Liczba rozwiązań w iloczynie kartezjańskim przedziałów, równania liniowgo o współczynnikach ze skończonej grupy abelowej.

Maciej Zakarczemny

Politechnika Krakowska

OBLICZA ALGEBRY, Kraków, 29 - 31 maja 2015

W pracy [8] udowodniłem następujące przypuszczenie Schinzla wypowiedziane w druku w 2008 r.

Twierdzenie 1.1.

Dla każdej skończonej grupy abelowej Γ i dowolnych $a_1, \ldots, a_k \in \Gamma$ oraz dla dowolnych liczb całkowitych dodatnich $b_1, b_2, \ldots, b_k$ liczba rozwiązań równania

$$\sum_{i=1}^{k} a_i x_i = 0$$

w nieujemnych całkowitych $x_i \leq b_i$ jest co najmniej

$$2^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1), \tag{1}$$

gdzie $D(\Gamma)$ to stała Dawenporta grupy Γ.
Współczynnik $2^{1-D(\Gamma)}$ jest najlepszym możliwym współczynnikiem niezależnym od a_i, b_i, a zależnym tylko od Γ.

Fakt, że jakiś dodatni współczynnik, zależny tylko od Γ, istnieje został już udowodniony w nieopublikowanej pracy M. Drmoty i M. Skałby [7].

Lematy i definicje.

Niech Γ będzie skończoną grupą abelową z działabem o zapisie multiplikatywnym.

Definicja 1.2.

Definujemy *stałą Dawenporta* $D(\Gamma)$ jako najmniejszą dodatnią liczbę całkowitą n taką, że dla każdego ciągu $g_1, \ldots, g_n$ elementów skończonej grupy abelowej Γ, istnieje niepusty zbiór indeksów

$$1 \leq i_1 < \ldots < i_t \leq n$$

takich, że:

$$g_{i_1} \cdot \ldots \cdot g_{i_t} = 1.$$

Dla grupy z notacją multiplikatywną. Twierdzenie (1.1) ma postać:

Dla każdej skończonej grupy abelowej Γ oraz dla dowolnych $a_1, \ldots, a_k \in \Gamma$, oraz dla dowolnych całkowitych dodatnich $b_1, \ldots, b_k$ liczba rozwiązań równania $\prod_{i=1}^{k} {a_i}^{x_i} = 1$ w nieujemnych liczbach całkowitych $x_i \leq b_i$ jest co najmniej

$$2^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1). \tag{2}$$

Uwaga 1.3.

W Twierdzeniu (1.1) współczynnik $2^{1-D(\Gamma)}$ jest najlepszym możliwym współczynnikiem niezależnym od a_i, b_i, a zależnym tylko od Γ.

Dowód.

Na podstawie definicji stałej Dawenporta, możemy znaleźć $g_1, \ldots, g_{D(\Gamma)-1} \in \Gamma$ takie, że iloczyn elementów każdego niepustego podciągu tego ciągu jest różny od 1 w Γ.

Wtedy liczba rozwiązań równania $\prod_{i=1}^{D(\Gamma)-1} {g_i}^{x_i} = 1$, gdzie $x_i = 0$ lub $x_i = 1$, jest równa $1 = 2^{1-D(\Gamma)} \prod_{i=1}^{D(\Gamma)-1} (1+1)$. $\square$

Lemat 1.4.

Dla $n \geq 1$ mamy następującą równość w $\mathbb{Q}[x]$ oraz w pierścieniu grupowym $\mathbb{Q}[\Gamma]$:

$$1 + x + x^2 + \ldots + x^n = \sum_{j=0}^{n} 2^{j-n-1}(1 + x^j)(1 + x)^{n-j}. \tag{3}$$

Dowód.

Indukcja po n. □

Definicja 1.5.

Dla elementu $\sum_{g\in\Gamma} N_g g$ pierścienia grupowego $\mathbb{Q}[\Gamma]$ oraz liczby $n \in \mathbb{Q}$ piszemy

$$\sum_{g\in\Gamma} N_g g \succeq n \text{ wtedy i tylko wtedy gdy } N_1 \geq n.$$

Twierdzenie 1.1 w notacji mltiplikatywnej jest równoważne stwierdzeniu:

Dla każdej skończonej grupy abelowej Γ i dla dowolnych $a_1, \ldots, a_k \in \Gamma$ oraz dla dowolnych całkowitych $b_1, \ldots, b_k$ mamy

$$\prod_{i=1}^{k}(1 + a_i + \ldots + {a_i}^{b_i}) \succeq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1), \tag{4}$$

gdzie $D(\Gamma)$ jest stałą Dawenporta grupy Γ.

Dowód.

Interpretujemy równanie $\prod_{i=1}^{k}(1 + a_i + \ldots + {a_i}^{b_i}) = \sum_{g \in \Gamma} N_g g$ kombinatorycznie.
Rozważmy ciągi ${a_1}^{x_1}, {a_2}^{x_2}, \ldots, {a_k}^{x_k}$, które mają iloczyn równy 1 w Γ, gdzie $x_i \leq b_i$ to nieujemne liczby całkowite.
Zauważmy, że N_1 zlicza właśnie takie ciągi.
Zatem liczba rozwiązań równania $\prod_{i=1}^{k} {a_i}^{x_i} = 1$ w nieujemnych liczbach całkowitych $x_i \leq b_i$ jest równa N_1.
Wynika stąd, że

$$N_1 \geq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1)$$

wtedy i tylko wtedy gdy (4) zachodzi. □

Lemat 1.6.

Niech Γ będzie skończoną grupą abelową.
Dla dowolnych $a_1, \ldots, a_k \in \Gamma$ mamy

$$(1 + a_1) \cdot \ldots \cdot (1 + a_k) \succeq 2^{1-D(\Gamma)} \cdot 2^k. \tag{5}$$

Dowód

Dla pełności ekspozycji przytoczymy dowód Olson'a (patrz [3]).
Dowód będzie indukcją ze względu na k.
Dla $k \leq D(\Gamma) - 1$ mamy

$$(1 + a_1) \cdot \ldots \cdot (1 + a_k) \succeq 1 \geq 2^{1-D(\Gamma)} \cdot 2^k$$

i relacja jest prawdziwa.
Załóżmy, że relacja jest prawdziwa dla liczby czynników mniejszej od k, gdzie $k > D(\Gamma) - 1$.

