

2011年5月17日(2011年5月31日訂正)

山田光太郎

kotaro@math.titech.ac.jp

集合と位相第一講義資料 6

前回までの補足

ツオルンの補題の使い方 前回の補足として、今回ツオルンの補題の使い方をやってみます。

質問について

- 短い質問をたくさんくださった方がありましたが、箇条書きになっていない(一目でいくつの質問があるかわからない)ので、ひとつひとつ分解して回答する手間をかける気が起きませんでした。今回は回答いたしません。
- 質問用紙の目的：(1) 受講者の理解度を講師が理解する。(2) 受講者が質問を考えることにより復習をし、理解度を深める。(3) プレゼンテーション能力の開発。したがって、何も考えていないような質問、何を言っているかわからない質問の評価は低くなります。

前回までの訂正

- 講義で、順序関係の条件 $x \preceq x$ が抜けていたそうです。
- 板書で $X \times X = \{\varphi : \{0, 1\} \rightarrow X \mid \varphi(1), \varphi(2) \in X\}$ と書いたそうです。 $\{0, 1\}$ でなく $\{1, 2\}$ ですね。
- 講義資料 5, 5 ページ 14 行目：(誤) 必要がる (正) **必要がある**
- 講義資料 5, 6 ページ, 下から 4 行目：(誤) ひつずつ (正) **ひとつずつ**
- 講義資料 5, 8 ページ：(誤) 属 (正) 族
- 講義資料 5, 10 ページ 4 行目：(誤) $\pi_X(G_m) = Y$ (正) $\pi_Y(G_m) = Y$
- 講義資料 5, 10 ページ 12 行目： $a \in X$ を $a \in A'$ に訂正

授業に関する御意見

- 「順序」がゲシュタルト崩壊しました。 山田のコメント： そう？
- 新しい記号が出てくると混乱してしまいます。 山田のコメント： だから落ち着いて定義に立ち戻る。
- 講義資料がとてもわかりやすくありがたいです。 山田のコメント： それは間違いないと...
- 先生は日本語、ドイツ語、フランス語、英語の 4ヶ国語に通じておられるようですが、旅行が趣味なのですか？(立ち入った質問ですみません...) 山田のコメント： 通じていません。趣味というより(嫌いではないが)仕事ででかけます。
- 実は複素数には大小があると思っていました。あせりました。 山田のコメント： 髪は測れないのです。
- 集合論の演習を独学で行う場合、どのような参考書を用いればよいでしょうか？ 山田のコメント： 最初の授業で挙げたようなものではないかでしょうか。
- □: ダランベルシアン, Q.E.D.: 量子電磁力学です! 山田のコメント: 文脈依存
- 面白かったです。 山田のコメント: 私もです。
- (・・・)(髪切った?)は正確には() (髪切った?)だと思います。 山田のコメント: そんなにあどろかなくても
- 特になし。 山田のコメント: Ich, auch.
- 今回の授業は意外と納得することが多くて、質問を考えるのが難しかったです。授業内容に誤りがあったのか、むしろ気になります。 山田のコメント: でもありました。
- 先生は授業前毎回予想外の場所にいるので毎回驚きます。 山田のコメント: 次はどこにしよう。
- 公理と同値関係にあるものが「補題」と呼ばれていることに少し違和感を感じました。
- Zorn の補題って、どこらへんが補題なんですか。 山田のコメント: ですわね。
- 選択公理を認めることでこんなに話が展開していくことに驚くばかりです。 山田のコメント: そうとも言います。
- 同値関係が使えることはどっち条件ですか。 山田のコメント: 必要条件

質問と回答

質問： 講義資料 2 の問 2-5 : 写像 $f: X \rightarrow Y$ と $g: Y \rightarrow X$ で $g \circ f = \text{id}_X$ かつ f は全射でないような具体例を挙げなさい, という問題がわからないので教えてください。

お答え： x ではなく X ですね。 $X = Y = \mathbb{N}$ として $f: \mathbb{N} \rightarrow \mathbb{N}, g: \mathbb{N} \rightarrow \mathbb{N}$ を

$$f(x) = x + 1, \quad g(x) = \begin{cases} x - 1 & (x \geq 2) \\ 1 & (x = 1) \end{cases}$$

とすればよい。

質問： 順序集合 (X, \preceq) に次をみたす全順序 \leq を入れることができるか。 $x \preceq y$ のとき $x \leq y$ お答え： どうでしょう。

