Содержание

1 Определения, первые наблюдения

Обозначения:

- будем считать, что A — поднмножество (конечное, непустое) абелевой группы или коммутативного кольца R.
- $A + B = \{a + b \mid a \in A, b \in B\}$, аналогично произведение.

Элементарные оценки:

- $|A| \leqslant |A + A| \leqslant \frac{|A|(|A|+1)}{2}$.
- $\max\{|A|, |B|\} \leqslant |A + B| \leqslant |A||B|$.
- $|A| \leqslant |A + \ldots + A| \leqslant \overline{C}^k_{|A|}$.

2 Простые структурные теоремы

Пусть $|A + B| = |A|$ в абелевой группе G. Если $0 \in B$, то $A \subset A + B \Rightarrow A + B = A$. Иначе возьмём $b_0 \in B$ и рассмотрим $|A + (B - b_0)| = |A + B| = |A| \Rightarrow A + B = b_0 + A$.

Определим $H = Sym(A) = \{h \in G \mid h + A = A\}$. Это, очевидно, подгруппа, называется она группой симметрии A. Пусть теперь $(g + H) \cap A \neq \varnothing$ для $g \in G$. Тогда $a \in A \cap (g + H) \Rightarrow a = g + h, h \in H$. По определению $a + H \subset A$, но тогда $g + h + H = g + H$.

Теорема 1. *Если $|A + B| = |A|$, $H = \{h \in G \mid h + A = A\}$, то B является подмножеством смежного класса по H, а A — объединением смежных классов по H.*

В частности для $\mathbb{R}$ получаем, что $|A + B| = |A| \Rightarrow |B| = 1$.

Для $\mathbb{Z}_p$ точно также получаем, что либо $H = 0$, либо $H = \mathbb{Z}_p$, отсюда $|A + B| = |A| \Rightarrow A = \mathbb{Z}_p$ или $|B| = 1$.

Утверждение 1. Для любых подмножеств $A, B \subset \mathbb{R}$ выполнено $|A + B| \leqslant |A| + |B| - 1$.

Доказательство. Запишем $A = \{a_0 < \ldots < a_{k-1}\}, B = \{b_0 < \ldots < b_{l-1}\}$. Тогда легко предъявить цепочку элементов $A + B$: $a_0 + b_0 < a_0 + b_1 < a_0 + b_2 < \ldots < a_0 + b_{l-1} < a_1 + b_{l-1} < \ldots < a_{k-1} + b_{l-1}$. В ней $k + l - 1$ элемент. □

Теорема 2. $|A + A| = 2|A| - 1 \Leftrightarrow A$ — *арифметическая прогрессия.*

Доказательство. $A = \{a_0 < \ldots < a_{k-1}\}$. Предъявим цепочку $2a_0 < a_0 + a_1 < 2a_1 < a_1 + a_2 < \ldots < 2a_{k-2} < a_{k-2} + a_{k-1} < 2a_{k-1}$, ясно, что других элементов быть не может.

С другой стороны $a_{i-1} + a_i < a_{i+1} + a_{i-1} < a_i + a_{i+1}$, значит $a_{i+1} + a_{i-1} = 2a_i$, значит в самом деле это прогрессия. □

Теорема 3. *Пусть* $A, B \subset \mathbb{R}, |A| = |B|$, *тогда* $|A+B| = |A| + |B| - 1 \Leftrightarrow$ A, B — *арифметические прогрессии с одинаковой разностью.*

Доказательство. Пусть для начала $|A| = |B| = k$. Предъявим цепочку $a_0 + b_0 < a_0 + b_1 < a_1 + b_1 < \ldots < a_{k-1} + b_{k-1}$, других элементов быть не может.

С другой стороны $a_i + b_i < a_{i+1} + b_i < a_{i+1} + b_{i+1}$, значит $a_{i+1} + b_i = a_i + b_{i+1} \Rightarrow a_{i+1} - a_i = b_{i+1} - b_i$.

Также $a_{i-1} + b_i < a_{i-1} + b_{i+1} < a_i + b_{i+1}$, значит $a_{i-1} + b_{i+1} = a_i + b_i \Rightarrow a_i - a_{i-1} = b_{i+1} - b_i$, что доказывает теорему в этом частном случае.

Пусть теперь $|A| = k \leqslant l = |B|$. Пусть $1 \leqslant t \leqslant l - k$ — произвольный параметр. Разобьём $B = B_1 \sqcup B_2 \sqcup B_3$ на три части $B_1 = \{b_0 < \ldots < b_{t-1}\}, B_2 = \{b_t < \ldots < b_{k+t-1}\}, B_3 = \{b_{k+t} < \ldots < b_{l-1}\}$.

