強制法入門

Eureka GAP

2017 年 5 月 5 日

1　集合論の基礎事項

1.1　ZFC

集合論においてすべての対象は集合です．集合の元もまた集合でなくてはならないため，たとえば { 太郎, 次郎, 三郎 } といったものは考察の対象にはなりません．集合というものを規定しているのが次に述べる ZFC とよばれる公理系であり，集合論における結果はすべて ZFC からの論理的帰結です．ZFC の公理は以下のものから成ります．

外延性　$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$.

集合はその元によって決定されることを意味します．

内包性　ϕ を自由変数として z を含まないような論理式として，[*1]

$$\forall x \exists z \forall v (v \in z \leftrightarrow v \in x \wedge \phi).$$

ある集合 x の「論理式で規定されるような」部分集合の存在を保証します．このとき存在が示される集合 z は $\{v \in x : \phi\}$ と表記されます．

空集合　$\exists z \forall x (x \notin z)$.

元を持たない集合の存在を保証します．このとき存在が示される集合 z は $\emptyset$ と表記され，空集合（empty set）と呼ばれます．

対　$\forall x \forall y \exists z (v \in z \leftrightarrow (v = x \vee v = y))$.

x, y を集合としたときに x, y のみを元とする集合の存在を保証します．このとき存在が示される集合 z は $\{x, y\}$ と表記され，対（pair）と呼ばれます．また，$\{x, x\}$ のことを $\{x\}$ と略記します．さらに，順序対（ordered pair）$\langle x, y \rangle$ は $\{\{x\}, \{x, y\}\}$ と定義できます．

和集合　$\forall x \exists z \forall v (v \in z \leftrightarrow \exists y \in x (v \in y))$.

ある集合 x の元の元の全体からなる集合の存在を保証します．このとき存在が示される集合 z は $\bigcup x$ と表記されます．特に $\bigcup \{x, y\}$ は $x \cup y$ と書かれます．

無限　$\exists z (\emptyset \in z \wedge \forall v \in z (v \cup \{v\} \in z))$.

$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots\}$ を部分集合として含むような無限集合の存在を保証します．後で述べるように，この公理からは自然数全体の集合の存在が導けます．

[*1] この仮定がないと，$v \notin z$ を ϕ としたときなどに矛盾が生じます．

冪集合　$\forall x \exists z (v \in z \leftrightarrow v \subseteq x)$.

ある集合 x の部分集合全体からなる集合の存在を保証します．このとき存在が示される集合 z は $\mathcal{P}(x)$ と表記され，x の冪集合と呼ばれます．

置換　$\phi(u, v)$ は u, v を自由変数（の一部）として含む論理式として，

$$\forall u \exists! v \phi(u, v) \to \forall x \exists z \forall v (v \in z \leftrightarrow \exists u \in x \phi(u, v)).$$

「論理式で規定される」写像による集合の像が集合として存在することを保証します．

基礎　$\forall x (x \neq \emptyset \to \exists y \in x (x \cap y = \emptyset))$.

空集合でない限り $\in$-極小元が存在することを意味します．この公理は普段の数学にはあまり出てきませんが，集合論においては大切な公理です．

選択公理　$\forall x \exists f (f$ は関数 $\wedge \forall y \in x (y \neq \emptyset \to f(y) \in y))$.

ZFC から選択公理を除いた公理系もしばしば用いられ，それを ZF とよびます．

ZFC とその帰結において存在が示されるようなものを集合とよぶため，単なる集合の集まりでは集合になるとは限りません．たとえば，すべての集合の集まり $V = \{x : x = x\}$ は集合ではありません．V のように論理式で規定される集合の集まりはクラス（class）とよばれ，集合ではないクラスを真のクラスといいます．V は真のクラスです．$x \in V$ などのように，真のクラスであっても集合と同様の表記をすることがあります．あらゆる数学的対象は集合として定義できます．

Example 1.1.

- 集合 A, B の直積とは $A \times B = \{\langle x, y \rangle : x \in A \wedge y \in B\}$ のことである．
- 関係とは順序対からなる集合のことである．
- 関係 R に対し $\mathrm{dom}(R) = \{x : \exists y (\langle x, y \rangle \in R)\}$，$\mathrm{ran}(R) = \{y : \exists x \langle x, y \rangle \in R\}$ と定める．f が関数あるいは写像であるとは，f が関係であり，$\forall x \in \mathrm{dom}(f) \exists! y \in \mathrm{ran}(f) (\langle x, y \rangle \in f)$ を満たすことである．

このように関数は集合として定義できますし，次の節で説明するように自然数もまた集合です．自然数さえ定義できれば，整数や有理数，さらに実数も集合として定義できますし，位相や多様体などのより複雑な対象もまた集合とみなせるでしょう．結局のところ，あらゆる数学は集合論の言葉で記述することが可能であり，普通の数学はすべて ZFC から導かれている結果なのだと言えます．

1.2　順序数と基数

まずは順序の復習から始めます．

Definition 1.2. 集合 A 上の半順序（partial order）R とは，次の条件を満たす関係 R のことである．

(1) 推移性：$\forall x, y, z \in A (xRy \wedge yRz \to xRz)$.
(2) 非反射性：$\forall x \in A \neg xRx$.

