集合に群構造が入ることと選択公理

alg-d
http://alg-d.com/math/ac/

2012 年 4 月 22 日

定理. 選択公理 $\Longleftrightarrow$ 任意の非空集合 X に群構造を入れることができる

証明. $(\Longrightarrow)$ X が有限集合の時は自明 ($\mathbb{Z}/n\mathbb{Z}$ を考えればよい) だから，X は無限集合とする．$\mathcal{P}_{\mathrm{fin}}(X) := \{x \subset X \mid x$ は有限集合 $\}$ とする．選択公理より，$|X| = |\mathcal{P}_{\mathrm{fin}}(X)|$，即ち全単射 $X \longrightarrow \mathcal{P}_{\mathrm{fin}}(X)$ が存在する．

> ※ 実は「任意の無限集合 X に対し $|X| = |\mathcal{P}_{\mathrm{fin}}(X)|$」は選択公理と同値である．証明は基数の性質の定理 9 を参照.

よって $\mathcal{P}_{\mathrm{fin}}(X)$ に群構造を入れられることを示せばよい.

自然な同一視 $\mathcal{P}(X) = 2^X$ で考えると $\mathcal{P}_{\mathrm{fin}}(X) = \{f \in 2^X \mid$ 有限個の $x \in X$ を除いて $f(x) = 0\}$ である．$2 = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$ は体だから，それの直積である 2^X は自然に環となる．このとき明らかに $\mathcal{P}_{\mathrm{fin}}(X) \subset 2^X$ は (加法についての) 部分群である．故に $\mathcal{P}_{\mathrm{fin}}(X)$ に群構造を入れることができた.

> ※ 同じことだが，直接演算を定義しても証明できる．$\mathcal{P}_{\mathrm{fin}}(X)$ 上の二項演算を対称差 $\triangle$ で定義する．(これが 2^X での加法に対応する．) 即ち
>
> $$x \triangle y := (x \cup y) \setminus (x \cap y) = (x \cup y) \cap (x^c \cup y^c)$$
>
> $(\mathcal{P}_{\mathrm{fin}}(X), \triangle)$ は群になる.
>
> > $\because$) $\emptyset \in \mathcal{P}_{\mathrm{fin}}(X)$ が単位元，$x \in \mathcal{P}_{\mathrm{fin}}(X)$ の逆元が x 自身であることは明らかだ

から，結合律を示せばよい．$x, y, z \in \mathcal{P}_{\mathrm{fin}}(X)$ に対し

$$\begin{aligned}
(x \triangle y) \triangle z &= [(x \cup y) \cap (x^c \cup y^c)] \triangle z \\
&= ([(x \cup y) \cap (x^c \cup y^c)] \cup z) \cap ([(x \cup y) \cap (x^c \cup y^c)]^c \cup z^c) \\
&= ([(x \cup y) \cup z] \cap [(x^c \cup y^c) \cup z]) \cap ([(x^c \cap y^c) \cup (x \cap y)] \cup z^c) \\
&= ([x \cup y \cup z] \cap [x^c \cup y^c \cup z]) \cap ((x^c \cap y^c) \cup (x \cap y) \cup z^c) \\
&= (x \cup y \cup z) \cap (x^c \cup y^c \cup z) \cap (x^c \cup y \cup z^c) \cap (y^c \cup x \cup z^c) \\
&= (x \cup y \cup z) \cap (x \cup y^c \cup z^c) \cap (x^c \cup y^c \cup z) \cap (x^c \cup y \cup z^c) \\
&= (x \cup [(y \cup z) \cap (y^c \cup z^c)]) \cap (x^c \cup (y^c \cap z^c) \cup (y \cap z)) \\
&= (x \cup [(y \cup z) \cap (y^c \cup z^c)]) \cap (x^c \cup [(y^c \cap z^c) \cup (y \cap z)]) \\
&= (x \cup [(y \cup z) \cap (y^c \cup z^c)]) \cap (x^c \cup [(y \cup z) \cap (y^c \cup z^c)]^c) \\
&= (x \cup (y \triangle z)) \cap (x^c \cup (y \triangle z)^c) \\
&= x \triangle (y \triangle z)
\end{aligned}$$

故に結合律が成り立つ．

($\Longleftarrow$) 整列可能定理を示す．$X \neq \emptyset$ を任意の集合とする．単射 $\lambda \longrightarrow X$ が存在しないような順序数 λ が存在するので，そのような λ を 1 つ取っておく．

※ $\lambda := \{\beta : 順序数 \mid 単射\ \beta \longrightarrow X\ が存在する\ \}$ と置けばよい．基数の性質の命題の証明を参照.

簡単のため，$X \cap \lambda = \emptyset$ とする．

仮定により $X \cup \lambda$ を群にすることができる．(その積を $\cdot$ とする．) このとき

$$任意の\ x \in X\ に対して，ある\alpha \in \lambda が存在して\ x \cdot \alpha \in \lambda$$

が成立する．

$\because$) 成立しないと仮定する．即ちある $x \in X$ が存在して，任意の $\alpha \in \lambda$ に対して $x \cdot \alpha \notin \lambda$ となる．写像 $f : \lambda \longrightarrow X$ を $f(\alpha) := x \cdot \alpha$ で定義すれば，これは積 $\cdot$ の性質により単射となり λ の取り方に矛盾する．

さて，直積 $\lambda \times \lambda$ に辞書式順序を入れる．するとこれは整列順序になる．そこで $g : X \longrightarrow \lambda \times \lambda$ を

$$g(x) := \min\{\langle \alpha, \beta \rangle \in \lambda \times \lambda \mid x \cdot \alpha = \beta\}$$

と定義すると，g は単射であり，よって X は整列可能である． $\square$

この定理を見てすぐに思いつくのは,「群」の部分を環や体などの別の構造にしたらどうなるか, という問題である. まず次の 2 点に注意する.

(1) $\mathcal{P}_{\mathrm{fin}}(X) \subset 2^X$ は積についても閉じている. 故に $\mathcal{P}_{\mathrm{fin}}(X)$ は (1 を持たない) 環になる.

> ※ $\mathcal{P}(X)$ の $\cap$ が 2^X の積に対応している. 勿論, 先ほどと同様に直接 $(\mathcal{P}_{\mathrm{fin}}(X), \triangle, \cap)$ が環になることを示すこともできる.

(2) $\Longleftarrow$ の証明には積 $\cdot$ から得られる写像が単射であることしか使っていない. 特に, 積 $\cdot$ が

$$\text{任意の } x, y, z \text{ に対して } x \cdot y = x \cdot z \Longrightarrow y = z$$
$$\text{任意の } x, y, z \text{ に対して } x \cdot z = y \cdot z \Longrightarrow x = y$$

という性質を満たしていれば先の証明は実行できる. (この条件を満たすことを消約 (cancellative) と言うことにする.)

(1)(2) より次の系が分かる.

系. 前定理は「群」の部分を

- 消約亜群 (亜群=magma=二項演算を持つ集合)
- 消約半群
- 消約アーベル半群
- quasigroup ($\forall a, b \exists x, y (a \cdot x = b,\ y \cdot a = b)$ を満たす消約亜群)
- loop (単位元を持つ quasigroup)
- アーベル群
- (1 の存在を仮定しない結合分配) 環

に変更しても成立する.

参考文献

[1] Does every non-empty set admit a group structure (in ZF)? - MathOverflow