Dowód c.d

Zatem $k \geq D(\Gamma)$.
Z definicji stałej Dawenporta możemy założyć, bez straty dla ogólności rozważań, że

$$a_1 \cdot \ldots \cdot a_t = 1 \text{ dla pewnego } 1 \leq t \leq D(\Gamma).$$

Z założenia indukcyjnego

$$\prod_{i=2}^{t}(1 + {a_i}^{-1}) \prod_{i=t+1}^{k}(1 + a_i) \succeq 2^{1-D(\Gamma)} \cdot 2^{k-1},$$

$$\prod_{i=2}^{k}(1 + a_i) \succeq 2^{1-D(\Gamma)} \cdot 2^{k-1}.$$

Dowód c.d

Zatem

$$\prod_{i=1}^{k}(1+a_i) = \prod_{i=2}^{k}(1+a_i) + a_1 \prod_{i=2}^{k}(1+a_i)$$

$$= \prod_{i=2}^{k}(1+a_i) + a_1 \cdot \ldots \cdot a_t \prod_{i=2}^{t}(1+a_i{}^{-1}) \prod_{i=t+1}^{k}(1+a_i)$$

$$= \prod_{i=2}^{k}(1+a_i) + \prod_{i=2}^{t}(1+a_i{}^{-1}) \prod_{i=t+1}^{k}(1+a_i)$$

$$\succeq 2^{1-D(\Gamma)} \cdot 2^{k-1} + 2^{1-D(\Gamma)} \cdot 2^{k-1} = 2^{1-D(\Gamma)} \cdot 2^{k}.$$

Dowód Twierdzenia 1.1

Trzeba pokazać, że:

Dla każdej skończonej grupy abelowej Γ i dla dowolnych $a_1, \ldots, a_k \in \Gamma$ oraz dla dowolnych całkowitych $b_1, \ldots, b_k$ mamy

$$\prod_{i=1}^{k}(1 + a_i + \ldots + {a_i}^{b_i}) \succeq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1), \tag{6}$$

gdzie $D(\Gamma)$ jest stałą Dawenporta grupy Γ.

Dowód Twierdzenia 1.1

Korzystając z tożsamości (3) dostajemy

$$\prod_{i=1}^{k}(1+a_i+\ldots+{a_i}^{b_i}) = \prod_{i=1}^{k}\sum_{j=0}^{b_i} 2^{j-b_i-1}(1+{a_i}^{j})(1+a_i)^{b_i-j} \qquad (7)$$

$$= \sum_{\substack{0\le j_1\le b_1\\ 0\le j_2\le b_2\\ \vdots\\ 0\le j_k\le b_k}} \prod_{i=1}^{k} 2^{j_i-b_i-1}(1+{a_i}^{j_i})(1+a_i)^{b_i-j_i}.$$

Dowód Twierdzenia 1.1 c.d.

Z lematu (1.6) mamy

$$\sum_{\substack{0\le j_1\le b_1\\ 0\le j_2\le b_2\\ \vdots\\ 0\le j_k\le b_k}} \prod_{i=1}^{k} 2^{j_i-b_i-1}(1+a_i^{j_i})(1+a_i)^{b_i-j_i}$$

$$\succeq 2^{1-D(\Gamma)} \sum_{\substack{0\le j_1\le b_1\\ 0\le j_2\le b_2\\ \vdots\\ 0\le j_k\le b_k}} \prod_{i=1}^{k} 2^{j_i-b_i-1}2^{1+b_i-j_i} = 2^{1-D(\Gamma)} \sum_{\substack{0\le j_1\le b_1\\ 0\le j_2\le b_2\\ \vdots\\ 0\le j_k\le b_k}} 1$$

$$= 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i+1).$$

Dowód Twierdzenia 1.1 c.d.

Zatem

$$\prod_{i=1}^{k}(1 + a_i + \ldots + {a_i}^{b_i}) \succeq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1).$$

Twierdzenie (1.1) można przepisać w następującej postaci:

Niech $n_1 \mid n_2 \mid \ldots \mid n_l$ liczby całkowite dodatnie, a_{ij} liczby całkowite, b_i liczby całkowite dodatnie, gdzie $1 \leq i \leq k$, $1 \leq j \leq l$, wtedy liczba rozwiązań układu kongruencji

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \ldots + a_{k1}x_k \equiv 0 \pmod{n_1}, \\ a_{12}x_1 + a_{22}x_2 + \ldots + a_{k2}x_k \equiv 0 \pmod{n_2}, \\ \vdots \\ a_{1l}x_1 + a_{2l}x_2 + \ldots + a_{kl}x_k \equiv 0 \pmod{n_l}, \end{cases}$$

w nieujemnych $x_i \leq b_i$, jest co najmniej

$$2^{1-D(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_l})} \prod_{i=1}^{k} (b_i + 1).$$

Uwagi historyczne

Andrzej Schinzel w pracy [4], postawił hipotezę dotyczącą przypadku jednej kongruencji:
Niech $n \in \mathbb{N}$, $a_i \in \mathbb{Z}$ i $b_i \in \mathbb{N}\,(1 \leq i \leq k)$.
Liczba $N(n; a_1, b_1; \ldots; a_k, b_k)$ rozwiązań kongruencji

$$\sum_{i=1}^{k} a_i x_i \equiv 0 \,(\mathrm{mod}\ n), \ \text{gdzie } 0 \leq x_i \leq b_i$$

spełnia nierówność $N(n; a_1, b_1; \ldots; a_k, b_k) \geq 2^{1-n} \prod_{i=1}^{k} (b_i + 1)$.
Ponieważ dla $k = n - 1$

$$N(n; \underbrace{1, 1; \ldots; 1, 1}_{n-1 \text{ razy}}) = 1 = 2^{1-n} \prod_{i=1}^{k} (1 + 1).$$

Zatem 2^{1-n} jest najlepszym możliwym współczynnikiem niezależnym od a_i, b_i, a zależnym tylko od n.

Jest to szczególny przypadek Twierdzenia (1.1) gdy Γ to grupa cykliczna $\mathbb{Z}_n$.
W pracy [4] zostały udowodnione dwa twierdzenia,
pierwsze dotyczące przypadku jednej kongruencji (nierówność zachodzi, przy dodatkowym założeniu, że $(a_i, n) = 1$ dla wszystkich $i \leq k$),
oraz drugie dotyczące ogólnego przypadku grup abelowych:
dla każdej skończonej grupy abelowej Γ, oraz każdego wektora $[a_1, \ldots, a_k] \in \Gamma^k$, liczba rozwiązań równania $a_1x_1 + \ldots + a_kx_k = 0$, w nieujemnych całkowitych $x_i \leq b_i$, jest co najmniej

$$2^{-(\tau(\chi(\Gamma))-1)(|\Gamma|-1)} \prod_{i=1}^{k} (b_i + 1),$$

gdzie $\tau(\chi(\Gamma))$ liczba dzielników charakterystyki Γ.

Następnie we wspólnej pracy z A. Schinzlem [6] pokazaliśmy, że w przypadku jednej kongruencji modulo n, ze współczynnikami a_i, twierdzenie zachodzi przy dodatkowym założeniu, że dla dowolnych $i, j \leq k$ albo $(a_i, n)|(a_j, n)$ lub $(a_j, n)|(a_i, n)$ lub $n|[a_i, a_j]$.

Schinzel w pracy [5] udowodnił między innymi następujące twierdzenie.

Niech $n = \prod_{\lambda=1}^{l} q_\lambda^{\alpha_\lambda}$, gdzie q_λ to różne liczby pierwsze, $\alpha_\lambda > 0$ oraz

$$\sum_{\lambda=1}^{l} \frac{1}{q_\lambda} \leq 1 + \frac{\min\{l, 2l-5\}}{n}.$$

Niech a_i, b_i całkowite, $b_i > 0, 1 \leq i \leq k$.
Wtedy liczba $N(n; a_1, b_1; \ldots; a_k, b_k)$ rozwiązań kongruencji

$$\sum_{i=1}^{k} a_i x_i \equiv 0 \pmod{n}, \text{ gdzie } 0 \leq x_i \leq b_i$$

spełnia nierówność

$$N(n; a_1, b_1; \ldots; a_k, b_k) \geq 2^{1-n} \prod_{i=1}^{k} (b_i + 1).$$

Twierdzenie to pociąga za sobą Twierdzenie (1.1) sformułowane na wstępie w przypadku jednej kongruencji modulo n, czyli równoważnie grupy $\mathbb{Z}_n$, dla n o gęstości 0.94, ponadto dla $n < 60$, lub $k < 16$ (patrz [5]).

