

環論 No.2要約

定義 2.1 (「生成される部分環」). R を単位元を持つ環とし、 T をその部分集合とする。 R の部分環 S が T で環として生成されるとは、次の三つの条件が満たされる時にいう。

1. S は T を部分集合として含む。
2. S は R の部分環である。
3. S は (1),(2) を満たす最小のものである。

補題 2.2. 単位元を持つ環 R と、その部分集合 T が与えられていたとする。このとき、 R の部分環 S で、 T で環として生成されるものがただ一つ存在する。 $(S$ のことを T で生成される R の部分環といい、 $\langle T \rangle_{ring}$ と書く。

注意: 「部分環」の定義により、 $\langle T \rangle_{ring}$ は (T が何であっても) 常に R の単位元 1_R を元としてもつ。しかし、単位元の存在を意識しておくために、以下では始めから T には R の単位元 1_R が入ったものだけを考えることにする。

例 2.1. \mathbb{C} の部分集合 T と、それによって生成される \mathbb{C} の部分環 $\langle T \rangle_{ring}$ の例。

1. $T = \{1\} \implies \langle T \rangle_{ring} = \mathbb{Z}$.
2. $T = \{1, \sqrt{-1}\} \implies \langle T \rangle_{ring} = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$
3. $T = \{1, \sqrt{2}\} \implies \langle T \rangle_{ring} = \mathbb{Z} + \mathbb{Z}\sqrt{2}$
4. $T = \mathbb{Q} \cup \{\sqrt{2}\} \implies \langle T \rangle_{ring} = \mathbb{Q} + \mathbb{Q}\sqrt{2}$
5. $T = \mathbb{Q} \cup \{\sqrt[3]{2}\} \implies \langle T \rangle_{ring} = \mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}\sqrt[3]{4}$

補題 2.2 の証明の途中で、次の補題が必要になるので、ここに掲げておく。

補題 2.3 (「任意個数の部分環の共通部分はまた部分環である。」). R は環であるとし、 $\{S_\lambda\}_{\lambda \in \Lambda}$ は R の部分環の族であったとする。このとき、共通部分 $S = \bigcap_{\lambda \in \Lambda} S_\lambda$ もまた R の部分環になる。

実際には、生成される部分環には次のパターンのものがよく使われる。

定義 2.4. R を環、 S をその部分環とする。 R の元 r_1, \dots, r_n が与えられたとき、 R の部分集合 $S \cup \{r_1, \dots, r_n\}$ で生成される部分環を、 $S[r_1, \dots, r_n]$ と書き、 S 上 $\{r_1, \dots, r_n\}$ で生成された環とよぶ。

この記法によれば、上の例の (4),(5) はそれぞれ次のように書ける。

$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\sqrt{2}, \quad \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}\sqrt[3]{4}$$

このように、 $S[r_1, \dots, r_n]$ が実際にはどのような元をもつか決定することも基本的で、重要である。それは通常次の手順で行う。

1. $S[r_1, \dots, r_n]$ の候補 T を探す。
2. T は $S[r_1, \dots, r_n]$ を部分集合として含むことを証明する。
3. T は R の部分集合であることを証明する。
4. T の元は S と、 r_1, \dots, r_n から構成し得ることを証明する。言い換えると、 $S \cup \{r_1, \dots, r_n\}$ を部分集合として含む R の部分環は、必ず T を含むことを証明する。

定義 2.5. R は環であるとする。このとき、 X を変数とする R 係数の一変数多項式の全体

$$\left\{ \sum_{i=0}^n a_i X^i; \quad n \in \mathbb{N}, a_i \in R \right\}$$

は環をなす。(足し算、かけ算は通常のものを考える。) この環を (X を変数とする) R 上の一変数多項式環という。

定理 2.6. X を変数とする R 上の一変数多項式環は、 R と、 X とで生成される。

$$\left\{ \sum_{i=0}^n a_i X^i; \quad n \in \mathbb{N}, a_i \in R \right\} = \langle R \cup \{X\} \rangle_{ring} = R[X]$$

(したがって、これからは R 上の一変数多項式環のことを $R[X]$ と書く。)

注意

本講義の範囲では他に $\mathbb{C}[X], \mathbb{Q}[X]$ 等が重要になる。 $(\mathbb{R}, \mathbb{C}, \mathbb{Q}$ は全て体である。すなわち積は可換であり、0以外の各元は逆元を持つ。)

[発展] (講義の中で解説はしない。興味のある人は各自研究のこと。)

同様にして、2変数多項式環 $R[X, Y]$, 3変数多項式環 $R[X, Y, Z]$ 等が定義される。

$$R[X, Y] = \left\{ \sum_{\substack{i, j \geq 0 \\ (\text{有限和})}} a_{i,j} X^i Y^j; a_{i,j} \in R \right\}$$

$$R[X, Y, Z] = \left\{ \sum_{\substack{i, j, k \geq 0 \\ (\text{有限和})}} a_{i,j,k} X^i Y^j Z^k; a_{i,j,k} \in R \right\}$$

さらに一般に、 X_1, X_2, \dots, X_n を変数とする R 係数の多項式環が定義される。

$$R[X_1, X_2, \dots, X_n] = \left\{ \sum_{\substack{i_1, i_2, \dots, i_n \geq 0 \\ (\text{有限和})}} a_{i_1, i_2, \dots, i_n} X_1^{i_1} X_2^{i_2} X_3^{i_3} \dots X_n^{i_n}; a_{i_1, i_2, \dots, i_n} \in R \right\}$$

多項式 $p = \sum a_{i_1, i_2, \dots, i_n} X_1^{i_1} X_2^{i_2} X_3^{i_3} \dots X_n^{i_n}$ は書くのが面倒なので、多重指数を用いると便利である。 $I = \{i_1, i_2, \dots, i_n\}$, $a_I = a_{i_1, i_2, \dots, i_n}$, $X^I = X_1^{i_1} X_2^{i_2} X_3^{i_3} \dots X_n^{i_n}$ という略記法を用いると、 p は $\sum_I a_I X^I$ と簡略化して書ける。定義により、環 $R[X_1, \dots, X_n]$ は環 $R[X_1, \dots, X_{n-1}]$ 上の X_n を変数とする一変数多項式環と同じものとみなせる。