環の極大イデアルの存在と選択公理

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

2012 年 4 月 3 日

定義. 次の性質を満たす $(R, +, \cdot, 0)$ を環という.

1. $(R, +, 0)$ はアーベル群である.
2. $(R, \cdot)$ は半群である.
3. 分配律 $(x+y)z = xz + yz,\ x(y+z) = xy + xz$ が成り立つ.
4. 0 以外の元を少なくとも一つ持つ.

※ ここでは乗法単位元 1 の存在を仮定しない.

定義. R を環とする.

1. 「任意の $x \in R$ に対し $x1 = x$」となる元 $1 \in R$ を右単位元という. 右単位元を持つ環を右単位的環ということにする.
2. 「任意の $x \in R$ に対し $1x = x1 = x$」となる元 $1 \in R$ を単位元という. 単位元を持つ環を単位的環という.
3. $e^2 = e$ となる元 $e \in R$ を冪等元 (idempotent) という.
4. $eRe = Re$ となる冪等元 $e \in R$ を left semicentral idempotent という. (左半中心冪等元と訳すことにする.)
5. 乗法が可換である環を可換環という.
6. 「$xy = 0 \Longrightarrow x = 0$ または $y = 0$」を満たす単位的可換環を整域という.
7. 任意の元が既約元の積に一意的に分解できる整域を一意分解整域という.

定義. 環 R の部分集合 $I \neq \emptyset$ が次の性質を満たすとき, I を左イデアルという.

1. $I \subset R$ は加法についての部分群である.

2. 任意の $x \in I$ と任意の $r \in R$ に対し $rx \in I$.

環 R の部分集合 $I \neq \emptyset$ が次の性質を満たすとき，I を右イデアルという．

1. $I \subset R$ は部分群である．
2. 任意の $x \in I$ と任意の $r \in R$ に対し $xr \in I$.

左イデアルかつ右イデアルであるような $I \subset R$ を両側イデアルという．ここでは，両側イデアルを単にイデアルと呼ぶことにする．また $I \subsetneq R$ となるイデアル I を真のイデアルという．真の左イデアルも同様.

定理. 次の命題は (ZF 上) 同値.

1. 選択公理
2. 右単位的環は極大左イデアルを持つ.
3. 右単位的環は極大イデアルを持つ.
4. 右単位的環の真の左イデアルはある極大左イデアルに含まれる.
5. 右単位的環の真のイデアルはある極大イデアルに含まれる.
6. 冪等元 ($\neq 0$) を持つ環は極大左イデアルを持つ.
7. 左半中心冪等元 ($\neq 0$) を持つ環は極大イデアルを持つ.
8. 単位的可換環は極大イデアルを持つ.
9. 一意分解整域は極大イデアルを持つ.

※ 命題「単位的環は極大イデアルを持つ」を Krull の定理と呼ぶようです.

証明. ($1 \Longrightarrow 2$) R を右単位的環とする．$X := \{\mathfrak{a} \subsetneq R \mid \mathfrak{a}$ は左イデアル $\}$ と置く．任意の $r \in R$ に対し $r0 = 0$ であるから $0 \subset R$ は左イデアル，よって $0 \in X$ となるから X は空でない.

X に $\subset$ で順序を入れる．$C \subset X$ を部分全順序とする．$I := \bigcup_{\mathfrak{a} \in C} \mathfrak{a}$ は左イデアルである.

$\because$) 任意の $x, y \in I$ と $r \in R$ を取る．I の定義より，ある $\mathfrak{a}, \mathfrak{b} \in C$ が存在して $x \in \mathfrak{a}$, $y \in \mathfrak{b}$ となる．C の全順序性より $\mathfrak{a} \subset \mathfrak{b}$ または $\mathfrak{b} \subset \mathfrak{a}$ である．$\mathfrak{a} \subset \mathfrak{b}$ としても一般性を失わない．このとき $x \in \mathfrak{a} \subset \mathfrak{b}$ であるから $x - y \in \mathfrak{b} \subset I$ である．また $rx \in \mathfrak{a} \subset I$ も成立する．故に I は左イデアルである.

