Wprowadzenie do teorii grup

Jakub Kądziołka

25 lutego 2021

Na grupy możemy patrzeć z dwóch perspektyw. Czysto algebraicznie, grupa to zbiór, oraz działanie na nim określone, która spełnia pewne prawa. Bardziej zmotywowane jest jednak podejście geometryczne.

1 Izometrie płaszczyzny

Definicja 1.1. Izometrią nazywamy funkcję $f\colon \mathbb{R}^2 \to \mathbb{R}^2$, która zachowuje odległość:

$$|PQ| = |f(P)f(Q)|.$$

Ćwiczenie 1.1. Ile różnych wartości izometrii f musimy znać, aby jednoznacznie określić jej wartość dla każdego innego punktu?

Wniosek. Każda izometria jest połączeniem translacji, obrotu i potencjalnej symetrii osiowej.

Będziemy rozważać izometrie, które nie zmieniają pewnej konkretnej figury. Na przykład, narysujmy trójkąt równoboczny $\triangle ABC$. Obracając go wokół środka o 60°, otrzymujemy dokładnie ten sam trójkąt. Jedynie wierzchołki zamienią się miejscami, lecz figurę rozważamy jako zbiór punktów, więc nie ma to znaczenia.

Pytanie. Jakie możemy określić izometrie, dla których $f(\triangle ABC) = \triangle ABC$?

Ćwiczenie 1.2. Udowodnij, że znalazłeś wszystkie takie izometrie (powinno być ich 6).

Zauważmy, że gdy złożymy dwie z izometrii które znaleźliśmy, $f_1 \circ f_2$, to również otrzymamy izometrię, która już jest w naszym zbiorze.

Pytanie. Spróbujmy więc określić minimalny zestaw izometrii, z których możemy wytworzyć wszystkie inne.

Oznaczmy pewien obrót jako r, pewną symetrię według osi jako s. Nasz zbiór izometrii możemy wtedy określić jako

$$\{\text{id},\ r,\ r \circ r,\ s,\ s \circ r,\ s \circ r \circ r\}$$

lub, krócej

$$\left\{1,\ r,\ r^2,\ s,\ sr,\ sr^2\right\}$$

Gdy na te symetrie patrzymy jako obiekty same w sobie, to otrzymujemy *grupę izometrii płaszczyznowych trójkąta równobocznego*.

2 Grupa jako zbiór i działanie

Definicja 2.1. *Grupą* $(G, \star)$ nazywamy zbiór G (*nośnik grupy*) wraz z dwu-argumentowym działaniem $\star\colon G \times G \to G$, które spełnia następujące warunki:

1. Działanie jest *łączne* — dla każdego $a, b, c \in G$ mamy $(a \star b) \star c = a \star (b \star c)$.
2. Istnieje *element neutralny* 1_G, który spełnia $a \star 1_G = 1_G \star a = a$.
3. Dla każdego $g \in G$ mamy *element odwrotny* $h \in G$, taki że $g \star h = h \star g = 1_G$.
4. Dla każdych $g, h \in G$ mamy $g \star h \in G$.

W naszej grupie trójkąta równobocznego, zbiorem jest

$$D_6 = \{1,\ r,\ r^2,\ s,\ sr,\ sr^2\},$$

a działaniem jest złożenie funkcji $\circ$.

Uwaga. Gdy działanie grupy wynika z kontekstu, do grupy $(G, \star)$ możemy się odnosić mówiąc o zbiorze G.

Na przykład na grupę izometrii trójkąta możemy mówić D_6. Ogólniej, grupę izometrii płaszczyznowych n-kąta foremnego nazywamy *grupą diedralną* (z ang. *dihedral*) i oznaczamy... istnieje kilka notacji, takich jak Dih_n lub D_n. My pozostańmy przy D_{2n}, gdzie w indeksie zapisujemy liczbę elementów.

Uwaga. Zbiór, na którym utworzona jest grupa nazywamy *nośnikiem*.

Uwaga. Gdy grupa, w której operujemy jest oczywista, będziemy zapisywać element neutralny 1_G jako 1, nie powtarzając nazwy grupy.

