代数学 II 要約 NO.3

今日のテーマ:

1 変数多項式環とその剰余環

定義 3.1. 環 R が与えられているとする。このとき、X を変数とする 1 変数多項式の全体

$$\{a_nX^n+a_{n-1}X^{n-1}+a_{n-2}X^{n-2}+\dots a_2X^2+a_1X+a_0; n \text{ は正の整数}, a_i \in R\}$$

は (多項式の通常の和、積のもとで) 環をなす。この環のことを R 上の 1 変数多項式環とよび、$R[X]$ で書き表す。$R[X]$ の (0 以外の) 元 $f(X) = \sum_i a_iX^i$ に対して、その次数 $\deg(f)$ が、

$$\deg(f) = \max\{i; a_i \neq 0\}$$

により定義される。(0 の次数は $-\infty$ と定義する。)

この講義では体の上の 1 変数多項式環について考えることが多いが、体以外の環、特に整域ではない環の上の 1 変数多項式環については妙なことが起こることも覚えておいてよい。(演習問題を解く時などに役立つ。) 例えば、$(\mathbb{Z}/6\mathbb{Z})[X]$ においては、$(2X+1)(3X+2) = X+2$ と、1 次式と 1 次式の積が 1 次式になる場合がある。

体上の多項式、及び多項式環を扱う時には、次のようなよい性質がある。

定理 3.1. 体 k 上の *1* 変数多項式環 $k[X]$ に対して、次のことが成り立つ。

(1) $f, g \in k[X] \setminus \{0\}$ に対して、

$$\deg(fg) = \deg(f) + \deg(g)$$

がなりたつ。

(2) (割り算の原理) 任意の $f, g \in k[X]$ (ただし $g \neq 0$) にたいして、ある $q, r \in k[X]$ が一意的に存在して、

$$f = qg + r \qquad (\deg(r) < \deg(g))$$

がなりたつ。

(3) $k[X]$ のイデアル I に対して、ある $f \in k[X] \setminus \{0\}$ が存在して、

$$I = f(X)k[X]$$

と書ける。

割り算の原理または上の定理の (3) から導かれる次の定理は 1 変数多項式環を調べる際に実に強力な武器を与える。

定理 3.2. 体 k 上の多項式 $f, g \in k[X] \setminus \{0\}$ に対して、次のような多項式 $a, b, d \in k[X]$ が存在する。

(1) d は f, g の公約数である。*(*すなわち、$f, g \in dk[X]$*)*

(2) $af + bg = d$.

実は d は f, g の (普通の意味での) 最大公約数であることがすぐにわかるが、ここではそこまでは述べない。詳しく知りたい方は代数学 I または C の復習をして欲しい。

が与えられているとき、新しい環 $k[X]/I$ が定まる。この環が次回以降の議論の中心になる。

今回はとりあえず次の補題のみをあげておこう。

補題 3.1. $k[X]/(f(X)k[X])$ での X のクラスを α と書くと、$f(\alpha) = 0$.

余談: 前回の講義で、$R \setminus \{0\}$ という記号を用いたが、これは、R から $\{0\}$ をひっこ抜いた集合、もっと正確に言うと、R の元のうち 0 以外のものを集めたもの

$$R \setminus \{0\} = \{r \in R; r \neq 0\}$$

である。もっと一般に、 S の部分集合 T があたえられたとき、

$$S \setminus T = \{s \in S; s \notin T\}$$

と定義する。

問題 3.1. $\mathbb{R}[X]/((X^2+1)\mathbb{R}[X])$ の中での X のクラスを α と書くことにする。このとき、

(1) α^2 を簡単にせよ。

(2) $(3+4\alpha)(3-4\alpha)$ を簡単にせよ。

(3) $5+12\alpha$ には実は逆元がある。それを求めよ。

(ヒント: X のクラスの呼び名は上の α よりももっとふさわしいものがある。それが何であるかに気づけばやさしいだろう。(但し上の問題では α はあくまでも α と呼ぶこと。))