

代数学演習 I 問題 NO.9

一意分解環・単項イデアル整域・ユークリッド整域編 (1)

今回も「環」といえば単位元を持つ可換環であるとし、「環の準同型」は単位元を保つものだけを考えることにします。

定義 9.1. 整域 R が一意分解環 (unique factorization domain:UFD) であるとは、 $R \setminus \{0\}$ の任意の元 x が素元の積に

$$x = p_1 p_2 \cdots p_k (p_1, \dots, p_k \text{ は } R \text{ の素元})$$

のように書けるときに言います。(p_1, \dots, p_k の中には同じものがあってもよい。)

定義 9.2. 整域 R が単項イデアル整域 (principal ideal domain:PID) であるとは、 R のすべてのイデアルが単項イデアル (一つの元で生成されるイデアル) であるときに言います。

定義 9.3. 整域 R がユークリッド整域 (Euclidian domain:ED) であるとは、整列順序集合 W と写像 $\rho: R \rightarrow W$ (「重さ」を調べる写像) があって、次の性質を満たすときに言います。

- (1) R の元 a の「重さ」 $\rho(a)$ が最小 $\Leftrightarrow a = 0$
- (2) R の元 a, b ($a \neq 0$) に対して、

$$b = aq + r, \quad q, r \in R, \quad \rho(r) < \rho(a)$$

となる q, r が存在する。

これから暫くの間 (3 回ぐらい) 上の 3 つのタイプの環が主題になります。基本的には、

$$\text{ED} \implies \text{PID} \implies \text{UFD}$$

という事実と、諸例、それに定義の意味が分るようになれば OK です。まず上に上げた定義のうちの幾つかの用語に関する問題から始めます。

問題 9.1. 環 R の元 a について、次の二つは同値であることを示しなさい。

- (1) a は素元である。すなわち a が bc を割り切れれば、 b か c かのどちらかは a の倍元である。
- (2) a で生成される R のイデアル aR は素イデアルである。

例題 9.1. (整列集合の定義の確認) R をユークリッド整域とし、 $\rho: R \rightarrow W$ を定義 9.3 に出てくる写像とします。この時、任意の R の部分集合 S に対して、 S の中で重さが最小のもの (「一番軽いもの」) があることを示しなさい。

「 W が整列集合である」とは、「 W の任意の部分集合 X は最小元を持つ」ということでした。そこで、「 S の元の重さの集合」

$$\{\rho(a); \quad a \in S\}$$

を X として採用すると、この中に最小元がある筈です。これを $\rho(a_0)$ とすれば、 a_0 が求めるものということになります。(注意：一番軽い元は一つとは限りません。)

問題 9.2. ユークリッド整域は単項イデアル整域であることを示しなさい。(ヒント： R をユークリッド整域とし、 I をそのイデアルの一つとします。 $I = 0$ なら単項 (0 で生成される) のでよい。 $I \neq 0$ なら、 $I \setminus \{0\}$ の元のうち、一番軽い元をとってみなさい。)

問題 9.3. \mathbb{Z} はユークリッド整域であることを、定義に沿って示しなさい。($W = ?$, $\rho = ?$)

問題 9.4. 体 K 上の一変数多項式環 $K[X]$ はユークリッド整域であることを、定義に沿って示しなさい。

問題 9.5. $\omega = \frac{-1+\sqrt{-3}}{2}$ (1 の三乗根の一つ) とするとき、 $\mathbb{Q}[\omega]$ は体であることを示しなさい。

問題 9.6. $\mathbb{Z}[\sqrt{-1}]$ は「重み関数」 ρ を

$$\begin{array}{ccc} \rho: \mathbb{Z}[\sqrt{-1}] & \rightarrow & \mathbb{Z}_{\geq 0} \\ \cup & & \cup \\ m + n\sqrt{-1} & \mapsto & m^2 + n^2 \end{array}$$

で定義することにより、ユークリッド環となることを示しなさい。(ヒント: $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$, $\beta \neq 0$ とするとき、 α を β で割った商を求めるには、 α/β を $\mathbb{Z}[\sqrt{-1}]$ の元で近似してみなさい。)

問題 9.7. (1) 任意の複素数 z に対して、ある $\gamma \in \mathbb{Z}[\sqrt{-2}]$ があって、 z と γ との距離 $|\gamma - z|$ は 1 以下であることを示しなさい。(ヒント: 複素平面上に $\mathbb{Z}[\sqrt{-2}]$ の元をプロットしてみなさい。)

(2) $\mathbb{Z}[\sqrt{-2}]$ は「重み関数」 ρ を

$$\begin{array}{ccc} \rho: \mathbb{Z}[\sqrt{-2}] & \rightarrow & \mathbb{Z}_{\geq 0} \\ \cup & & \cup \\ m + n\sqrt{-2} & \mapsto & m^2 + 2n^2 \end{array}$$

で定義することにより、ユークリッド環となることを示しなさい。

問題 9.8. $\omega = \frac{-1+\sqrt{-3}}{2}$ (1 の三乗根の一つ) とします。このとき、 $\mathbb{Z}[\omega]$ はユークリッド環であることを示しなさい。

問題 9.9. (各 1) 次の $\mathbb{Z}[\sqrt{-1}]$ のイデアルを簡単な形になおしなさい。

- (1) $(3 + 4\sqrt{-1}, 5)$
- (2) $(5 + 12\sqrt{-1}, 13)$
- (3) $(7 + 8\sqrt{-1}, 9)$

問題 9.10. まだ 0 問の人限定サービス問題 (のつもり) 2 つの整数 a, b を適当にみつくり、 a, b でユークリッドの互除法を行い、 a, b の gcd d と、 $al + bm = d$ を満たす整数 l, m を 1 組見つけよ。方法は (できれば) 講義のプリントにある二次行列を用いる方法で行うこと。また、あまりに簡単すぎないこと。他の人とかぶらなければこの問題は何人が解いても良い。

問題 9.11. まだ 1 問以下の人限定サービス問題 (のつもり) 2 つの $\mathbb{Z}[\sqrt{-1}]$ の元 a, b を適当にみつくり、 a, b でユークリッドの互除法を行い、 a, b の gcd d と、 $al + bm = d$ を満たす $\mathbb{Z}[\sqrt{-1}]$ の元 l, m を 1 組見つけよ。あまりに簡単すぎないこと。もちろん問題 9.9 から取ってきた a, b でも良い。他の人とかぶらなければこの問題は何人が解いても良い。