W aneksie do pracy Schinzla [5] Jerzy Kaczorowski pokazał, że

$$N(n; a_1, b_1; \ldots; a_k, b_k) \geq \frac{1}{n^{\binom{n+k-1}{k}}} \prod_{i=1}^{k} (b_i + 1).$$

W kolejnej pracy Karol Cwalina i Tomasz Schoen [1] pokazali, że Twierdzenie (1.1) zachodzi dla jednej kongruencji modulo n, tym samym zakończyli dowód Twierdzenia (1.1) w szczególnym przypadku grupy cyklicznej $\mathbb{Z}_n$, z najlepszym możliwym współczynnikiem 2^{1-n}.

W pracy Olsona [3] znajduje się dowód nierówności z Twierdzenia (1.1), dla dowolnej grupy abelowej Γ, ale w szczególnym przypadku $b_1 = b_2 = \ldots = b_k = 1$, co sugeruje, że właściwym wykładnikiem jest $1 - D(\Gamma)$, patrz także Schinzel([4],p.364).
Ostatecznie, w pracy [8], używając zupełnie innej metody udowodniłem Twierdzenie (1.1).
W kolejnej pracy [9], która jest obecnie w recenzji w Colloquium Mathematicum, rozważałem przypadek równania niejednorodnego.

Przypadek niejednorodny

Przypadkiem niejednorodnym zajmowałem się w pracy [9] pokazując dwa twierdzenia:

Twierdzenie 2.1.

Dla każdej skończonej grupy abelowej Γ oraz dowolnych $g, a_1, \ldots, a_k \in \Gamma$, jeśli istnieje rozwiązanie równania $\sum_{i=1}^{k} a_i x_i = g$ w nieujemnych całkowitych $x_i \leq b_i$, gdzie b_i są całkowite dodatnie, wtedy liczba takich rozwiązań jest co najmniej

$$3^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1). \tag{8}$$

Uwaga

Niech $\Gamma = n\mathbb{Z}_2$ będzie sumą prostą n grup cyklicznych rzędu 2, $a_1, a_2, \ldots, a_n$ będzie bazą dla Γ.

Wtedy liczba rozwiązań równania $\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i$ w nieujemnych liczbach całkowitych $x_i \leq b_i = 2$, wynosi 1.

Ponieważ $D(\Gamma) = n + 1$ (patrz Olson [1]) oraz $1 = 3^{1-D(\Gamma)} \prod_{i=1}^{n}(2+1)$.

Otrzymujemy, że $3^{1-D(\Gamma)}$ jest najlepszym możliwym współczynnikiem niezależnym od a_i, b_i, g, a zależnym tylko od Γ.

Twierdzenie 2.3.

Dla każdej skończonej grupy abelowej Γ, oraz dowolnych $g, a_1, \ldots, a_k \in \Gamma$, jeśli istnieje rozwiązanie równania $\sum_{i=1}^{k} a_i x_i = g$ w nieujemnych całkowitych $x_i \leq b_i$, gdzie $b_i \in \{2^s - 1 : s \in \mathbb{N}\}$, wtedy liczba takich rozwiązań jest co najmniej

$$2^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1). \tag{9}$$

Lemat 2.4.

Dla każdej skończonej grupy abelowej Γ i dla wszystkich $a_1, \ldots, a_k, g \in \Gamma$, liczba rozwiązań równania $\prod_{i=1}^{k} {a_i}^{x_i} = g$ w nieujemnych całkowitych $x_i \leq b_i$ jest równa N_1, gdzie

$$g^{-1} \prod_{i=1}^{k} (1 + a_i + \ldots + {a_i}^{b_i}) = \sum_{h \in \Gamma} N_h h,$$

jest tożsamością w $\mathbb{Q}[\Gamma]$.

Dowód.

Interpretujemy równanie $g^{-1}\prod_{i=1}^{k}(1+a_i+\ldots+{a_i}^{b_i})=\sum_{h\in\Gamma}N_h h$ kombinatorycznie.
Dla $g\in\Gamma$ rozważmy ciągi ${a_1}^{x_1}, {a_2}^{x_2},\ldots,{a_k}^{x_k}$, które mają iloczyn g, gdzie $x_i\leq b_i$ są nieujemnymi liczbami całkowitymi.
Wtedy N_1 zlicza te ciągi.
Zatem liczba rozwiązań równania $\prod_{i=1}^{k}{a_i}^{x_i}=g$ w nieujemnych liczbach całkowitych $x_i\leq b_i$ jest równa N_1. □

Twierdzenie 3.1 w multiplikatywnej notacji jest równoważne stwierdzeniu:

Dla każdej skończonej grupy abelowej Γ, dla wszystkich $g, a_1, \ldots, a_k \in \Gamma$, jeśli istnieje rozwiązanie równania $\prod_{i=1}^{k} {a_i}^{x_i} = g$ w nieujemnych całkowitych $x_i \leq b_i$, gdzie b_i są dodatnimi liczbami całkowitymi, wtedy zachodzi relacja:

$$g^{-1} \prod_{i=1}^{k} (1 + a_i + \ldots + {a_i}^{b_i}) \succeq 3^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1), \tag{10}$$

gdzie $D(\Gamma)$ jest stałą Dawenporta grupy Γ.

Dowód.

Wynika z Lematu 3.4 i Definicji 1.5. □

Twierdzenie 3.3 w multiplikatywnej notacji jest równoważne stwierdzeniu:

Dla każdej skończonej grupy abelowej Γ, dla wszystkich $g, a_1, \ldots, a_k \in \Gamma$ oraz dla wszystkich dodatnich całkowitych $b_1, b_2, \ldots, b_k \in \{2^s - 1 : s \in \mathbb{N}\}$, jeśli istnieje rozwiązanie równania $\prod_{i=1}^{k} {a_i}^{x_i} = g$ w nieujemnych całkowitych liczbach $x_i \leq b_i$, wtedy zachodzi relacja:

$$g^{-1} \prod_{i=1}^{k} (1 + a_i + \ldots + {a_i}^{b_i}) \succeq 2^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1). \tag{11}$$

Dowód.

Wynika z Lematu (3.4) i Definicji (1.5). □

Lemat 2.5.

Dla każdej skończonej grupy abelowej Γ oraz dla wszystkich $g, a_1, a_2, \ldots, a_k \in \Gamma$, jeśli istnieje rozwiązanie równania $\prod_{i=1}^{k} {a_i}^{x_i} = g$ w nieujemnych liczbach całkowitych $x_i \leq 1$, wtedy

$$g^{-1} \prod_{i=1}^{k} (1 + a_i) \succeq 2^{1-D(\Gamma)} \cdot 2^k. \tag{12}$$

Dowód.

Możemy założyć, że $\prod_{i=1}^{t} a_i = g$, gdzie $1 \leq t \leq k$.