Uwaga. Często działanie grupy traktujemy notacyjnie jak mnożenie, oznaczając $a \star b$ jako ab, a element odwrotny do a jako a^{-1}. Należy jednak pamiętać, że działanie zwykle nie jest przemienne.

Pytanie. Zaproponuj inną grupę niż symetrie wielokąta foremnego.

Pytanie. Czy grupa musi mieć skończoną liczbę elementów?

3 Grupa liczb całkowitych

Pytanie. Czy $(\mathbb{Z}, +)$ tworzy grupę?

Widzimy, że tak. Przytoczona wcześniej notacja może być tutaj myląca, bo przecież $1 + x = x$ wcale nie zachodzi. Dlatego też często możemy spotkać alternatywną notację *addytywną*, gdzie działanie oznaczmy $a + b$, element neutralny 0, a element odwrotny $-a$.

Uwaga. Zwyczajowo, notację addytywną stosujemy tylko dla grup, których działanie jest przemienne. Grupy z działaniem przemiennym nazywamy *przemiennymi* lub *abelowymi*.

4 Przykłady grup i nie-grup

Przykład 4.1. Czy $\{0, 1, \dots, 5\}$ wraz z dodawaniem tworzy grupę?

Nie, chociażby dlatego, że 1 nie ma elementu odwrotnego.

Przykład 4.2. Czy $\{-5, -4, \dots, 5\}$ wraz z dodawaniem tworzy grupę?

Nie, bo zbiór wartości działania nie zawiera się w nośniku grupy. Jest to ważna rzecz, gdy sprawdzamy, czy mamy do czynienia z grupą — do tego stopnia, że niektóre podręczniki dodają czwarty warunek:

4. Dla każdych $g, h \in G$ zachodzi $g \star h \in G$ (domknięcie).

Przykład 4.3. Ustalmy pewne n i określmy

$$a +_n b = a + b \bmod n.$$

Czy $+_n$ tworzy grupę nad $\{0, 1, \dots, n-1\}$?

Grupę tę będziemy nazywać $\mathbb{Z}/n\mathbb{Z}$ — później zobaczymy dlaczego.

Przykład 4.4. Czy $(\mathbb{Q}, \times)$ tworzy grupę?

Przykład 4.5. Czy $(\mathbb{Q} \setminus \{0\}, \times)$ tworzy grupę?

Grupę tę będziemy oznaczać $\mathbb{Q}^\times$. Ogólniej, dla zbioru A, $A^\times \subseteq A$ będzie podzbiorem elementów odwracalnych.[1]

Przykład 4.6. Niech p będzie liczbą pierwszą i

$$a \cdot_p b = a \cdot b \bmod p$$

Czy $\cdot_p$ tworzy grupę nad

$$\{1, 2, \dots, p-1\}?$$

Połączenie powyższych notacji sugeruje nazwę $(\mathbb{Z}/p\mathbb{Z})^\times$.

Pytanie. Co jeżeli p nie będzie pierwsze?

Przykład 4.7. Niech $n \in \mathbb{Z}_+$. Określmy G jako zbiór liczb $1 \leq k < n$ względnie pierwszych z n. Czy $(G, \cdot_n)$ to grupa?

Przykład 4.8. Czy liczby wymierne o nieparzystym mianowniku (oczywiście, w formie skróconej) tworzą grupę, gdy działaniem jest dodawanie? Zaliczamy liczby całkowite, jako $n/1$, w tym zero.

Przykład 4.9. Liczby wymierne o mianowniku co najwyżej 2, gdzie działaniem jest dodawanie.

Przykład 4.10. Co, gdyby działaniem było mnożenie? (nie, bo zero. Co gdy wywalimy zero?)

[1] Ćwiczenie dla zaawansowanych: udowodnić, że jeżeli $(A, \times)$ to monoid, to $(A^\times, \times)$ tworzy grupę.

W powyższych przykładach, działanie grupy jest przemienne. Takie grupy nazywamy *przemiennymi* lub *abelowymi*. Nie wszystkie grupy są przemienne, chociażby rozważana na początku grupa diedralna D_6 może służyć jako kontrprzykład (tak jak z resztą grupa izometrii płaszczyznowych dla każdego innego wielokąta foremnego). Poza tym mamy:

Przykład 4.11. (Grupa permutacji) Rozważmy S_n, zbiór permutacji n elementów. Rozważmy te permutacje jako funkcje $\{1, \ldots, n\} \to \{1, \ldots, n\}$, wtedy zbiór tych funkcji tworzy grupę, gdzie działaniem jest $\circ$.

