環論 (第 3 回)

3. 部分環

今回は「部分環」の概念を説明する. また例として, 代数体の整環を取り上げる.

定義 3-1.
可換環 A の部分集合 B $(1_A \in B)$ が A と同じ演算で環となるとき, B を A **の部分環**と言う.

例えば, $\mathbb{Z}$, $\mathbb{Q}, \mathbb{R}$ は $\mathbb{C}$ と同じ演算で環をなすので $\mathbb{C}$ の部分環である.

定理 3-1 (部分環の判定法)
可換環 A の部分集合 B が次の (i), (ii), (iii) を満たすとき, B は A の部分環となる.

(i) $x, y \in B \Rightarrow x - y \in B$.

(ii) $x, y \in B \Rightarrow x \cdot y \in B$.

(iii) $1_A \in B$.

[証明]
$1_A \in B$ より, 条件 (i) から

$$0_A = 1_A - 1_A \in B.$$

次に B 上で $+$ が定義できることを確認する. $x, y \in B$ とする. 0_A, $y \in B$ なので

$$-y = 0_A - y \in B.$$

従って

$$x + y = x - (-y) \in B.$$

これで B に A の演算で足し算と掛け算が定義できることが分かった. また $B \subseteq A$ に注意すると, B のこの演算は定義 1-1 の条件を全て満たすことが分かる. よって B は A の部分環になる.

□

[補足] 可換環 A とその部分環 B を考える.

(1) $0_B = 0_A$, $1_B = 1_A$ である.

(2) A が整域ならば, B も整域である.

(3) A が体でも, B が体とは言えない. 例えば, $\mathbb{C}$ は体だが, $\mathbb{Z}$ は体ではない.

例題 3-1
例題 1-1 の可換環 $A = \{(a, b) \mid a, b \in \mathbb{R}\}$ を考える．演算は

$$\begin{aligned}(a,b)+(c,d) &\stackrel{\text{def}}{=} (a+c, b+d),\\ (a,b)\cdot(c,d) &\stackrel{\text{def}}{=} (ac, ad+bc).\end{aligned}$$

で定義され, $0_A = (0,0), \quad 1_A = (1,0)$. また $B = \{(a,0) \mid a \in \mathbb{R}\}$ とする．このとき, B が A の部分環であることを示せ.

[証明]
定理 3-1 の (i)-(iii) の条件をそれぞれ確認すればよい .

(i) $(a,0),\ (b,0) \in B\ (a,\ b \in \mathbb{R})$ とする.

$$(a,0)-(b,0) = (a-b,0) \in B. \quad (\because a-b \in \mathbb{R})$$

(ii) $(a,0),\ (b,0) \in B\ (a,\ b \in \mathbb{R})$ とする.

$$(a,0)\cdot(b,0) = (ab, a\times 0 + 0\times b) = (ab,0) \in B. \quad (\because ab \in \mathbb{R})$$

(iii) $1 \in \mathbb{R}$ より, $1_A = (1,0) \in B$.

以上より B は A の部分環である.

□

問題 3-1 $\mathbb{C}$ の部分集合を

$$A = \left\{ \frac{n}{2^k} \;\middle|\; n, k \in \mathbb{Z},\ k \geq 0 \right\}$$

で定める．定理 3-1 の (i), (ii), (iii) の条件をチェックし, A が $\mathbb{C}$ の部分環であることを示せ.

定理 3-2

$\sqrt{n} \notin \mathbb{Q}$ を満たす整数 n に対して,

$$A = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$

と置く. また,

$$x = a + b\sqrt{n},\ y = c + d\sqrt{n} \in A\ (a, b, c, d \in \mathbb{Z})$$

とする. このとき, 次が成り立つ.

(1) $x = y \Rightarrow (a, b) = (c, d)$.

(2) A は $\mathbb{C}$ の部分環.

(3) 写像 $N : A \to \mathbb{Z}\ (a + b\sqrt{n} \mapsto a^2 - nb^2)$ に対し, 次が成り立つ.

$$N(xy) = N(x)N(y) \quad (x, y \in A).$$

(4) $x \in A^\times \iff N(x) = \pm 1$.