質問： 空集合は全順序集合ですか？ お答え： はい。

質問： 対角集合で Δ_X と Δ のどちらが正しいのですか？ 気分によって使い分けて良いのでしょうか。

お答え： だれもがこの意味で使う記号ではないので, どちらでも (その文脈で定義すれば) 正しい。

質問： 8 ページのフォントが小さい気がするのですが, 何か意味があるのですか？

お答え： 気にしないでください, という意味です。

質問： 実無限・可能無限なる概念を知ったのですが, 無限個の要素を持つ集合を考えるときは実無限の考え方によっているのですか？ お答え： そうです。

質問： 補題と命題の違いがよくわかりません。

お答え： 意味としてはどちらも定理。何かを示すための補助的な定理が補題。“定理”と大きく出するには少々気が引けるようなものが命題。

質問： $\{x \text{ の濃度} \mid x \text{ は集合}\}$ が集合であるか知らないと講義資料 5 の 5 ページに書いてありますが, $A = \{x \text{ の濃度} \mid x \text{ は } A \text{ 以外の集合}\}$ の場合は明らかに集合であると思って良いですか？

お答え： なぜ明らかと思うのですか？

質問： 今回の授業 (5 月 10 日), Th. 任意のベクトル空間には基底が存在する のあたりの内容で質問があります。この定理での基底を次のように定めていますが, 私が写し間違えたのでしょうか？ 下の定義によると, 例で出された $R: Q$ 上のベクトル空間 (∞ 次元) において基底をとることができないように思えるのですが...

V は線型空間とする。このとき, $W \subset V$ が V の基底であるとは, W が以下の①, ②を満たすことと定める。① W の任意の有限部分集合 $\{v_1, v_2, \dots, v_k\}$ が一次独立, ② すべての $v \in V$ は W の有限個の元の線型結合でかける。

お答え： なぜできないと思うのでしょうか。

質問： 「任意のベクトル空間に基底が存在する」というのは,

$\{(u, b) \mid u \subset V \text{ 部分空間}, b: u \text{ の基底}\}$ で

$(u_1, b_1) \preceq (u_2, b_2)$ を $u_1 \subset u_2$ かつ $b_1 \subset b_2$ とした時

(u, b, \preceq) が帰納的順序集合

ということから, u の極大元と b の極大元が存在するということから

u の上界 V には基底が存在する

ということ言えばそれで証明できたことになるのでしょうか？

お答え： そうです。

質問： ツォルンの補題が補題たる所以は何ですか。

お答え： そうですね。なんで補題なんですか。もともとは何かを証明するために用意した命題だと思われませんが。

質問： 一般連続体仮説は $\forall A, B [|A| \leq |B| \leq |2^A| \wedge |B| \neq |2^A| \Rightarrow |A| = |B|]$ と表されますが, これは $(|A| \leq |B| \leq |2^A|$ の前提のもとで) $|B| \neq |2^A|$ でさえあれば, A から B への全単射が存在することを意味します。特に B が整列集合ならば A も整列集合になります (できます)。このようなことを用いて “一般連続体仮説 \Rightarrow 選択公理” が示されるのではないのでしょうか？ (一方, 集合論 ZF のもとでは “選択公理 \Rightarrow 一般連続体仮説” は一般にはなりたちません。それは選択公理はなりたつが一般連続体仮説がなりたない ZF のモデルが存在するからです。これは P. J. Cohen の強制法 (forcing) を用いて示すことができます。なお, forcing は Boolean valued model などの方法に発展し, 物理においても用いられる (ようです)。)

お答え： なぜ一般連続体仮説から選択公理が示せると思うのでしょうか。

質問: X の任意の部分集合が最小元を持つかどうか考えるとき, そもそも元が「最小かどうか」をちゃんと判断できるのか? (例えば $C \supset \{i, 2i\}$) と思ったのですが, それは選択公理を認めるかどうかにかかっているんですか?

お答え: 順序を定義しなければ最小元を定義することはできません. そして, “順序を定義できる” のが選択公理の帰結.

質問: 選択公理を認めると証明できる命題をいくつかやりましたが, そのような命題は他にもたくさんあるのですか? どのような命題のときに選択公理を用いるのか区別できません.

お答え: 見ただけで区別できるとは思いません.