Mamy tożsamości:

$$g^{-1}\prod_{i=1}^{k}(1+a_i) = g^{-1}\prod_{i=1}^{t} a_i \prod_{i=1}^{t}(1+a_i^{-1}) \prod_{i=t+1}^{k}(1+a_i) =$$

$$= \prod_{i=1}^{t}(1+a_i^{-1}) \prod_{i=t+1}^{k}(1+a_i).$$

□

Dowód.

Z Twierdzenia (1.1)

$$\prod_{i=1}^{t}(1+a_i^{-1})\prod_{i=t+1}^{k}(1+a_i) \succeq 2^{1-D(\Gamma)}2^k.$$

Zatem

$$g^{-1}\prod_{i=1}^{k}(1+a_i) \succeq 2^{1-D(\Gamma)}2^k.$$

□

Lemat 2.6.

Jeśli $0 \leq t < b$, *gdzie* t, b *są całkowite, wtedy* $b - t + 1 \geq (\frac{2}{3})^t(b+1)$.

Dowód.

Sprawdzamy, że funkcja $f(x) = 2(\frac{3}{2})^x - x - 2$ jest rosnąca w przedziale $(1, \infty)$. Ponieważ $f(0) = f(1) = 0, f(2) = \frac{1}{2}$ dostajemy $2(\frac{3}{2})^t \geq t + 2$ dla nieujemnych liczb całkowitych t.
Zatem $1 - \frac{t}{b+1} \geq 1 - \frac{t}{t+2} \geq (\frac{2}{3})^t$, więc $b - t + 1 \geq (\frac{2}{3})^t(b+1)$. $\square$

Lemat 2.7.

Dla $s \geq 1$ mamy następującą równość w pierścieniu grupowym $\mathbb{Q}[\Gamma]$:

$$1 + x + x^2 + \ldots + x^{2^s - 1} = \prod_{j=1}^{s} (1 + x^{2^{j-1}}). \tag{13}$$

Dowód.

Indukcja matematyczna ze względu na s.
Dla $s = 1$ mamy

$$1 + x = \prod_{j=1}^{1}(1 + x^{2^{j-1}})$$

i równość jest prawdziwa.
Załóżmy, że równość jest prawdziwa dla $s - 1$, gdzie $s > 1$.
Wtedy dla s mamy kolejno

$$1 + x + x^2 + \ldots + x^{2^s - 1} = (1 + x^{2^{s-1}})(1 + x + x^2 + \ldots + x^{2^{s-1}-1}) =$$

$$= (1 + x^{2^{s-1}}) \prod_{j=1}^{s-1}(1 + x^{2^{j-1}}) = \prod_{j=1}^{s}(1 + x^{2^{j-1}}),$$

czyli równość zachodzi. □

Dowód Twierdzenia 3.1

Trzeba pokazać, że:

Dla każdej skończonej grupy abelowej Γ, dla wszystkich $g, a_1, \ldots, a_k \in \Gamma$, jeśli istnieje rozwiązanie równania $\prod_{i=1}^{k} {a_i}^{x_i} = g$ w nieujemnych całkowitych $x_i \leq b_i$, gdzie b_i są dodatnimi liczbami całkowitymi, wtedy zachodzi relacja:

$$g^{-1} \prod_{i=1}^{k} (1 + a_i + \ldots + {a_i}^{b_i}) \succeq 3^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1), \tag{14}$$

gdzie $D(\Gamma)$ jest stałą Dawenporta grupy Γ.

Dowód Twierdzenia 3.1

Możemy znaleźć $0 \leq t_i \leq b_i$, gdzie $1 \leq i \leq k$, takie że
${a_1}^{t_1} {a_2}^{t_2} \cdot \ldots \cdot {a_k}^{t_k} = g$.
Z definicji stałej Dawenporta, możemy założyć,że:

$$\sum_{i=1}^{k} t_i \leq D(\Gamma) - 1. \tag{15}$$

Niech $t_i = b_i$ dla $1 \leq i \leq s \leq k$; $t_i < b_i$ dla $s+1 \leq i \leq k$;
jeśli $t_i < b_i$ dla $1 \leq i \leq k$, wtedy weźmy $s = 0$.

Mamy równania

$$g^{-1}\prod_{i=1}^{s}(1+a_i+\ldots+a_i^{b_i})\prod_{i=s+1}^{k}({a_i}^{t_i}+{a_i}^{t_i+1}+\ldots+a_i^{b_i})=$$

$$=\Big(\Big(\prod_{i=1}^{s}a_i^{b_i}\Big)\Big(\prod_{i=s+1}^{k}a_i^{t_i}\Big)\Big)^{-1}\prod_{i=1}^{s}(1+a_i+\ldots+a_i^{b_i})\cdot$$

$$\cdot\prod_{i=s+1}^{k}({a_i}^{t_i}+{a_i}^{t_i+1}+\ldots+a_i^{b_i})=$$

$$=\prod_{i=1}^{s}(1+a_i^{-1}+\ldots+(a_i^{-1})^{b_i})\prod_{i=s+1}^{k}(1+a_i+\ldots+{a_i}^{b_i-t_i}).$$

Z Twierdzenia 1.1

$$\prod_{i=1}^{s}(1+a_i^{-1}+\ldots+(a_i^{-1})^{b_i})\prod_{i=s+1}^{k}(1+a_i+\ldots+{a_i}^{b_i-t_i})\succeq$$

$$\succeq 2^{1-D(\Gamma)}\Big(\prod_{i=1}^{s}(b_i+1)\Big)\Big(\prod_{i=s+1}^{k}(b_i-t_i+1)\Big).$$

Mamy z Lematu 3.6, że

$$2^{1-D(\Gamma)}\Big(\prod_{i=1}^{s}(b_i+1)\Big)\Big(\prod_{i=s+1}^{k}(b_i-t_i+1)\Big) \geq$$

$$\geq 2^{1-D(\Gamma)}\Big(\prod_{i=1}^{s}(b_i+1)\Big)\Big(\prod_{i=s+1}^{k}(\tfrac{2}{3})^{t_i}(b_i+1)\Big) =$$

$$= 2^{1-D(\Gamma)}(\tfrac{2}{3})^{\sum_{i=s+1}^{k} t_i}\prod_{i=1}^{k}(b_i+1) \geq 2^{1-D(\Gamma)}(\tfrac{2}{3})^{\sum_{i=1}^{k} t_i}\prod_{i=1}^{k}(b_i+1).$$

Ponieważ (15) zatem dalej

$$2^{1-D(\Gamma)}\left(\tfrac{2}{3}\right)^{\sum_{i=1}^{k} t_i}\prod_{i=1}^{k}(b_i+1) \geq$$

$$\geq 2^{1-D(\Gamma)}\left(\tfrac{2}{3}\right)^{D(\Gamma)-1}\prod_{i=1}^{k}(b_i+1) = 3^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1).$$

Skąd

$$g^{-1}\prod_{i=1}^{s}(1+a_i+\ldots+a_i^{b_i})\prod_{i=s+1}^{k}({a_i}^{t_i}+{a_i}^{t_i+1}+\ldots+a_i^{b_i})\succeq 3^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1).$$

Ostatecznie

$$g^{-1}\prod_{i=1}^{k}(1+a_i+\ldots+a_i^{b_i})\succeq 3^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1).$$

Dowód Twierdzenia 3.3

Niech $b_i = 2^{s_i} - 1$, gdzie $s_i \in \mathbb{N}$.
Bierzemy $0 \leq t_i \leq b_i$, gdzie $1 \leq i \leq k$ takie, że $a_1^{t_1} a_2^{t_2} \cdot \ldots \cdot a_k^{t_k} = g$.
Ponieważ $0 \leq t_i \leq 2^{s_i} - 1$ możemy znaleźć $\epsilon_{ji} \in \{0, 1\}$ takie, że

$$t_i = \sum_{j=1}^{s_i} \epsilon_{ji} 2^{j-1}$$

dla $1 \leq i \leq k$.