Przykład 4.12. (Iloczyn grup) Niech $(G, \star)$ i $(H, *)$ będą pewnymi grupami. Na zbiorze

$$G \times H = \{(g, h) : g \in G \wedge h \in H\}$$

możemy stworzyć grupę definiując działanie jako

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2).$$

(jak wygląda element neutralny w iloczynie grup? a elementy odwrotne?)

Przykład 4.13. (Grupa trywialna) Najmniejsza możliwa grupa to taka, która ma tylko element neutralny. Grupę tą możemy oznaczać na kilka sposobów: 0, 1, $\{1\}$.

5 Właściwości grup

Niezależnie od tego, jaką grupę zdefiniujemy, będzie ona spełniać pewne proste własności:

Fakt 5.1. Niech G będzie grupą.

- W G istnieje *dokładnie* jeden element neutralny.
- Dla każdego $g \in G$ istnieje *dokładnie* jeden element odwrotny.
- Jak h jest odwrotnością g, to g jest odwrotnością h, czyli $(g^{-1})^{-1} = g$.
- $(ab)^{-1} = b^{-1}a^{-1}$.

Dowód.

- Jeżeli 1 i $1'$ to elementy neutralne, to z jednej strony[2] mamy $1 \cdot 1' = 1'$, bo 1 jest neutralny, a z drugiej strony $1 \cdot 1' = 1$ bo $1'$ jest neutralny. Stąd, $1 = 1'$.
- Niech h i h' będą odwrotne do g. Podobnie to poprzedniego punktu, rozważmy hgh'.

□

(przerywnik: injekcja, surjekcja, bijekcja)

Lemat 5.2. Ustalmy pewne stałe $g \in G$. Funkcja $f : G \to G$ określona przez $x \mapsto gx$ jest bijekcją.

(dwa dowody: istnieje funkcja odwrotna, albo bezpośrednio injekcja i surjekcja)
(przykład: $(\mathbb{Z}/7\mathbb{Z})^\times$ i $g = 3$. *permutacja*)

[2]Wspomniane strony są tutaj dość dosłowne

6 Izomorfizmy

Rozważmy grupy

$$\mathbb{Z} = (\{\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}, +)$$
$$10\mathbb{Z} = (\{\ldots,\ -30,\ -20,\ -10,\ 0,\ 10,\ 20,\ 30,\ \ldots\}, +)$$

Są to różne grupy, ale powierzchownie. Wszystko zachowuje się tak samo, jakby nasze elementy różniły się tylko nazwami. Formalnie taką równoważność nazywamy *izomorfizmem*.

Definicja 6.1. Dane są grupy $(G, \star)$ i $(H, *)$. Bijekcję $\varphi : G \to H$ nazywamy *izomorfizmem*, jeżeli dla wszystkich $g_1,\ g_2 \in G$ zachodzi

$$\varphi(g_1 \star g_2) = \varphi(g_1) * \varphi(g_2).$$

Jeśli istnieje izomorfizm między G a H, to mówimy że grupy te są *izomorficzne*, co zapisujemy $G \cong H$.

Przykład 6.1. $\mathbb{Z} \cong 10\mathbb{Z}$

Przykład 6.2. $G \times H \cong H \times G$, gdzie izomorfizm jest dany przez $(g, h) \mapsto (h, g)$.

Przykład 6.3. Funkcja tożsamościowa $\mathrm{id} : G \to G$ jest izomorfizmem, więc $G \cong G$.

Przykład 6.4. Oprócz tego istnieje inny izomorfizm $\mathbb{Z} \to \mathbb{Z}$ — jaki? $x \mapsto -x$.

Definicja 6.2. Izomorfizm $\varphi : G \to G$ nazywamy *automorfizmem*.

Przykład 6.5. $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$ — jakim wzorem dany jest ten izomorfizm? Co trzeba sprawdzić?