質問: U : 集合, $X = \wp(U) \ni A, B$, X の 2 項関係 $A \supset B$ は順序関係だが一般に全順序でない. と, 板書されていたのですが, ではどのような場合全順序となるのでしょうか.

お答え: $\wp(U)$ の包含関係ですか? $|U| \geq 2$ なら全順序にはなりません.

質問: \preceq は何と呼ばばいいのですか? 「ラッパ」でいいですか?

お答え: 声を出して読んだのを聞いたことはありません.

質問: \mathcal{G} は何と読むのですか. お答え: じー

質問: 帰納的とは「具体的なものを一般化する」ことです. 帰納的順序集合の帰納と上界はどう結びつくのですか.

お答え: どうも “数学的帰納法” との関係のような気がします.

質問: 順序関係には, 大小関係「 \leq 」と包含関係「 \subset 」以外にどのようなものがありますか.

質問: 順序関係の授業で出た以外の例を教えてください.

お答え: 変なものはいくらでも作れる, というのが整列可能性定理.

質問: 順序集合 X の極大元と最大元について,

- 極大元 c は $\forall x \in X, c \preceq x \Rightarrow c = x$ だから, すべての x について, $c \preceq x, x \preceq c$ のいずれかが成り立たなければならぬわけではないから, 半順序にも存在しうる.
- 最大元 a は $\forall x \in X$ に対して $x \preceq a$ だから, 半順序には存在しない.

のですか. それとも, 最大元は, x, y に対して, $x \preceq y$ も $y \preceq x$ も成り立たなくても $x \preceq a, y \preceq a$ であれば存在するのですか.

お答え: 全順序集合でなくても最大元をもつ場合があります. たとえば $\wp(U)$ に包含関係で半順序 (講義では順序) を与えると U は最大元.

質問: 極大元や最小元という言葉が出たが, 極大と最大はどう違うのか.

お答え: 定義が違う.

質問: ある $x, y \in X$ について, $x \preceq y$ と $y \preceq x$ とも言えなくても, もし

$$\begin{cases} x \preceq y \text{ かつ } y \preceq x \text{ と言えるならば } x = y \\ x \preceq y \text{ かつ } y \preceq z \text{ と言えるならば } x \preceq z \end{cases}$$

ということであれば, (X, \preceq) は順序集合という事でしょうか.

お答え: この講義の用語ではそうです.

質問: ツオルンの補題において, 「 $a \in X$ に対して... $a \preceq c$ 」という条件が含まれていますが, この a は何のために設定されているのでしょうか? 「 $\exists c \in X$ s.t. $c \preceq x \Rightarrow c = x$ for all $x \in X$ 」で十分な気がします.

お答え: あっても良いですね. たとえばベクトル空間の基底の存在定理. 適当な有限次元部分空間に基底をとり, それを延長して基底をとることができる, というのをいうためには $a \preceq c$ が必要.

質問: 結局, 半順序という用語は一度しか聞きませんでしたが, 今の数学界では順序関係という用語の方が一般的なんですか. そのあたりの違いがわかりません.

お答え: “数学界” などと大きく構える必要はなく, 文脈から読み取ればよい.

質問: 定理 5.5 (ツオルンの補題) は, 「帰納的順序集合は極大元をもつ」ということですか? お答え: そうです.

質問: 定理 5.5 で「帰納的順序集合 (X, \preceq) と $a \in X$ に対して, $c \in X$ で $a \preceq c$ かつ次を満たすものが存在する」とありますが, この部分を「帰納的順序集合 (X, \preceq) に対して次を満たす $c \in X$ が存在する」と書き換えてしまうと, 定理 5.5 の主張は異なったものになってしまうのでしょうか. 講義資料の書き方に違和感を覚えました.

お答え: 違和感の正体がわかりません. どちらでもよいと思います.

質問: \sim_R は $\subset, =, \preceq$ などの関係をまとめて一般的に書いたものですか?

お答え: まとめた, というのは変な気がします, そういうものを含んだ概念です.