今，R の右単位元を 1 とすれば任意の $\mathfrak{a} \in X$ に対して $1 \notin \mathfrak{a}$ である．故に $1 \notin I$ となる．よって $I \subset R$ は真の左イデアルとなる．即ち $I \in X$ であり，I は C の上界となる．従って Zorn の補題より X は極大元を持つ．それが R の極大左イデアルである．

1$\Longrightarrow$3 の証明も同様である．

$(1 \Longrightarrow 4)$ 右単位的環 R の真の左イデアルを $\mathfrak{b}$ とする．$X := \{\mathfrak{a} \subsetneq R \mid \mathfrak{a}$ は左イデアル，$\mathfrak{b} \subset \mathfrak{a}\}$ と置き，1$\Longrightarrow$2 と同じように Zorn の補題を適用すればよい．

1$\Longrightarrow$5 も同様.

$(1 \Longrightarrow 6)$ R を環とし，$e\,(\neq 0) \in R$ を冪等元とする．$\mathfrak{a} := \{x \in R \mid xe = 0\}$ は左イデアルである．

$\because$) $0e = 0$ だから $\mathfrak{a} \neq \emptyset$．任意の $x, y \in \mathfrak{a}$ と $r \in R$ を取る．このとき $(x-y)e = xe - ye = 0$，$(rx)e = r(xe) = 0$ となるから $x - y, rx \in \mathfrak{a}$．故に $\mathfrak{a}$ は左イデアルである．

また $R = Re \oplus \mathfrak{a}$ (左イデアルの直和) となる

$\because$) $R = Re + \mathfrak{a}$ は明らかなのであとは $Re \cap \mathfrak{a} = 0$ を示せばよい．そこで $xe \in Re \cap \mathfrak{a}$ を任意に取る．e が冪等元であることにより $xe = x(e^2) = (xe)e = 0$ である．

もし $\mathfrak{a} = 0$ であれば e は右単位元となるから，既に示された 2 により R は極大左イデアルを持つ．なので $\mathfrak{a} \neq 0$ とする．$X := \{\mathfrak{b} \subsetneq R \mid \mathfrak{b}$ は左イデアル，$\mathfrak{a} \subset \mathfrak{b}\}$ と置く．$\mathfrak{a} \in X$ だから $X \neq \emptyset$．X に $\subset$ で順序を入れる．$C \subset X$ を部分全順序とする．$I := \bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ は左イデアルである．

$\because$) 1$\Longrightarrow$2 のときと同様.

明らかに $\mathfrak{a} \subset I$ である．$I = R$ と仮定する．すると $e \in I$ となるから，ある $\mathfrak{b} \in C$ が存在して $e \in \mathfrak{b}$ となる．すると $R = Re \oplus \mathfrak{a} \subset \mathfrak{b}$ となるから $\mathfrak{b} \subsetneq R$ に矛盾する．故に $I \neq R$ である．即ち $I \in X$ で，I は C の上界となる．

従って Zorn の補題より X は極大元を持つ．それが R の極大左イデアルである．

$(3 \Longrightarrow 7)$ R を環とし，$e\,(\neq 0) \in R$ を左半中心冪等元とする．1$\Longrightarrow$6 のときと同様，$\mathfrak{a} := \{x \in R \mid xe = 0\}$ は左イデアルで，$R = Re \oplus \mathfrak{a}$ となる．$\mathfrak{a} \subset R$ は両側イデアルである．

$\because$) 右イデアルであることを示せばよい．任意の $x \in \mathfrak{a}$ と $r \in R$ を取る．e が左半中心冪等元だから $Re = eRe$，故にある $r' \in R$ が存在して $re = er'e$ となる．このとき

$(xr)e = x(re) = x(er'e) = (xe)r'e = 0$．故に $xr \in \mathfrak{a}$．

故に環同型 $R/\mathfrak{a} \cong Re$ が成り立つ．Re は右単位的環である．従って仮定 3 により $Re\,(\cong R/\mathfrak{a})$ は極大イデアルを持つ．剰余環の性質から R も極大イデアルを持つことが分かる．

$2 \Longrightarrow 8$，$3 \Longrightarrow 8$，$\cdots$，$7 \Longrightarrow 8$ と $8 \Longrightarrow 9$ は自明.

$(9 \Longrightarrow 1)$ 選択公理と同値な次の命題を示す.

