Combinatorial Number Theory

Martin Henk

based on lecture notes of Terence Tao
and the book by
Terence Tao and Van H. Vu *Additive Combinatorics*

Contents

1 Basics

1.1 Notation. *Let A, B subsets of an Abelian group Z.*

i) $A + B = \{a + b : a \in A,\, b \in B\}$.

ii) $A - B = \{a - b : a \in A,\, b \in B\}$.

iii) $kA = \underbrace{A + A + \ldots + A}_{k \text{ times}}$, $k \in \mathbb{Z}_{\geq 1}$.

iv) $t + B = \{t\} + B$ *for* $t \in Z$.

1.2 Proposition. *Let $A \subset \{1, \ldots, N\}$ such that $a + a' \notin A$ for all $a, a' \in A$, i.e., A is a sumfree subset of $\{1, \ldots, N\}$. Then $|A| \leq \lfloor \frac{N+1}{2} \rfloor$.*

1.3 Proposition. *Let $A, B \subset \mathbb{Z}$ be finite. Then $|A + B| \leq |A|\,|B|$.*

1.4 Proposition. *Let $A, B \subset \mathbb{Z}$ be finite. Then $|A + B| \geq |A| + |B| - 1$.*

1.5 Definition [Torsion-free]. *An Abelian group is caleld* torsion-free *if for all $x \in Z \setminus \{0\}$ and all $m \in \mathbb{Z}_{\geq 1}$ it holds $m\,x \neq 0$.*

1.6 Remark. *We will need the fact that each fnitely generated torsion-free group is isomorphic to a lattice.*

1.7 Definition [Freiman isomorphism]. *Let $A \subseteq Z$, $A' \subseteq Z'$ subsets of Abelian group Z, Z', and let $k \geq 2$. A* Freiman isomorphism of order k *is a bijective map $\Phi : A \to B$ such that for all $a_1, \ldots, a_k \in A$ and $a'_1, \ldots, a'_k \in A'$*

$$\sum_{i=1}^{k} \Phi(a_i) = \sum_{i=1}^{k} \Phi(a'_i) \Longleftrightarrow \sum_{i=1}^{k} a_i = \sum_{i=1}^{k} a'_i.$$

1.8 Remark.

i) *If Φ is a Freiman isomorphism of order k then also of order $k' \leq k$.*

ii) *The composition of Freiman isomorphisms is again a Freiman isomorphism.*

iii) *Let $\Phi : A \to A'$ be a Freiman isomorphism, and let $U_1, U_2 \subset A$. Then $|U_1 + U_2| = |\Phi(U_1) + \Phi(U_2)|$.*

1.9 Lemma. *Let $A \subseteq Z$ be a finite subset of an Abelian torsion free group. For every $k \geq 2$ exists a Freiman isomorphism $\Phi : A \to \Phi(A) \subseteq \mathbb{Z}$.*

1.10 Theorem. *Let $A, B \subseteq Z$ be finite subsets of an Abelian torsion free group Z. Then $|A + B| \geq |A| + |B| - 1$.*

1.11 Remark. *Let $A, B \subseteq \mathbb{Z}/N\mathbb{Z}$. Then $|A + B| \geq \max\{|A|, |B|\}$ which is best possible as a (non-trivial) subgroup shows.*

1.12 Theorem [Cauchy-Davenport]. *Let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ for a prime p. Then $|A+B| \geq \max\{|A|+|B|-1, p\}$.*

1.13 Lemma. *Let $A, B \subseteq Z$ be finite subsets of an Abelian group Z. Then the following statements are equivalent:*

i) $|A+B| = |A|$.

ii) $|A-B| = |A|$.

iii) $|A+mB-nB| = |A|$ *for all* $m, n \in \mathbb{Z}_{\geq 0}$, $(m,n) \neq (0,0)$.

iv) $|A+mB-nB| = |A|$ *for a pair* $m, n \in \mathbb{Z}_{\geq 0}$ *with* $(m,n) \neq (0,0)$.

v) *There exists a subgroup $U \leq G$ such that B is a subset of a coset w.r.t. U and A is the union of cosets w.r.t. U.*