ここで $\langle x, y \rangle \in R$ を xRy と表記している．A の任意の非空部分集合が最小元をもつような半順序 R を A 上の整列順序（well-order）とよぶ．集合 A とその上の整列順序の順序対 $\langle A, R \rangle$ を整列集合とよぶ．

選択公理からは次の命題を示すことができることに注意しましょう．

Theorem 1.3 (整列可能定理)**.** 任意の集合に対して，その上の整列順序が存在する．

では順序数を定義します．

Definition 1.4. 集合（またはクラス）x が推移的（transitive）であるとは，$\forall y \in x \forall z \in y (z \in x)$ となっていることである．

Definition 1.5. 順序数（ordinal）とは，推移的かつ $\in$ によって整列順序づけられているような集合である．

順序数の例はこの後にすぐ出てきます．順序数という名前は次の定理に由来します．

Theorem 1.6. 任意の整列集合 $\langle A, R \rangle$ に対して，それと順序同型となる順序数 C が一意に存在する．すなわち，全単射 $f \colon A \to C$ が存在して，$\forall x, y \in A (xRy \leftrightarrow f(x) \in f(y))$ である．

また，順序数には大小関係を自然に入れることができます．

Definition 1.7. 順序数 α, β に対して，その大小関係を $\alpha < \beta \iff \alpha \in \beta$ と定義する．

定義より、最小の順序数は $\emptyset$ と分かります．続いて，ある順序数の次に大きな順序数を得る操作を定義します．

Definition 1.8. $S(\alpha) = \alpha \cup \{\alpha\}$ とする．$S(\alpha)$ という形で書くことのできる順序数を後続順序数（successor ordinal）といい，そうでない順序数を極限順序数（limit ordinal）という．

任意の順序数 α に対して $S(\alpha)$ は α よりも大きな順序数のうち最小のものであることは容易に示されます．

Definition 1.9. $\forall \beta \leq \alpha (\beta = \emptyset \vee \beta$は後続順序数$)$ となる順序数 α を自然数（natural number）という．これらは $0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}, 3 = \{0, 1, 2\}, \ldots, n = \{0, 1, \ldots, n-1\}$ というように表記される．

ここで，無限公理と内包性公理を用いると，自然数全体の集合が存在が言えます．自然数全体の集合もまた順序数であり，ω と書かれます．ω は最小の極限順序数です．ここで順序数に関する準備は終えて，次に濃度と基数について定義することにします．

Definition 1.10. 集合 A の濃度とは，A と全単射が存在するような最小の順序数を指し，$|A|$ と書く．

選択公理によって，任意の集合の濃度を定義できます．というのも，選択公理からは **Theorem 1.3.** が導かれるので，任意の集合には整列順序を入れることができ，それは必ずある順序数と順序同型となるからです．

Definition 1.11. 順序数 α が基数であるとは，$|\alpha| = \alpha$ となることである．

つまり，基数とは濃度を表すような順序数のことです．自然数や ω といった順序数は基数ですが，例えば $S(\omega) = \{0, 1, \ldots, \omega\}$ はそれより小さな順序数 ω との間に全単射が存在するので基数ではありません．最小の無限基数 ω は $\aleph_0$ と書かれ，無限基数はその大きさの順に $\aleph_1, \aleph_2, \ldots, \aleph_\omega, \ldots$ あるいは $\omega_1, \omega_2, \ldots, \omega_\omega \ldots$ のように表記されます．基数の和や積，冪計算は次のように定義されます．

Definition 1.12. κ, λ を基数とする．κ と λ の和と積はそれぞれ $\kappa + \lambda = |\kappa \times \{0\} \cup \lambda \times \{1\}|, \kappa \cdot \lambda = |\kappa \times \lambda|$ と定める．また，κ^λ は，λ から κ への関数全体の集合の濃度を表す．

ここでようやく連続体仮説（Continuum Hypothesis，CH）とは何かを説明することができます．CH とは

$$2^{\aleph_0} = \aleph_1$$

という命題を指します．以上，長々と順序数と基数について述べてきましたが，今回の発表において順序数と基数のフォーマルな定義自体はあまり問題にはなりません．分かっていてほしいのは

- 基数とは集合の大きさを表すためのパラメータである
- 順序数とは集合の元を数え上げるためのパラメータである

ということです．たとえば，可算集合の大きさを表すために基数 $\aleph_0 = \omega$ が用いられ，その $\aleph_0$ 個の元を数え上げるために ω 未満の順序数，すなわち自然数が用いられるわけです．

1.3 モデルと無矛盾性証明

次にモデルという概念を導入します．

Definition 1.13. 文 ϕ のクラス M への相対化とは，ϕ に含まれる量化子 $\forall x, \exists x$ をすべて $\forall x \in M, \exists x \in M$ に置き換えてできた文のことで，ϕ^M と書く．相対化 ϕ^M が成り立つ（すなわち ZFC から導かれる）とき，文 ϕ は M において真であるという．また，文の集合 Σ に属する文がすべて M において真ならば，M は Σ のモデルであるという．