Przykład 6.6. Ogólniej, $\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times$ dla dowolnej liczby pierwszej p. Zakładamy tutaj istnienie pierwiastka pierwotnego modulo p.

Przykład 6.7. (Chińskie twierdzenie o resztach) Jeżeli m i n są względnie pierwsze, to

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

7 Podgrupy

Definicja 7.1. Dana jest grupa $(G, \star)$. Jeżeli pewien podzbiór $H \subseteq G$ tworzy grupę z tym samym działaniem $\star$, to mówimy że H jest *podgrupą* G, co zapisujemy $H \leq G$.
Jeżeli $H \neq G$ (czyli $H \subsetneq G$), to mówimy że H jest *podgrupą właściwą*.

Co musimy sprawdzić o danym podzbiorze, aby przekonać się, że jest grupą? Łączność działania otrzymujemy za darmo.

- $a \in H \wedge b \in H \Longrightarrow a \star b \in H$.
- $a \in H \Longrightarrow a^{-1} \in H$.

Pytanie. Co z elementem neutralnym?

- Podzbiór jest niepusty.

Przykład 7.1. $2\mathbb{Z}$ jest podgrupą $\mathbb{Z}$, izomorficzną do całego $\mathbb{Z}$.

Przykład 7.2. W grupie permutacji S_n określmy podzbiór $\{\tau \in S_n : \tau(n) = n\}$. Jest on podgrupą S_n (czemu?), która z resztą jest izomorficzna do S_{n-1}.

Przykład 7.3. W grupie $G \times H$, zbiór $\{(g, 1_H) : g \in G\}$ jest podgrupą. Do czego jest izomorficzna?

Uwaga. Grupy zwykle uznajemy za takie same, jeżeli są izomorficzne. W przypadku podgrup możemy mieć tak, że $H_1 \leq G$, $H_2 \leq G$, $H_1 \cong H_2$, ale $H_1 \neq H_2$. Wtedy podgrupy te uznajemy za różne. (przykład? $G \times G$)

Pytanie. Jakie możemy zdefiniować podgrupy, niezależnie od naszej głównej grupy G?

Przykład 7.4. W każdej grupie $G \leq G$ i $\{1_G\} \leq G$.

Przykład 7.5. (Podgrupa generowana przez element) Oznaczmy

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\}.$$

Jest to podgrupa (czemu?). Nazywamy ją *podgrupą generowaną przez g*.

Pytanie. Jak wygląda $\langle 3 \rangle < \mathbb{Z}$?

Przykład 7.6. W D_6, $\langle r \rangle \cong \mathbb{Z}/3\mathbb{Z}$.

Ćwiczenie 7.1. Prawda czy fałsz?

a) Jeżeli A i B są podgrupami, to $A \cap B$ również jest podgrupą.

b) Jeżeli A i B są podgrupami, to $A \cup B$ również jest podgrupą.

c) Każdą podgrupę $A < G \times H$ można przedstawić jako $A_1 \times A_2$, gdzie $A_1 < G$ i $A_2 < H$.

8 Rzędy, twierdzenie Lagrange'a

Z podgrupami związane jest ważne twierdzenie, ale najpierw...
W teorii grup występują dwa znaczenia słowa *rząd*.

Definicja 8.1. *Rzędem* grupy nazywamy liczbę jej elementów. Liczbę tą oznaczamy $|G|$.

Definicja 8.2. *Rzędem* elementu g (oznaczanym $\operatorname{ord} g$) nazywamy najmniejszą dodatnią liczbę całkowitą $k \in \mathbb{Z}_+$, dla której $g^k = 1$. Jeżeli taka liczba nie istnieje, to $\operatorname{ord} g = \infty$.

Ćwiczenie 8.1. Udowodnij, że w grupie skończonego rzędu wszystkie elementy mają skończony rząd.

Pytanie. Jaki jest związek pomiędzy tymi dwoma definicjami?

$\operatorname{ord} g = |\langle g \rangle|$.

Twierdzenie 8.3 (Lagrange)**.** Jeżeli grupa G jest skończona i $H \leq G$, to $|G|$ dzieli się przez $|H|$.

Dowód tego twierdzenia zostawimy sobie na następny raz.

