1, \dots, k\} \cap Y = \emptyset$ , więc, gdyby  $\{1, \dots, k, k+1\} \cap Y \neq \emptyset$ , to liczba  $k+1$  musiałaby należeć do  $Y$  i byłaby wtedy elementem najmniejszym w  $Y$ . Ponieważ założyliśmy, że w  $Y$  nie ma elementu najmniejszego, więc musi być  $\{1, \dots, k, k+1\} \cap Y = \emptyset$ , czyli  $k+1 \in X$ . Zatem, na mocy ZIM,  $X = \mathbb{N}$ . To oznacza, że  $Y = \emptyset$ . Uzyskana sprzeczność kończy rozumowanie.

(2) Dowodzimy teraz, że z ZM wynika ZIM. Założymy, że  $X \subseteq \mathbb{N}$  spełnia warunki (B) i (I) i że, nie wprost,  $X \neq \mathbb{N}$ . Wówczas  $Y = \mathbb{N} \setminus X$  jest niepusty. Ma więc element najmniejszy  $n_0$ . Wtedy  $n_0 - 1$  jest liczbą naturalną (!) należącą do  $X$ . Więc  $n_0 = (n_0 - 1) + 1 \in X$ , bo  $X$  jest induktywny. Sprzeczność.  $\diamond$

## 1.2 Działania algebraiczne

Podstawowym pojęciem w algebrze jest pojęcie działania (dwuargumentowego). **Algebra** jest działem matematyki badającym **struktury algebraiczne**, czyli zbiory z działaniami.

**Definicja 1.1** Niech  $A$  będzie dowolnym zbiorem. Funkcję  $f : A \times A \rightarrow A$ , która każdej uporządkowanej parze  $(\alpha, \beta)$  elementów zbioru  $A$  przyporządkowuje element  $f(\alpha, \beta)$  tego samego zbioru, nazywamy **działaniem dwuargumentowym** w zbiorze  $A$ . Na oznaczenie działania używamy jakiegoś specjalnego znaczka, na przykład  $+$ ,  $\cdot$ ,  $\times$ ,  $\circ$ ,  $*$  (itp.), i zamiast  $f(\alpha, \beta)$  (itp.) piszemy  $\alpha + \beta$  (itp.). Element  $\alpha * \beta \in A$  nazywamy **wynikiem** działania  $*$  na parze  $(\alpha, \beta) \in A \times A$ .

**Definicja 1.2** Działanie  $*$  :  $A \times A \longrightarrow A$  nazywamy **łącznym**, gdy

$$\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma \quad (1.3)$$

dla dowolnych  $\alpha, \beta, \gamma \in A$ . Działanie  $*$  nazywamy **przemiennym**, gdy

$$\alpha * \beta = \beta * \alpha \quad (1.4)$$

dla dowolnych  $\alpha, \beta \in A$ .

**Przykład 1.** Znamy doskonale działania **dodawania** i **mnożenia** w zbiorze  $\mathbb{Z}$  liczb całkowitych. Działania te są łączne i przemienne. Również łączne i przemienne są działania dodawania i mnożenia w zbiorze  $\mathbb{Q}$  liczb wymiernych oraz w zbiorze  $\mathbb{R}$  liczb rzeczywistych. Działania  $- : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$  i  $:: \mathbb{R}_{>0} \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$  odejmowania liczb rzeczywistych i dzielenia dodatnich liczb rzeczywistych nie są ani przemienne ani łączne. Działanie  $\triangleright : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$  dane wzorem  $a \triangleright b = 2a + b$  nie jest ani łączne ani przemienne. Na przykład  $1 \triangleright 2 = 4 \neq 5 = 2 \triangleright 1$ . Oraz  $1 \triangleright (2 \triangleright 3) = 2 + (2 \triangleright 3) = 2 + (4 + 3) = 9$ , a  $(1 \triangleright 2) \triangleright 3 = (2 + 2) \triangleright 3 = 8 + 3 = 11$ . Działanie  $\triangle : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$  dane wzorem  $x \triangle y = \frac{x+y}{2}$  jest przemienne, ale nie jest łączne. Działanie  $\max$ , które każdej parze  $(a, b) \in \mathbb{R} \times \mathbb{R}$  przyporządkowuje  $\max\{a, b\}$ , jest przemienne i łączne.  $\diamond$

**Uwaga.** Łączność działania jest w pewnym sensie bardziej podstawową jego własnością niż przemienność. Jeżeli dane działanie  $*$  jest łączne, to można jednoznacznie zdefiniować *wynik*  $\alpha * \beta * \gamma$  jako  $\alpha * (\beta * \gamma)$  lub  $(\alpha * \beta) * \gamma$ . Podobnie ma się rzecz z  $\alpha_1 * \alpha_2 * \dots * \alpha_n$ , gdzie tylko porządek  $\alpha_i$  jest istotny. W szczególności, gdy wszystkie  $\alpha_i$  są równe  $\alpha$  dostajemy  $n$ -tą *potęgę*  $\alpha^n$ . Prawdłowo należy ją określić indukcyjnie ( $\alpha^1 = \alpha$  i  $\alpha^{n+1} = \alpha^n * \alpha$ ), a zapisywać jakoś tak:  $\alpha^{*n}$ .

**Ćwiczenie 1.5** Niech  $X$  będzie dowolnym zbiorem niepustym i niech  $\mathcal{B}ij(X)$  oznacza zbiór wszystkich bijekcji zbioru  $X$  na zbiór  $X$ . W  $\mathcal{B}ij(X)$  określamy działanie **składania**: Jeżeli  $f, g \in \mathcal{B}ij(X)$ , to  $f \circ g$  jest zdefiniowane przez  $(f \circ g)(x) = f(g(x))$  dla każdego  $x \in X$ . Udowodnić, że w ten sposób zdefiniowaliśmy działanie dwuargumentowe i że jest ono łączne, ale (gdy  $|X| > 2$ ) nie jest przemienne.

**Definicja 1.3** Jeżeli w pewnym zbiorze  $B$  zadane są dwa działania  $\wedge$  i  $\vee$ , to mówimy, że działanie  $\vee$  jest **rozdzielne względem działania**  $\wedge$ , gdy

$$u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w) \quad (1.5)$$

dla dowolnych  $u, v, w \in B$ .

