代数学 III 要約 NO.2

今日のテーマ: $\boxed{\text{体に一つの代数的な元を付け加えた体}}$

定義 2.1. 体 L の部分集合 K が L の**部分体**であるとは、K 自身が L の演算で体になっているときに言う。また、このとき L は K の**拡大体**であるとも言う。

定義 2.2 (体に元を付け加えてできる体). 体 L と、その部分体 K, および L の元 α が与えられているとする。このとき、K と α とを含む L の部分体のうち最小のものを $k(\alpha)$ と書き (丸括弧に注意)、K に α を付け加えてできる体と呼ぶ。

補題 2.3.

$$K(\alpha) = \{\frac{a(\alpha)}{b(\alpha)}; a, b \text{ は } K \text{ 係数の多項式}\}$$

定義 2.4. 体 K は体 L の部分体であるとする。$\alpha \in L$ が K 上のある代数方程式

$$f(\alpha) = 0 \qquad (f \in K[X], f \neq 0)$$

を満足するとき、 α は K 上**代数的**であると呼ぶ。また、このような f のうち、次数が最小のものを α の**最小多項式**と呼ぶ。

とくに断らない限り、最小多項式は**モニック**なものを選ぶのが普通である。

$\mathbb{Z}$ や、体 K 上の一変数多項式環 $K[X]$ はユークリッド環であったことを思い出そう。これは簡単に言えばこれらの環上では 余りを許した意味での割り算 ができることを意味している。

命題 2.5. ユークリッド整域 R は PID である。すなわち、R の元 p, q にたいして、そのある a, b が存在して、

$$ap + bq = d \tag{E}$$

(d は p, q の R での最大公約数) が成り立つ。

(E) 式のおかげで、ユークリッド環 (もっと一般に、PID) の 剰余環 の割り算は良い性質を持つ。これが今回の技術的なキモである。

命題 2.6. 体 k 上の 多項式 $p(X)$ と $q(X)$ が互いに素なら、$R = k[X]/p(X)k[X]$ のなかでの $q(X)$ のクラス $\overline{q(X)}$ は可逆である。とくに、p が $k[X]$ のなかで既約ならば、$R = k[X]/p(X)k[X]$ は体である。

上の命題で、p が既約でなければ、環 $R = k[X]/p(X)k[X]$ は体ではないことが容易に分かる。したがって、p が既約であることは R が体であることの必要十分条件である。

上の命題と同様に、次のことも成り立つ。(今回のテーマとは少しずれるが、本講義全体のなかでは重要である。)

定理 2.7. 素数 p にたいして、$\mathbb{Z}/p\mathbb{Z}$ は体である。(この体を $\mathbb{F}_p$ と書く。)

そして、今回のメインはこちら:

定理 2.8. 体 K が体 L の部分体であって、$\alpha \in L$ が K 上代数的であれば、

(1) $K(\alpha)$ の任意の元は α の K 係数の多項式で書くことができる。
(2) α の最小多項式を f とおくと、$K(\alpha)$ は $L_1 = K[X]/f(X)K[X]$ と同型である。
(3) もっと詳しく言うと、環準同型 $\varphi : L_1 \to L$ で、X のクラスを α に写すものが (唯一つ) あって、φ は L_1 と $K(\alpha)$ との同型を与える。$K(\alpha)$ の任意の元は α の K 係数の多項式で書くことができる。

上の定理は、K 上代数的な数 α がどんな数かロクスッポ知らなくても、その最小多項式が分かってさえいれば剰余環のコトバで $K(\alpha)$ が理解できることを示している。

問題 2.1. α が $\mathbb{Q}$ 上の方程式 $X^5 - X + 1 = 0$ の解であるとするとき

(1) α の逆元を α の 4 次以下の $\mathbb{Q}$ 係数の多項式で表しなさい。
(2) $1 + \alpha^2$ の逆元を α の 4 次以下の $\mathbb{Q}$ 係数の多項式で表しなさい。