Używając (13) z Lematu (3.7) otrzymujemy

$$a_i^{-t_i}(1 + a_i + \ldots + a_i^{b_i}) = a_i^{-t_i} \prod_{j=1}^{s_i}(1 + a_i^{2^{j-1}}) =$$

$$= a_i^{-\sum_{j=1}^{s_i} \epsilon_{ji} 2^{j-1}} \prod_{j=1}^{s_i}(1 + a_i^{2^{j-1}}) = \prod_{j=1}^{s_i} a_i^{-\epsilon_{ji} 2^{j-1}} \prod_{j=1}^{s_i}(1 + a_i^{2^{j-1}}) =$$

$$= \prod_{j=1}^{s_i} a_i^{-\epsilon_{ji} 2^{j-1}}(1 + a_i^{2^{j-1}}) =$$

$$= \prod_{j=1}^{s_i}(a_i^{-\epsilon_{ji} 2^{j-1}} + a_i^{(1-\epsilon_{ji})2^{j-1}}) = \prod_{j=1}^{s_i}(1 + a_i^{\eta_{ji} 2^{j-1}}),$$

gdzie $\eta_{ji} = 1 - 2\epsilon_{ji} \in \{-1, 1\}$.

Zatem

$$g^{-1}\prod_{i=1}^{k}(1+a_i+\ldots+{a_i}^{b_i}) = \prod_{i=1}^{k} a_i^{-t_i}(1+a_i+\ldots+{a_i}^{b_i}) = \prod_{i=1}^{k}\prod_{j=1}^{s_i}(1+a_i^{\eta_{ji}2^{j-1}}).$$

Z Twierdzenia (1.1)

$$\prod_{i=1}^{k}\prod_{j=1}^{s_i}(1+a_i^{\eta_{ji}2^{j-1}}) \succeq 2^{1-D(\Gamma)}\prod_{i=1}^{k}\prod_{j=1}^{s_i}2 = 2^{1-D(\Gamma)}\prod_{i=1}^{k}2^{s_i} =$$

$$= 2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1),$$

co daje

$$g^{-1}\prod_{i=1}^{k}(1+a_i+\ldots+{a_i}^{b_i}) \succeq 2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1).$$

[1.] Karol CWALINA and Tomasz SCHOEN, *The number of solutions of a homogeneous linear congruence*, Acta Arith. 153 (2012), pp. 271-279.

[2.] John E. OLSON, *A Combinatorial Problem on Finite Abelian Groups,I.* J. Number Theory 1, (1969), pp. 8-10.

[3.] John E. OLSON, *A Combinatorial Problem on Finite Abelian Groups,II.* J. Number Theory 1, (1969), pp. 195-199.

[4.] Andrzej SCHINZEL, *The number of solutions of a linear homogeneous congruence.* Diophantine Approximation: Festschrift for Wolfgang Schmidt (H.-P.Schlickewei, K. Schmidt, R.F. Tichy, eds.), pp. 363-370 (Developments in Mathematics 16, Springer-Verlag, 2008).

[5.] Andrzej SCHINZEL, *The number of solutions of a linear homogeneous congruence II.* In: Chen,W., Gowers, T., Halberstam, H., Schmidt, W., Vaughan, R.C. (eds.) Analytical Number Theory: Essays in Honour of Klaus F. Roth. Cambridge University Press, 2009, pp. 402-413, with appendix by Jerzy KACZOROWSKI.

[6.] Andrzej SCHINZEL and Maciej ZAKARCZEMNY, *On a linear homogeneous congruence.*, Colloq. Math., 106 (2006), pp. 283-292.

[7.] Michael DRMOTA i Mariusz SKAŁBA, *Equidistribution of Divisors modulo m.* Preprint.(1997).

[8.] Maciej ZAKARCZEMNY, *Number of solutions in a box of a linear homogeneous equation in an Abelian group*, Acta Arith. 155 (2012), pp. 227-231.

[9.] Maciej ZAKARCZEMNY, *Number of solutions in a box of a linear equation in an Abelian group*, (to appear).

Dziękuję za uwagę

Bibliografia uzupełniająca

[10.] W.R. ALFORD, Andrew GRANVILLE and Carl POMERANCE, *There are infinitely many Carmichael numbers*, Annals of Mathematics, 140 (1994), pp. 703-722.

[11.] Emre ALKAN, *Davenport constant for finite abelian group*, Indag. Mathem.,19(1), pp. 1-21.

[12.] Gerard Jennhwa CHANG, Sheng-Hua CHEN, Yongke QU, Guoqing WANG, and Haiyan ZHANG, *On the number of subsequences with a given sum in a finite abelian group*, The Electronic Journal of Combinatorics 18 (2011).

[13.] Harold DAVENPORT, *Proceedings of the Midwestern Conference on Group Theory and Number Theory*, Ohio State Univ., (1966).

[14.] Weidong GAO, Alfred GEROLDINGER, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math.24 (2006).

[15.] Alfred GEROLDINGER, Franz HALTER-KOCH, *Non-Unique Factorizations, Algebraic, Combinatorial and Analytic Theory*, volume 278 of Pure and Applied Mathematics. Chapman & Hall/CRC, (2006).

[16.] Alfred GEROLDINGER, Rudolf SCHNEIDER, *On Davenport's constant*, J. Combin. Theory Ser. A 61 (1992).

[17.] Roy MESHULAM, *An uncertainty inequality and zero subsums*, Discrete Mathematics 84 (1990) pp. 197-200.

[18.] Władysław NARKIEWICZ, J. ŚLIWA, *Finite abelian groups and factorization problems II*, Colloq. Math., 46(1)(1982), pp. 115-122.

[19.] Peter van EMDE BOAS, *A combinatorial problem on finite abelian groups II*, Raports ZW-1969-007, Mathematical Centre, Amsterdam, (1969).

[20.] Peter van EMDE BOAS, D. KRUYSWIJK, *A combinatorial problem on finite abelian groups III*, Raports ZW-1969-008, Mathematical Centre, Amsterdam, (1969).

O stałej Dawenporta

Stała Dawenporta

Definujemy *stałą Dawenporta* $D(\Gamma)$ jako najmniejszą dodatnią liczbę całkowitą n taką, że dla każdego ciągu $g_1, \ldots, g_n$ elementów skończonej grupy Abelowej Γ, istnieje niepusty ciąg indeksów

$$1 \leq i_1 < \ldots < i_t \leq n$$

takich, że w grupie Γ zachodzi równość:

$$g_{i_1} + \ldots + g_{i_t} = 0.$$

Dla przykładu:
Niech $\mathbb{Z}_{n_1}$ będzie grupą cykliczna o rzędzie n_1 wtedy $D(\mathbb{Z}_{n_1}) = n_1$.
Niech $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ będzie sumą prostą grup cyklicznych o rzędach odpowiednio n_1, n_2 gdzie $n_1 | n_2$ wtedy $D(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}) = n_1 + n_2 - 1$, patrz John E.Olson [2], [3].