**Przykład 2.** Działanie mnożenia liczb jest rozdzielne względem działania dodawania liczb (to znaczy, że  $a \cdot (b + c) = a \cdot b + a \cdot c$  dla dowolnych liczb  $a, b, c$ ).

**Ćwiczenie 1.6** W zbiorze  $\mathcal{P}(X)$  wszystkich podzbiorów danego zbioru  $X$  znamy działania<sup>2</sup> **iloczynu** (oznaczanego symbolem  $\cap$ ) i **sumy** (oznaczanego symbolem  $\cup$ ). Udowodnić, że każde z nich jest rozdzielne względem drugiego.

<sup>2</sup>Używamy też nazw pełnych: **iloczyn teoriomnościowy** i **suma teoriomnościowa**. Zbiór  $A \cap B$  nazywamy również **przekrojem** zbiorów  $A$  i  $B$ . Zobacz KOM.

**Definicja 1.4** Element  $\varepsilon \in A$  nazywamy **elementem neutralnym** działania  $*$  w zbiorze  $A$ , gdy dla dowolnego  $\alpha \in A$  zachodzą równości:

$$\varepsilon * \alpha = \alpha * \varepsilon = \alpha. \quad (1.6)$$

Przykład 3. Jasne, że liczba 0 jest elementem neutralnym dodawania liczb (naturalnych, całkowitych, wymiernych, rzeczywistych), liczba 1 jest elementem neutralnym mnożenia liczb. Zbiór *pusty*  $\emptyset \in \mathcal{P}(X)$  jest elementem neutralnym sumy teoriomnogościowej, a zbiór *pełny*  $X \in \mathcal{P}(X)$  jest elementem neutralnym iloczynu teoriomnogościowego w  $\mathcal{P}(X)$ . Zwykle mnożenie w zbiorze  $2\mathbb{Z}$  liczb całkowitych parzystych nie ma elementu neutralnego! Również działanie  $\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto \min\{x, y\} \in \mathbb{R}$ , nie ma elementu neutralnego.  $\diamond$

**Ćwiczenie 1.7** Udowodnić, że działanie może mieć co najwyżej jeden element neutralny.

### 1.3 Grupa

Wprowadzimy teraz bardzo ważne pojęcie grupy.

**Definicja 1.5** Trójkę  $(\Gamma, *, \varepsilon)$ , gdzie  $\Gamma$  jest zbiorem,  $*$  jest działaniem  $\Gamma \times \Gamma \rightarrow \Gamma$  oraz  $\varepsilon \in \Gamma$ , nazywamy **grupą**, gdy spełnione są następujące aksjomaty:

- (1) działanie  $*$  jest łączne (zobacz (1.3));
- (2) element  $\varepsilon$  jest elementem neutralnym działania  $*$  (zobacz (1.6));
- (3) dla każdego  $\alpha \in \Gamma$  istnieje taki element  $\tilde{\alpha} \in \Gamma$ , że  $\alpha * \tilde{\alpha} = \tilde{\alpha} * \alpha = \varepsilon$ .

**Ćwiczenie 1.8** Jeżeli  $\alpha \in \Gamma$ , to element  $\tilde{\alpha}$ , którego istnienie zapewnia punkt (3), nazywa się **elementem odwrotnym** do  $\alpha$  lub **odwrotnością**  $\alpha$ . Udowodnić, że dany element grupy ma dokładnie jedną odwrotność. Oznaczamy ją  $\alpha^{-1}$ .

**Ćwiczenie 1.9** Udowodnić, że odwrotność odwrotności danego elementu równa jest temu elementowi:  $(\alpha^{-1})^{-1} = \alpha$ .

**Ćwiczenie 1.10** Dowieść, że jeśli  $\alpha, \beta$  są elementami grupy, to  $(\alpha * \beta)^{-1} = \beta^{-1} * \alpha^{-1}$ .

**U w a g a.** Gdy zadaniem działaniem  $*$  w grupie jest **dodawanie** zazwyczaj oznaczane symbolem  $+$ , to mówimy, że ta grupa jest grupą **typu addytywnego**. W takim przypadku element neutralny  $\varepsilon$  nazywa się **zerem** i zazwyczaj oznacza symbolem  $0$ , element odwrotny do  $\alpha$  nazywa się **elementem przeciwnym** do  $\alpha$ , i oznacza symbolem  $-\alpha$ . Wówczas równości w aksjomatach grupy z definicji D1.5 mają postać:

- (1)  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ ,
- (2)  $0 + \alpha = \alpha + 0 = \alpha$ ,
- (3)  $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$ .

**Definicja 1.6** Jeżeli w danej grupie  $(\Gamma, *, \varepsilon)$  działanie  $*$  jest działaniem przemiennym, zobacz (1.4), to grupę nazywamy **grupą przemienną (komutatywną)** lub **grupą abelową**.

**Ćwiczenie 1.11** Dowieść, że następujące pary<sup>3</sup> są grupami abelowymi:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\{+1, -1\}, \cdot)$ ,  $(\mathbb{R}_{>0}, \cdot)$ .

Przykład. Najważniejszy przykład grupy spotykamy w ćwiczeniu C1.5. Odwrotnością bijekcji  $f \in \mathcal{B}ij(X)$  jest, oczywiście, bijekcja odwrotna  $f^{-1}$ . Elementem neutralnym zaś jest **identyczność** na  $X$ , oznaczana zazwyczaj  $\text{Id}_X$ . Grupa  $(\mathcal{B}ij(X), \circ)$  nazywa się **grupą bijekcji** zbioru  $X$ . Grupa ta, zobacz C1.5, jest grupą abelową wyłącznie w przypadku, gdy  $|X| \leq 2$ . W przypadku gdy  $X = [n] := \{1, 2, \dots, n\}$ , zbiór  $\mathcal{B}ij(X)$  oznaczamy symbolem  $S_n$ , jego elementy nazywamy **permutacjami**, a samą grupę  $(S_n, \circ)$  nazywamy  $n$ -tą **grupą symetryczną**. Ponieważ element  $\sigma \in S_n$  jest funkcją określoną na zbiorze  $[n]$ , więc zadajemy go wypisując w jednej linii elementy zbioru  $[n]$  a tuż pod nimi ich obrazy:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Zbiór  $S_n$  ma  $n!$  (*en silnia*) elementów. Zobacz też KOM. ◇

**Ćwiczenie 1.12** Niech  $\sigma, \tau \in S_7$  będą zadane przez

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 1 & 2 & 4 & 5 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

Wyznaczyć następujące elementy grupy  $S_7$ :  $\sigma \circ \tau$ ,  $\tau \circ \sigma$ ,  $\sigma^4$ ,  $\tau^{-1}$ ,  $\sigma^{-3} := (\sigma^{-1})^3$ .

