

基礎事項の補足

鈴木雄太 (立教大学)

2024 年 7 月 9 日 版

数論ないしは解析数論に不慣れな方がつまづきそうな基礎事項を簡単にまとめる.

1 漸近記法について (簡易版) (編集中)

1.1 Vinogradov の記号

まずは, Vinogradov の記号 $\ll$ を導入する:

Notation C.1.1 (Vinogradov の記号). 集合 X の上で定義された関数

$$f: X \rightarrow \mathbb{C} \quad \text{と} \quad g: X \rightarrow \mathbb{R}_{\geq 0}$$

と X の部分集合 $S \subseteq X$ に対して, 次のように定める:

$f(x) \ll g(x)$ が $x \in S$ の範囲で成り立つ

$\stackrel{\text{def}}{\iff}$ ある実数 $C \geq 0$ が存在して, すべての $x \in S$ に対して, $|f(x)| \leq C \cdot g(x)$ が成り立つ.

ここで範囲 S が文脈から読み取れる場合は,

「 $f(x) \ll g(x)$ が $x \in S$ の範囲で成り立つ」の代わりに単に 「 $f(x) \ll g(x)$ 」

と書く. また, 上の定数 C のことを **implicit constant** または **implied constant** と呼ぶ.

Example C.1.1.

(i) 範囲 $x \in \mathbb{R}$ で $\sin x \ll 1$. 実際, $C := 1$ とすると, $|\sin x| \leq C \cdot 1$ が $x \in \mathbb{R}$ で成り立つ.

(ii) 範囲 $|x| \geq \frac{1}{2}$ で $x \ll x^2$ が成り立つ. 実際, $C := 2$ とすると, $|x| \geq \frac{1}{2}$ の範囲で

$$|x| = \frac{|x|}{|x|} \cdot |x| \leq \frac{|x|}{\frac{1}{2}} \cdot |x| = 2 \cdot |x|^2 = C \cdot x^2$$

が成り立つ. (ここで「範囲 $|x| \geq \frac{1}{2}$ で」という部分は「範囲 $x \in \mathbb{R} \setminus (-\frac{1}{2}, +\frac{1}{2})$ で」という

ことの砕けた表現であるが、問題なく理解できるだろう.)

(iii) 範囲 $x \in [0, 1]$ で $x^2 \ll x$ が成り立つ. 実際, $C := 1$ とすると, $x \in [0, 1]$ の範囲で

$$x^2 = x \cdot x \leq 1 \cdot x = C \cdot x$$

が成り立つ. (範囲が変わったことで (ii) とは逆向きの関係になっていることに注意!)

(iv) 範囲 $|x| \leq \frac{1}{2}$ で $\log(1+x) \ll |x|$. 実際, Taylor 展開すれば, 範囲 $|x| \leq \frac{1}{2}$ で

$$\begin{aligned} |\log(1+x)| &= \left| x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots \right| \\ &\leq |x| + |x|^2 + |x|^3 + |x|^4 + \cdots \\ &= |x| \cdot (1 + |x| + |x|^2 + |x|^3 + \cdots) \\ &\leq |x| \cdot (1 + \frac{1}{2} + (\frac{1}{2})^2 + (\frac{1}{2})^3 + \cdots) = 2 \cdot |x| \end{aligned}$$

が成立する. (なので, implicit constant として $C := 2$ が使える.)

また, パラメータに依存した場合に Vinogradov の記号を使うこともある:

Notation C.1.2 (パラメータに依存した Vinogradov の記号). 集合 A で添字付けられた関数族

$$(f_a: X_a \rightarrow \mathbb{C})_{a \in A} \quad \text{と} \quad (g_a: X_a \rightarrow \mathbb{R}_{\geq 0})_{a \in A}$$

と部分集合 $T \subseteq A$ および部分集合たち $S_a \subseteq X_a$ ($a \in T$) に対して, 次のように定める:

すべての $a \in T$ に対して $f_a(x) \ll_a g_a(x)$ が $x \in S_a$ の範囲で成り立つ

$\stackrel{\text{def}}{\iff}$ すべての $a \in T$ に対して, ある実数 $C(a) \geq 0$ が存在して,

すべての $x \in S_a$ に対して, $|f_a(x)| \leq C(a) \cdot g_a(x)$ が成り立つ.