質問: 集合 A のべき集合 $\wp(A)$ の二項関係が $\{(u_1, u_2) \in \wp(A) \times \wp(A) \mid u_1 \subsetneq u_2\}$ のように与えられたら, これは講

義資料の Thm 5.2 の 1, 2 番目の条件を満たしていないので順序関係ではないですね？

お答え： この講義の意味では順序関係ではありません．

質問： 今回の講義で二項関係・順序関係といった、「関係」と名前のついた集合が登場しましたが、同値関係も集合なの
 でしょうか？

お答え： そうです．

質問： 順序集合 (X, \preceq) に対し、 X の任意の部分集合が最大限 (原文ママ：最大元のことか) を持つとき、 (X, \preceq) は整
 列集合であるとは言えないのでしょうか．

お答え： この講義の定義では整列集合ではありません．

質問： $c \in X$ 、任意の $x \in X$ に対して $c \preceq x$ が成り立つならば $c = x$ 、このとき c は極大元であると言っていますが、な
 ぜ極大という名前がついているのですか？ c より大きい元は存在しないのだから最大元とした方がいいような気が
 します．

お答え： $U = \{1, 2, 3\}$ 、 $\mathcal{U} := \mathfrak{P}(U) \setminus \{\emptyset, U\}$ としてみます． $\mathcal{U} = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{3, 1\}\}$ ですが、集合
 の包含関係が定める順序に関する極大元はなんでしょう．この場合、最大元とよんでいいのでしょうか？

質問： 半順序集合 (X, \preceq) に対して、極大 (小) 元は上 (下) 限ですか？

お答え： 上の例を考えてみてください．

質問： 順序集合は一般に半順序集合のことですね．

お答え： どちらが一般的かはなんとも言えません．この講義では、あなたが“半順序集合”とよびたいものを“順序集
 合”呼んでいます．

質問： “任意の”と“すべての”という言葉に使いわけはありますか？例えば「 $\forall x \in \mathbf{R}$ に対して $f(x) = 0$ 」と「 $f(x) = 0$
 for all $x \in \mathbf{R}$ 」は同値に思えます．(f は $\mathbf{R} \rightarrow \mathbf{R}$ の関数とします．) もし使いわけがあるとしたら、“任意の”と
 “すべての”をおきかえた時に不都合が起こる例を教えてください．

お答え： 同義です．

質問： 極大元と最大元という言葉の違いに自信が持てません．「集合と位相」(内田伏一著)によると $a \in X$ が極大元
 $a \preceq x$ かつ $a \neq x$ となる元 $x \in X$ が存在しない、 $a \in X$ が $A(A \neq \emptyset, A \subset X)$ の最大元 $a \in A \forall x \in A a \preceq x$ が
 成り立つ．とあります．極大元と最大元の違いは、半順序集合の内を考えるか、半順序集合の部分集合の内で考え
 るかという違いと認識できますか．

お答え： “認識”という曖昧な語ではなくしっかり“定義”を捉えてください．

質問： 集合 X の 2 項関係 $R \subset X \times X$ は $X \subset Y$ のとき $R \subset Y \times Y$ だから、 R は集合 Y の 2 項関係でもあるという
 ことですか？つまり X の 2 項関係であり Y の 2 項関係であるものがあってもよいのですか？写像では普通対応関
 係が同じでも値域が違えば違う写像としますが．

お答え： どちらを全体集合とみなすか、というのがかならず書いてあるか文脈で読み取れます．“ X の 2 項関係”とい
 うようにいいます．

質問： 全順序の性質を満たす \preceq はたくさん存在して、定義によるので、任意の集合 X に対して順序集合 (X, \preceq) は必ず
 作れる...ということになりますか．又集合 Y では半順序であった \preceq の定義が集合 X に限れば全順序となる場
 合、 \preceq は全順序ですか．それとも半順序ですか？

お答え： 前半：任意の集合に対して全順序が存在することは正しい．しかし“ので”がおかしい．後半： Y の半順序、
 X の全順序．

質問： $x \preceq z \Rightarrow x \preceq y, y \preceq z$ は成り立ちますか？

お答え： \Rightarrow の左側に y がないので分かりません．

質問： 講義における集合族を集合系といい、集合族を集合の集合として使っている本もありますが、どちらが一般的
 のでしょうか．

お答え： さあ、どうでしょう．文脈からその都度読み取るのがよいと思います．

質問： 前回、選択公理の写像がわからないとぶっきらぼうに書いてしまい、申し訳ありませんでした．二晩中考えて、
 ようやく選択公理についてなにを言っているのかわかりました．でも $\prod_{\lambda \in \Lambda} U_\lambda$ と数列の違いが未だにわかりませ
 ん．違うのでしょうか (後略)

お答え： $\prod_{\lambda \in \Lambda} U_\lambda$ の要素とも数列とも思えるものの具体例 (具体的な状況) を挙げてごらん下さい．

6 同値関係・商集合

同値関係

定義 6.1. 集合 X の二項関係 \sim が同値関係であるとは、次が成り立つことである：

- 任意の $x \in X$ に対して $x \sim x$,
- 任意の $x, y \in X$ に対して $x \sim y$ ならば $y \sim x$,
- 任意の $x, y, z \in X$ に対して $x \sim y$ かつ $y \sim z$ ならば $x \sim z$.