1.14 Lemma. *Let $A, B, C \subseteq Z$ be finite subsets of an Abelian group Z. Then*

$$|A-B| \leq \frac{|A+C|\,|B+C|}{|C|}.$$

1.15 Corollary. *Let $A, B, A\prime, B' \subseteq Z$ be finite subsets of an Abelian group Z.*

i) *If $|A+B| = |A|$ and $|A'+B| = |A'|$. Then $|A \pm A'| \leq |A||A'|/|B|$.*

ii) *If $|A+B| = |A| = |A+B'|$ then $|B \pm B'| \leq |A|$.*

2 Plünnecke's Theorem

2.1 Theorem [Plünnecke]. *Let Z be an Abelian group, let $A, B \subseteq Z$ be finite, and let $K \geq 1$ such that $|A+B| \leq K|A|$. Then there exists a $A' \subseteq A$, $A' \neq \emptyset$, such that*

$$|A' + B + B| \leq K^2 |A'|$$

2.2 Definition [Plünnecke Graph]. *Let Z be an Abelian group. A graph $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ is called an* Plünnecke graph (of depth 2) *with vertices $V_0 \cup V_1 \cup V_2 \subset Z$ and directed edges $E_{0\to1} \cup E_{1\to2}$ if every edge $E_{0\to1}$ starts in V_0 and ends in V_1, every edge $E_{1\to2}$ starts in V_1 and ends in V_2 and the following* Plünnecke property *is fulfilled:*

$$\begin{aligned} &\text{if } a \to a+b \in E_{0\to1} \text{ and } a+b \to a+b+c \in E_{1\to2} \\ &\text{then } a \to a+c \in E_{0\to1} \text{ and } a+c \to a+b+c \in E_{1\to2}. \end{aligned} \tag{Pp}$$

2.3 Remark. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be Plünnecke graph.*

i) *Each $a \to a+b \in E_{0\to1}$ induced an injection between $\{a+b \to a+b+c \in E_{1\to2}\}$ (all edges of $E_{1\to2}$ starting in $a+b$ and $\{a \to a+c \in E_{0\to1}\}$ (all edges of $E_{0\to1}$ emanating from a).*

ii) *Each $d \to c+d \in E_{1\to2}$ induced an injection between $\{d-b \to d \in E_{0\to1}\}$ (all edges of $E_{0\to1}$ ending in d and $\{-b+c+d \to c+d \in E_{0\to1}\}$ (all edges of $E_{1\to2}$ ending inc + d).*

iii) *We may always assume that the sets V_i are pairwise disjunct.*

2.4 Definition. *Let $G = (V, E)$ be a graph. For $V' \subseteq V$ let $G(V') = \{v \in V : \exists\, v' \in V' \text{ with } (v, v') \in E\}$ be all nodes which can be reached via a path of length 1 starting in V'. Recursively, $G^k(V')$ be all nodes which can be reached via a path of length k starting in V'.*

2.5 Remark. *With respect to finite subsets $A, B \subseteq Z$ of an Abelian group Z we consider the following* Plnnecke graph *$G(A, B) = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$, where $V_0 = A$, $V_1 = A + B$, $V_2 = A + B + B$ and $E_{0\to1} = \{a \to a+b : a \in A,\, b \in B\}$ and $E_{1\to2} = \{a+b \to a+b+c : a \in A,\, b, c \in B\}$. In terms of the graph $G(A, B)$, Theorem 2.1 says:*
Suppose $|V_1| \leq K\,|V_0|$ then there exists a nonempty subset $A' \subseteq V_0$ such that

$$G^2(A') \leq K^2\,|A'|.$$

2.6 Lemma [Menger's theorem]. *Let $G = (V, E)$ be a directed graph. For subsets $V_0, V_1 \subset V$ let* $\mathrm{maxflow}(V_0, V_1)$ *be the maximal number of vertex disjoint paths from V_0 to V_1, and let* $\mathrm{mincut}(V_0, V_1)$ *be the minimal number of vertices which have to be removed from V such that V_0 and V_1 are disconnected. Then*

$$\mathrm{maxflow}(V_0, V_1) = \mathrm{mincut}(V_0, V_1).$$

First, we prove Remark 2.5 for arbitrary Plünnecke graphs in the case $K = 1$. More precisely,