Stała Dawenporta oszacowania

Niech $\Gamma = \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_r}$, oraz niech $g_1, \ldots, g_r$ baza Γ, gdzie $ord(g_i) = n_i$ dla $1 \leq i \leq r$. Wtedy ciąg

$$\underbrace{g_1, \ldots, g_1}_{n_1-1}, \underbrace{g_2, \ldots, g_2}_{n_2-1}, \ldots, \underbrace{g_r, \ldots, g_r}_{n_r-1},$$

nie ma podciągu niepustego o sumie równej 0.
Zatem:

$$D(\Gamma) - 1 \geq \sum_{i=1}^{r} (n_i - 1).$$

Stała Dawenporta oszacowania

W 1960, D.Kruyswijk i J.E. Olson udowodnili niezależnie następujący rezultat:

Twierdzenie 3.12. *Jeśli* Γ *jest* $p-$*grupą lub* $r(\Gamma) \leq 2$, *to*

$$D(\Gamma) - 1 = \sum_{i=1}^{r}(n_i - 1).$$

Stała Dawenporta oszacowania

P.van Emde Boas, A combinatorial problem on finite abelian groups II, Raports ZW-1969-007, Mathematical Centre, Amsterdam, 1969.

$$D(\Gamma) - 1 > \sum_{i=1}^{r} (n_i - 1) \text{ dla } \Gamma = \mathbb{Z}_2^{4k} \oplus \mathbb{Z}_{4k+2}, \text{ gdzie } k \text{ cakowite dodatnie.}$$

Stała Dawenporta oszacowania

Potem pokazano, że dla każdego $r \geq 4$ jest nieskończenie wiele grup z $r(\Gamma) = r$ oraz $D(\Gamma) - 1 > \sum_{i=1}(n_i - 1)$.

A.Geroldinger, R.Schneider, On Davenport's constant, J. Combin. Theory Ser. A 61 (1992)

Twierdzenie 3.13. *Mamy* $D(\Gamma) - 1 > \sum_{i=1}^{r}(n_i - 1)$ *w każdym z następujących przypadków:*

1. $\Gamma = \mathbb{Z}_m \oplus \mathbb{Z}_n^2 \oplus \mathbb{Z}_{2n}$, *gdzie* $m, n \geq 3$ *są nieparzyste oraz* $m|n$.
2. $\Gamma = \mathbb{Z}_2^i \oplus \mathbb{Z}_{2n}^{5-i}$, *gdzie* $n \geq 3$ *jest nieparzyste oraz* $2 \leq i \leq 4$.
3. $\Gamma = \mathbb{Z}_2^3 \oplus \mathbb{Z}_{2m} \oplus \mathbb{Z}_{2n}$, *gdzie* $m \geq 1$, $n \geq 3$ *są nieparzyste oraz* $m|n$.
4. $\Gamma = \mathbb{Z}_n^n \oplus \mathbb{Z}_{nm}$, *gdzie* $n, m \geq 2$, $m|n - 1$.

Stała Dawenporta oszacowania

Przykład:

Niech $\Gamma = \mathbb{Z}_3^3 \oplus \mathbb{Z}_6$, natomiast $\{e_1, e_2, e_3, e_4\}$ zbiór generatorówΓ, gdzie $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = \mathrm{ord}(e_3) = 3, \mathrm{ord}(e_4) = 6$.
Ponadto niech
$g_1 = -e_1 + e_2 + e_3 + e_4$, $g_2 = e_1 - e_2 + e_3 + e_4$, $g_3 = e_1 + e_2 - e_3 + e_4$,
$g_4 = -e_1 + e_2 + e_3 - e_4$, $g_5 = e_1 + e_2 + e_3 + e_4$,
$g_6 = e_2 - e_3 - e_4$, $g_7 = -e_2 + e_3 - e_4$.
Wtedy ciąg $g_1, g_1, g_2, g_2, g_3, g_3, g_4, g_4, g_5, g_5, g_6, g_7$ nie ma niepustego podciągu o sumie 0 w $\mathbb{Z}_3^3 \oplus \mathbb{Z}_6$.

Przykład:

Niech $\Gamma = \mathbb{Z}_2^4 \oplus \mathbb{Z}_6$, natomiast $\{e_1, e_2, e_3, e_4, e_5\}$ zbiór generatorówΓ, gdzie $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = \mathrm{ord}(e_3) = \mathrm{ord}(e_4) = 2, \mathrm{ord}(e_5) = 6$.
Ponadto niech
$g_i = e_i + e_5$, dla $1 \leq i \leq 4$, $g_5 = e_2 + e_3 + e_4 + e_5$,
$g_6 = e_1 + e_3 + e_4 + e_5$, $g_7 = e_1 + e_2 + e_4 + e_5$, $g_8 = e_1 + e_2 + e_3 + 2e_5$
Wtedy ciąg $g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_8, g_8$ nie ma niepustego podciągu o sumie 0 w $\mathbb{Z}_2^4 \oplus \mathbb{Z}_6$.

Stała Dawenporta oszacowania

Twierdzenie 3.14. *Niech* $\Gamma = \mathbb{Z}_2^r \oplus \mathbb{Z}_n$, *gdzie* $n \geq 3$ *nieparzyste. Wtedy* $D(\Gamma) - 1 = \sum_{i=1}^{r}(n_i - 1)$, *wtedy i tylko wtedy gdy* $r \leq 4$.

Hipoteza 3.15. Jeśli $r(\Gamma) = 3$ lub $\Gamma = \mathbb{Z}_n^r$, gdzie $n, r \geq 3$, to $D(\Gamma) - 1 = \sum_{i=1}^{r}(n_i - 1)$.

Stała Dawenporta oszacowania

Górne oszacowania na stałą Davenporta.

Van Emde Boas and Kruyswijk i Meshulam

Twierdzenie 3.16. *Niech $n \geq 2$ wykładnik Γ.*
$D(\Gamma) \leq n + \lfloor n \log \frac{|\Gamma|}{n} \rfloor$.*(Dokładne dla grup cyklicznych.)*

Hipoteza 3.17. (znacznie lepsze niż dotychczas znane ograniczenie):
Jeśli $|G| > 1$, $r(\Gamma) = r$, to $D(\Gamma) \leq \sum_{i=1}^{r}(n_i - 1) + r = \sum_{i=1}^{r} n_i$.

R.B. Eggleton and P.Erdös, Two combinatorial problems in group theory, Acta Arith. **21**(1972),111-116.

Twierdzenie 3.18. *Jeśli Γ niecykliczna grupa abelowa, to $D(\Gamma) \leq \frac{1}{2}|G| + 1$.*

Notacja multiplikatywna

Działanie wewnętrzne

Działaniem wewnętrznym (lub krócej działaniem) w zbiorze A nazywamy dowolne odwzorowanie produktu kartezjańskiego AxA w zbiór A. Innymi słowy mówimy, że w zbiorze A określone jest działanie wewnętrzne, jeśli każdej parze uporządkowanej (a,b) elementów zbioru A przyporządkowany jest dokładnie jeden element zbioru A (zwany wynikiem działania na elementach a i b).