**Ćwiczenie 1.13** Niech  $\alpha$  będzie elementem grupy  $(\Gamma, *)$ . Niech funkcja  $f_\alpha : \Gamma \rightarrow \Gamma$  będzie zadana przez  $f_\alpha(\xi) = \alpha * \xi$ . Dowieść, że  $f_\alpha$  jest bijekcją zbioru  $\Gamma$ . Dowieść też, że

$$f_\alpha \circ f_\beta = f_{\alpha * \beta}, \quad \text{oraz} \quad (f_\alpha)^{-1} = f_{\alpha^{-1}}$$

dla dowolnych  $\alpha, \beta \in \Gamma$ .

## 1.4 Pierścień przemienny. Ciało

Pierścienie, jakie występują w dużych ilościach w elementarnej teorii liczb, należą do klasy pierścieni przemiennych z jedyneką.

**Definicja 1.7** Układ  $(\mathcal{R}, +, \cdot, 0, 1)$ , gdzie  $\mathcal{R}$  jest zbiorem,  $+$  i  $\cdot$  są działaniami w zbiorze  $\mathcal{R}$ , zwanymi **dodawaniem** i **mnożeniem**, a  $0 \in \mathcal{R}$  (**zero**) i  $1 \in \mathcal{R}$  (**jedynka**) są dwoma wyróżnionymi elementami, nazywamy **pierścieniem przemiennym z jedyneką**, gdy spełnione są następujące aksjomaty:

- (1)  $(\mathcal{R}, +, 0)$  jest grupą abelową;
- (2) mnożenie  $\cdot$  jest rozdzielne względem dodawania  $+$ ;
- (3) mnożenie  $\cdot$  jest łączne i przemienne;
- (4) jedynka 1 jest elementem neutralnym mnożenia.

<sup>3</sup>Gdy, wskazując grupę, podajemy tylko *parę*  $(\Gamma, *)$ , należy samodzielnie ustalić element neutralny, zobacz C1.7. Czasem, gdy z kontekstu jest jasne, jakie działanie mamy na myśli, wskazujemy tylko zbiór  $\Gamma$ .

Przykład 1. Znane nam przykłady pierścieni (przemiennej z jedyką):

- pierścień liczb całkowitych  $(\mathbb{Z}, +, \cdot, 0, 1)$ ,
- pierścień liczb wymiernych  $(\mathbb{Q}, +, \cdot, 0, 1)$ ,
- pierścień liczb rzeczywistych  $(\mathbb{R}, +, \cdot, 0, 1)$ .

◇

**ZADANIE 1.6** Udowodnić, że w każdym pierścieniu zachodzą równości

$$(1) \quad \alpha \cdot 0 = 0, \quad (2) \quad (-\alpha) \cdot (-\beta) = \alpha \cdot \beta.$$

ROZWIĄZANIE. (1) Mamy

$$\alpha \cdot 0 + \alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0.$$

Pierwsza z tych równości wynika z rozdzielności mnożenia względem dodawania, druga z faktu, że 0 jest elementem neutralnym dodawania. Dodajmy teraz  $-(\alpha \cdot 0)$  do lewej strony tej równości:

$$-(\alpha \cdot 0) + [\alpha \cdot 0 + \alpha \cdot 0] = [-(\alpha \cdot 0) + \alpha \cdot 0] + \alpha \cdot 0 = 0 + \alpha \cdot 0 = \alpha \cdot 0.$$

Dodając ten sam element  $-(\alpha \cdot 0)$  do prawej strony dostajemy 0. W ten sposób równość (1) jest udowodniona. Dla sprawdzenia równości (2), zauważmy, że:

$$(-\alpha) \cdot \beta + \alpha \cdot \beta = (-\alpha + \alpha) \cdot \beta = 0 \cdot \beta = \beta \cdot 0 = 0.$$

Widzimy stąd, że  $(-\alpha) \cdot \beta$  jest elementem przeciwnym do  $\alpha \cdot \beta$ . Zatem

$$(-\alpha) \cdot (-\beta) = -(\alpha \cdot (-\beta)) = -((-\beta) \cdot \alpha) = -(-(\beta \cdot \alpha)) = \beta \cdot \alpha = \alpha \cdot \beta.$$

Takiego typu proste manipulacje z aksjomatami pierścienia w dalszym ciągu będziemy pozostawiali Czytelnikowi. ◇

**U w a g a.** Gdy  $\alpha$  jest elementem pierścienia  $\mathcal{R}$  i  $n$  jest liczbą całkowitą, to definiujemy  $n\alpha \in \mathcal{R}$  następująco:  $0\alpha = 0$ ,  $1\alpha = \alpha$ ,  $(n+1)\alpha = n\alpha + \alpha$  dla  $n \in \mathbb{N}$ , oraz  $n\alpha = -(-n)\alpha$ , gdy  $n < 0$ .

**Ćwiczenie 1.14** Niech  $\alpha, \beta$  będą dowolnymi elementami pierścienia. Udowodnić szczegółowo (przez indukcję), że dla  $m, n \in \mathbb{Z}$  prawdziwe są równości: **(1)**  $n(m\alpha) = (nm)\alpha$ , **(2)**  $(n+m)\alpha = n\alpha + m\alpha$ , **(3)**  $n(\alpha + \beta) = n\alpha + n\beta$ , **(4)**  $(n\alpha) \cdot \beta = \alpha \cdot n\beta = n(\alpha \cdot \beta)$ .

**Ćwiczenie 1.15** Niech  $\alpha$  będzie elementem pierścienia. Zdefiniować przez indukcję  $n$ -tą potęgę,  $\alpha^n$  dla wykładnika naturalnego  $n$ . Następnie udowodnić przez indukcję, że  $(\alpha^m)^n = \alpha^{mn}$  dla dowolnych  $m, n \in \mathbb{N}$ .