2.7 Proposition. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be a Plünnecke graph with $|V_1| < |V_0|$. Then there exists a nonempty subset $A' \subseteq V_0$ such that $G^2(A') < |A'|$.*

2.8 Definition [Magnification Ratio]. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be a Plünnecke graph with respect to a group Z.*

i)
$$\mathrm{D}(G) = \min_{A'\subseteq V_0,\, A'\neq\emptyset} \frac{|G^2(A')|}{|A'|}$$
is called magnification ratio *of the graph.*

ii) *Let $\overline{G} = (\overline{V_0}, \overline{V_1}, \overline{V_2}, \overline{E}_{0\to1}, \overline{E}_{1\to2})$ be another Plünnecke graph with respect to a group $\overline{Z}$. The Cartesian product*
$$G \times \overline{G} = (V_0 \times \overline{V_0}, V_1 \times \overline{V_1}, V_2 \times \overline{V_2}, E_{0\to1} \times \overline{E}_{0\to1}, E_{1\to2} \times \overline{E}_{1\to2})$$
is a Plünnecke graph with respect to $Z \times \overline{Z}$. Here the product of two edges $a \to b$ and $\overline{a} \to \overline{b}$ is just $(a, \overline{a}) \to (b, \overline{b})$.

2.9 Remark.

i) *Proposition 2.7 says: if $|V_1| < |V_0|$ then $\mathrm{D}(G) < 1$.*

ii) *Let $Z = \mathbb{Z}^k$, $A = \{0\}$, $B = \{e_1, \dots, e_k\}$, where e_i denotes the i-th unit vector. The Plünnecke graph $G(A, B)$ is denoted by G_k and it is*
$$\mathrm{D}(G_k) = \frac{k(k+1)}{2}.$$
For the associated reflected graph $G_k^\intercal$ (all edges are reversed) we find $\mathrm{D}(G_k^\intercal) = \frac{2}{k(k+1)}$.

2.10 Lemma. *Let $G, \overline{G}$ be Plünnecke graphs. Then*
$$\mathrm{D}(G \times \overline{G}) = \mathrm{D}(G) \cdot \mathrm{D}(\overline{G}).$$

2.11 Proposition. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be a Plünnecke graph with $|V_1| < K\,|V_0|$, $K \geq 1$. Then $\mathrm{D}(G) \leq K^2$, i.e., there exists a nonempty subset $A' \subseteq V_0$ such that $G^2(A') \leq K^2\,|A'|$.*

Observe, Proposition 2.11 implies Theorem 2.1.

2.12 Corollary. *Let A, B finite subsets of an Abelian group Z and let $|A+B| \leq K\,|A|$ for some $K \geq 1$. For any $n \in \mathbb{N}$ there exists $A_n \subseteq A$, $A_n \neq \emptyset$, such that*
$$|A_n + nB| \leq K^{c_n}\,|A_n|,$$
where c_n depends only on n (in fact, it can be shown that $c_n = n$ works).

2.13 Corollary [Sumset Estimate]. *Let A, B finite subsets of an Abelian group Z and let $|A+B| \le K\,|A|$ for some $K \ge 1$. For any $n, m \in \mathbb{N}$ we have*

$$|nB - mB| \le K^{c_{n,m}}\,|A|,$$

where $c_{n,m}$ depends only on n and m.

2.14 Corollary. *Let A, B finite subsets of an Abelian group Z and let $|A+B| \le K\,|A|$ for some $K \ge 1$. Let $\delta \in (0,1)$. Then there exists $A' \subseteq A$ with $|A'| \ge (1-\delta)|A|$ and*

$$|A' + B + B| \le \frac{2\,K^2}{\delta}\,|A| \quad \left(\le \frac{2\,K^2}{\delta(1-\delta)}\,|A'|\right).$$

2.15 Proposition. *There exist subsets $A, B \subset \mathbb{Z}^2$ with $|A| \sim n^2$, $|B| \sim n$, such that $|A+B| \sim n^2$, but $|A+B+B| \sim n^3$.*