木 $(T, \leq)$ は極大部分全順序集合を持つ.

※ $(T, \leq)$ を順序集合とする．$t \in T$ に対し $t^{\downarrow} := \{s \in T \mid s \leq t\}$ と書くことにする．任意の $t \in T$ に対し $(t^{\downarrow}, \leq)$ が全順序になるとき，$(T, \leq)$ を木と呼ぶ．同値性の証明は Zorn の補題・極大原理の定理 1 を参照.

$(T, \leq)$ を木とする．T の元を不定元とする多項式環 $\mathbb{Q}[T]$ を考える．$G \subset T$ で生成されるイデアル $G\mathbb{Q}[T] \subset \mathbb{Q}[T]$ は素イデアルである.

$L := \{G \subset T \mid (G, \leq)$ は全順序 $\}$ と置き $S := \mathbb{Q}[T] \setminus \bigcup_{G \in L} G\mathbb{Q}[T]$ を考える．素イデアルの和集合の補集合だから，S は積閉集合である．そこで $R := S^{-1}\mathbb{Q}[T]$ を考える．R は一意分解整域である．よって仮定 9 より極大イデアル $\mathfrak{m} \subset R$ を持つ.

$c \in \mathfrak{m}$ を取る．$c = x/s$ ($x \in \mathbb{Q}[T], s \in S, x$ と s は共通因子を持たない) と表示する．$x = q_0 f_0 + \cdots + q_n f_n$ ($q_i \in \mathbb{Q}^{\times}$，$f_i$ は T の元の積，$i \neq j \Rightarrow f_i \neq f_j$) と書ける．$c$ は非可逆だから $x \notin S$，即ち $x \in \bigcup_{G \in L} G\mathbb{Q}[T]$ だから $x \in G\mathbb{Q}[T]$ となる $G \in L$ が存在する．故に有限集合 $A \in L$ で二条件

$$\left.\begin{array}{l} f_0, \cdots, f_n \text{ は } A \text{ の中に因子を持つ.} \\ A \text{ の各元は } f_0, \cdots, f_n \text{ のどこかに因子として現れる.} \end{array}\right\} (*)_c$$

を満たすものが存在する．このような A は一意には定まらないが，高々有限個しかない．よって $E(c) := \{\max A \mid A$ は $(*)_c$ を満たす $\}$ は有限集合．定義から，$t \in E(c)$ のとき $c \in t^{\downarrow}R$ である.

$$D := \{t \in T \mid \text{任意の } c \in \mathfrak{m} \setminus \{0\} \text{ に対してある } r \in E(c) \text{ と } t \text{ が比較可能 }\}$$

と定める.

(a) $D \subset \mathfrak{m}$ である.

$\because$) $t \in D \setminus \mathfrak{m}$ と仮定する．$\mathfrak{m} \subset R$ は極大イデアル，よってある $a \in R$ と $c \in \mathfrak{m}$ が存在して $at + c = 1$ とできる．$\{t\} \in L$ であるから $t \in R$ は非可逆．故に $c \neq 0$．D

の定義よりある $r \in E(c)$ が有って t と r は比較可能．（この時 $c \in r^{\downarrow}R$ でもある．）
(i)$r \leq t$ の時．$c \in r^{\downarrow}R \subset t^{\downarrow}R$ であり，定義から $t \in t^{\downarrow}R$ だから $1 = at + c \in t^{\downarrow}R$
(ii)$t \leq r$ の時．$t \in r^{\downarrow}R$ だから $1 = at + c \in r^{\downarrow}R$

R の定義より $t^{\downarrow}R$ や $r^{\downarrow}R$ が R と一致することはありえない．よって (i)(ii) のどちらにしろ矛盾．故に $D \subset \mathfrak{m}$ である．

(b) D は全順序で，$t \in D$ に対して $t^{\downarrow} \subset D$ である．

$\because$) $t, s \in D$ とすると (a) により $t + s \in \mathfrak{m}$．よって $t + s$ は非可逆．従ってある全順序集合 $G \subset T$ が存在して $t + s \in G\mathbb{Q}[T]$ である．この時 $t, s \in G$ となるから，t と s は比較可能である．即ち $(D, \leq)$ は全順序である．