例 6.2. • $X \ni x, y$ に対して $x \sim y$ を $x = y$ で定めると、これは同値関係である (自明な同値関係) .
 • 写像 $f: X \rightarrow Y$ に対して $x \sim_f y$ を $f(x) = f(y)$ となること、と定義するとこれは同値関係である .
 これを、写像 f が誘導する同値関係という .

例 6.3 (群作用が導く同値関係). G を群とする . すなわち演算 $\cdot: G \times G \rightarrow G$ が定義されて次を満たしている : (1) 任意の $a, b, c \in G$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (2) ある $e \in G$ が存在して、任意の $a \in G$ に対して $a \cdot e = e \cdot a = a$. (3) 任意の $a \in G$ に対して $a \cdot a^{-1} = a^{-1} \cdot a = e$ となる $a^{-1} \in G$ が存在する .

集合 X から X への全単射全体の集合を \mathcal{F}_X と書くことにする . 群 G の集合 X への作用とは、写像 $\rho: G \rightarrow \mathcal{F}_X$ で次を満たすものである : $\rho(e) = \text{id}_X$ かつ $\rho(a \cdot b) = \rho(a) \circ \rho(b)^{*1}$.

いま、群 G の集合 X への作用 ρ が与えられているとき、 $x \sim_G y$ であることを、 $y = \rho(g)(x)$ となる $g \in G$ が存在することと定めるとこれは同値関係である .

商集合

命題 6.4. 集合 X に同値関係 \sim が与えられているとする . このとき、写像 $q: X \ni x \mapsto \{y \in X \mid x \sim y\} \in \mathfrak{P}(X)$ を考えると、任意の x_1, x_2 に対して $q(x_1) = q(x_2)$ または $q(x_1) \cap q(x_2) = \emptyset$ である . とくに、前者のための必要十分条件は $x_1 \sim x_2$ である .

証明 : $q(x_1) \cap q(x_2) \ni y_0$ とすると $x_1 \sim y_0$ かつ $x_2 \sim y_0$ だから $x_1 \sim x_2$. このとき、任意の $y_1 \in q(x_1)$ に対して $x_1 \sim y_1$ が成り立つから $x_1 \sim x_2$ から $x_2 \sim y_1$. したがって $y_1 \in q(x_2)$ となるので $q(x_1) \subset q(x_2)$. 同様に $q(x_2) \subset q(x_1)$ なので $q(x_1) = q(x_2)$.

定義 6.5. 集合 X に同値関係 \sim が与えられているとき、命題 6.4 の写像 q の像 $q(X)$ を (X の \sim による) 商集合といい、 X/\sim とかく . このとき、全射 $q: X \rightarrow X/\sim$ を射影、 $x \in X$ に対して $q(x)$ を x の同値類とよぶ . x の同値類はしばしば $[x]$ と書かれる .

例 6.6. 空でない集合 X, Y の直積 $X \times Y$ 上の同値関係を $(x, y) \sim (x', y') \Leftrightarrow x = x'$ で定義する . このとき、 $y_0 \in Y$ を固定して $\iota: X \ni x \mapsto [(x, y_0)] \in X \times Y/\sim$ とすると ι は全単射 .

誘導写像 集合 X に同値関係 \sim が与えられているとし、商集合への射影を $q: X \rightarrow X/\sim$ とする .

2011 年 5 月 17 日 (2011 年 5 月 31 日訂正)

*1 一般に \mathcal{F}_X は写像の合成を演算として群になる . このとき ρ が G の X への作用とは、 G から \mathcal{F}_X の準同型のことである . とくに $\rho(e) = \text{id}_X$, $\rho(g^{-1}) = \{\rho(g)\}^{-1}$ が成り立つ .