3 Covering

3.1 Lemma [Ruzsa's quotient lemma]. *Let A, B finite subsets of an Abelian group Z. Then there exists a set $X \subseteq Z$ with $|X| \leq \frac{|A+B|}{|A|}$ such that $B \subseteq X + A - A$, i.e., B is covered by at most $\frac{|A+B|}{|A|}$ translates of $A - A$.*

3.2 Corollary. *If $|A+A| \sim |A|$ then $nA-mA$ can be covered by $O(1)$ translates of $A - A$.*

3.3 Lemma. *Let Z be a finite Abelian group and let $A \subseteq Z$, $A \neq \emptyset$. Then G can be covered by $O(\frac{|Z|}{|A|} \log |Z|)$ translates of A, i.e., there exists $X \subseteq Z$, $|X| \in O(\frac{|Z|}{|A|} \log |Z|)$ such that $G = X + A$.*

3.4 Lemma [Improved quotient lemma]. *Let A, B finite subsets of an Abelian group Z. Then there exists a set $X \subseteq Z$ with $|X| \leq 2\frac{|A+B|}{|A|}$ such that B is covered by $X + A - A$ at least $\frac{|A|}{2}$ times, i.e., for every $y \in B$ there are at least $\frac{|A|}{2}$ triplets $(x, a, a') \in X + A - A$ such that $y = x + a - a'$.*

3.5 Theorem. *Let A be a finite subset of an Abelian group Z such that $|A + A| \sim |A|$. For any fixed $n, m \geq 0$ there exists a set $X_{n,m} \subseteq Z$ with $|X_{n,m}| \in O(\log |A|)$ such that $mA - nA \subseteq X_{n,m} + A$.*

3.6 Proposition. *There exist finite subsets A, B of an Abelian group Z such that $|A + B| \sim |A|$, but $|A - B| \geq |A|^{2-\log 6/\log 7}$.*

3.7 Proposition. *Let A, B finite subsets of an Abelian group Z such that $|A + B| \sim |A|$. Then for every $\epsilon > 0$ there exists a subset $A' \subseteq A$ such that $|A'| \sim |A|$ and $|A' - B| \leq C_\epsilon |A|^{1+\epsilon}$.*

3.8 Proposition. *For any integer $n \geq 1$ there exist finite subsets A, B of an Abelian group Z such that $|A + B| \sim |A| \sim C^n$, $|B| \sim n$, but $|A' - B| \geq n|A'|$ for all non-empty subsets of A.*

4 Freiman's theorem

4.1 Definition. *Let A, A' be subsets of a an Abelian group Z.*

i) *$A' \subseteq A$ is called a* refinement *of A if $|A'| \sim |A|$.*

ii) *A' is a called a* small convolution *of A if there exists an $X \subseteq Z$ with $|X| = O(1)$ and $A' = X + A$.*

4.2 Remark. *Let A be a finite subset of an Abelian group Z which is essentially closed under addition, i.e., $|A + A| \sim |A|$.*

i) *If A' is a refinement of A then $|A' + A'| \sim |A'|$.*

ii) *If A' is a* small convolution *of A then $|A' + A'| \sim |A'|$.*

iii) *If Φ is a Freiman Isomorphism of order $k \geq 2$ then $|\Phi(A)+\Phi(A)| \sim |\Phi(A)|$.*

4.3 Theorem [Finite Torsion]. *Let Z be an Abelian group of Torsion $r < \infty$. Let $A \subseteq Z$ with $|A + A| \sim |A|$. Then A is a refinement of a subgroup $U \leq Z$.*

4.4 Definition [Generalized arithmetic progression].

i) *Let $N = (N_1, \ldots, N_d) \in \mathbb{N}^d$ and let $[0, N] = \{n \in \mathbb{Z}^d : 0 \leq n_i \leq N_i,\ 1 \leq i \leq d\}$. d is called the* rank *of the* box *$[0, N]$, and $|[0, N]| = \prod_{i=1}^{d}(N_i + 1)$ is called the* (discrete) volume *of the box $[0, N]$.*

ii) *Let Z be an Abelian group, let $\Phi : \mathbb{Z}^d \to Z$ be an affine homomorphism, and let $[0, N] \subset \mathbb{Z}^d$ be a box of rank d. The image $\Phi([0, N])$ is called a* (generalized) arithmetic progression *of* dimension *d,* length *N and volume $|[0, N]|$. If $\Phi|_{[0,N]}$ is injective the progression is called* proper.