$A + B \subset (a_0 + B_1) \sqcup (A + B_2) \sqcup (a_{k-1} + B_3)$. С другой стороны $|a_0 + B_1| = t, |A + B_2| \geqslant 2k - 1, |a_{k-1} + B_3| = l - k - t$, поэтому $|A + B_2| = 2k - 1, |A| = |B_2| = k \Rightarrow A, B_2$ — это арифметические прогрессии с равным шагом. В силу произвольности параметра, получаем утверждение теоремы. □

3 e-преобразование и теорема Коши-Давенпорта

Пусть $A, B \subset G, e \in G$, тогда определим преобразование пары множеств $A_{(e)} = A \cup (B + e), B_{(e)} = B \cap (A - e)$.

Чтобы B было непустым, нужно $b \in B \Rightarrow b = a - e, a \in A \Rightarrow e = a - b \in A - B$.

Свойства:

- Пусть $a \in A_{(e)} \Rightarrow a \in A$ или $a \in B + e$. Тогда $a + B_{(e)} \subset A + B$ в том и другом случае.
- По формуле включения исключения $|A_{(e)}| = |A| + |B| - |A \cap (B + e)| = |A| + |B| - |B_{(e)} + e| \Rightarrow |A_{(e)}| + |B_{(e)}| = |A| + |B|$.
- $B_{(e)} \subset B, A \subset A_{(e)}$.

Теорема 4 (Коши-Давенпорта)**.** *Пусть* $A, B \subset \mathbb{Z}_p$, *тогда* $|A+B| \geqslant \min\{|A|+|B|-1, p\}$.

Доказательство. Проведём индукцию по мощности $|B|$. База $|B| = 1$ очевидна. Докажем переход $k \Rightarrow k + 1$.

Пусть $e \in A - B$ — произвольный элемент и выполнено $|B_e| < |B|$, тогда по индукции $|A + B| \geqslant |A_{(e)} + B_{(e)}| \geqslant \min\{|A_{(e)} + B_{(e)} - 1, p\} = \min\{|A| + |B| - 1, p\}$. Осталось показать, что найдётся такое e, что $B_{(e)} \neq B$.

Пусть $B_{(e)} = B \Leftrightarrow B \subset A - e \Leftrightarrow B + e \subset A$ для всех e. Таким образом $A+B-B \subset A$. Так как $0 \in B-B$, то $A+B-B = A$ и по структурной теореме $B - B \subset H$, где H — группа симметрии множества A. Тогда либо $B - B = 0$, то есть $|B| = 1$, либо $A = \mathbb{Z}_p$, то есть так или иначе шаг доказан. □

Все наши утверждения допускают следующее обобщение.

Теорема 5 (Кнезер)**.** *Пусть G — абелева группа, A, B — её конечные непустые подмножества, $H = Sym(A+B)$. Тогда $|A+B| \geqslant |A+H|+|B+H|-|H|$.*

4 Критические пары в $\mathbb{Z}_p$

Определение 1. Если $A, B \subset \mathbb{Z}_p$ таковы, что $A + B \neq \mathbb{Z}_p$, $|A + B| = |A| + |B| - 1$, то такая пара множеств называется критической.

Теорема 6 (Воспер)**.** *Если A, B — критическая пара, то выполнено одно из следующих условий:*

- $\min\{|A|, |B|\} = 1$
- $|A + B| = p - 1, 2 \leqslant |A| \leqslant p - 1, B = \overline{c - A}, \{c\} = \mathbb{Z}_p \setminus (A + B)$
- *A, B — арифметические прогрессии с одинаковой разностью*

Доказательство.

Лемма. *Если (A, B) — критическая и $|A + B| = |A| + |B| - 1 < p - 1$, A — арифметическая прогрессия, то B — прогрессия с той же разностью.*

Лемма. *Если $\min\{|A|, |B|\} = 2$, (A, B) — критическая, то A, B — арифметические прогрессии с одинаковой разностью.*

Лемма. *Если $\min\{|A|, |B|\} \geqslant 2$, (A, B) — критическая, $|A + B| = |A| + |B| - 1 < p - 1$, тогда $(\overline{A + B}, -A)$ — критическая.*

Полагаем, что $\min\{|A|, |B|\} \geqslant 2$, $|A + B| = |A| + |B| - 1 < p - 1$.