命題 6.7. 写像 $f: X \rightarrow Y$ が “ $x \sim y$ ならば $f(x) = f(y)$ ” を満たしているとする. 全射 $\bar{f}: X/\sim \rightarrow f(X) \subset Y$ で $f = \iota \circ \bar{f} \circ q$ となるものがただ一つ存在する. ただし $\iota: f(X) \rightarrow Y$ は包含写像である. とくに \bar{f} が全単射になるための必要十分条件は $f(x) = f(y)$ ならば $x \sim y$ が成り立つ, すなわち, f が誘導する同値関係が \sim と一致することである.

証明: $[x] \in X/\sim$ に対して $q(x) = [x]$ となる $x \in X$ を一つとり $y = f(x)$ とする. もう一つ $q(x') = [x]$ となる x' をとると $x \sim x'$ なので $f(x') = f(x) = y$. したがって y の値は $[x]$ を定めるとただ一つ定まる. これを $\bar{f}([x])$ とすれば, それが求める写像である.

定義 6.8. 命題 6.7 の \bar{f} を f が誘導する写像という.

例 6.9. 写像 $f: \mathbf{R} \ni t \mapsto (\cos t, \sin t) \in \mathbf{R}^2$ が誘導する \mathbf{R} の同値関係を \sim と書く. すると $x \sim y$ であるための必要十分条件は $y - x$ が 2π の整数倍となることである. このとき, 次の誘導写像は全単射:

$$\bar{f}: \mathbf{R}/\sim \rightarrow f(\mathbf{R}) = S^1 = \{(x, y) \mid x^2 + y^2 = 1\} \subset \mathbf{R}^2.$$

いま, 加群 \mathbf{Z} の \mathbf{R} への作用を $\rho(n)(x) = x + 2\pi n$ ($n \in \mathbf{Z}, x \in \mathbf{R}$) と定めると, この作用が誘導する同値関係は \sim と一致する. この意味で $S^1 = \mathbf{R}/\mathbf{Z}$ と書くことがある.

例 6.10. • 自然数全体の集合を N とし, $N \times N$ の二項関係

$$(x, y) \sim (x', y') \iff x + y' = x' + y$$

は同値関係である. これは, 写像 $f: N \times N \ni (x, y) \mapsto x - y \in \mathbf{Z}$ (\mathbf{Z} は整数全体の集合) から誘導される同値関係で, 全単射 $\bar{f}: (N \times N)/\sim \rightarrow \mathbf{Z}$ を与える.

• 整数全体の集合を Z とし, $Z \times (Z \setminus \{0\})$ の同値関係を

$$(x, y) \sim (x', y') \iff xy' = x'y$$

で定めると, $(Z \times (Z \setminus \{0\}))/\sim$ と Q (有理数全体の集合) の間の全単射が存在する.

問題

6-1 X の同値関係は $X \times X$ のどのような部分集合か.

6-2 例 6.3 の関係 \sim_G が同値関係になることを示しなさい. 同値関係の性質の各々が, 群演算の性質とどのように対応しているかを観察しなさい.

6-3 正の整数 n を一つ固定する. 整数 x, y に対して $x - y$ が n で割り切れるとき x と y は n を法として合同である, といい, $x \equiv y \pmod{n}$ と書く.

- “ n を法として合同である” という関係は Z の同値関係であることを示しなさい.
- この同値関係による Z の商集合を Z_n あるいは Z/nZ と書く. Z_n の要素の個数はいくつか.
- 写像 $\alpha: Z \times Z \ni (x, y) \mapsto [x + y] \in Z_n$ は $[\alpha]: Z_n \times Z_n \rightarrow Z_n$ を誘導することを確かめなさい. とくに $x, y \in Z$ の同値類 $[x], [y]$ に対して $[\alpha]([x], [y])$ を $[x] + [y]$ と書くことにする.
- 写像 $\mu: Z \times Z \ni (x, y) \mapsto [xy] \in Z_n$ は $[\mu]: Z_n \times Z_n \rightarrow Z_n$ を誘導することを確かめなさい. この $[\mu]([x], [y])$ を $[x][y]$ と書くことにする.
- 0 と n を法として合同でない整数 x を一つ固定し, 写像 $Z_n \ni \xi \mapsto [x]\xi \in Z_n$ を考える. この写像が全単射になるのはどんなときか.