ある公理系 Σ のモデルとは，その内部で Σ を成り立たせる具体的な世界のことです．M が ZFC のモデルだとすると，ZFC から導かれる文 ϕ は必ず M においても真，すなわち ϕ^M が成り立ちます．次の補題で示されるように，モデルを作ることで Σ の（相対的な）無矛盾性を示すことが可能となります．

Theorem 1.14. Σ を文の集合とし，あるクラス M は空でない Σ のモデルであるとする．このとき，ZF(C) が無矛盾ならば，Σ もまた無矛盾である．

Proof. Σ から矛盾が導かれるとする．このとき，ある文 ϕ について，$\phi \wedge \neg\phi$ を Σ から導くことが可能だが，M は Σ のモデルなので，$\phi^M \wedge \neg\phi^M$ となる．よって，ZF(C) が矛盾する． □

上の命題において，ZF(C) が無矛盾であるという仮定は外すことができません．なぜなら，Gödel の不完全性定理により，ZF(C) は無矛盾である限り，自身の無矛盾性を示すことはできないからです．集合論では，このようにモデルを構成することで様々な命題の無矛盾性を示します．ここで一つとても簡単なモデルの例をあげておきましょう．

Example 1.15. $M = \{\emptyset\}$ とすると，M は空集合・外延性・内包性公理・$\forall x(x = \emptyset)$ のモデルである．よって，ZF(C) が無矛盾であれば，「空集合・外延性・内包性公理・$\forall x(x = \emptyset)$」もまた無矛盾である．

集合論では様々な言明の相対化を考えることになるのですが，相対化によって意味がかわってしまうものとそうでないものがあります．

Definition 1.16. 論理式 $\phi(v_0, \ldots, v_{n-1})$ がクラス M に関して絶対的である（absolute for M）とは，

$$\forall v_0, \ldots, v_{n-1} \in M(\phi^M(v_0, \ldots, v_{n-1}) \leftrightarrow \phi(v_0, \ldots, v_{n-1}))$$

となることである．

クラス M の取り方によっては，とても簡単な論理式すらも絶対的ではありませんが，実は今回に限っては絶対性のチェックが大変な箇所は非常に少なくなっています．あらかじめその問題の箇所を注意しておくと，「κ が基数である」という言明は ZFC のモデルに関してさえ絶対的ではありません．ZFC のモデル M において「κ が基数である」という言明が真であったとしても，κ が本当に基数である保証はないのです．その理由について簡単に説明しましょう．κ が基数であることを確かめるにはそれよりも小さな順序数との全単射が存在しないことを確かめなくてはなりませんが，M の中にそのような全単射が存在しなければ，κ は M の中では基数としてふるまいます．しかし、M の外には κ が基数であることを否定するような全単射があるかもしれません．もしあったなら、M の外では κ はもはや基数ではありません．今回はこのような基数についての箇所以外の絶対性の議論には立ち入らないことにします．

2　証明の概要

準備をおえたところで，今回の無矛盾性証明のアウトラインをなぞっておきましょう．連続体仮説 CH はもともと集合論の創始者である Georg Cantor によって 19 世紀末に予想された命題です．20 世紀に入ってからも CH は集合論の主要な未解決問題として残りましたが，1938 年，Kurt Gödel によって，ZF が無矛盾ならば，ZFC+CH もまた無矛盾であることが示されました[*2]．これはつまり，ZF が矛盾しない限り ZFC からは ¬CH が導かれないということです．一方で ZFC+¬CH の無矛盾性はなかなか示すことができなかったのですが，1963 年，Paul Cohen によって次が示されました．

Theorem 2.1. ZFC が無矛盾ならば，ZFC+¬CH もまた無矛盾である．

ゆえに，CH は ZFC から証明も反証もされない，すなわち独立命題であると示されたのです．このとき Cohen が用いた証明テクニックが強制法（forcing）です．強制法はその汎用性から様々な無矛盾性証明に用いられるようになり，集合論を大きく発展させることになりました．[*3]今回の目標は **Theorem 2.1** を示すことですが，ここでは，もとの証明ではなく，より洗練された現代的な証明に沿って説明したいと思います．その証明の流れは以下のようになります．

Step 1　ZFC の可算推移的モデル（c.t.m.）M をとる．
Step 2　M を拡大することで $M[G]$ を構成する．
Step 3　$M[G]$ が ZFC のモデルとなっていることを示す．
Step 4　¬CH が $M[G]$ において真であることを示す．

この手順をふむことで ZFC+¬CH のモデル $M[G]$ が構成されるので，**Theorem 1.14** より **Theorem 2.1** を示すことができます．Step 2 におけるモデル $M[G]$ の構成には poset というものを用います．poset の取り方によらず $M[G]$ は ZFC のモデルになりますが，その poset の組み合わせ論的性質は $M[G]$ に大きく影響し，用いる poset を工夫することで $M[G]$ はさまざまな独立命題のモデルになります．使う poset を変更するだけで異なる無矛盾性証明を得ることが可能というのが強制法の強みです．今回の発表では Step 1 の箇所は強制法の本質に関係しない部分なので省くことにして，次の章から Step 2 以降について解説します．[*4]