次に $t \in D$ として $v \in t^{\downarrow}$ を取る．任意の $c \neq 0$ を取る．$t \in D$ だからある $r \in E(c)$ が存在して t と r は比較可能となる．
(i) $r \leq t$ の時．$r, v \in t^{\downarrow}$ だから，T が木であることより r と v は比較可能である．
(ii) $t \leq r$ の時．$v \leq t \leq r$，即ち r と v は比較可能である．

よって (i)(ii) のどちらの場合でも $v \in D$ となる．

(c) $\mathfrak{m} \subset DR$ である．

$\because$) $c \in \mathfrak{m} \setminus DR$ と仮定する．$c \in \mathbb{Q}[T]$ と仮定してよい．勿論 $c \neq 0$ である．この時 $D \cap E(c) = \emptyset$ である．

$\because$) $t \in D \cap E(c)$ と仮定すると (b) から $c \in t^{\downarrow}R \subset DR$ となり矛盾する．

$E(c) = \{t_0, \cdots, t_k\}$ と書く．(各 t_i は互いに異なるとする．) $t_0, \cdots, t_k \notin D$ だから，各 $0 \leq i \leq k$ に対して「ある b_i $(\neq 0) \in \mathfrak{m}$ が存在して，全ての $r \in E(b_i)$ に対し t_i と r は比較不可能」が成り立つ．$b_i \in \mathbb{Q}[T]$ としてよい．

$q_0, \cdots, q_k \in \mathbb{Q}$ として $x = c + q_0 b_0 + \cdots + q_k b_k$ を考える．この時，$c, b_0, \cdots, b_k$ に含まれる各項が互いに打ち消してしまわないように q_i を選ぶ．($\mathbb{Q}$ が無限体なのでこのようなことは可能である．)

$w \in E(x)$ とする．$E(x)$ の定義より $(*)_x$ を満たすような全順序有限集合 A で $w = \max A$ となるものが存在する．

$$A_c := \{a \in A \mid a \text{ は } c \text{ に含まれる項のどれかに因子として含まれる}\}$$

と置くと，q_i の選び方から A_c は $(*)_c$ を満たす．故に $t_j = \max A_c$ となる番号 j が

存在する．$A_c \subset A$ だから $t_j = \max A_c \le \max A = w$．この j について，

$$A_{b_j} := \{a \in A \mid a \text{ は } b_j \text{に含まれる項のどれかに因子として含まれる }\}$$

と置くと，A_{b_j} は $(*)_{b_j}$ を満たす．故に $r := \max A_{b_j} \in E(b_j)$ であり，$A_{b_j} \subset A$ だから $r = \max A_{b_j} \le \max A = w$ となる．T は木だから t_j と r は比較可能になるが，これは b_j の取り方に矛盾する．故に $\mathfrak{m} \subset DR$ である．

(a)(c) により $\mathfrak{m} = DR$ である．部分全順序 $D \subset T$ が極大でないと仮定する．$D \subsetneq \widetilde{D} \subset T$ となる部分全順序 $\widetilde{D} \subset T$ が存在する．$t \in \widetilde{D} \setminus D$ を一つ取ると，(b) より全ての $r \in D$ に対し $r < t$ となることが分かる．すると $\mathfrak{m} = DR \subsetneq t^{\downarrow}R \subsetneq R$ となり，$\mathfrak{m}$ の極大性に矛盾する．従って $D \subset T$ は極大である． □

9 $\Longrightarrow$ 1 には別の証明もあるので紹介しておく．(詳しくは [5] を参照．)

$\{X_\lambda\}_{\lambda \in \Lambda}$ を互いに素な非空集合の族とする．選択集合の存在を示す．$X := \bigcup_{\lambda \in \Lambda} X_\lambda$ として $\mathcal{C} := \{A \subset X \mid \text{任意の } \lambda \in \Lambda \text{ に対して } |A \cap X_\lambda| \le 1\}$ と置く．明らかに，$(\mathcal{C}, \subset)$ の極大元は選択集合である．