Wniosek. $x^{|G|} = 1$

9 Prezentacje

Wróćmy do podgrupy generowanej przez element. W jednym z podręczników zostało to zwizualizowane następująco:

> Włóż x do pudełka, szczelnie zamknij i mocno potrząśnij. W rezultacie otrzymamy piękną eksplozję w postaci $\langle x \rangle$.

Tak właściwie, nie musimy się ograniczać do jednego elementu. Jak dorzucimy do naszego pudełka y, to otrzymamy... każdą kombinację potęg x i y.

Definicja 9.1. Niech $S \subset G$. Podgrupa *generowana* przez S, oznaczana $\langle S \rangle$, to zbiór elementów które możemy zapisać jako skończony iloczyn elementów S i ich odwrotności. Jeżeli $\langle S \rangle = G$ to mówimy że S jest zbiorem *generatorów* grupy G.

Pytanie. Jaki element jest generatorem $\mathbb{Z}$? (czy tylko 1, czy też -1)

Może dałoby się w ten sposób kompaktowo opisywać nowe grupy, z którymi się spotykamy? Na przykład, $\mathbb{Z}$ to grupa generowana przez jeden element:

$$\mathbb{Z} \cong \langle a \rangle$$

Problem jest taki, że nasze generatory mają pewne właściwości. Na przykład, $\mathbb{Z}/100\mathbb{Z}$ jest również generowana przez jeden generator, ale spełnia $a^{100} = 1$. Zapisujmy więc też te właściwości (tzw. *relacje*):

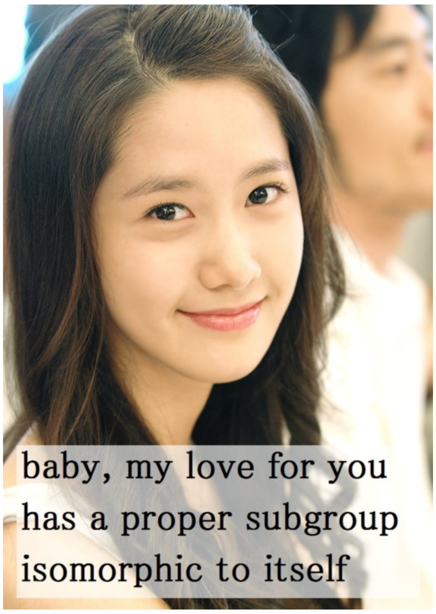
$$\mathbb{Z}/n\mathbb{Z} \cong \langle a \mid a^{100} = 1 \rangle$$

Taka kombinacja generatorów i relacji nazywana jest *prezentacją grupy*.

Ćwiczenie 9.1. Znajdź prezentację dla D_{2n}.

10 Zadania

Zadanie 1. O co chodzi w tym żarcie?



(tłumaczenie: bejbe, moja miłość do ciebie jest izomorficzna do właściwej podgrupy samej siebie)

Zadanie 2. Wykaż, że $D_6 \cong S_3$, ale $D_{24} \ncong S_4$.

Zadanie 3. *Grupą cykliczną* nazywamy grupę G w której istnieje *generator* $g \in G$, taki że $\langle g \rangle = G$. Wykaż że:

a) Grupy cykliczne równego (skończonego) rzędu są izomorficzne. Podobnie, wszystkie nieskończone grupy cykliczne są izomorficzne.

b) Każda grupa, której rząd jest liczbą pierwszą jest cykliczna.

c) Każda podgrupa grupy cyklicznej jest cykliczna.

d) W grupie cyklicznej skończonego rzędu n istnieje, dla każdego $d \mid n$, dokładnie jedna podgrupa rzędu d.

Ile elementów rzędu d jest w grupie cyklicznej rzędu n?

Zadanie 4. Zaproponuj figury (tj. zbiory punktów), których grupy izometrii płaszczyznowych są izomorficzne do

a) $\mathbb{Z}/n\mathbb{Z}$

b) $\mathbb{Z}$

Zadanie 5. Dany jest zbiór G oraz łączne działanie $\star : G \times G \to G$. Ponadto wiadomo, że

- istnieje element $1_G \in G$ (element neutralny od lewej), który spełnia $1_G \star g = g$ dla każdego $g \in G$.
- dla każdego $g \in G$ istnieje $h \in G$ (element odwrotny od lewej), który spełnia $h \star g = e$.