[*2] 実際には ZFC+GCH が無矛盾であることを示しました．GCH とは一般連続体仮説とよばれるもので，CH の自然な一般化です．
[*3] Cohen はその業績を認められて 1966 年にフィールズ賞を授与されています．
[*4] 実はこの証明の説明には厳密でない箇所があります．実際には M と $M[G]$ はそれぞれ ZFC の十分大きな有限部分のモデル，ZFC+¬CH の十分大きな有限部分のモデルとしなければいけないのです．というのも，Gödel の不完全性定理関連の事情により，

3　M[G] の構成

この章では Step 2 の作業をします．モデル $M[G]$ を構成するには poset とその generic フィルターを用います．まずそれらについての基本的事項を述べることにします．

Definition 3.1. poset とは，集合 P とその上の推移的かつ反射的な関係 $\leq$，そして $\leq$ に関する最大元 1 の組 $\mathbb{P} = \langle P, \leq, 1\rangle$[*5]である．

Definition 3.2. $\mathbb{P}$ を poset，$p, q \in P$ とする．p が q の拡大（extension）であるとは，$p \leq q$ となることである．2 つの元 p, q が共存可能（compatible）であるとは，p と q の共通拡大が存在することである．

なぜ拡大や共存可能というのか気になるかもしれませんが，これに限らずこの章に出てくる言葉の意味は後になって徐々に明らかになります．

Definition 3.3. $\mathbb{P}$ を poset とする．$D \subseteq P$ が $\mathbb{P}$ で稠密（dense）であるとは，$\forall p \in P \exists d \in D(d \leq p)$ ということである．

Definition 3.4. poset $\mathbb{P}$ の上のフィルター（filter）とは，$G \subseteq P$ で次を満たすもののことである：

(1) $\forall p \in G \forall q \in P(p \leq q \to q \in G)$
(2) $\forall p, q \in G \exists r \in G(r \leq p \wedge r \leq q)$

M を ZFC の c.t.m. とする．G が M 上 $\mathbb{P}$-generic であるとは，それが $\mathbb{P}$ のフィルターであり，かつ次を満たすことである：

(3) $\forall D \in M(D \subseteq P \wedge D \text{ は } P \text{ で稠密} \to G \cap D \neq \emptyset)$

M が可算集合であることから，generic なフィルター G は簡単に存在を示すことが可能です．

Lemma 3.5. M が ZFC の c.t.m. であり，$\mathbb{P}$ を poset とする．$p \in P$ ならば，p を元として含む M 上 $\mathbb{P}$-generic な G が存在する．

Proof. M に属する稠密部分集合はもちろん可算なので，それらを $D_n (n \in \omega)$ と数え上げる．p_n を帰納的に $p_0 = p$，p_{n+1} を D_n に属する p_n の拡大として定めると $G = \{q : \exists n(q \leq p_n)\}$ は M 上 $\mathbb{P}$-generic. □

しかし，この G は必ずしも M には属していないということに注意しましょう．以降，つねに M は ZFC の c.t.m. で，$\mathbb{P}$ は M に属する poset，そして G は M 上 $\mathbb{P}$-generic であるとします．次に $M[G]$ を構成します．

Definition 3.6. 集合 $\dot{x}$ が $\mathbb{P}$-name であるとは，その任意の元が $\mathbb{P}$-name と P の元の順序対になっていることである．

ZFC からは ZFC の集合モデルの存在は示すことができないからです．厳密には以下のような議論がなされます．ZFC+¬CH が矛盾を導くとすれば，そのときに用いられる仮定は高々有限です．それらの仮定のモデルを $M[G]$ として構成すれば **Theorem 1.14** と同様の議論により ZFC もまた矛盾を導きます．この $M[G]$ の構成に必要な，M の満たすべき ZFC の公理もまた有限なので，その場合は M の存在を示すことが可能です．こういったメタ数学的な都合は一度考え始めると大変なので，最初のうちはあまり気にしすぎないのがよいと思い注釈に回すことにしました．

[*5] 3 つ組 $\langle x, y, z\rangle$ は $\langle\langle x, y\rangle, z\rangle$ のように定義します．

この $\mathbb{P}$-name は再帰的に定義されるものです．例えば，空集合 $\emptyset$ は $\mathbb{P}$-name です．$p, q \in P$ とすれば，$\{\langle \emptyset, p\rangle\}$ や $\{\langle \emptyset, p\rangle, \langle \{\langle \emptyset, p\rangle\}, q\rangle\}$ なども $\mathbb{P}$-name となります．

