§7. 因数定理

定義　可換環 R 上の多項式 $f \in R[X]$ に対して，$f(a) = 0$ をみたす $a \in R$ を f の**根**という．

定理 7.1 (剰余定理・因数定理)　可換環 R 上の多項式 $f(X)$ と R の元 a に対して，

$$f(X) = (X - a)g(X) + r$$

をみたす $g(X) \in R[X],\ r \in R$ が存在する．さらに，a が f の根ならば，

$$f(X) = (X - a)g(X)$$

をみたす $g(X) \in R[X]$ がとれる．

定理 7.2　整域 R 上の多項式は，R において $\deg f$ より多くの根を持たない．

補題 7.3　A を有限アーベル群とする (乗法群とし単位元を 1 で表す)．任意の自然数 n に対して $x^n = 1$ をみたす $x \in A$ の個数が n 以下ならば，A は巡回群である．

定理 7.4　整域 R の単元群 $R^\times$ の有限部分群は巡回群である．とくに，K が体ならば，$K^\times$ の有限部分群は巡回群である．

定理 7.5　有限体 F の乗法群 $F^\times$ は巡回群である．

定義　$m > 2$ を自然数とする．以下の条件をみたす整数 g を m を法とする**原始根**という:

> 「m と素な任意の整数 a に対して，
>
> $$a \equiv g^j \pmod{m}$$
>
> をみたす自然数 j が存在する (これは，法 m に関する位数 $\varphi(m)$ をもつ整数の存在と同値)．」

系 7.6　任意の奇素数 p に対して，p を法とする**原始根**が存在する．