Лемма. *В указанном предположении, если известно, что $A + B$ — арифметическая прогрессия, то A, B — арифметические прогрессии с одинаковой разностью.*

Доказательство. $A+B$ — арифметическая прогрессия, значит $\overline{A + B}$ тоже прогрессия с такой же разностью. Тогда по лемме $(\overline{A + B}, -A)$ — критическая и так как $\overline{A + B}$ — арифметическая прогрессия, то по другой лемме $-A$ и A — прогрессии с той же разностью (с точностью до знака). Еще одно применение леммы даёт нам то, что A и B — арифметические прогрессии с одинаковой разностью. □

Лемма. *Если (A, B) — критическая, $0 \in B, |A| = k \geqslant 2, |B| = l \geqslant 3, |A + B| = |A| + |B| - 1 < p - 1$. Тогда найдётся $e \in A$, такое что $(A_{(e)}, B_{(e)})$ — критическая пара, такая что $A_{(e)} + B_{(e)} = A + B$ и $2 \leqslant |B_{(e)}| < |B|$.*

Доказательство. Возьмём произвольное $e \in A$. $A_{(e)} + B_{(e)} \subset A + B$. По тоереме Коши-Давенпорта $|A_{(e)}| + |B_{(e)}| - 1 \leqslant |A_{(e)} + B_{(e)}| \leqslant |A + B| = |A|+|B|-1 = |A_{(e)}|+|B_{(e)}|-1 \Rightarrow |A_{(e)}+B_{(e)}| = |A+B| \Rightarrow A_{(e)}+B_{(e)} = A+B$.

$X = \{e \in A : |B_{(e)}| < |B|\}$. Покажем, что $|X| \geqslant 2$. Если $e \in X$, то $B \cap (A - e) \subsetneq B$. Рассмотрим $Y = A \setminus X$. Для $e \in Y$ выполнено $B \subset A - e$. Пусть $Y \neq \varnothing$, иначе все тривиально. Пусть $Y \neq \varnothing$, тогда $\forall e \in A : B + e \subset A$. По теореме Коши-Давенпорта $|Y| + |B| - 1 \leqslant |Y + B| \leqslant |A| = k$. $|Y| + l - 1 = k - |X| + l - 1 \leqslant k \Rightarrow |X| \geqslant l - 1 \geqslant 2$.

Пусть $\forall e \in X, B_{(e)} = 0$. $B' = B \setminus \{0\}$, тогда $\forall e \in X \to B' \cap (A - e) = \varnothing \Leftrightarrow \forall e \in X \to (B' + e) \cap A = \varnothing$. Тогда $(B' + X) \cap A = \varnothing \Rightarrow (X + B') \subset (A + B) \setminus A$. $|X| + l - 2 \leqslant |X| + |B'| - 1 \leqslant |A + B| - |A| = |B| - 1 = l - 1$. $|X| + l - 2 \leqslant l - 1 \Rightarrow |X| \leqslant 1$, противоречие. □

Индукция по $|B|$. База $|B| = 2$ следует из леммы.

Переход: $|B| = k + 1 \geqslant 3$. Сдвинем B на элемент b_0 и будем считать, что без ограничения общности $0 \in B$. По лемме, $\exists e \in A : (A_{(e)}, B_{(e)})$ — критическая, $A_{(e)} + B_{(e)} = A + B, 2 \leqslant |B_{(e)}| < |B|$. По предположению индукции, $A_{(e)}, B_{(e)}$ — арифметические прогессии с одинаковой разностью, значит $A + B$ — тоже. Тогда по доказанной лемме, A, B — арифметические прогрессие с одинаковой разностью. □

5 Неравенство Плюннеке-Руже

Теорема 7 (Неравенство треугольника Руже)**.** *Для любых конечных непустых $A, B, C \subset G$ выполнено $|A - B| \leqslant \frac{|A-C||B-C|}{|C|}$.*

Доказательство. $A = \{a_0, \ldots, a_{k-1}\}, B = \{b_0, \ldots, b_{l-1}\}$. Пусть $e \in A - B$, определим $a_{(e)}$ — наименьший по номеру элемент A, который может давать e. Рассмотрим $f : (e, c) \mapsto (a_{(e)} - c, c - b_{(e)})$. Если $f(e_1, c_1) = f(e_2, c_2)$, то $a_{(e_1)} - c_1 = a_{(e_2)} - c_2, c_1 - b_{(e_1)} = c_2 - b_{(e_2)}$, тогда $a_{(e_1)} - b_{(e_1)} = a_{(e_2)} - b_{(e_2)} \Rightarrow e_1 = e_2 \Rightarrow c_1 = c_2$. Стало быть, это инъекция. Значит $|A - B||C| \leqslant |A - C||C - B|$. □

Как следствие $|A - A| \leqslant \frac{|A+A|^2}{|A|}$.

Теорема 8 (Неравенство Плюннеке-Руже)**.** *Пусть $A, B \subset G$ — конечные нупустые, $|A + B| \leqslant \alpha|A|$. Тогда $\exists \varnothing \neq X \subset A$, такое что $|X + kB| \leqslant \alpha^k|A|$.*

Доказательство. Пусть $\varnothing \neq X \subset A : \forall \varnothing \neq Z \subset A \to \frac{|X+B|}{|X|} \leqslant \frac{|Z+B|}{|Z|}$. □