ここで範囲 $T, (S_a)_{a \in A}$ が文脈から読み取れる場合は,

「すべての $a \in T$ に対して $f_a(x) \ll_a g_a(x)$ が $x \in S_a$ の範囲で成り立つ」

の代わりに単に

$$\lceil f_a(x) \ll_a g_a(x) \rceil$$

と書く. また, 集合 A が $A = A_1 \times \cdots \times A_n$ のような直積である場合は

$$\lceil f_{(a_1, \dots, a_n)}(x) \ll_{(a_1, \dots, a_n)} g_{(a_1, \dots, a_n)}(x) \rceil$$

の代わりに

$$\lceil f_{(a_1, \dots, a_n)}(x) \ll_{a_1, \dots, a_n} g_{(a_1, \dots, a_n)}(x) \rceil$$

と書く.

- このようにパラメータ $a_1, \dots, a_n$ の値に対応して implicit constant $C(a_1, \dots, a_n)$ の値を変えなければいけない場合, 「implicit constant は $a_1, \dots, a_n$ に依存する」という.
- 一方で, implicit constant が $a_1, \dots, a_n$ の値に対応しないで一様に取れる場合, 「implicit constant は絶対定数である」という.
- 依存性が文脈から明らかな場合は Vinogradov 記号の添字部分を省略することもある.

Example C.1.2. すべての $k \in \mathbb{N}$ に対して範囲 $x \geq 0$ で (つまり, Notation C.1.2 にて $A = T = \mathbb{N}, X_k = S_k = \mathbb{R}_{\geq 0}$)

$$x^k \ll_k e^x$$

が成り立つ. 実際,

$$x^k = k! \cdot \frac{x^k}{k!} \leq k! \cdot \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^k}{k!} + \dots\right) = k! \cdot e^x$$

である. ここで implicit constant として使った $k!$ は k に対して一様には取り直せない.

1.2 Landau の記号

次に, 誤差項に毎回名前をつけるのを避けるのに使える Landau の記号 (O) を導入する:

Notation C.1.3 (Landau の記号). 集合 X の上で定義された関数

$$g: X \rightarrow \mathbb{R}_{\geq 0}$$

と文脈から明らかな範囲 $S \subseteq X$ に対して, 記号

$$O(g(x))$$

で,

「範囲 $x \in S$ において $f(x) \ll g(x)$ と評価される項 $f(x)$ の省略」

を表す. 同様に, 関数族

$$(g_a: X_a \rightarrow \mathbb{R}_{\geq 0})_{a \in A}$$

と文脈から明らかな範囲 $T \subseteq A, S_a \subseteq X_a$ ($a \in T$) に対して, 記号

$$O_a(g_a(x))$$

で,

「すべての $a \in T$ に対して, 範囲 $x \in S_a$ で $f_a(x) \ll_a g_a(x)$ と評価される項 $f_a(x)$ の省略」

を表す. 注意であるが:

- 同じ記号 $O(g(x))$ であっても, 省略されている関数は場所によって異なりうる.
- 記号 $O(g(x))$ で省略されている関数が x 以外の変数に依存する可能性を排除しない. (この記号によって, x 以外の変数, 例えば y を変数として持つ関数 $f(x, y)$ が省略されていたとすると, 関数の値自体は y に依存しうるが, 依然として評価 $f(x, y) \ll g(x)$ は成立していなければならない.)

Example C.1.3.

(i) 範囲 $x \geq 0$ と $d \in \mathbb{N}$ で

$$\sum_{\substack{n \leq x \\ d|n}} 1 = \frac{x}{d} + O(1)$$

が成立する. この右辺は

$$\frac{x}{d} - \left\{ \frac{x}{d} \right\}$$

の省略であり, $O(1)$ に対応する部分は実際に

$$\left| -\left\{ \frac{x}{d} \right\} \right| = \left\{ \frac{x}{d} \right\} \leq 1 \cdot 1$$

と評価できるので $\ll 1$ と評価できる項である. (implicit constant は絶対定数.)

(ii) 範囲 $|x| \leq \frac{1}{2}$ で $\log(1+x) = x + O(x^2)$. 実際, Taylor 展開を考えれば,

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4!} + \cdots$$

となるが, 範囲 $|x| \leq \frac{1}{2}$ で

$$\left| -\frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4!} + \cdots \right| \leq x^2 \cdot \left(\left(\frac{1}{2} \right) + \left(\frac{1}{2} \right)^2 + \cdots \right) \leq x^2$$

だから

$$R(x) = -\frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4!} + \cdots$$

とおけば

$$\log(1+x) = x + R(x) \quad \text{かつ} \quad R(x) \ll x^2$$

が分かる.

