代数学 II 要約 NO.6

今日のテーマ:

有限体の乗法群の構造と、有限体の存在

定義 6.1. 体 K に対して

$$K^\times = \{x \in K; x \text{ は } K \text{ で可逆 }\} (= K \setminus \{0\})$$

は群になる。これを K の乗法群と呼ぶ。$K^\times$ の元 x にたいし、x の ($K^\times$ の元としての群論での意味の) 位数を x の乗法的位数、あるいは単に位数と呼ぶ。つまり、

$$(x \text{ の位数}) = \min\{n \in \mathbb{Z}; n > 0, x^n = 1\}.$$

今回は有限体に対してその乗法群の構造を調べ、さらに有限体の存在について述べる。

補題 6.1. 体 K の元の数が q であるとすると、K の任意の元は

$$X^q - X$$

の根である。

補題 6.2. 体 k の上の任意の (既約とは限らない) 多項式 $F(X)$ に対して、ある k の有限次拡大体 L で、$F(X)$ を L 上で考えれば一次式の積に分解するようなものが存在する。

定理 6.1. 素数 p と正の整数 n にたいして、 元の数が $q = p^n$ の体は存在する。もっと詳しくいうと、$X^q - X \in F_p[X]$ が一次式の積に分解するような体 L (前の補題によって存在する) をとり、L のなかの $X^q - X$ の根の全体を K とおくと、K は体で、その元の数は q になる。

補題 6.3. 有限体 K に対して、

$$a_n = \#\{x; x \text{ の位数は } n\}$$

と定義すると、

(1) $a_n \neq 0$ であるのは n が $q-1$ の約数の時に限る。
(2) $a_n \leq \varphi(n) = (1$ から n までの整数で, n と互いに素なものの数)

定理 6.2. 有限体 K にたいして、位数が $\#(K) - 1$ であるような K の元 x が存在する。言い換えると、K の乗法群 $K^\times$ は巡回群である。

問題 6.1. $\mathbb{F}_{23}^\times$ の生成元 (位数が 22 の元) を一つ求めなさい。(もちろん理由も書くこと)

諸君のレポートは理学部二号棟 5 階東端の数学閲覧室の前にぶら下がっている袋にあるので各自とっていくこと