Jeżeli *:AxA→A jest działaniem wewnętrznym w A, to zazwyczaj wynik działania $*$ na elementach a,b∈A oznaczamy przez: a*b (nie zaś przez *(a,b)).

Dla oznaczenia działań wewnętrznych stosujemy często symbole: $*, +, \cdot$. W przypadku użycia symbolu $+$ mówić możemy o notacji addytywnej (działanie nazywamy wówczas dodawaniem, zaś wynik - sumą); w przypadku użycia $\cdot$ o multiplikatywnej (działanie nazywamy mnożeniem, zaś wynik iloczynem). Przy stosowaniu notacji multiplikatywnej często symbol działania pomija się, tzn. zamiast $a \cdot b$ piszemy ab.

Działanie zewnętrzne

Niech A i F będą dowolnymi zbiorami niepustymi. Działaniem zewnętrznym w zbiorze A nazywamy dowolne odwzorowanie produktu kartezjańskiego FxA w zbiór A. Zbiór F nazywamy zbiorem operatorów.

Grupa abelowa

Grupę $(G, +)$ nazywamy **abelową**, gdy dla każdych $a, b \in G$ zachodzi:

Przemienność

$a + b = b + a$

Łączność

$(a + b) + c = a + (b + c)$

Istnienie elementu neutralnego

$\exists_e a + e = a$

Istnienie elementu przeciwnego

$\forall_a \exists_b a + b = e$, gdzie e jest elementem neutralnym

Fundamentalne twierdzenie o skończonych grupach abelowych

Niech Γ będzie skończoną grupą abelową. Dla n całkowitego dodatniego, niech $\mathbb{Z}_n$ oznacza cykliczną grupę z n elementami. Na podstawie Fundamentalnego Twierdzenia dla Skończonych Grup Abelowych mamy

$$\Gamma \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r} \cong \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \ldots \oplus \mathbb{Z}_{q_s},$$

gdzie $r = r(\Gamma)$ to ranga Γ, $s = s(\Gamma)$ to całkowita ranga Γ, $n_1, \ldots, n_r$, to liczby całkowite takie, że $1 < n_1 | n_2 | \ldots | n_r$ oraz $q_1, g_2 \ldots, q_s$ to potęgi liczb pierwszych. Ponadto $n_1, \ldots, n_r, q_1, g_2 \ldots, q_s$ są jednoznacznie wyznaczone przez Γ. Ponadto n_r to wykładnik Γ. Niech s całkowite dodatnie, elementy $g_1, \ldots, g_s$ z Γ są niezależne jeśli $g_i \neq 0$ dla $1 \leq i \leq s$ i dla dowolnych $m_1, m_2, \ldots, m_s \in \mathbb{Z}$,

$$\sum_{i=1}^{s} m_i g_i = 0 \text{ implikuje } m_1 g_1 = \ldots = m_s g_s = 0.$$

Ponadto tworzą bazę jeśli są niezależne oraz $\Gamma = \langle g_1 \rangle \oplus \ldots \oplus \langle g_s \rangle$.

Pierścień

Pojęcie pierścienia.

Definicja *Niech R będzie zbiorem niepustym.*

(1) *Algebrę $(R, +, \cdot)$ nazywamy* **pierścieniem,** *gdy $(R, +)$ jest grupą abelową, działanie $\cdot$ jest łaczne oraz rozdzielne względem działania $+$, to znaczy*

$$\forall x, y, z \in R[x \cdot (y + z) = x \cdot y + x \cdot z],$$

$$\forall x, y, z \in R[(y + z) \cdot x = y \cdot x + z \cdot x].$$

Działanie $+$ nazywamy **dodawaniem** *w pierścieniu R, a działanie $\cdot$* **mnożeniem.** *Element neutralny dodawania nazywamy* **zerem** *i oznaczamy przez 0. Pierścień $(R, +, \cdot)$ nazywamy* **pierścieniem zerowym,** *jeżeli $R = \{0\}$.*

(2) *Algebrę $(R, +, \cdot)$ nazywamy* **pierścieniem przemiennym,** *gdy jest pierścieniem i gdy mnożenie jest przemienne.*

(3) *Algebrę $(R, +, \cdot)$ nazywamy* **pierścieniem z jedynką,** *gdy jest pierścieniem i gdy mnożenie ma element neutralny, który wówczas nazywamy* **jedynką** *i oznaczamy przez 1.*

(4) *Algebrę $(R, +, \cdot)$ nazywamy* **ciałem,** *gdy jest niezerowym pierścieniem przemiennym z jedynką i gdy dla każdego elementu różnego od 0 istnieje element odwrotny względem mnożenia.*

Uwaga *Niech $(R, +, \cdot)$ będzie ciałem. Wówczas:*

(1) *R zawiera co najmniej dwa elementy,*

(2) *$(R, +)$ jest grupą abelową,*

(3) *$(R^*, \cdot)$ jest grupą abelową, gdzie $R^* = R \setminus \{0\}$.*

Pierścień przykłady

Przykłady:

(1) **Pierścienie liczbowe.** $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ są przykładami pierścieni przemiennych z jedynką. $(\mathbb{N},+,\cdot)$ nie jest pierścieniem. Ponadto $(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ są ciałami, zaś $(\mathbb{Z},+,\cdot)$ nie jest.

(2) **Pierścienie reszt.** Niech $n \in \mathbb{N}$ i rozważmy $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ z działaniami $\oplus_n$ oraz $\otimes_n$. $(\mathbb{Z}_n,\oplus_n,\otimes_n)$ są przykładami pierścieni przemiennych z jedynką. $(\mathbb{Z}_n,\oplus_n,\otimes_n)$ na ogół nie jest ciałem, chyba że n jest liczbą pierwszą.

(3) **Pierścienie wielomianów.** Niech $\mathbb{R}[x]$ będzie zbiorem wielomianów zmiennej x o współczynnikach rzeczywistych. Wówczas $(\mathbb{R}[x],+,\cdot)$ jest pierścieniem przemiennym z jedynką, który nie jest ciałem, gdzie $+$ i $\cdot$ oznaczają działania, odpowiednio, dodawania i mnożenia wielomianów.

(4) **Pierścienie macierzy.** Niech F będzie dowolnym ciałem, niech $M(n,F)$ oznacza zbiór macierzy kwadratowych stopnia n o współczynnikach z ciała F. $(M(n,F),+,\cdot)$ jest pierścieniem z jedynką, przy czym $+$ i $\cdot$ oznaczają tu, odpowiednio, dodawanie i mnożenie macierzy. Pierścień ten na ogół nie jest przemienny.

(5) **Pierścień endomorfizmów.** Niech V będzie przestrzenią liniową. $(V,+)$. Oznaczmy przez $End(V)$ zbiór endomorfizmów liniowych przestrzeni V. $(End(V),+\circ)$ jest pierścieniem z jedynką, który na ogół nie jest przemiennt, przy czym $+$ i $\circ$ są tu działaniami, odpowiednio, dodawania i składania przekształceń liniowych.