※ 上述の A は代数体の整環の一例であり, 整数論の重要な研究対象である. $n = -1$ の場合を考えると,

$$A = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

となる. この環はガウス整数環と呼ばれ, フェルマーの最終定理の $n = 4$ の場合「$x^4 + y^4 = z^4$ は自然数解 (x, y, z) を持たない」の証明に応用を持つ. 詳しくは「素数と 2 次数体の整数論 (青木 昇著)」を参照のこと.

[証明]

(1) $x = y$ とする. $b \neq d$ と仮定すると,

$$\sqrt{n} = \frac{a - c}{d - b} \in \mathbb{Q}$$

となり矛盾. 従って $b = d$ であり, $(a, b) = (c, d)$ が言える.

(2) 定理 3-1 の部分環の条件を確認すればよい.

(i) $x - y = (a - c) + (b - d)\sqrt{n}$ であり, $a - c,\ b - d \in \mathbb{Z}$ より, $x - y \in A$.

(ii) $xy = ac + bdn + (ad + bc)\sqrt{n}$ であり, $ac + bdn \in \mathbb{Z},\ ad + bc \in \mathbb{Z}$ より, $xy \in A$.

(iii) $1 = 1 + 0 \cdot \sqrt{n} \in A$.

以上より, A は $\mathbb{C}$ の部分環である.

(3) について.

$$\begin{aligned} N(xy) &= N\big(ac+bdn+(ad+bc)\sqrt{n}\,\big) \\ &= (ac+bdn)^2 - n(ad+bc)^2 \\ &= (a^2-nb^2)(c^2-nd^2) \\ &= N(x)N(y). \end{aligned}$$

(4) $x \in A^\times$ のとき, $xz = 1$ を満たす $z \in A$ がある. よって

$$N(x)N(z) = N(xz) = 1.$$

$N(x), N(y)$ は整数なので, $N(x) = \pm 1$.

逆に $N(x) = \pm 1$ とする. $z = a - b\sqrt{n} \in A$ とおくと,

$$xz = a^2 - nb^2 = N(x) = \pm 1.$$

よって $xz = 1$ または $x(-z) = 1$. 従って $x \in A^\times$.

□

例題 3-2.

$\mathbb{C}$ の部分環

$$A = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

を考える. このとき, 次を示せ.

$$A^\times = \{\pm 1,\ \pm\sqrt{-1}\}.$$

[証明]

$x = a + b\sqrt{-1}$ $(a, b \in \mathbb{Z})$ とおく. 定理 3-2 より,

$$x \in A^\times \iff N(x) = \pm 1 \iff a^2 + b^2 = \pm 1.$$

$a^2 + b^2 \geq 0$ より,

$$x \in A^\times \iff a^2 + b^2 = 1 \iff (a, b) = (\pm 1, 0),\ (0, \pm 1) \iff x = \pm 1,\ \pm\sqrt{-1}.$$

よって結論を得る.

□

問題 3-2

(1) $\mathbb{C}$ の部分環

$$A = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$$

を考える. このとき, $A^\times$ を求めよ.

(2) $\mathbb{C}$ の部分環

$$A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

を考える. $3 + 2\sqrt{2} \in A^\times$ を示し, さらに $|A^\times| = \infty$ を示せ.

例題 3-3.
$\mathbb{C}$ の任意の部分環は $\mathbb{Z}$ を含むことを示せ.

※ これは, $\mathbb{Z}$ が $\mathbb{C}$ に含まれる最小の部分環であることを意味する.

[証明]
A を $\mathbb{C}$ の部分環とする. $1 \in A$ より, 自然数 n に対して,

$$n = \underbrace{1 + 1 + \cdots + 1}_{n\text{ 個}} \in A.$$

よって $\mathbb{N} \subseteq A$. また

$$0 = 1 - 1 \in A.$$

最後に負の整数 m に対し, $0,\ |m| \in A$ より

$$m = 0 - |m| \in A.$$

よって $\mathbb{Z} \subseteq A$. $\square$