**Ćwiczenie 1.16** Udowodnić przez indukcję, że dla dowolnych elementów  $\alpha, \beta$  pierścienia przemiennej i dowolnej liczby  $n \in \mathbb{N}$  zachodzą równości (piszemy  $\varphi\psi$  zamiast  $\varphi \cdot \psi$ ):

$$(\alpha + \beta)^n = \alpha^n + \binom{n}{1} \alpha^{n-1} \beta + \dots + \binom{n}{n-1} \alpha \beta^{n-1} + \beta^n; \quad (1.7)$$

$$\alpha^n - \beta^n = (\alpha - \beta)(\alpha^{n-1} + \alpha^{n-2} \beta + \dots + \alpha \beta^{n-2} + \beta^{n-1}). \quad (1.8)$$



**Definicja 1.8** Element  $\eta \in \mathcal{R}$  danego pierścienia  $(\mathcal{R}, +, \cdot, 0, 1)$  nazywamy **jednością** lub **elementem odwracalnym**, gdy istnieje taki element  $\xi \in \mathcal{R}$ , że  $\eta \cdot \xi = 1$ . W takiej sytuacji element  $\xi$  nazywamy **odwrotnością**  $\eta$  i oznaczamy  $\xi = \eta^{-1}$ . Zbiór wszystkich jedności  $\mathcal{R}$  oznaczamy symbolem  $\mathcal{R}^*$ .

**Ćwiczenie 1.17** Udowodnić, że jeżeli  $\mathcal{R}$  jest pierścieniem przemiennym z jedyneką, to trójka  $(\mathcal{R}^*, \cdot, 1)$  jest grupą abelową.

**Ćwiczenie 1.18** Grupa  $\mathcal{R}^* = (\mathcal{R}^*, \cdot, 1)$  nazywa się **grupą jedności pierścienia  $\mathcal{R}$** . Wyznaczyć grupy jedności pierścieni  $\mathbb{Z}$ ,  $\mathbb{Q}$  i  $\mathbb{R}$ .

**Definicja 1.9** Element  $\alpha$  pierścienia  $\mathcal{R}$  nazywamy **dzielnikiem zera**, gdy  $\alpha \neq 0$  i w  $\mathcal{R}$  istnieje taki element  $\beta \neq 0$ , że  $\alpha \cdot \beta = 0$ . Pierścień nie zawierający żadnych dzielników zera nazywa się **dziedziną całkowitości**. W dziedzinach całkowitości (zwanymi też **pierścieniami bez dzielników zera**) zachodzi więc prawo:  $\alpha\beta = 0 \Rightarrow \alpha = 0 \text{ lub } \beta = 0$ .

Poznamy teraz definicję ciała:

**Definicja 1.10** Pierścień przemienny z jedyneką nazywa się **ciałem**, gdy każdy jego różny od zera element jest odwracalny. Jeżeli  $\alpha$  jest niezerowym elementem ciała, to jego odwrotność oznaczamy  $\alpha^{-1}$  lub  $\frac{1}{\alpha}$ . Konsekwentnie piszemy również  $\frac{\alpha}{\beta}$  zamiast  $\alpha\beta^{-1}$ .

Przykład. Z ćwiczenia C1.18 widzimy, że pierścienie  $\mathbb{Q}$  i  $\mathbb{R}$  są ciałami.  $\diamond$

**Ćwiczenie 1.19** Udowodnić, że ciało jest dziedziną całkowitości.

**Ćwiczenie 1.20** Udowodnić, że skończona dziedzina całkowitości jest ciałem.

## 1.5 Liczby zespolone

Matematyka w żaden sposób nie potrafi się obejść bez liczb zespolonych. Również matematyka olimpijska wyraźnie kuleje bez tych liczb. Należy więc przyswoić sobie podstawową wiedzę ich dotyczącą. Im wcześniej tym lepiej.

Liczby rzeczywiste utożsamiamy z punktami prostej – **osi liczbowej**. Podobnie, liczby zespolone utożsamimy z punktami płaszczyzny.

**Definicja 1.11** Napis postaci  $a + bi$ , gdzie  $a, b \in \mathbb{R}$  nazywamy **liczbą zespoloną**. Zbiór liczb zespolonych oznaczamy symbolem  $\mathbb{C}$ . W zbiorze tym wykonujemy działania  **dodawania** i **mnożenia** następująco:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \quad (1.9)$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \quad (1.10)$$

Dodawanie i mnożenie liczb zespolonych jest łatwe: mówi o tym reguła:

**rób to co w szkole pamiętając, że  $i^2 = -1$ .**

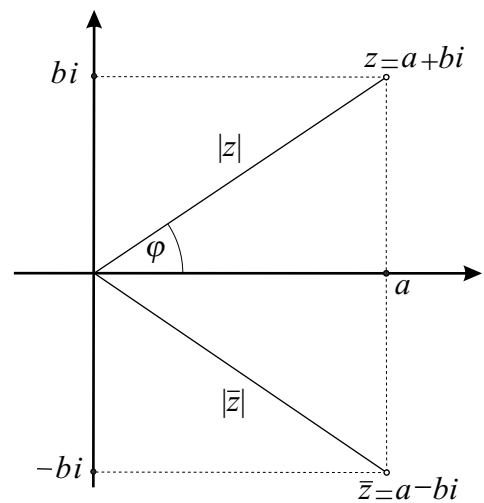
Wygodnym jest utożsamiać liczbę zespoloną  $z = a + bi$  z punktem płaszczyzny o współrzędnych kartezjańskich  $(a, b)$ . W takiej sytuacji odciętą  $a$  nazywamy **częścią rzeczywistą** liczby  $z$  i oznaczamy  $a = \operatorname{Re} z$ , a rzędną  $b$  nazywamy **częścią urojoną** liczby  $z$  i oznaczamy  $b = \operatorname{Im} z$ . Utożsamiamy też liczbę rzeczywistą  $a$  z liczbą zespoloną  $a + 0i$ . W ten sposób traktujemy zbiór  $\mathbb{R}$  liczb rzeczywistych jako podzbiór zbioru liczb zespolonych  $\mathbb{C}$ .

Geometrycznie,  $\mathbb{R}$  pokrywa się z osią odciętych, zwaną w tym kontekście **osią rzeczywistą**. Oś rzędnych nazywamy wtedy **osią urojoną**. Liczby zespolone leżące na osi urojonej nazywa się **liczbami czysto urojonymi**.

