Wykład 3
Grupy cykliczne

Definicja 3.1. Niech a będzie elementem grupy $(G, \cdot, e)$. Jeżeli istnieje liczba naturalna k taka, że $a^k = e$, to najmniejszą taką liczbę naturalną k nazywamy *rzędem elementu* a. W przeciwnym przypadku (tzn. gdy $a^n \neq e$ dla każdego $n \in \mathbb{N}$) mówimy, że rząd elementu a jest równy ∞ (nieskończoność). Rząd elementu a oznaczamy przez $o(a)$.

Przykład 3.2. Zauważmy, że $o(-1) = 2$ w grupie $\mathbb{R}^*$, gdyż w tym przypadku $e = 1$ oraz $-1 \neq 1$ i $(-1)^2 = 1$. Natomiast w grupie $\mathbb{R}^+$ mamy, że $o(-1) = \infty$, bo wówczas $e = 0$ oraz dla każdego $n \in \mathbb{N}$ jest $n \cdot (-1) = -n \neq 0$.

Uwaga 3.3. Przykład 3.2 pokazuje, że należy być bardzo ostrożnym przy wyznaczaniu rzędu elementu grupy. Przede wszystkim musimy rozumieć naturę działania grupowego oraz wiedzieć jak wygląda element neutralny tej grupy.

Uwaga 3.4. Ze Stwierdzeń 2.16 i 2.17 wynika od razu, że dla dowolnego elementu a skończonego rzędu grupy G zachodzi wzór:

$$o(a) = |\langle a \rangle|.$$

W szczególności z Twierdzenia 2.9 mamy, że **rząd dowolnego elementu grupy skończonej jest dzielnikiem jej rzędu.**

Stwierdzenie 3.5. *Niech a będzie elementem skończonego rzędu grupy $(G, \cdot, e)$. Wtedy dla dowolnego całkowitego k:*

$$a^k = e \iff o(a) \mid k.$$

Dowód. Jeśli $o(a) \mid k$, to istnieje $s \in \mathbb{Z}$ takie, że $k = s \cdot o(a)$. Zatem $a^k = a^{s \cdot o(a)} = (a^{o(a)})^s = e^s = e$. Na odwrót, załóżmy, że $a^k = e$. Wtedy istnieją $q, r \in \mathbb{Z}$ takie, że $k = q \cdot o(a) + r$ i $0 \leqslant r < o(a)$. Stąd $e = a^k = a^{q \cdot o(a) + r} = a^{q \cdot o(a)} \cdot a^r = e \cdot a^r = a^r$, czyli $a^r = e$. Ale $r < o(a)$, więc $r \notin \mathbb{N}$, czyli $r = 0$. Zatem $k = q \cdot o(a)$ i $o(a) \mid k$. $\square$

Stwierdzenie 3.6. *Jeżeli a i b są elementami skończonych względnie pierwszych rzędów grupy G oraz $a \cdot b = b \cdot a$, to $o(ab) = o(a) \cdot o(b)$.*

Dowód. Oznaczmy: $n = o(a)$, $m = o(b)$. Wtedy $m, n \in \mathbb{N}$, $(m, n) = 1$ oraz $a^n = e$ i $b^m = e$. Z Twierdzenia 1.14, $(ab)^k = a^k b^k$ dla każdego $k \in \mathbb{Z}$. W szczególności $(ab)^{mn} = a^{mn} b^{mn} = e \cdot e = e$, skąd $l = o(ab) \leqslant mn$. Ale $e = (ab)^l = a^l b^l$, więc $e = (a^l b^l)^n = = a^{ln} b^{ln} = e b^{ln} = b^{ln}$, czyli $b^{ln} = e$. Zatem ze Stwierdzenia 3.5, $m \mid ln$. Ale $(m, n) = 1$, więc z zasadniczego twierdzenia arytmetyki, $m \mid l$. Analogicznie pokazujemy, że $n \mid l$.