2 総和記号について

(準備中)

3 初等整数論の基礎事項

Notation C.3.1. 以下, 整数 n, d に対して, 標準全射 (つまり, $(\bmod d)$ の余りを取る写像)

$$\mathbb{Z} \rightarrow \mathbb{Z}/d\mathbb{Z}$$

による n の像のことを $n \pmod{d}$ と書くことにする.

Lemma C.3.1 (中国剰余定理). 互いに素な自然数 d, e に対して, 環準同型

$$\phi: \mathbb{Z}/de\mathbb{Z} \rightarrow (\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/e\mathbb{Z}); x \pmod{de} \mapsto (x \pmod{d}, x \pmod{e})$$

は環同型である.

Proof. 与えられた写像 ϕ が環準同型であること (和, 積, 積の単位元を保つこと) は明らか. よって ϕ が全単射であることを示せばよい. 環準同型 ϕ の定義域 $\mathbb{Z}/de\mathbb{Z}$ と値域 $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/e\mathbb{Z})$ は要素数の等しい有限集合なので, ϕ の単射性のみ示せば良い. 実際に $x \pmod{de}, y \pmod{de} \in \mathbb{Z}/de\mathbb{Z}$ が $\phi(x \pmod{de}) = \phi(y \pmod{de})$ を満たしたとすると, ϕ の定義より

$$x \equiv y \pmod{d} \quad \text{かつ} \quad x \equiv y \pmod{e}$$

である. ここで d と e は互いに素なので,

$$x \equiv y \pmod{de}$$

つまり $x \pmod{de} = y \pmod{de}$ が言えた. よって ϕ は単射である. (注: この証明は一般の環に対する中国剰余定理を示すには使えない, $\mathbb{Z}/n\mathbb{Z}$ の有限性を用いた簡易的な議論を用いている.) $\square$

Definition C.3.1. 実数 x に対して,

$$[x] := \max\{n \in \mathbb{Z} \mid n \leq x\} \quad \text{および} \quad \{x\} := x - [x]$$

とおき, それぞれ実数 x の**整数部分**および**小数部分**と呼ぶ.

4 数論的関数の取り扱い

Definition C.4.1 (数論的関数).

- (1) 自然数上で定義された複素数値関数を**数論的関数**と呼ぶ.
- (2) 数論的関数 f が**乗法的**であるとは, $f(1) = 1$ であり, 任意の自然数 m, n に対して

$$(m, n) = 1 \implies f(mn) = f(m)f(n)$$

が成立することを言う.

(3) 数論的関数 f が**完全乗法的**であるとは, $f(1) = 1$ であり, 任意の自然数 m, n に対して

$$f(mn) = f(m)f(n)$$

が成立することを言う.

Definition C.4.2 (Dirichlet convolution). 数論的関数 f, g に対して, f と g の **Dirichlet convolution** と呼ばれる数論的関数 $f * g$ を, 自然数 n に対して

$$(f * g)(n) := \sum_{dm=n} f(d)g(m)$$

で定める. (ここで右辺の和は $dm = n$ を満たす自然数の組 (d, m) に渡る.)

Proposition C.4.1. 以下, f, g, h を任意の数論的関数とし, 数論的関数 δ を, 自然数 n に対して

$$\delta(n) := \mathbb{1}_{n=1}$$

で定める. このとき, Dirichlet convolution に対して, 以下の基本的な性質が成立する:

- (i) (結合則) $((f * g) * h) = (f * (g * h))$.
- (ii) (交換則) $f * g = g * f$.
- (iii) (単位元) $f * \delta = f$.
- (iv) (分配則) $f * (g + h) = (f * g) + (f * h)$.

Proof. 一旦, 省略. □

Proposition C.4.2 (和の変数変換). 次のものを考える:

- 有限集合 X, Y .
- 関数 $f: Y \rightarrow \mathbb{C}$.
- 全単射 $\varphi: X \rightarrow Y$.

このとき,

$$\sum_{y \in Y} f(y) = \sum_{x \in X} f(\varphi(x))$$

が成立する.