Niech  $z = a + bi$  będzie liczbą zespoloną. Kładziemy (zobacz rysunek obok):

$$|z| = \sqrt{a^2 + b^2}, \quad \bar{z} = a - bi.$$

Liczba rzeczywista(!)  $|z|$  nazywa się **modułem** liczby zespolonej  $z$ . Jest ona odległością punktu  $(a, b)$  od początku układu współrzędnych. Liczbę  $\bar{z}$  nazywamy liczbą **sprzężoną** (do) liczby  $z$ . Geometrycznie:  $\bar{z}$  jest odbiciem punktu  $z$  w osi rzeczywistej.



Rys. 1.2

**Ćwiczenie 1.21** Sprawdzić, że dla dowolnej liczby zespolonej  $z$  zachodzą następujące równości:  $z + \bar{z} = 2 \operatorname{Re} z$  oraz  $z - \bar{z} = 2i \operatorname{Im} z$ .

**Ćwiczenie 1.22** Udowodnić równości:

$$(1) \quad \overline{z + w} = \bar{z} + \bar{w}, \quad (2) \quad \overline{z \cdot w} = \bar{z} \cdot \bar{w}, \quad (1.11)$$

$$(3) \quad z \cdot \bar{z} = |z|^2, \quad (4) \quad |z \cdot w| = |z| \cdot |w|. \quad (1.12)$$

**Ćwiczenie 1.23** Udowodnić i podać interpretację geometryczną następującej, tak zwanej **nierówności trójkąta**:  $|z + w| \leq |z| + |w|$  dla dowolnych  $z, w \in \mathbb{C}$ . *Wskazówka.* Zobacz rysunek 1.3a.

**Ćwiczenie 1.24** Sprawdzić, że jeżeli  $z = a + bi \neq 0$ , to liczba

$$z^{-1} := \frac{a}{|z|^2} + \frac{-b}{|z|^2}i = \frac{\bar{z}}{|z|^2}$$

jest **odwrotnością** liczby  $z$  w tym sensie, że  $z \cdot z^{-1} = z^{-1} \cdot z = 1$ .

Fakt, że każda liczba zespolona  $z \neq 0$  ma odwrotność  $z^{-1}$  (oznaczaną też oczywiście  $\frac{1}{z}$ ) pokazuje, że w zbiorze  $\mathbb{C}$  wykonalne jest **dzielenie** liczb (nie przez zero!). W praktyce dzielenie polega na mnożeniu licznika i mianownika przez liczbę sprzężoną do mianownika:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i.$$

**Ćwiczenie 1.25** Uzasadnić, że  $|z/w| = |z|/|w|$ . Oraz, że niezerowa liczba  $z \in \mathbb{C}$  ma moduł równy 1 wtedy i tylko wtedy, gdy  $z^{-1} = \bar{z}$ .

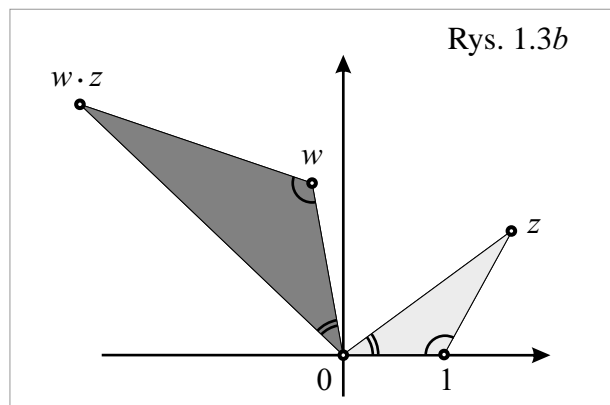
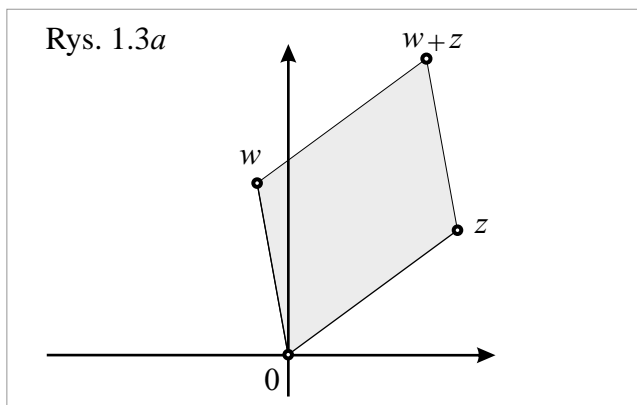
**Ćwiczenie 1.26** Niech  $z = 2+3i$ ,  $w = 4-i$ . Narysować liczby  $z$ ,  $\bar{z}$ ,  $z+w$ ,  $z^2$ ,  $zw$ ,  $\bar{z}^3w^{-2}$ , a także zbiór  $\{kz+lw : k, l \in \mathbb{Z}\}$ .

**Ćwiczenie 1.27** Udowodnić, że zbiór  $\mathbb{C}$  wraz z wprowadzonymi działaniami dodawania i mnożenia jest ciałem. W szczególności w  $\mathbb{C}$  nie ma dzielników zera, zobacz C1.19. To znaczy, że jeżeli  $zw = 0$ , to  $z = 0$  lub  $w = 0$ , porównaj D1.9.

### Interpretacja geometryczna dodawania i mnożenia

Bardzo ważnym jest zrozumienie geometrii liczb zespolonych. Sama algebra nie wystarczy!

Z formuły (1.9) łatwo wywnioskować, że punkt płaszczyzny odpowiadający sumie  $w+z$  jest jednoznacznie wyznaczony przez warunek: punkty odpowiadające liczbom  $0$ ,  $w$ ,  $w+z$ ,  $z$  są wierzchołkami równoległoboku, zobacz rysunek 1.3a. Widzimy stąd i z **zasady równoległoboku** dodawania wektorów, że przekształcenie  $A_w : z \mapsto w+z$  polegające na dodawaniu ustalonej liczby zespolonej  $w$  do zmiennej liczby  $z$  jest, z geometrycznego punktu widzenia, **translacją**, która przesuwa punkt  $0$  w punkt  $w$ .



Aby zobaczyć interpretację geometryczną mnożenia liczb zespolonych użyjemy **współrzędnych biegunowych** ( $r, \varphi$ ) niezerowego (tzn. różnego od początku układu) punktu  $(a, b)$ , który utożsamiamy z liczbą zespoloną  $z = a+bi$ . Tutaj  $r = |z|$  jest modułem liczby  $z$ , zaś  $\varphi$  jest miarą kąta między dodatnią częścią osi rzeczywistej i półprostą  $h_{0z}$ . Kąt ten nazywamy **argumentem** liczby  $z$  i oznaczamy  $\text{Arg } z$ . Liczbę  $\varphi$  definiujemy z dokładnością do  $2\pi$ . Jeżeli  $\text{Arg } z = \varphi$ , to, z elementarnej trygonometrii, mamy (porównaj rysunek 1.2):

$$z = |z| \cos \varphi + i|z| \sin \varphi = |z|(\cos \varphi + i \sin \varphi). \quad (1.13)$$

Taki zapis nazywamy **postacią trygonometryczną** liczby zespolonej  $z$ .