Ponieważ $m \mid l$ i $n \mid l$ oraz $(m,n) = 1$, więc $mn \mid l$, czyli $mn \leqslant l$. Ale wcześniej pokazaliśmy, że $l \leqslant mn$, więc ostatecznie $l = mn$, czyli $o(ab) = o(a) \cdot o(b)$. $\square$

Stwierdzenie 3.7. *Jeżeli a jest elementem nieskończonego rzędu grupy $(G, \cdot, e)$, to dla dowolnych liczb całkowitych k i l:*

$$a^k = a^l \iff k = l.$$

W szczególności grupa $\langle a \rangle$ jest nieskończona. Ponadto grupa $\langle a \rangle$ posiada dokładnie dwa generatory: a i a^{-1}.

Dowód. Załóżmy, że istnieją różne liczby całkowite k, l takie, że $a^k = a^l$. Bez zmniejszania ogólności możemy zakładać, że $k > l$. Wtedy $k - l \in \mathbb{N}$ i $a^{k-l} = e$, co przeczy temu, że $o(a) = \infty$. Implikacja odwrotna jest oczywista.

Ponieważ $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$, więc $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Ale $\langle a^{-1} \rangle \subseteq \langle a \rangle$, więc $\langle a^{-1} \rangle = \langle a \rangle$, czyli a^{-1} jest generatorem grupy $\langle a \rangle$. Ponadto z pierwszej części dowodu $a^{-1} \neq a$. Niech teraz $b \in \langle a \rangle$ będzie generatorem grupy $\langle a \rangle$. Wtedy istnieje liczba całkowita k taka, że $b = a^k$ oraz $a \in \langle a^k \rangle$. Zatem istnieje $l \in \mathbb{Z}$ takie, że $a = (a^k)^l = a^{kl}$. Zatem z pierwszej części dowodu $kl = 1$, skąd $k = 1$ lub $k = -1$ oraz $b = a$ lub $b = a^{-1}$. $\square$

Lemat 3.8. *Niech a będzie elementem skończonego rzędu grupy G. Wówczas dla dowolnej liczby całkowitej k:*

$$\langle a^k \rangle = \langle a^{(o(a),k)} \rangle.$$

Dowód. Oznaczmy $d = (o(a), k)$. Wtedy $d \mid k$, więc $k = dl$ dla pewnego $l \in \mathbb{Z}$, skąd $a^k = (a^d)^l \in \langle a^d \rangle$. Zatem $\langle a^k \rangle \subseteq \langle a^d \rangle$. Ponadto z elementarnej teorii liczb wiemy, że istnieją liczby całkowite x, y takie, że $d = o(a)x + ky$. Stąd $a^d = a^{o(a)x+ky} = a^{o(a)x} \cdot a^{ky} =$ $= e \cdot a^{ky} = (a^k)^y \in \langle a^k \rangle$. Zatem $\langle a^d \rangle \subseteq \langle a^k \rangle$ i ostatecznie $\langle a^d \rangle = \langle a^k \rangle$. $\square$

Twierdzenie 3.9. *Niech a będzie elementem skończonego rzędu grupy $(G, \cdot, e)$. Wtedy:*
(i) dla dowolnego naturalnego dzielnika d liczby $o(a)$ zachodzi wzór:

$$o(a^d) = \tfrac{o(a)}{d},$$

(ii) dla dowolnej liczby całkowitej k zachodzi wzór:

$$o(a^k) = \tfrac{o(a)}{(o(a),k)}.$$

Dowód. (i) Zauważmy, że $\frac{o(a)}{d} \in \mathbb{N}$ i $(a^d)^{\frac{o(a)}{d}} = a^{d \cdot \frac{o(a)}{d}} = a^{o(a)} = e$. Zatem $k = o(a^d) \leqslant \frac{o(a)}{d}$. Ale $e = (a^d)^k = a^{dk}$, więc ze Stwierdzenia 3.5 mamy, że $o(a) \mid dk$. Zatem $\frac{o(a)}{d} \mid k$, czyli $\frac{o(a)}{d} \leqslant k$ i ostatecznie $k = \frac{o(a)}{d}$.