4.5 Remark. *With the notation as above let $\Phi(0) = a$ and $\Phi(e_i) = v_i$, $1 \leq i \leq d$, where e_i are the unit vectors of $\mathbb{Z}^d$. Then*

$$\Phi([0, N]) = \left\{ a + \sum_{i=1}^{d} n_i\, v_i : 0 \leq n_i \leq N_i,\ 1 \leq i \leq d \right\},$$

and a is called base point *and v_i are called* basis vectors *of the arithmetic progression $\Phi([0, N])$.*

4.6 Proposition. *Let Z be an Abelian group, $\Phi : \mathbb{Z}^d \to Z$ be a Freiman isomorphism of order (at least) 2, and let $[0, N] \subset \mathbb{Z}^d$ be a box. Then $\Phi([0, N])$ is essentially closed under addition, i.e., $|\Phi([0, N]) + \Phi([0, N])| \sim |\Phi([0, N])|$.*

4.7 Theorem [Freiman]. *Let Z be a torsion-free Abelian group, and let $A \subset Z$ be essentially closed under addition, i.e., $|A + A| \sim |A|$. Then A is a refinement of a small convolution of a proper generalized arithmetic progression P of bounded rank, i.e., there exists a set $X \subset Z$, $X = O(1)$, with $A \subseteq X + P$, and $|A| \sim |X + P| \sim |P|$.*

4.8 Lemma. *Let A be a finite subset of a torison-free Abelian group Z. Let $n, N \in \mathbb{N}$ such that $2\,|nA - nA| < N$. Then there exists a subset $A' \subseteq A$ with $|A'| \geq |A|/n$ and a Freiman isomorphism $\Phi : A' \to B \subset \mathbb{Z}/N\,\mathbb{Z}$ of order n.*

4.9 Lemma. *Let $N \in \mathbb{N}$, $A \subseteq \mathbb{Z}/N\,\mathbb{Z}$ with $|A| \sim N$ and $|A + A| \sim |A|$. Then the set $2A - 2A$ contains a generalized proper arithmetic progression P of bounded rank with $|P| \sim N$.*

4.10 Definition. *Let Z be an Abelian (additive) group. Let $e : Z \times Z \to S^1 = \{z \in \mathbb{C} : |z| = 1\}$ be a map such that*

i) $e(x + x', y) = e(x, y)e(x', y)$ *and* $e(x, y + y') = e(x, y)e(x, y')$

ii) *for all x (or y) $\in Z \setminus \{0\}$ exists y (or x) $\in Z \setminus \{0\}$ such that $e(x, y) \neq 1$.*

e is called a bi-character.

4.11 Remark.

i) $e(0, y) = e(x, 0) = 1$, $e(x, -y) = e(-x, y) = \overline{e(x, y)}$.

ii) *For $\mathbb{Z}/N\mathbb{Z}$ the function $e(x, y) : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to S^1$ with $e(x, y) = e^{2\pi\,\mathrm{i}\,xy/N}$ is a bi-character.*

iii) *Let e_1, e_2 be bi-characters with respect to groups Z_1, Z_2. Then $e_1 \otimes e_2 : (Z_1 \times Z_2) \times (Z_1 \times Z_2)$ with $(e_1 \otimes e_2)(x_1 \times x_2, y_1, \times y_2) = e_1(x_1, y_1) \cdot e_2(x_2, y_2)$, $x_1, y_! \in Z_1$, $x_2, y_2 \in Z_2$, is a bi-character on $Z_1 \times Z_2$.*

iv) *Every finite Abelian group has a bi-character.*

4.12 Lemma. *Let Z be a finite Abelian group, and let $e : Z \times Z \to S^1$ be a bi-character. Then*

$$\frac{1}{|Z|} \sum_{x \in Z} e(x, y)\overline{e(x, y')} = \delta_{y,y'} \quad \text{and} \quad \frac{1}{|Z|} \sum_{y \in Z} e(x, y)\overline{e(x', y)} = \delta_{x,x'},$$

where $\delta_{x,y} = 1$ if $x = y$ and 0 otherwise.