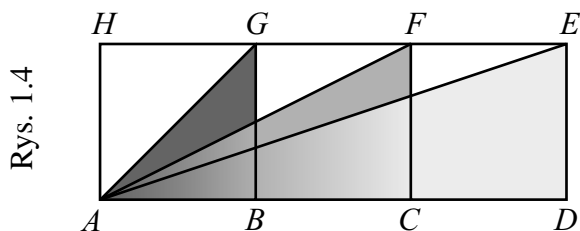
Pomnożmy dwie liczby zespolone zadane w postaci trygonometrycznej:

$$\begin{aligned} & |z|(\cos \varphi + i \sin \varphi) \cdot |w|(\cos \psi + i \sin \psi) \\ &= |z| \cdot |w| [(\cos \varphi \cos \psi - \sin \varphi \sin \psi) + i(\cos \varphi \sin \psi + \sin \varphi \cos \psi)] \\ &= |zw| [\cos(\varphi + \psi) + i \sin(\varphi + \psi)]. \end{aligned}$$

Ostatnia równość wynika z drugiej tożsamości (1.12) i z elementarnej trygonometrii, zobacz PLA T2.29. Wnioskujemy stąd, że zachodzi następująca *reguła mnożenia*:

**mnożąc liczby zespolone mnożymy ich moduły i dodajemy ich argumenty.**

Używając tej reguły z łatwością rozwiążemy ćwiczenie:



**Ćwiczenie 1.28** Niech  $ABGH$ ,  $BCFG$  i  $CDEF$  będą kwadratami, zobacz rysunek 1.4. Wykazać, że suma miar kątów:  $\sphericalangle DAE$ ,  $\sphericalangle CAF$ ,  $\sphericalangle BAG$  jest równa  $90^\circ$ .  
Wskazówka. Pomnożyć:  $(3 + i)(2 + i)(1 + i)$ .

## Potęgowanie i pierwiastkowanie

Bardzo ważnym wnioskiem z reguły mnożenia jest **wzór de Moivre'a**:

$$(\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi. \quad (1.14)$$

Wnioskiem ze wzoru de Moivre'a jest fakt, że dla liczby zespolonej  $w = |w|(\cos \varphi + i \sin \varphi)$ ,  $w \neq 0$ , istnieje dokładnie  $n$  **pierwiastków  $n$ -tego stopnia** z liczby  $w$ :

$$z_k = \sqrt[n]{|w|} \left( \cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right). \quad (1.15)$$

Należy tak długo przyglądać się liczbom  $z_k$ , aż stanie się jasne, że tworzą wierzchołki pewnego  $n$ -kąta foremnego i każda z nich spełnia warunek  $z_k^n = w$ . Patrz rysunek 1.5a.

**Ćwiczenie 1.29** Przedstawić w postaci  $a + bi$  liczby:  $(1 + i)^{2011}$ ,  $(1 + \sqrt{3}i)^{2010}$ .

**Ćwiczenie 1.30** Zapisać w postaci  $a + bi$ :  $(1 + i \operatorname{tg} \varphi)^n$ ,  $(1 + \cos \varphi + i \sin \varphi)^n$ .

**Ćwiczenie 1.31** Używając wzoru dwumiennego (zobacz (1.7)) i wzoru de Moivre'a udowodnić, że dla dowolnego  $x \in \mathbb{R}$  zachodzą równości

$$\sin 3x = -4 \sin^3 x + 3 \sin x, \quad \cos 5x = 16 \cos^5 x - 20 \cos^3 x + 5 \cos x.$$

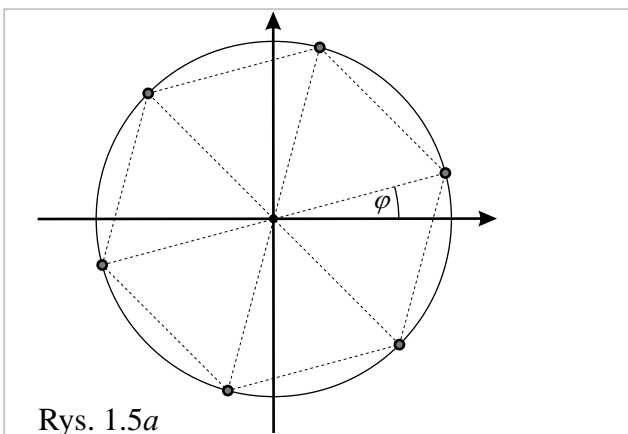
**Ćwiczenie 1.32** Udowodnić, że jeżeli  $az^2 + bz + c = 0$  dla pewnych liczb zespolonych  $a \neq 0, b, c$  i  $z$ , to zachodzi równość  $z = \frac{-b + \sqrt{\Delta}}{2a}$ , gdzie  $\sqrt{\Delta}$  oznacza jeden z pierwiastków stopnia drugiego z liczby  $\Delta := b^2 - 4ac$ .

**Ćwiczenie 1.33** Każdy pierwiastek równania kwadratowego  $z^2 - 2(\cos \varphi)z + 1 = 0$ , przy dowolnym parametrze  $\varphi \in \mathbb{R}$ , jest liczbą zespoloną o module 1.

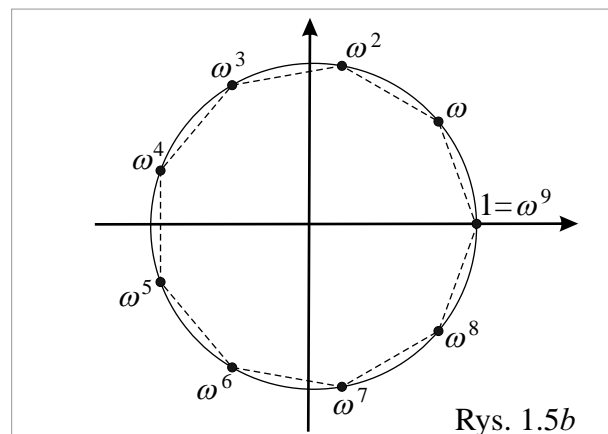
**Ćwiczenie 1.34** Narysować 6-elementowy zbiór pierwiastków stopnia 6 z liczby  $i$ . Wskazówka. Zaznaczony na rysunku 1.5a kąt  $\varphi$  ma miarę  $\pi/12$ .