(ii) Z Lematu 3.8 mamy, że $\langle a^k \rangle = \langle a^{(o(a),k)} \rangle$. Ale $d = (o(a), k)$ jest naturalnym dzielnikiem $o(a)$, więc z (i) oraz z Uwagi 3.4 uzyskujemy, że $\frac{o(a)}{(o(a),k)} = o(a^{(o(a),k)}) =$ $|\langle a^{(o(a),k)} \rangle| = |\langle a^k \rangle| = o(a^k)$. $\square$

Twierdzenie 3.10. *Załóżmy, że $\langle a\rangle$ jest skończoną grupą cykliczną rzędu n. Niech d będzie dzielnikiem naturalnym liczby n. Wtedy w grupie $\langle a\rangle$ istnieje dokładnie $\varphi(d)$ elementów rzędu d i są one postaci $a^{\frac{n}{d}\cdot k}$, gdzie $k \in \{1,\ldots,d\}$ oraz $(k,d)=1$.*

Dowód. Niech $k \in \{1,\ldots,d\}$ będzie takie, że $(k,d)=1$. Wtedy $(\frac{n}{d}\cdot k, n) = (\frac{n}{d}\cdot k, \frac{n}{d}\cdot d) = \frac{n}{d}\cdot(k,d) = \frac{n}{d}\cdot 1 = \frac{n}{d}$. Zatem z Twierdzenia 3.9, $o(a^{\frac{n}{d}\cdot k}) = \frac{n}{\frac{n}{d}} = d$.

Niech teraz $b \in \langle a\rangle$ będzie elementem rzędu d. Wtedy istnieje liczba naturalna $m \leqslant n$ taka, że $b = a^m$ oraz z Twierdzenia 3.9, $d = o(a^m) = \frac{n}{(m,n)}$, skąd $(m,n) = \frac{n}{d}$. Ale $(m,n) \mid m$, więc istnieje $k \in \mathbb{N}$ takie, że $m = \frac{n}{d}\cdot k$. Ponadto $\frac{n}{d} = (m,n) = (\frac{n}{d}\cdot k, \frac{n}{d}\cdot d) = \frac{n}{d}\cdot(k,d)$, więc $(k,d)=1$. Ale $m \leqslant n$, więc $\frac{n}{d}\cdot k \leqslant n$, skąd $k \leqslant d$.

Jeśli $k,l \in \{1,\ldots,d\}$, $(k,d) = (l,d) = 1$ oraz $a^{\frac{n}{d}\cdot k} = a^{\frac{n}{d}\cdot l}$, to $a^{\frac{n}{d}\cdot(k-l)} = e$, więc ze Stwierdzenia 3.5, $n \mid \frac{n}{d}\cdot(k-l)$, skąd $d \mid k-l$. Ale $k,l \in \{1,\ldots,d\}$, więc $k = l$. $\square$

Wniosek 3.11. *Skończona grupa cykliczna $\langle a\rangle$ rzędu n posiada dokładnie $\varphi(n)$ generatorów i są one postaci: a^k, gdzie $k \in \{1,\ldots,n\}$ oraz $(k,n)=1$.*

Dowód. Element $b \in \langle a\rangle$ jest generatorem grupy $\langle a\rangle$ wtedy i tylko wtedy, gdy $o(b) = n$. Zatem z Twierdzenia 3.10 grupa $\langle a\rangle$ posiada dokładnie $\varphi(n)$ generatorów i są one postaci: $a^{\frac{n}{n}\cdot k} = a^k$, gdzie $k \in \{1,\ldots,n\}$ oraz $(k,n)=1$. $\square$

Twierdzenie 3.12. *Każda podgrupa grupy cyklicznej jest grupą cykliczną.*

Dowód. Niech $(G,\cdot,e)$ będzie grupą cykliczną o generatorze a i niech H będzie dowolną jej podgrupą. Jeśli $H = \{e\}$, to $H = \langle e\rangle$, czyli grupa H jest cykliczna. Załóżmy więc dalej, że $H \neq \{e\}$. Wtedy istnieje $k \in \mathbb{Z}$ takie, że $e \neq a^k \in H$. Stąd $k \neq 0$ i $a^{-k} = (a^k)^{-1} \in H$. Zatem $k \in \mathbb{N}$ lub $-k \in \mathbb{N}$ i z zasady minimum istnieje najmniejsza liczba naturalna m taka, że $a^m \in H$. Wtedy $\langle a^m\rangle \subseteq H$. Weźmy dowolne $h \in H$. Istnieje $s \in \mathbb{Z}$ takie, że $h = a^s$. Ale $s = qm + r$ dla pewnych $q,r \in \mathbb{Z}$, $0 \leqslant r < m$, więc $a^s = a^{qm+r} = a^{qm}\cdot a^r = (a^m)^q \cdot a^r$, skąd $a^r = a^s \cdot (a^m)^{-q} \in H$, czyli $a^r \in H$. Ponadto $0 \leqslant r < m$, więc z minimalności m, $r \notin \mathbb{N}$, czyli $r = 0$. Zatem $h = (a^m)^q \in \langle a^m\rangle$, czyli $H \subseteq \langle a^m\rangle$ i ostatecznie $H = \langle a^m\rangle$. $\square$