(6) **Pierścienie funkcji.** Niech $(R,+_R,\cdot_R)$ będzie pierścieniem, niech $X \neq \emptyset$. W rodzinie funkcji

$$R^X = \{f : X \to R : f \text{ jest funkcją}\}$$

definiujemy działania

$$(f+g)(x) = f(x) +_R g(x) \text{ oraz } (f\cdot g)(x) = f(x)\cdot_R g(x).$$

$(R^X,+,\cdot)$ jest pierścieniem, który jest przemienny, gdy R jest przemienny.

(7) **Skończony produkt pierścieni.** Niech $(R_1,+_1,\cdot_1),\ldots,(R_n,+_n,\cdot_n)$ będą pierścieniami. W produkcie kartezjańskim $R = R_1 \times \ldots \times R_n$ definiujemy działania "po współrzędnych":

$$(a_1,\ldots,a_n)+(b_1,\ldots,b_n) = (a_1 +_1 b_1,\ldots,a_n +_n b_n),$$

Pierścień grupowy

Pierścień grupowy. Niech $(G, \cdot_G)$ będzie grupą, niech $(R, +_R, \cdot_R)$ będzie pierścieniem.
Niech $R[G] = \{f \mid f : G \to \mathrm{R} \text{ prawie wszędzie równa } 0\}$.
W zbiorze $R[G]$ definiujemy w następujący sposób działania:

$$(f+g)(x) = f(x) +_R g(x),$$

$$(f \cdot g)(x) = \sum_{y \in G} f(x \cdot_G y^{-1}) \cdot_R g(y).$$

wtedy $(R[G], +, \cdot)$ jest pierścieniem.

Pierścień grupowy, sumy formalne

Niech G będzie dowolną grupą skończoną z działaniem o zapisie multiplikatywnym oraz niech R to dowolny pierścień.
Przez $R[G]$ oznaczamy zbiór wszystkich formalnych wyrażeń w postaci.

$$\sum_{g \in G} \alpha_g g, \ \alpha_g \in R, \, g \in G.$$

Przyjmujemy

$$\sum_{g \in G} \alpha_g g = \sum_{g \in G} \beta_g g$$

wtedy i tylko wtedy gdy $\alpha_g = \beta_g$ dla wszystkich $g \in G$. Przy zapisie elementów w $R[G]$ pomijamy składniki ze współczynnikami 0.
Piszemy: 0 zamiast $\sum_{g \in G} 0g$, g zamiast $1g$, $-\alpha g$ zamiast $(-\alpha)g$,
a element neutralny grupy G oznaczamy symbolem 1 tak jak element pierścienia R.

Pierścień grupowy, sumy formalne

W zbiorze $R[G]$ wprowadzamy działania dodawania i mnożenia przez skalary

$$\sum_{g\in G}\alpha_g g+\sum_{g\in G}\beta_g g=\sum_{g\in G}(\alpha_g+\beta_g)g.$$

$$\beta\sum_{g\in G}\alpha_g g=\sum_{g\in G}(\beta\alpha_g)g.$$

Wprowadzamy mnożenie

$$\left(\sum_{g\in G}\alpha_g g\right)\cdot\left(\sum_{g\in G}\beta_g g\right)=\sum_{x\in G}\left(\sum_{gh=x}\alpha_g\beta_h\right)x.$$

Pierścień grupowy, sumy formalne

W zbiorze $K[G]$ wprowadzamy działania dodawania i mnożenia przez skalary tak jak czyni się to z wektorami dodawanie:

$$(\alpha_1 g_1 + \cdots + \alpha_n g_n) + (\beta_1 g_1 + \cdots + \beta_n g_n) = (\alpha_1 + \beta_1) g_1 + \cdots + (\alpha_n + \beta_n) g_n;$$

mnożenie przez skalary:

$$\alpha \cdot (\beta_1 g_1 + \cdots + \beta_n g_n) = (\alpha\beta_1) g_1 + \cdots + (\alpha\beta_n) g_n.$$

Wprowadzamy jeszcze jedną operację, którą jednak wygodniej zapisać w skrótowej postaci. Jest to operacja mnożenia:

$$\Big(\sum_{g\in G} \alpha_g g\Big) \cdot \Big(\sum_{g\in G} \beta_g g\Big) = \sum_{x\in G} \gamma_x x,$$

gdzie $\gamma_x = \sum_{gh=x} \alpha_g \beta_h$.

Iloczyn kartezjański

Iloczyn kartezjański

Niech $\{G_i : i \in I\}$ będzie rodziną grup, gdzie I jest co najwyżej przeliczalnym zbiorem indeksów. Rozważmy zbiór

$$\prod_{i \in I} G_i = G_1 \times G_2 \times \ldots \times G_n \times \ldots = \{(g_1, g_2, \ldots, g_n, \ldots) : g_i \in G_i, i \in I\}$$

z działaniem

$$(g_1, g_2, \ldots, g_n, \ldots)(h_1, h_2, \ldots, h_n, \ldots) \stackrel{\text{def}}{=} (g_1 h_1, g_2 h_2, \ldots, g_n h_n, \ldots).$$

Powyższe działanie wprowadza w tym zbiorze strukturę grupy, gdyż

- elementem neutralnym jest $e = (e_1, e_2, \ldots, e_n, \ldots)$, gdzie e_i jest elementem neutralnym grupy G_i dla każdego $i \in I$,
- elementem odwrotnym do elementu $g = (g_1, g_2, \ldots, g_n, \ldots)$ jest $g^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}, \ldots)$.

Powyższą konstrukcję nazywa się **iloczynem kartezjańskim** grup i oznacza symbolem $\prod_{i \in I} G_i$.

W definicji zastosowano dla każdej grupy zapis multyplikatywny.

Iloczyn prosty

Iloczyn prosty

Iloczynem (produktem) prostym (zewnętrznym) grup G_i określonych wyżej nazywa się podgrupę iloczynu kartezjańskiego grup $\prod_{i\in I} G_i$ określonego równością

$$\coprod_{i\in I} G_i \stackrel{\text{def}}{=} \{(g_1, g_2, \ldots, g_n, \ldots) \colon \exists_m \, \forall_{i>m} \, g_i = e_i\}.$$

Iloczyn prosty jest więc zbiorem tych elementów iloczynu kartezjańskiego, których prawie wszystkie współrzędne są jedynkami odpowiednich grup. Grupa, która może być wyrażona jako suma prosta właściwych podgrup jest nazywana **rozkładalną**, w przeciwnym wypadku nosi ona nazwę **nierozkładalnej**.

Uwagi

Jeżeli $I = \{1, 2, \ldots, n\}$ jest zbiorem skończonym, to iloczyn prosty pokrywa się z iloczynem kartezjańskim grup, wówczas do jego oznaczenia stosuje się również zapis $G_1 \times G_2 \times \ldots \times G_n$.

Jeżeli jednak $I = \mathbb{N}$ jest zbiorem przeliczalnym, a G_i są nietrywialne dla nieskończenie wielu $i \in I$, to $\coprod G_i < \prod G_i$.

Suma prosta

Jeżeli rozważamy grupy A_i z addytywnym sposobem zapisu, to iloczyn prosty nazywa się wówczas **sumą prostą** i pisze

$$\bigoplus_{i\in I} A_i.$$