4.13 Remark. *Let $\mathbb{C}^Z$ be the set of all complex-valued functions on Z. For $f, g \in \mathbb{C}^Z$ let*

$$\langle f, g \rangle_Z = \frac{1}{|Z|} \sum_{x \in Z} f(x)\,\overline{g(x)}.$$

i) *$\langle \cdot, \cdot \rangle$ is an inner product on $\mathbb{C}^Z$.*

ii) *$e(\cdot, y)$, $y \in Z$, form an orthonormal system.*

iii) *Let $f \in \mathbb{C}^Z$. Then*

$$f = \sum_{y \in Z} \langle f, e(\cdot, y) \rangle_Z\, e(\cdot, y).$$

4.14 Definition [Fourier transform]. *Let $f \in \mathbb{C}^Z$, where Z is a finite Abelian group, and let $e : Z \times Z \to S^1$ be a bi-character. Then $\widehat{f} : Z \to \mathbb{C}$ with*

$$\widehat{f}(y) = \langle f, e(\cdot, y)\rangle_Z = \frac{1}{|Z|} \sum_{x \in Z} f(x)\, \overline{e(x,y)}$$

is called the Fourier transform *of f.*

4.15 Theorem. *Let Z be a finite Abelian group, and let $e : Z \times Z \to S^1$ be a bi-character. Let $f \in \mathbb{C}^Z$.*

i) $f(x) = \sum_{y \in Z} \widehat{f}(y)\, e(x,y)$ (Fourier inversion formula)

ii) $\frac{1}{|Z|} \sum_{x \in Z} f(x)\overline{g(x)} = \sum_{y \in Z} \widehat{f}(y)\, \overline{\widehat{g}(y)}$ (Plancherel formula)

iii) $\frac{1}{|Z|} \sum_{x \in Z} |f(x)|^2 = \sum_{y \in Z} |\widehat{f}(y)|^2$ (Parseval relation)

4.16 Definition [Convolution]. *Let $f, g \in \mathbb{C}^Z$. Then $f \star g \in \mathbb{C}^Z$ with*

$$f \star g(x) = \frac{1}{|Z|} \sum_{y \in Z} f(y)\, g(x-y)$$

is called convolution *of f and g.*

4.17 Lemma.

i) $\widehat{f \star g}(y) = \widehat{f}(y)\, \widehat{g}(y)$.

ii) *Let $\tilde{f}(x) = \overline{f(-x)}$. Then $\widehat{\tilde{f}}(y) = \overline{\widehat{f}(y)}$.*

4.18 Proposition. *Let $A \subseteq Z$ with characteristic function χ_A, and let $c = |A|/|Z|$. Then*

i) $\sum_{y \in Z} |\widehat{\chi_A}(y)|^2 = c$.

ii) $|\widehat{\chi_A}(y)| \le c$.

iii) *Let $\epsilon \in (0,1]$. Then $|\{y \in Z : |\widehat{\chi_A}(y)| \ge \epsilon\, c\}| \le \epsilon^2 \frac{1}{c}$.*

iv) $\sum_{y \in Z} |\widehat{\chi_A}(y)|^4 \le c^3$.

4.19 Remark. *Let $f(x) = \chi_A \star \chi_A \star \chi_{-A} \star \chi_{-A}$. Then $f(x) \neq 0$ if and only if $x \in 2\,A - 2\,A$, and it holds $\widehat{f}(y) = |\widehat{\chi_A}(y)|^4$.*

4.20 Lemma. *Let $A \subseteq Z$, $|A|/|Z| = c$, and let $|A + A| \le K\,|A|$. Let*

$$\Lambda = \left\{ y \in Z : |\widehat{\chi_A}(y)| \ge \frac{c}{2\sqrt{K}} \right\} \text{ and}$$
$$X = \left\{ x \in Z : |e(x,y) - 1| < \frac{1}{4} \text{ for all } y \in \Lambda \right\}.$$

Then $X \subseteq 2A - 2A$.