Twierdzenie 3.13. *Grupa cykliczna nieskończona $\langle a\rangle$ posiada nieskończenie wiele podgrup i są one postaci: $\langle a^n\rangle$, gdzie $n = 0,1,\ldots$*

Dowód. Z Twierdzenia 3.12 wynika, że każda podgrupa H grupy $\langle a\rangle$ jest postaci $H = \langle a^k\rangle$ dla pewnego $k \in \mathbb{Z}$. Ale $a^k = (a^{-k})^{-1} \in \langle a^{-k}\rangle$, więc $\langle a^k\rangle \subseteq \langle a^{-k}\rangle$ oraz $\langle a^{-k}\rangle \subseteq \langle a^k\rangle$, bo $a^{-k} \in \langle a^k\rangle$, więc $\langle a^k\rangle = \langle a^{-k}\rangle$, czyli $H = \langle a^n\rangle$ dla pewnego $n = 0,1,\ldots$

Niech $m,n \in \{0,1,\ldots\}$ będą takie, że $\langle a^m\rangle = \langle a^n\rangle$. Wtedy $a^m \in \langle a^n\rangle$, więc istnieje $k \in \mathbb{Z}$ takie, że $a^m = (a^n)^k = a^{nk}$. Zatem ze Stwierdzenia 3.7, $m = nk$, czyli $n \mid m$. Analogicznie pokazujemy, że $m \mid n$. Stąd $m \mid n$ i $n \mid m$ oraz $n,m \in \{0,1,\ldots\}$, więc $m = n$. $\square$

Przykad 3.14. Ponieważ $\mathbb{Z}^+ = \langle 1\rangle$ i $o(1) = \infty$, więc z Twierdzenia 3.13 wynika, że wszystkimi podgrupami grupy $\mathbb{Z}^+$ są: $\langle n\rangle = \{n\cdot k :\ k \in \mathbb{Z}\}$ dla $n = 0,1,\ldots$ Zauważmy,

że podgrupa $\langle n\rangle$ jest nam dobrze znana już od szkoły podstawowej, gdyż jej elementami są wszystkie całkowite wielokrotności liczby n. Ponadto ze Stwierdzenia 3.7 wynika, że grupa $\mathbb{Z}^+$ posiada dokładnie dwa generatory: 1 i -1.

Twierdzenie 3.15. *Wszystkimi podgrupami skończonej grupy cyklicznej $\langle a\rangle$ są podgrupy postaci $\langle a^d\rangle$, gdzie d przebiega wszystkie dzielniki naturalne liczby $o(a)$. W szczególności liczba wszystkich podgrup grupy $\langle a\rangle$ jest równa liczbie wszystkich dzielników naturalnych liczby $o(a)$.*

Dowód. Jeśli $\langle a^{d_1}\rangle = \langle a^{d_2}\rangle$ dla pewnych dzielników naturalnych d_1, d_2 liczby $o(a)$, to z Twierdzenia 3.9 i z Uwagi 3.4: $\frac{n}{d_1} = o(a^{d_1}) = |\langle a^{d_1}\rangle| = |\langle a^{d_2}\rangle| = o(a^{d_2}) = \frac{n}{d_2}$, czyli $d_1 = d_2$.