Definition 3.7. M に属する $\mathbb{P}$-name 全体を $M^{\mathbb{P}}$ とする．また，$\mathbb{P}$-name $\dot{x}$ に対して $\dot{x}^G = \{\dot{y}^G : \exists p \in G(\langle \dot{y}, p\rangle \in \dot{x})\}$ と再帰的に定義する．このとき，$M[G] = \{\dot{x}^G : \dot{x} \in M^{\mathbb{P}}\}$ を M の generic 拡大とよぶ．

これまでの $M[G]$ の構成を振り返りましょう．generic 拡大にとって poset の元とは generic 拡大の一部の情報をもつような部品だと思うことができます．p が q の拡大であるとき，p とは q の情報をすべてもつような上位互換の部品です．一方で，q よりも p から構成される対象の自由度は小さくなるので $p \leq q$ と書かれます．また，共存可能な poset の元は，互いに矛盾しないような情報をもつと思うことができるので，共存可能な元の集合であるフィルターは，generic 拡大の設計図にあたります．$M[G]$ とはフィルター G を介して M から構成される対象物の全体であり，その原料となるのが，$\mathbb{P}$-name です．poset の元が情報をもつとはどういうことなのか，フィルターのもつ generic 性はどこで用いられるのかは追って説明します．

4 M[G] は ZFC のモデルである

次は Step 3 です．ここでは次を示すのが目標です．

Theorem 4.1. $M[G]$ は $M \cup \{G\}$ を元として含む ZFC の c.t.m. である．

この定理をいくつかの補題に分割して示します．

Lemma 4.2. $M \cup \{G\} \subseteq M[G]$ である．

Proof. 任意の M の元に対応する $\mathbb{P}$-name を構成しよう．$x \in M$ として，$\check{x}$ を次のように再帰的に定義する．

$$\check{x} = \{\langle \check{y}, 1\rangle : y \in x\}$$

このとき明らかに $\check{x}$ は M に属する $\mathbb{P}$-name であり，$\check{x}^G = x$ となるので，$M \subseteq M[G]$ である．また，

$$\dot{G} = \{\langle \check{p}, p\rangle : p \in P\}$$

と定めれば，$\dot{G}^G = G$ となるので，これが G に対応する $\mathbb{P}$-name であり，$G \in M[G]$ である． □

ZFC のうちのいくつかの公理が $M[G]$ で真であることは容易に確かめることができます．

Lemma 4.3. $M[G]$ において空集合，対，無限公理は真である．

Proof. まず，空集合と無限公理は $\emptyset, \omega \in M \subseteq M[G]$ よりよい．次に，$\dot{x}^G, \dot{y}^G \in M[G]$ に対して，

$$\mathrm{pair}(\dot{x}, \dot{y}) = \{\langle \dot{x}, 1\rangle, \langle \dot{y}, 1\rangle\}$$

と定める．このとき，$\mathrm{pair}(\dot{x}, \dot{y})^G = \{\dot{x}^G, \dot{y}^G\}$ であるから，対の公理は $M[G]$ で成り立つ． □

Lemma 4.4. $M[G]$ において外延性公理と基礎の公理は真である．

Proof. 一般に，クラス M が推移的ならば，外延性公理については M への相対化が

$$\forall x, y \in M(\forall z \in M(x \in z \leftrightarrow y \in z) \to x = y)$$

と書けることから，M において真であると言える．$M[G]$ が推移的であることは $M[G]$ の構成より明らかなので，外延性公理は $M[G]$ において真である．基礎の公理は任意のクラスで成り立つ．[*6] □

残りの公理が $M[G]$ において真であることを示すには強制関係というアイデアが必要となります．強制関係を導入することでより詳細な $M[G]$ の情報を得ることができます．

Definition 4.5. $\dot{v}_0, \ldots, \dot{v}_{n-1}$ を $\mathbb{P}$-name とし，$p \in P$ とする．$\phi(v_0, \ldots, v_n)$ を論理式として，p を元として含む任意の M 上 $\mathbb{P}$-generic な G に対して，$\phi^{M[G]}(\dot{v}_0^G, \ldots, \dot{v}_{n-1}^G)$ が成り立つとき，$p \Vdash_{\mathbb{P},M} \phi(\dot{v}_0, \ldots, \dot{v}_{n-1})$ と書く．

$\Vdash$ についている添字はしばしば省略されます．強制関係について重要なのは次の 2 つの定理です．

Theorem 4.6 (真理性補題)**.**

$$\exists p \in G(p \Vdash \phi(\dot{v}_0, \ldots, \dot{v}_{n-1})) \iff \phi^{M[G]}(\dot{v}_0^G, \ldots, \dot{v}_{n-1}^G)$$

Theorem 4.7 (定義可能性補題)**.** ある論理式 $\psi(x, y, v_0, \ldots, v_{n-1})$ が存在して，

$$p \Vdash \phi(\dot{v}_0, \ldots, \dot{v}_{n-1}) \iff \psi^M(p, \mathbb{P}, \dot{v}_0, \ldots, \dot{v}_{n-1})$$

となる．[*7]

