代数学 III 要約 NO.3

今日のテーマ

多項式環の剰余環として体を作る

$\alpha = \sqrt{2}$ **のとき、** $\mathbb{Q}[\alpha]$ **の元は** $a + b\alpha$ $(a, b \in \mathbb{Q})$ **と書くことができ、それらの和、差、積、商の公式は** $\alpha^2 - 2 = 0$ **という関係式だけから書き下すことができるのであった。もっと一般に、代数方程式を満たす元を体に「付け加える」ことができる。(補題** 3.1**, 定理** 3.1**) それには、多項式環をうまく用いる。**

定義 3.1. 体 K **の元を係数に持つような** X **を変数とする一変数多項式の全体を** $K[X]$ **と書き、** K **上の (**X **を変数とする) 一変数多項式環と呼ぶ。**

ついでに環とイデアルの定義を思い出しておこう。詳しくは代数 I **の講義を復習すること。**

定義 3.2.

(1) R **が (単位元を持つ可換) 環であるとは、**R **に和、差、積が定義されていて、積は可換、かつ** R **は乗法に関する単位元** 1 **を持つときにいう。**

(2) R **の部分集合** I **が** R **のイデアルであるとは、**I **が加法、減法について閉じていて、なおかつ次の条件が成り立つときにいう。**

$$r \in R, x \in I \implies rx \in I$$

(3) **環** R **のイデアル** I **が与えられたとき、**R/I **なるあたらしい環を構成することができる。**R/I **の元** $\overline{a}$ **は** $a \in R$ **の元のクラスであり、クラス分けは、**

$$\overline{a} = \overline{b} \quad \Leftrightarrow \quad a - b \in I$$

で決まる。

補題 3.1. 体 K **上の多項式** $f(X) \in K[X]$ **に対して、**$I = f(X)K[X]$ **は** $K[X]$ **のイデアルである。**

$$R = K[X]/f(X)K[X]$$

は環であって、X **の** $K[X]$ **における剰余類 (クラス) を** α **と書くと、**α **は** $f(\alpha) = 0$ **を満足する。さらに、** f **が** K **上既約 (それ以上** K **上の多項式の積に分解できない) ならば、この環** R **は実は体である。**

定義 3.3. 体 L とその部分体 K が与えられているとする。$a \in L$ に対して、a が満足する K 上の方程式、すなわち

$$f(X) \in K[X] \setminus \{0\} \text{ かつ } f(a) = 0$$

をみたすもののうち次数が最小のものを、a の K 上の最小多項式と呼ぶ。

以下では、とくに断らない限り最小多項式と言えばモニックのものを指すことにする。
つぎの定理は、「方程式の解を付け加えること」が形式的にはどのようなことを意味するかを説明する。

定理 3.1. 体 L とその部分体 K が与えられているとする。$a \in L$ の K 上の最小多項式を f とかくと、

(1) **f は必ず既約である。**
(2) **$g \in K[X]$ が $g(a) = 0$ を満足するとすると、g は f で割り切れる。**
(3) **$K[X]/f(X)K[X]$ は $K(a)$ と同型である。**

問題 3.1. X の 4 次式 $f \in \mathbb{Q}[X]$ で、$a = \sqrt{5} + \sqrt{7}$ にたいして $f(a) = 0$ を満たすようなものを見つけなさい。

問題 3.2. 前問の f は $\mathbb{Q}$ 上既約であることを示しなさい。(前問と本問をあわせると、f が a の最小多項式であることがわかる。ただし今の段階ではかなり難しい問題である。この講義のもっとあとの段階まで進めば、この問題も非常に易しく解けるようになる。)