Szczególnie sympatycznym jest zbiór wszystkich pierwiastków  $n$ -tego stopnia z liczby 1.

**Ćwiczenie 1.35** Udowodnić, że zbiór  $\mu_n(\mathbb{C})$  wszystkich pierwiastków stopnia  $n$  z 1 jest grupą względem mnożenia.



Rys. 1.5a



Rys. 1.5b

**Ćwiczenie 1.36** Udowodnić, że grupa  $(\mu_n(\mathbb{C}), \cdot)$  jest grupą cykliczną<sup>4</sup>.

### Tożsamości trygonometryczne

Liczby zespolone, dzięki swojej budowie pozwalają zgrabnie uzasadniać tożsamości trygonometryczne, zobacz na przykład C1.31. Inny przykład widzimy w rozwiązaniu kolejnego zadania:

**ZADANIE 1.7** Udowodnić, że dla dowolnego  $x \neq 2l\pi$  zachodzi równość

$$\frac{1}{2} + \sum_{k=1}^N \cos kx = \frac{\sin(N + \frac{1}{2})x}{2 \sin \frac{x}{2}}.$$

<sup>4</sup>Grupę  $\Gamma$  nazywamy **grupą cykliczną**, gdy istnieje taki element  $\omega \in \Gamma$ , że zachodzi równość zbiorów  $\Gamma = \{\omega^n : n \in \mathbb{Z}\}$ . Patrz rysunek 1.5b, gdzie pokazano przypadek  $n = 9$ .

ROZWIĄZANIE. Weźmy liczbę zespoloną  $z = \cos x + i \sin x$  i niech  $w = \cos \frac{x}{2} + i \sin \frac{x}{2}$  będzie (jednym z dwóch) pierwiastkiem kwadratowym z liczby  $z$ . Dzięki wzorowi de Moivre'a wiemy, że rozważana suma jest częścią rzeczywistą liczby

$$\frac{1}{2} \sum_{k=-N}^N z^k = \frac{1}{2} z^{-N} \sum_{k=0}^{2N} z^k = \frac{1}{2} z^{-N} \frac{z^{2N+1} - 1}{z - 1} = \frac{w(z^{N+1}w^{-1} - z^{-N}w^{-1})}{2w(zw^{-1} - w^{-1})},$$

czyli liczby

$$\frac{w^{2N+1} - \overline{w^{2N+1}}}{2(w - \bar{w})} = \frac{2i \sin(2N+1)\frac{x}{2}}{2 \cdot 2i \sin \frac{x}{2}}.$$

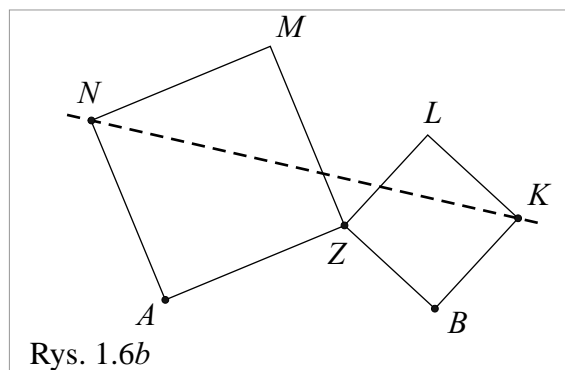
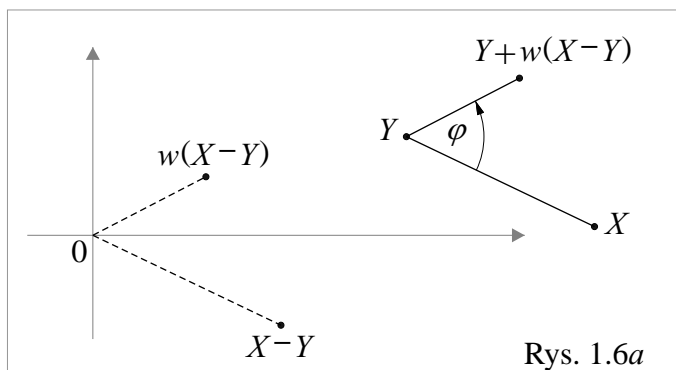
Należy tak długo sprawdzać napisane równości, aż wszystko będzie jasne.  $\diamond$

**Ćwiczenie 1.37** Udowodnić, że  $\sum_{k=0}^N \sin kx = \frac{\sin \frac{Nx}{2} \sin \frac{(N+1)x}{2}}{\sin \frac{x}{2}}$  dla  $x \neq 2l\pi$ .

### Obroty i podobieństwa spiralne

Z reguły mnożenia widzimy, że przekształcenie  $M_w : z \mapsto wz$ , tzn. mnożenie przez ustaloną niezerową liczbę zespoloną  $w$  jest, z geometrycznego punktu widzenia, złożeniem  $J_0^\lambda \circ R_0^\varphi$  dwóch przekształceń płaszczyzny: **obrotu**  $R_0^\varphi$  wokół punktu  $0 = (0, 0)$  o kąt  $\varphi = \text{Arg } w$ , i **jednokładności**  $J_0^\lambda$  o środku  $0$  i skali  $\lambda = |w|$ . Zobacz rysunek 1.3b, gdzie widać dwa podobne trójkąty  $\Delta(0)(1)(z)$  i  $\Delta(0)(w)(zw) = M_w(\Delta(0)(1)(z))$ . W szczególności, mnożenie przez  $i$  jest obrotem wokół  $0$  o kąt prosty (przeciwnie do ruchu wskazówek zegara). Podobnie, mnożenie przez  $-i$  jest obrotem o kąt prosty, tym razem zgodnie z ruchem wskazówek zegara. Złożenia obrotów i jednokładności o wspólnym środku nazywamy w geometrii **podobieństwami spiralnymi**, zobacz PLA.