Udowodnij, że $(G, \star)$ to grupa (tj. udowodnij, że elementy odwrotne i neutralny działają też od prawej).

Zadanie 6. Podzbiór $H \subseteq G$ jest skończony, niepusty i sprawdziliśmy już, że działanie grupy jest domknięte — dla $a, b \in H$ mamy $ab \in H$. Udowodnij, że $H \leq G$ (w związku z wcześniejszą dyskusją pozostaje udowodnić, że odwrotności będą się zawierać w H).

Zadanie 7. Wykaż, że istnieją tylko dwie grupy rzędu 4.

Zadanie 8.

a) Udowodnij, że $\operatorname{ord} ab = \operatorname{ord} ba$.

b) Podaj przykład grupy oraz pewnych elementów a, b, c, takich że $\operatorname{ord} abc \neq \operatorname{ord} bac$.

Zadanie 9. Rodzinę $\mathcal{S}$ niektórych podzbiorów zbioru $\{1, \ldots, n\}$ nazywamy *dobrą*, jeżeli dla każdych dwóch zbiorów $A, B \in \mathcal{S}$, do $\mathcal{S}$ należą również $A \cup B$, $A \setminus B$, $B \setminus A$. Znajdź, w zależności od n, największy możliwy rozmiar *dobrej* rodziny, która nie zawiera *wszystkich* podzbiorów $\{1, \ldots, n\}$.

Zadanie 10. Wykaż, że dla każdej grupy G istnieje liczba n, taka że S_n zawiera podgrupę izomorficzną z G.

Zadanie 11. Na stole położono n monet w rzędzie, każda moneta odwrócona orłem do góry. W każdym kroku, jeśli to możliwe, wybieramy jakiegoś orła, usuwamy go z rzędu, a następnie odwracamy monetę bezpośrednio po lewej i po prawej (sąsiadujące monety mogą być reszką, ale muszą być, tj. nie możemy wybrać skrajnej monety).

Udowodnić, że możemy tak wybrać monety w kolejnych krokach aby usunąć wszystkie monety oprócz dwóch, wtedy i tylko wtedy, gdy $n \not\equiv 1 \pmod 3$.

Zadanie 12. Dana jest liczba pierwsza p. Dodatnią liczbę całkowitą n nazwiemy *ładną* wtedy i tylko wtedy, gdy suma reszt z dzielenia liczb $n,\ n^2,\ n^3,\ \ldots,\ n^{p-1}$ przez p jest równa $\frac{1}{2}p(p-1)$. Udowodnić, że w zbiorze $\{1,\ \ldots,\ p-1\}$ liczb ładnych jest nieparzyście wiele.

Zadanie 13. Niech $\operatorname{Aut} G$ będzie zbiorem automorfizmów $G \to G$. Sprawdź, że $(\operatorname{Aut} G, \circ)$ jest grupą. Wykaż, że jeżeli p jest liczbą pierwszą, to $\operatorname{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Zadanie 14. Podgrupą maksymalną $H < G$ grupy G nazywamy taką podgrupę właściwą, która zawiera wszystkie inne właściwe podgrupy G.

a) Wykaż, że $\mathbb{Q}^\times$ nie ma podgrupy maksymalnej.

b) Znajdź wszystkie grupy, dla których istnieje podgrupa maksymalna.

Zadanie 15. Oblicz rząd grupy

$$\langle a, b, c \mid ab = c^2a^4,\ bc = ca^6,\ ac = ca^8,\ c^{2018} = b^{2019} \rangle$$

11 Wykorzystane materiały

- MIT Lecture Notes — Modern Algebra
  https://ocw.mit.edu/courses/mathematics/18-703-modern-algebra-spring-2013/lecture-notes/
- Evan Chen — An Infinitely Large Napkin
  https://web.evanchen.cc/napkin.html
- Evan Chen — Math 55a Lecture Notes (Honors Abstract and Linear Algebra)
  https://web.evanchen.cc/notes/Harvard-55a.pdf
- Michael Artin — Algebra
- Zadania z Olimpiady Matematycznej
- Jerzy Rutkowski — Algebra abstrakcyjna w zadaniach