

## 今日のテーマ

## 体の乗法群

体  $K$  に対して、 $K \setminus \{0\}$  は(乗法に関して) 群をなす。これを  $K$  の乗法群と呼び、 $K^\times$  で書き表す。

参考: 一般に、(単位元をもつ結合的な) 環  $R$  に対して  $R$  の元で、 $R$  内に逆元をもつようなものの全体を  $R^\times$  と書く。 $R^\times$  も乗法に関して群をなす。)

有限群  $G$  に対して、 $G$  の元の個数(位数)を  $|G|$  と書くと  $G$  の任意の元  $g$  は  $g^{|G|} = 1$  を満たすこと(ラグランジュの定理)を思い出しておこう。

補題 5.1. 有限体  $K$  に対して、 $\#(K) = q$  と書くと、 $K^\times$  の任意の元  $x$  に対して、 $x^{q-1} = 1$  がなりたつ。

系 5.1. 有限体  $K$  に対して、 $\#(K) = q$  と書くと、 $K$  の任意の元  $x$  に対して、 $x^q = x$  がなりたつ。とくに、 $K$  の元は  $X^q - X$  の根の全体とちょうど一致する。

$$X^q - X = \prod_{a \in K} (X - a)$$

系 5.2.  $\mathbb{F}_p$  上の既約  $d$ -次式は必ず  $X^{p^d} - X$  の約数である。

## 問題 5.1.

- (1)  $\mathbb{F}_{11}$  の(次数が 2 以上の) 既約多項式  $p(X)$  を一つ選びなさい。
- (2) 上の  $p(X)$  に対して、 $K = \mathbb{F}_{11}[X]/p(X)\mathbb{F}_{11}[X]$  のなかの  $X$  のクラスを  $a$  とおく。この時、 $a, a+1$  の逆元をそれぞれ求めなさい。

問題 5.2. 二桁以上の素数  $p$  を二つ選んで、それぞれに対して  $\mathbb{F}_p^\times$  の生成元を一つ挙げなさい。

問題 5.3. 「参考」の部分、 $R^\times$  が群であることの証明をせよ。