Niech H będzie dowolną podgrupą grupy $\langle a\rangle$. Wtedy z Twierdzenia 3 istnieje $k \in \mathbb{Z}$ takie, że $H = \langle a^k\rangle$. Ale z Lematu 3.8, $\langle a^k\rangle = \langle a^{(o(a),k)}\rangle$ i $(o(a), k)$ jest dzielnikiem naturalnym liczby $o(a)$, więc twierdzenie zostało udowodnione. □

Uwaga 3.16. Z Twierdzenia 3.15 wynika, że istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy zbiorem wszystkich podgrup skończonej grupy cyklicznej $\langle a\rangle$ i zbiorem wszystkich dzielników naturalnych liczby $o(a)$. W szczególności wynika stąd, że **dla każdej liczby naturalnej d dzielącej rząd skończonej grupy cyklicznej $\langle a\rangle$ istnieje dokładnie jedna podgrupa rzędu d grupy $\langle a\rangle$.**

Stwierdzenie 3.17. *Jeżeli liczba naturalna n posiada co najmniej dwa różne, nieparzyste dzielniki pierwsze, to grupa $\mathbb{Z}_n^*$ nie jest cykliczna.*

Dowód. Z założenia istnieją różne, nieparzyste liczby pierwsze p, q oraz liczby naturalne α, β, m takie, że $n = p^\alpha q^\beta m$ oraz m nie jest podzielne ani przez p ani przez q. Z chińskiego twierdzenia o resztach wynika zatem, że istnieją $a, b \in \mathbb{Z}_n^*$ takie, że $a \equiv -1 \pmod{p^\alpha}$, $a \equiv 1 \pmod{q^\beta m}$ oraz $b \equiv 1 \pmod{p^\alpha m}$ i $b \equiv -1 \pmod{q^\beta}$. Ponieważ liczby p i q są nieparzyste, więc $a \neq 1$ i $b \neq 1$. Gdyby $a = b$, to $1 \equiv -1 \pmod{p^\alpha}$, skąd $p^\alpha | 2$ i mamy sprzeczność. Zatem $a \neq b$ i wobec tego $\{1, a\} \neq \{1, b\}$. Ponadto $a^2 \equiv 1 \pmod{p^\alpha}$ i $a^2 \equiv 1 \pmod{q^\beta m}$, więc $a^2 \equiv 1 \pmod{n}$, skąd $a \odot_n a = 1$, czyli $o(a) = 2$ w grupie $\mathbb{Z}_n^*$, skąd $\langle a\rangle = \{1, a\}$. Podobnie pokazujemy, że $\langle b\rangle = \{1, b\}$. Zatem grupa $\mathbb{Z}_n^*$ posiada dwie różne podgrupy rzędu 2, wic z Uwagi 3.16 ta grupa nie jest cykliczna. □

Uwaga 3.18. Z elementarnej teorii liczb wiadomo, że jeśli $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, gdzie $p_1, \ldots, p_s$ są różnymi liczbami pierwszymi oraz $\alpha_1, \ldots, \alpha_s$ są nieujemnymi liczbami całkowitymi, to liczba wszystkich dzielników naturalnych liczby n jest równa $\Theta(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_s + 1)$. Ponadto $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_s^{\alpha_s})$ i dla liczb pierwszych p oraz $\alpha \in \mathbb{N}$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Przykład 3.19. Niech $n \in \mathbb{N}$, $n > 1$. Wtedy $\mathbb{Z}_n^+ = \langle 1\rangle$ oraz $o(1) = n$. Zatem z Wniosku 3.11 grupa $\mathbb{Z}_n^+$ posiada dokładnie $\varphi(n)$ generatorów i są nimi liczby naturalne

$k \leqslant n$ względnie pierwsze z n. Ponadto podgrupy grupy $\mathbb{Z}_n^+$ są postaci: $\{0\}$ oraz $\langle d\rangle = \{0, d, 2d, \ldots, (\frac{n}{d}-1)\cdot d\}$, gdzie $d < n$ jest dzielnikiem naturalnym liczby n. Zatem grupa $\mathbb{Z}_n^+$ posiada dokładnie $\Theta(n)$ wszystkich podgrup.