強制法の議論において用いるのは定義とそれに続くこの 2 つの定理がほとんどです．この定理を示すのはかなり大変で面倒な仕事なので，それはまたの機会に譲ることにします．これらの定義と定理がどんな意味をもつのかを説明します．強制関係 $p \Vdash \phi$ とは poset の元 p のもつ部分情報だけから $M[G]$ において ϕ が成り立つということが帰結できるという意味です．$p \leq q$ のとき，$p \in G$ ならば G は上に閉なので必ず $q \in G$ です．よって，$q \Vdash \phi \Rightarrow p \Vdash \phi$ となり，p は q よりも多くの $M[G]$ に関する情報をもつことになります．**Theorem 4.6** は $M[G]$ で成り立つことは必ずある部品 p のもつ部分的な情報から帰結することを意味します．**Theorem 4.7** はこのような強制関係が M の内部で定義できることを意味しています．本来の強制関係の定義では，M に属するとは限らないような M 上 $\mathbb{P}$-generic な G について知っている必要があるので，いわば M の外側にいる立場の定義でした．しかし，実は M の内側にいたとしても（つまり M の情報しか持っていなかったとしても），p がどんな文を強制するのかということは分かるし，$M[G]$ で成り立つことの見当もつくのです．強制関係を用いることで ZFC の残りの公理も $M[G]$ において真であることを示すことができるのですが，すべて示すのは大変なので，今回は例として内包性公理だけ示すことにします．

Theorem 4.8. $M[G]$ は内包性公理を満たす．

Proof. 任意の $\dot{x} \in M^{\mathbb{P}}$ と任意の論理式 $\phi(v)$（ただし v 以外の自由変数は含まないとするが，含む場合も容易である）に対して，

$$z = \{v \in \dot{x}^G : \phi^{M[G]}(v)\} \in M[G]$$

を満たすことを示せばよい．この集合に対応する $\mathbb{P}$-name は，

$$\dot{z} = \{\langle \dot{v}, p \rangle \in \mathrm{dom}(\dot{x}) \times P : p \Vdash \dot{v} \in \dot{x} \wedge \phi(\dot{v})\}$$

[*6] 基礎の公理について何も考えなくてよい理由は私たちのモデルの定義が $\in$ モデル（$\in$ の解釈が一般の二項関係ではなく membership 関係に限定されているモデル）の定義になっているからです．

[*7] 右辺の式は $(p \Vdash^*_{\mathbb{P}} \phi(\dot{v}_0, \ldots, \dot{v}_{n-1}))^M$ と書かれたりします．

であり，$\dot{z}^G = z$ となる．これを確かめよう．まず，定義可能性補題より，M において内包性公理を用いることで $\dot{z} \in M$ と分かるので，$\dot{z} \in M^{\mathbb{P}}$ である．次に，$\dot{v}^G \in z$ とすると，$p \in G$ が存在して，$\langle \dot{v}, p\rangle \in \dot{z}$ である．$\dot{z}$ の定義より，$p \Vdash \dot{v} \in \dot{x} \wedge \phi(\dot{v})$ となるから，真理性補題より $\dot{v}^G \in \dot{x}^G$ かつ $\phi^{M[G]}(\dot{v})$ であるから，$\dot{z}^G \subseteq z$．逆に，$\dot{v}^G \in z$ とすると，$\dot{v}^G \in \dot{x}^G$ かつ $\phi^{M[G]}(\dot{v})$ である．真理性補題より，ある $p \in G$ が存在して $p \Vdash \dot{v} \in \dot{x} \wedge \phi(\dot{v})$ なので，$\langle \dot{v}, p\rangle \in \dot{z}$ だから $\dot{v}^G \in \dot{z}^G$ である．よって，$z \subseteq \dot{z}^G$ となり示された． □

5 M[G] は ¬CH を満たす

Step 4 に進みます．ここではうまく $\mathbb{P}$ をとることで $M[G]$ において ¬CH も真であるようにします．今回の証明で用いる poset は次のようなものです．

Definition 5.1.

$$\mathrm{Fn}(I, J) = \{p : p \text{ は関数} \wedge \mathrm{dom}(p) \subseteq I \wedge \mathrm{ran}(p) \subseteq J \wedge |p| < \omega\}$$

とし，$p, q \in \mathrm{Fn}(I, J)$ に対して $p \leq q \iff q \subseteq p$ と定める．このときの最大元は $\emptyset$ である．この poset を Cohen poset とよぶ．

以降 $\mathbb{P} = \langle \mathrm{Fn}(\kappa \times \omega, 2), \leq, \emptyset\rangle$ とします．ここで κ とは M における不可算基数です．