Proof. 集合 Y は有限集合なので, $\#Y = n$ とすれば

$$y_\bullet: \{1, \dots, n\} \rightarrow Y; i \mapsto y_i$$

という全単射 (添字付け) がある. 写像 φ は全単射なので, 逆写像 $\varphi^{-1}: Y \rightarrow X$ が取れて, φ^{-1} も全単射である. 全単射の合成は全単射なので, $i \in \{1, \dots, n\}$ に対して

$$x_i := \varphi^{-1}(y_i)$$

と定めることで, 全単射 (添字付け)

$$x_{\bullet}: \{1, \dots, n\} \rightarrow X; i \mapsto x_i$$

を作ることができる. 有限集合の上の和とは適当な添字付けの下での和なので

$$\sum_{y \in Y} f(y) = \sum_{i=1}^n f(y_i) = \sum_{i=1}^n f(\varphi(\varphi^{-1}(y_i))) = \sum_{i=1}^n f(\varphi(x_i)) = \sum_{x \in X} f(\varphi(x))$$

を得る. □

Definition C.4.3. 自然数 n に対して

$$\mathcal{D}(n) := \{d \in \mathbb{N} : d \mid n\}$$

と書く. (自然数 n の約数の集合.) (たぶん標準的な記号ではない.)

Proposition C.4.3. 自然数 n に対して,

$$\text{Decomp}(n) := \{(d, m) \in \mathbb{N}^2 \mid dm = n\}$$

と書くことにすると, 写像

$$\delta: \mathcal{D}(n) \rightarrow \text{Decomp}(n); d \mapsto (d, n/d)$$

は全単射である. 特に, Proposition C.4.2 より, 数論的関数 f, g と自然数 n に対して,

$$(f * g)(n) = \sum_{dm=n} f(d)g(m) = \sum_{d \mid n} f(d)g(n/d)$$

が成立する.

Proof. 集合 $\mathcal{D}(n)$ は n の約数の集合だから, $d \in \mathcal{D}(n)$ であれば $n/d \in \mathbb{N}$ である. よって, δ の像が常に $\text{Decomp}(n)$ に属するのは明らか. あとは逆写像を作ればよい. 逆写像の候補として

$$\pi: \text{Decomp}(n) \rightarrow \mathcal{D}(n); (d, m) \mapsto d$$

を考える. 写像 π の像が $\mathcal{D}(n)$ に属することは明らか. あとは

$$\pi \circ \delta = \text{id}_{\mathcal{D}(n)} \quad \text{および} \quad \delta \circ \pi = \text{id}_{\text{Decomp}(n)}$$

を示せば良い.

また, $\pi \circ \delta = \text{id}_{\mathcal{D}(n)}$ を示す. 任意に $d \in \mathcal{D}(n)$ を取る. すると,

$$\pi(\delta(d)) = \pi((d, n/d)) = d$$

となる. よって, $\pi \circ \delta = \text{id}_{\mathcal{D}(n)}$ である.

次に, $\delta \circ \pi = \text{id}_{\text{Decomp}(n)}$ を示す. 任意に $(d, m) \in \text{Decomp}(n)$ を取る. すると,

$$\delta(\pi((d, m))) = \delta(d) = (d, n/d)$$

であるが, $(d, m) \in \text{Decomp}(n)$ は $dm = n$ を意味するので

$$\delta(\pi((d, m))) = (d, m)$$

となる. よって, $\delta \circ \pi = \text{id}_{\text{Decomp}(n)}$ である.

以上で主張が示された. □

Proposition C.4.4. 互いに素な自然数 n_1, n_2 に対して, 写像

$$\mu: \mathcal{D}(n_1) \times \mathcal{D}(n_2) \rightarrow \mathcal{D}(n_1 n_2); (d_1, d_2) \mapsto d_1 d_2$$

は全単射である. 特に, Proposition C.4.2 より, 数論的関数 f と互いに素な自然数 n_1, n_2 に対して,

$$\sum_{d|n_1 n_2} f(d) = \sum_{\substack{d_1|n_1 \\ d_2|n_2}} f(d_1 d_2)$$

が成立する.

Proof. まず, μ の像が常に $\mathcal{D}(n_1 n_2)$ に属することを示す. 任意に $(d_1, d_2) \in \mathcal{D}(n_1) \times \mathcal{D}(n_2)$ をとる. すると, 約数の定義から $d_1 m_1 = n_1$ である自然数 m_1 と $d_2 m_2 = n_2$ である自然数 m_2 が取れる. すると, $d_1 d_2 m_1 m_2 = n_1 n_2$ であるから, 約数の定義より $\mu(d_1, d_2) = d_1 d_2 \in \mathcal{D}(n_1 n_2)$ である.