Lemat 3.20. *Niech a będzie elementem maksymalnego rzędu w skończonej grupie abelowej A. Wówczas $o(b) \mid o(a)$ dla każdego $b \in A$.*

Dowód. Załóżmy, że istnieje $b \in A$ takie, że $o(b)$ nie dzieli $o(a)$. Wtedy istnieje liczba pierwsza p oraz liczby naturalne m, n niepodzielne przez p i nieujemne liczby całkowite α, β takie, że $\alpha < \beta$ oraz $o(a) = p^\alpha m$ i $o(b) = p^\beta n$. Niech $x = a^{p^\alpha}$ i $y = b^n$. Wtedy z Twierdzenia 3.9, $o(x) = m$ oraz $o(y) = p^\beta$. Ale $(m, p^\beta) = 1$, gdyż p nie dzieli m, więc ze Stwierdzenia 3.6, $o(xy) = p^\beta m > p^\alpha m = o(a)$ i mamy sprzeczność. □

Twierdzenie 3.21. *Jeżeli A jest skończoną grupą abelową i dla każdej liczby naturalnej d dzielącej $|A|$ istnieje dokładnie jedna podgrupa rzędu d grupy A, to grupa A jest cykliczna.*

Dowód. Załóżmy, że przy tych założeniach grupa A nie jest cykliczna. Niech a będzie elementem maksymalnego rzędu w grupie A. Wtedy $\langle a\rangle \neq A$, więc istnieje $b \in A$ takie, że $b \notin \langle a\rangle$. Z Lematu 3.20, $o(b) \mid o(a)$. Zatem z Twierdzenia 3.15 istnieje w grupie $\langle a\rangle$ podgrupa H rzędu $o(b)$. Ale $|\langle b\rangle| = o(b)$, więc na mocy założenia $\langle b\rangle = H$, skąd $b \in H \subseteq \langle a\rangle$, czyli $b \in \langle a\rangle$ i mamy sprzeczność. Zatem grupa A jest cykliczna. □

Wniosek 3.22. Dla każdej liczby pierwszej p grupa $\mathbb{Z}_p^*$ jest cykliczna.

Dowód. Ponieważ p jest liczbą pierwszą, więc $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$, czyli $|\mathbb{Z}_p^*| = p-1$. Ponadto grupa $\mathbb{Z}_p^*$ jest abelowa. Niech $a \in \mathbb{Z}_p^*$ będzie elementem maksymalnego rzędu r. Wtedy z Uwagi 3.4, $r|p-1$, więc $r \leq p-1$. Ponadto z Lematu 3.20 mamy, że $o(b)|r$ dla każdego $b \in \mathbb{Z}_p^*$. Zatem $b^r = 1$ dla każdego $r \in \mathbb{Z}_p^*$. Wobec tego kongruencja $x^r - 1 \equiv 0 (mod\ p)$ ma co najmniej $p-1$ rozwiązań. Ale z twierdzenia Lagrange'a o liczbie pierwiastków kongruencji modulo liczba pierwsza wynika, że liczba rozwiązań tej kongruencji jest $\leq r$. Zatem $p-1 \leq r$ i ostatecznie $r = p-1$. Wobec tego $|\langle a\rangle| = |\mathbb{Z}_p^*|$, czyli a jest generatorem grupy $\mathbb{Z}_p^*$ i ta grupa jest cykliczna. □

Zagadka 1. Dla jakich liczb naturalnych k jest cykliczna grupa $\mathbb{Z}_{2^k}^*$?

Zagadka 2. Czy każda grupa posiadająca jedynie skończoną liczbę podgrup jest skończona?

Zagadka 3. Czy istnieje grupa nieskończona, której każdy element ma skończony rząd?

Zagadka 4. Udowodnij, że jeśli liczba naturalna n jest podzielna przez 4 i dzieli się przez pewną nieparzystą liczbę pierwszą, to grupa $\mathbb{Z}_n^*$ nie jest cykliczna.

Zagadka 5. Udowodnij, że jeżeli skończona grupa G ma rząd parzysty, to w G istnieje

element rzędu 2.

Zagadka 6. Niech $(A, +, 0)$ będzie grupą abelową i $a_1, a_2, \ldots, a_n \in A$. Udowodnij, że

$$\langle a_1, a_2, \ldots, a_n \rangle = \{k_1 a_1 + k_2 a_2 + \ldots + k_n a_n \mid k_1, k_2, \ldots, k_n \in \mathbb{Z}\}.$$

Zagadka 7. Udowodnij, że każda skończenie generowana podgrupa grupy $\mathbb{Q}^+$ jest cykliczna. Uzasadnij też, że grupa $\mathbb{Q}^+$ nie jest skończenie generowana.