Theorem 5.2. M 上 $\mathbb{P}$-generic な G に対して，

$$f_\alpha(n) = (\bigcup G)(\alpha, n)$$

は相異なる ω から 2 への関数．

Proof. フィルターの定義より，$\bigcup G$ は関数で，$\mathrm{dom}(\bigcup G) \subseteq \kappa \times \omega$ かつ $\mathrm{ran}(\bigcup G) \subseteq 2$ であることはよい．任意の $i \in \kappa \times \omega$ に対して

$$D_i = \{p \in P : i \in \mathrm{dom}(p)\}$$

とおくとこれは $\mathbb{P}$ において稠密であり，M に属するから，G の generic 性により，すべての i に対して $D_i \cap G \neq \emptyset$ となって $\mathrm{dom}(\bigcup G) = \kappa \times \omega$ が示される．[*8]よって，$\bigcup G$ は $\kappa \times \omega$ から 2 への関数であり，各 f_α は ω から 2 への関数である．さらに，$\alpha \neq \beta$ のとき，

$$D_{\alpha\beta} = \{p \in P : \exists n \in \omega(\langle \alpha, n\rangle, \langle \beta, n\rangle \in \mathrm{dom}(p) \wedge p(\alpha, n) \neq p(\beta, n))\}$$

とおくと，これもまた $\mathbb{P}$ において稠密で M に属するため，$D_{\alpha\beta} \cap G \neq \emptyset$ である．ゆえに，$f_\alpha \neq f_\beta$ である． □

この証明をよく眺めると，フィルターのもつ generic 性がどのように効いているのかが分かります．稠密集合とはほとんどの poset の元で成り立つようなごく一般的（generic）な性質を記述しています．フィルター G はこれらの稠密集合と交わることで，その性質を反映している構成物をつくることができるのです．上の定理で構成された f_α は $M[G]$ に含まれるので，$M[G]$ において $2^\omega \geq |\kappa|$ であることが示されます．よって，ここで κ を M における ω_1 よりも大きな不可算基数とおいてしまえばよいだろうと思えます．しかし，実はこれでは不十分で，もう一つだけ確認すべき事項があります．次の例を見てみましょう．

[*8] 同様にして $\mathrm{ran}(\bigcup G)$ が全射となることも示すことができます．

Example 5.3. κ を M における不可算基数とする．M 上 $\mathrm{Fn}(\kappa,\omega)$-generic な G によって generic 拡大すると $M[G]$ には κ から ω への全射が存在するため，κ は $M[G]$ においては基数ですらない．

つまり，一般には M の基数は $M[G]$ の基数であるとは限らないのです．ここで **Definition 1.16** とそれに続くコメントなどを参照してください．

Definition 5.4. $\mathbb{P}\in M$ を poset とするとき，$\mathbb{P}$ が基数を保存するとは，任意の M 上 $\mathbb{P}$ 上 generic な G について，M における基数が $M[G]$ においても基数となることである．[*9]

今回用いる Cohen poset $\mathbb{P}$ は基数を保存します．基数が保存されるかどうかは poset の組合せ論的性質から導かれます．

Definition 5.5. P を poset とする．$A\subseteq P$ が $\mathbb{P}$ の反鎖（antichain）であるとは，A の相異なる 2 元はすべて共存可能になっていないことである．poset $\mathbb{P}$ が可算鎖条件（countable chain condition，c.c.c.）を満たすとは，$\mathbb{P}$ の任意の反鎖が高々可算であることをいう．

Lemma 5.6. poset $\mathbb{P}$ は $P\in M$ かつ $(\text{c.c.c. を満たす})^M$ とする．$f\colon A\to B$ が $M[G]$ に属する関数のとき，M に属する関数 $F\colon A\to\mathcal{P}(B)$ が存在し，各 $a\in A$ に対して，$f(a)\in F(a)$ かつ $(|F(a)|\leq\omega)^M$ となる．

Proof. $f=\dot{f}^G$ となる $\dot{f}\in M^{\mathbb{P}}$ をひとつとる．このとき，ある $p\in G$ が存在して

$$p\Vdash \dot{f}\text{は}\check{A}\text{から}\check{B}\text{への関数.}$$

ここで

$$F(a)=\{b\in B:\exists q\leq p(q\Vdash \dot{f}(\check{a})=\check{b})\}$$

と $F\colon A\to\mathcal{P}(B)$ を定義する．これが求める F であることを確かめる．まず，定義可能性補題より $F\in M$．次に $(|F(a)|\leq\omega)^M$ であることを示す．M において選択公理を用いることで，$Q\colon F(a)\to P$ が M の元としてとれて，各 $b\in F(a)$ に対して，

$$Q(b)\leq p\wedge Q(b)\Vdash \dot{f}(\check{a})=\check{b}$$

となる．相異なる $F(a)$ の元 b,b' をとると，$Q(b)$ と $Q(b')$ は共存可能ではない．なぜなら，$Q(b)$ と $Q(b')$ の共通拡大が存在したとすると，その共通拡大を含む M 上 P-generic な H が存在し，このとき，$M[H]$ においては $\dot{f}^H\colon A\to B$ は $\dot{f}^H(a)=b$ かつ $\dot{f}^H(a)=b'$ を満たすことになってしまい矛盾するからである．よって，$\{Q(b):b\in F(a)\}$ は $\mathbb{P}$ の反鎖をなすが，$Q\in M$ より，M においてもこの集合は $\mathbb{P}$ の反鎖であり，$(\text{c.c.c. を満たす})^M$ より $(|F(a)|\leq\omega)^M$ である． □