あとは, μ の逆写像が存在することを示せばよい. 逆写像の候補として写像

$$\delta: \mathcal{D}(n_1 n_2) \rightarrow \mathcal{D}(n_1) \times \mathcal{D}(n_2); d \mapsto ((d, n_1), (d, n_2))$$

を考える. δ の像が必ず $\mathcal{D}(n_1) \times \mathcal{D}(n_2)$ に入っていることは最大公約数の定義から明らか. あとは

$$\delta \circ \mu = \text{id}_{\mathcal{D}(n_1) \times \mathcal{D}(n_2)} \quad \text{および} \quad \mu \circ \delta = \text{id}_{\mathcal{D}(n_1 n_2)}$$

を示せば良い.

まず, $\delta \circ \mu = \text{id}_{\mathcal{D}(n_1) \times \mathcal{D}(n_2)}$ を示す. 任意に $(d_1, d_2) \in \mathcal{D}(n_1) \times \mathcal{D}(n_2)$ を取る. すると,

$$\delta(\mu((d_1, d_2))) = \delta(d_1 d_2) = ((d_1 d_2, n_1), (d_1 d_2, n_2))$$

となる. ここで $(n_1, n_2) = 1$, $d_1 \in \mathcal{D}(n_1)$, $d_2 \in \mathcal{D}(n_2)$ より $(d_1 d_2, n_1) = (d_1, n_1) = 1$ だから

$$\delta(\mu((d_1, d_2))) = ((d_1, n_1), (d_2, n_2)).$$

最後に, $d_1 \in \mathcal{D}(n_1)$, $d_2 \in \mathcal{D}(n_2)$ つまり $d_1 \mid n_1$ かつ $d_2 \mid n_2$ であったことを思い出せば

$$\delta(\mu((d_1, d_2))) = (d_1, d_2)$$

を得る. よって, $\delta \circ \mu = \text{id}_{\mathcal{D}(n_1) \times \mathcal{D}(n_2)}$ である.

次に, $\mu \circ \delta = \text{id}_{\mathcal{D}(n_1 n_2)}$ を示す. 任意に $d \in \mathcal{D}(n_1 n_2)$ を取る. すると,

$$\mu(\delta(d)) = \mu(((d, n_1), (d, n_2))) = (d, n_1)(d, n_2)$$

であるが, $(n_1, n_2) = 1$ だったので

$$\mu(\delta(d)) = (d, n_1 n_2)$$

である. 最後に $d \in \mathcal{D}(n_1 n_2)$ つまり $d \mid n_1 n_2$ だったことを思い出せば

$$\mu(\delta(d)) = d$$

である. よって, $\mu \circ \delta = \text{id}_{\mathcal{D}(n_1 n_2)}$ である.

以上で主張が示された. □

Proposition C.4.5. 乗法的関数の Dirichlet convolution は再び乗法的である.

Proof. 乗法的関数 f, g を任意に取る. 任意の互いに素な自然数 n_1, n_2 に対して,

$$(f * g)(n_1 n_2) = \sum_{d \mid n} f(d)g\left(\frac{n_1 n_2}{d}\right) \quad (\text{Proposition C.4.3})$$

$$= \sum_{d_1 \mid n_1} \sum_{d_2 \mid n_2} f(d_1 d_2)g\left(\frac{n_1}{d_1} \frac{n_2}{d_2}\right) \quad (\text{Proposition C.4.4})$$

となる. この最後の和では, n_1/d_1 と n_2/d_2 は自然数である. また, $(n_1, n_2) = 1$ より, この最後の和では $(d_1, d_2) = (n_1/d_1, n_2/d_2) = 1$ なので, f, g の乗法性より

$$(f * g)(n_1 n_2) = \left(\sum_{d_1 \mid n_1} f(d_1)g(n_1/d_1) \right) \left(\sum_{d_2 \mid n_2} f(d_2)g(n_2/d_2) \right) = (f * g)(n_1)(f * g)(n_2)$$

を得る. よって $f * g$ も乗法的であることがわかった. □

Definition C.4.4. 自然数 d, n に対して

$$d \parallel n \stackrel{\text{def}}{\iff} d \mid n \text{ かつ } (d, n/d) = 1$$

と定める.

Remark C.4.1. 自然数 n , 素数 p , 非負整数 v に対して,

$$p^v \parallel n \iff p^v \mid n \text{ かつ } p^{v+1} \nmid n$$

つまり, $p^v \parallel n$ のとき n の素因数分解に現れる p のべきの指数は v である. ($v = 0$ を含める.)