Liczby zespolone są wobec tego mocnym narzędziem rachunkowym w planimetrii, gdzie utożsamiamy punkty płaszczyzny z liczbami zespolonymi. Na rysunku 1.6a pokazujemy wynik podobieństwa spiralnego  $J_Y^{|w|} \circ R_Y^{\text{Arg } w}(X)$ .



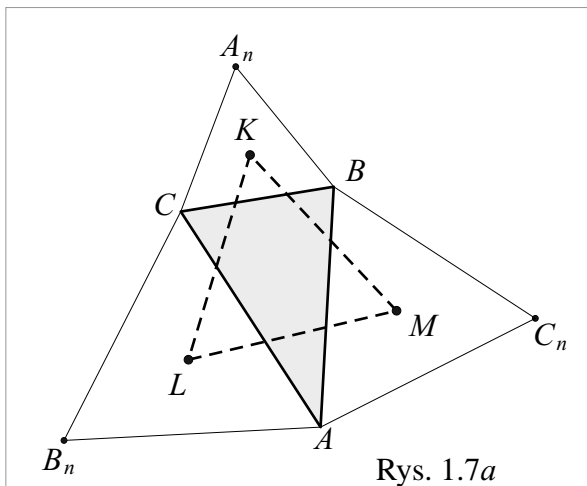
Pokażemy trzy klasyczne przykłady zastosowania tej idei w planimetrii.

**ZADANIE 1.8 (Zadanie o zakopanym skarbie.)** Na płaszczyźnie dane są ustalone dwa punkty  $A, B$  i zmienny punkt  $Z$ . Niech  $ZBKL$  i  $AZMN$  będą dwoma kwadratami zorientowanymi przeciwnie do ruchu wskazówek zegara. Udowodnić, że wszystkie proste  $l_{NK}$  przechodzą przez ten sam punkt (są współpękowe).

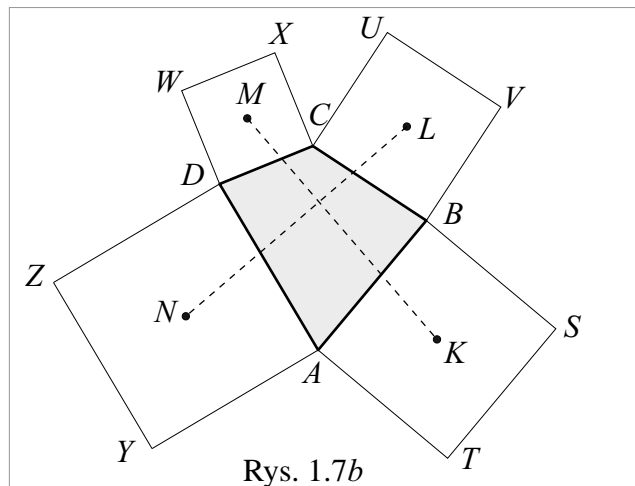
ROZWIĄZANIE. Mamy, wobec powyższego,  $N = A + i(Z - A)$ ,  $K = B + (-i)(Z - B)$ . Zatem środek odcinka  $\overline{NK}$  jest liczbą  $\frac{N+K}{2} = \frac{A+B+i(B-A)}{2}$ . Widzimy stąd, że środek odcinka  $\overline{NK}$  nie zależy od wyboru punktu  $Z$ . Przez ten środek przechodzą (oczywiście) wszystkie proste  $l_{NK}$ .  $\diamond$

**ZADANIE 1.9 (Zadanie o trójkątach Napoleona)** Na zewnątrz danego trójkąta  $\triangle ABC$ , na jego bokach, zbudowano trójkąty równoboczne  $\triangle BCA_n$ ,  $\triangle CAB_n$  i  $\triangle ABC_n$ . Udowodnić, że środki ciężkości tych trójkątów są wierzchołkami trójkąta równobocznego.

ROZWIĄZANIE. Oznaczmy  $\omega = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3}$ . Mnożenie przez liczbę  $\omega$  jest więc obrotem o kąt  $\frac{\pi}{3} = \text{Arg} \omega$ . Wobec tego,  $A_n = C + \omega(B - C)$ ,  $B_n = A + \omega(C - A)$  oraz  $C_n = B + \omega(A - B)$ , zob. rys. 1.7a. Chcemy uzasadnić, że zachodzi równość  $\omega(L - K) = M - K$ . Ponieważ środek ciężkości  $K$  jest średnią arytmetyczną odpowiednich wierzchołków, więc,  $3K = A_n + B + C = (1 + \omega)B + (2 - \omega)C$ . Podobnie,  $3L = (1 + \omega)C + (2 - \omega)A$  i  $3M = (1 + \omega)A + (2 - \omega)B$ . Korzystając z tych równości i (łatwej do zobaczenia, sprawdzić!) równości  $\omega^2 + 1 = \omega$ , po prostych rachunkach, dostaniemy równość  $\omega(3L - 3K) = 3M - 3K$ , czyli tezę.  $\diamond$



Rys. 1.7a



Rys. 1.7b

**ZADANIE 1.10 (Zadanie van Aubela)** Dany jest czworokąt wypukły  $ABCD$  i kwadraty zewnętrzne  $ABST$ ,  $BCUV$ ,  $CDWX$ ,  $DAYZ$ , zobacz rysunek 1.7b. Udowodnić, że jeżeli  $K, L, M, N$  są środkami tych kwadratów, to  $\overline{KM} \perp \overline{LN}$  oraz  $|KM| = |LN|$ .

ROZWIĄZANIE. Niech  $w = \frac{1}{\sqrt{2}}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$ . Jasne, że jeżeli  $EFGH$  jest kwadratem (zorientowanym dodatnio, tzn. tak jak kwadrat o wierzchołkach  $0, 1, 1 + i, i$ ), to jego środek jest obrazem  $J_E^{|w|}(\mathbb{R}_E^{\pi/4}(F))$ . Zatem, zgodnie z powiedzianym,

$$K = B + w(A - B), \quad L = C + w(B - C), \quad M = D + w(C - D), \quad N = A + w(D - A).$$

Korzystając z tych równości wyznaczamy

$$M - K = D - B + w(-A + B + C - D), \quad N - L = A - C + w(-A - B + C + D).$$

Sprawdzenie równości  $M_K = i(N - L)$ , z której wynika(!) teza, jest teraz oczywistym rachunkiem. Pozostawiamy go Czytelnikowi. Zauważmy jeszcze, że założenie o wypukłości czworokąta  $ABCD$  jest zdecydowanie nadmiarowe.  $\diamond$