定義 1（イデアル）　R を可換環とする。以下を見たす R の部分集合 I を R 上のイデアルという。

(I1)　$\forall x, y \in I, x + y \in I$
(I2)　$\forall x \in I, a \in R, ax \in I$

定義 2（剰余類）　可換環 R 上のイデアル I と任意の $x \in R$ に対して

$$x + I = \{x + a \mid a \in I\}$$

を x を代表元とする剰余類という。

定理 1　ある $x, y \in R$ が $x - y \in I$ であるとき、$x + I = y + I$ である。

証明 1　I の生成元が m であるとする。まず定義より $x + I$ の任意の元 a はある $q \in R$ によって

$$a = x + mq$$

と書くことができる。ここで仮定より、ある p によって $x - y = mp \Leftrightarrow x = y + mp$ となる。この x を代入すると

$$\begin{aligned} a &= y + mp + mq \\ &= y + m(p + q) \end{aligned}$$

となり、$a \in y + I$ が得られた。ここで a は任意の $x + I$ の元であるため $a \in x + I \Rightarrow a \in y + I$ が示された。同様にして $a \in y + I \Rightarrow a \in x + I$ が示される。以上より示された。

定義 3（剰余環）　可換環 R 上のイデアル I に対して

$$R/I = \{x + I \mid x \in R\}$$

として書かれる集合 R/I を R 上の剰余環という。

定理 2　可換環 R 上の剰余環 R/I は可換環となる。

証明 2

定理 3

定理 4（中国剰余定理 (Chinese Remainder Theorem)）　ある剰余環 Z/mZ に