Theorem 5.7. poset $\mathbb{P}\in M$ が M において c.c.c. を満たすとき，$\mathbb{P}$ は基数を保存する．

Proof. $v=0,v=1,\dots,v=\omega$ という論理式は絶対的[*10]なので，ω より大きな基数についてだけが問題になる．$\alpha,\beta\geq\omega$ とし，$\alpha<\beta$ とする．全射 $f:\alpha\to\beta$ が $M[G]$ 内に存在するとする．$B=\beta$，$A=\alpha<\beta$ とおいて先の補題を利用すれば，$F:\alpha\to\mathcal{P}(\beta)$ が M 内に存在する．このとき M において，$\beta\subseteq\bigcup_{\xi<\alpha}F(\xi)$ だから，$|\beta|\leq|\bigcup_{\xi<\alpha}F(\xi)|\leq|\alpha|$ となる．ゆえに，$|\alpha|=|\beta|$ となり，M において β は基数でない． □

[*9] 逆に $M[G]$ における基数 κ は M においても基数です．というのも，$M[G]$ において κ とそれより小さな順序数の間に全単射が存在しないならば，$M[G]$ よりも小さな M にもそのような全単射は存在しないからです．

[*10] これらの証明は絶対性に関してやや詳細に述べる必要があるのでここでは省略しますが，あまり大変ではありません．

最後に，今回用いた poset が c.c.c. を満たすことを確認します．その証明には次の組み合わせ論的事実を用います．

Lemma 5.8 (Δ-システム補題)**.** 有限集合からなる不可算集合族 F は Δ-システムであるような不可算な部分集合族 $D \subseteq F$ をもつ．ここで，集合族 $\{x_i : i \in I\}$ が Δ-システムであるとは，ある集合 r が存在して，任意の相異なる $i, j \in I$ に対して，$x_i \cap x_j = r$ となることである．また，この r を根（root）という．

Proof. ある自然数 n について，F の元はすべて n 元集合であると仮定しても一般性を失わない．$n = 0$ のときは自明である．n で補題が成立しているとして，F の元がすべて $n+1$ 元集合であると仮定しよう．ある a が存在して，$E = \{x \in F : a \in x\}$ が不可算なら，$\{x \backslash \{a\} : x \in E\}$ に対して帰納法の仮定を用いれば，Δ-システムをなす $D \subseteq E$ を見つけることができる．そのような a が存在しないと仮定する．この場合は互いに交わらない不可算な部分集合族 $D = \{x_\alpha : \alpha < \omega_1\}$ をとることが可能である．このことは，任意の $\alpha < \omega_1$ に対して，$\bigcup\{x_\beta : \beta < \alpha\}$ と交わる $x \in F$ は可算個しか存在しないことが仮定より言えるので，α に関する超限帰納法[*11]より示される． □

Theorem 5.9. *I を任意の集合，J を可算集合としたとき $\mathrm{Fn}(I, J)$ は c.c.c. を満たす．*

Proof. Δ-システム補題を用いる．$\mathrm{Fn}(I, J)$ の元を ω_1 個とり，それらを $\{p_\alpha : \alpha < \omega_1\}$ とおく．また，各 p_α の定義域を a_α とおく．ここで Δ-システム補題によって不可算な $X \subseteq \omega_1$ が存在して $\{a_\alpha : \alpha \in X\}$ が Δ-システムをなす．この根を r とすれば，r が有限で J は可算集合だから，p_α の r への制限は可算とおりの可能性しかない．よって不可算集合 $Y \subseteq X$ が存在し，すべての $\alpha \in Y$ に対して p_α の r への制限は一致する．したがって $\{p_\alpha : \alpha \in Y\}$ は共存可能である． □

よって，$\mathbb{P} = \mathrm{Fn}(\kappa \times \omega, 2)$ は c.c.c. を満たすので，**Theorem 5.7** より $\mathbb{P}$ は基数を保存します．

以上の議論をまとめます．κ を M における ω_1 よりも大きな不可算基数とします．Cohen poset $\mathrm{Fn}(\kappa \times \omega, 2)$ は少なくとも κ 個 ω から 2 への関数を付け加えるため，$M[G]$ においては $2^{\aleph_0} \geq \kappa$ となっています．ここで，Cohen poset はすべての基数を保存するので，M における基数と $M[G]$ における基数が一致していることに注意しましょう．よって，$M[G]$ においてはもはや CH は成り立っていません．ゆえに，$\neg$CH の相対的無矛盾性が証明されました．

参考文献

[1] K. Kunen 著，藤田博司訳．集合論　独立性証明への案内．日本評論社，2008.

[2] 新井敏康．数学基礎論．岩波書店，2011.

[*11] 超限帰納法とは次の定理を利用する証明法のことです:δ を順序数とする．すべての順序数 $\alpha < \delta$ に対して $(\forall \beta < \alpha \phi(\beta)) \to \phi(\alpha)$ が成り立つならば，$\forall \alpha < \delta \phi(\alpha)$ が成り立つ．この定理の証明は省略します．