代数学 II 要約 NO.8

今日のテーマ:

準同型、同型、有限体は元の数で完全に決まること

前回、次の系の証明 (と言う程難しくはなく、むしろ説明) が残ってしまっていた。

系 8.1. 素数 p と正の整数 n に対して、$\mathbb{F}_p$ 上の既約多項式 $f(X)$ で、その次数が n のものが存在する。

これをもう少し詳しく言うと、次のことが成り立つ。

定理 8.1. 素数 p と正の整数 n に対して、元の個数が $q = p^n$ であるような有限体 K が存在する *(*定理 *6.2)*。この K にたいして、次のことが成り立つ。

(1) $K^\times$ の *(*群としての*)* 生成元 a の $\mathbb{F}_p$ 上の最小多項式の次数は n である。
(2) $\mathbb{F}_p$ 上の n 次の既約多項式は必ず K で一次式の積に分解される。

このことを示すために、最小多項式、環の準同型等の復習をしておこう。

定義 8.1 (環の準同型の定義). 環の間の写像 $\phi : R \to S$ が準同型であるとは、次の条件が成り立つときにいう。

(1) $\phi(x+y) = \phi(x) + \phi(y)$ が任意の x, y についてなりたつ。
(2) $\phi(xy) = \phi(x)\phi(y)$ が任意の x, y についてなりたつ。
(3) $\phi(1_R) = \phi(1_S)$ がなりたつ

単射準同形写像のことを中への同型、全単射準同形写像のことを上への同型または単に同型とよぶ。

定理 8.2 (環の準同型定理). 環 R から環 S への準同型 ϕ に対して、

(1) ϕ の核 $\mathrm{Ker}(\phi)$ は R のイデアルである。
(2) ϕ の像 $\mathrm{Image}(\phi)$ は S の部分環である
(3) ϕ は $R/\mathrm{Ker}(\phi)$ と $\mathrm{Image}(\phi)$ との間の 同型を誘導する。

補題 8.1. 体 k の拡大体 K は k 上一つの元 α で生成されているとする。このとき、

(1) $\varphi : k[X] \to K$ を $\varphi(p(X)) = p(\alpha)$ できめると、φ は全射環準同型である。
(2) φ の核は (i) $\{0\}$ であるか、または (ii) ある多項式 $m(X) \in k[X]$ があって、 $m(X)k[X]$ の形をしている。
(3) 上で、(ii) の時には、$m(X)$ は $f(\alpha) = 0$ を満たす k 上の多項式のうち、次数が最小のものである。
(4) 上で、(i) の場合には $[K : k] = \infty$, (ii) の場合には $[K : k] = \deg(m)$ である。

定義 8.2. 上の (ii) の場合に、$m(X)$ のことを α の k 上の最小多項式とよぶ。(最小多項式は定数倍の違いの分だけ不定性があるが、とくに断らない限りはモニック (最高次の係数が 1) のものを採用して、その不定性を取り除くことにする。)

で生成される k の有限次拡大体であるとする。さらに、α の k 上の最小多項式を m とおく。このとき、もし、L の元 β で、$m(\beta)=0$ を満たすものがあれば、K から L への中への同型写像 φ で、$\varphi(\alpha)=\beta$ をみたすものが存在する。

定理 8.4. 体 K_1, K_2 の元の数がともに有限で、同じ q であるなら、K_1 と K_2 とは同型である (すなわち、K_1 から K_2 への上への同型写像 φ が存在する。

定義 8.3. 元の数が q の体 (上の定理により同型を除いて一つしかない) のことを $\mathbb{F}_q$ とかく。

$K^\times$ の構造を知ると、次のような問題も片付けられる。(とは言ってもこれは Fermat の定理 (あるいは群論の Lagrange の定理) の範疇である。)

問題 2.3 一般に、素数 p に対して、 10 進法で書いた整数を p で割った余りを「一定の桁数毎に区切って」 求める方法はいつでも存在するだろうか？ (但しもちろん $p=2$ と $p=5$ の場合は例外とする。)

時間が余ったら、次の問題も解説する予定。

問題 4.2 $K=\mathbb{F}_{37}[X]/(X^3-X+2)\mathbb{F}_{37}[X]$ での X のクラスを ξ と書くとき、 K での $12\xi^2+5\xi+1$ の逆元を求めなさい。 (なお、この K は実は体であるのだが、そこまでは示さなくてもよい。)

(なお、問題 4.1 では、このとき、 $a+b, a-b, ab, b^{-1}$ をそれぞれ ξ の 2 次式であらわしなさい。となっていましたが、これは 2 次以下の式のつもりでした。(ウエブ版では訂正済) 失礼を致しました。お詫びして訂正いたします。)

問題 8.1. 次のような (1)-(3) の例を ((4) が解きやすいように) 作り,(4) を求めなさい。

(1) 素数 $p>2$
(2) 正の整数 $n>2$
(3) $\mathbb{F}_p$ 上の相異なる n 次既約多項式 $f, g\in\mathbb{F}_p[X]$
(4) $\mathbb{F}_p[X]/f(X)\mathbb{F}_p[X]$ での g の一次式への分解

注意:上の問題の書き方 (とくに 4 番) は不適切であった。正しくは、(誤解の恐れを無くすため一度別の文字 Y を用いて) $K=\mathbb{F}_p[Y]/f(Y)F_p[Y]$ などとおき、$g(X)$ をこの K 上の多項式 ($K[X]$ の元) と改めてみなした時の g の分解という意味であった。

問題 8.2. 任意の有限体 K に対して、K 上の n 次の既約多項式が存在することを示しなさい。