X の元を不定元とする多項式環 $\mathbb{Q}[X]$ を考え $S := \mathbb{Q}[X] \setminus \bigcup_{A \in \mathcal{C}} A\mathbb{Q}[X]$ と置く．S は積閉集合であるから $S^{-1}\mathbb{Q}[X]$ を考えることが出来る．仮定により極大イデアル $\mathfrak{m} \subset S^{-1}\mathbb{Q}[X]$ が存在する．$\mathfrak{n} := \mathfrak{m} \cap \mathbb{Q}[X]$ と置く．$K := \mathfrak{n} \cap X$ とすれば $K\mathbb{Q}[X] = \mathfrak{n}$ であることが分かる．このとき，$K \in \mathcal{C}$ であることも分かる．$K\mathbb{Q}[X] = \mathfrak{n}$ から $K \in \mathcal{C}$ の極大性が従い，即ち K が選択集合である． □

注意 1. 各条件の中の「左」と「右」を入れ替えた命題も，やはり選択公理と同値になる．証明の中の左右を入れ替えればよい．

注意 2. 条件 7 の「左半中心」という条件が無い場合，極大イデアルが存在しないことがありえる．

例えば K を体として，K 上の次元が $\aleph_\omega$ となるような線型空間 V を考える．順序数 $\alpha \le \omega$ に対し $R_\alpha := \{f \in \mathrm{End}_K(V) \mid \mathrm{rank}(f) < \aleph_\alpha\}$ と定義して，環 R_ω を考える．集合 $\{R_\alpha \mid \alpha < \omega\}$ が環 R_ω の真のイデアル全体である．即ち R_ω は極大イデアルを持たない．しかし R_ω は冪等元をたくさん持っている．

注意 3. 条件 6 について．冪等元が無い環の場合，極大左イデアルが存在しないことがありえる．

例えば群 $\mathbb{Q}/\mathbb{Z}$ の部分群 $R := \left\{ \frac{m}{p^n} + \mathbb{Z} \,\middle|\, m, n \in \mathbb{Z} \right\}$ を考える．任意の $x, y \in R$ に対して $xy = 0$ として積を定義すれば，R は (0 でない) 冪等元を持たない可換環となる．このとき R は極大 (左) イデアルを持たない．

注意 4. 条件 2 について．分配律を仮定しない環の場合，(たとえ 1 が有っても) 極大左イデアルが存在しないことがありえる．

例えば群 $(\mathbb{Z}/3\mathbb{Z}, +)$ を考える．乗法 $\cdot$ を

$$0 \cdot 2 = 2 \cdot 0 = 0,\ 1 \cdot 2 = 2 \cdot 1 = 1,\ 2 \cdot 2 = 2,\ 0 \cdot 0 = 1,\ 0 \cdot 1 = 1 \cdot 0 = 2,\ 1 \cdot 1 = 0$$

で定めると $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ は分配律を満たさないが乗法単位元 2 を持つ環になる．$I \subset \mathbb{Z}/3\mathbb{Z}$ をイデアルとするとイデアルは部分群だから $I = 0$ または $I = \mathbb{Z}/3\mathbb{Z}$ しかありえない．しかし $0 \cdot 0 = 1$ だから 0 はイデアルでない．故に $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ は真のイデアルを持たない．

先の証明 $1 \Longrightarrow 2$ では 0 が左イデアルであることを使っているが，それを示す為に使う $x0 = 0$ を導くのに分配律を使っているのである．

参考文献

[1] W. Krull, Idealtheorie in Ringen ohne Endlichkeitsbedingung, Math. Ann. 101 (1929), 729–744, `http://www.springerlink.com/content/m5567m002273333p/`

[2] Wilfrid Hodges, Krull implies Zorn, J. London Math. Soc. 19 (1979), 285-287, `http://jlms.oxfordjournals.org/content/s2-19/2.toc`

[3] Henry E. Heatherly, Some ring theoretic equivalents to the Axiom of Choice, Henry Heatherly, University of Louisiana at Lafayette, `http://sections.maa.org/lams/proceedings/spring2004/`

[4] Patrick J. Morandi, Rings with no Maximal Ideals, `http://sierra.nmsu.edu/morandi/notes/mathematicalnotes.html`

[5] B. Banaschewski, A New Proof that ”Krull implies Zorn”, Mathematical Logic Quarterly, 40 (1994), 478–480, `http://onlinelibrary.wiley.com/doi/10.1002/malq.19940400405/abstract`