

環  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$  において、6 は

$$6 = 2 \cdot 3, \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

という2通りの既約元への分解をもつ。従って、 $\mathbb{Z}[\sqrt{-5}]$  における倍数の集合を考えると、  
(6の倍数) = (2の倍数)(3の倍数), (6の倍数) =  $(1 + \sqrt{-5}$ の倍数) $(1 - \sqrt{-5}$ の倍数)  
が成り立ち、イデアルの記号を用いると

$$(6) = (2)(3), \quad (6) = (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad (1)$$

となる。(1) は単項イデアルの範囲ではこれ以上分解できない。一方、 $\mathbb{Z}[\sqrt{-5}]$  は一意分解整域ではないから単項イデアル整域ではない。よって、 $\mathbb{Z}[\sqrt{-5}]$  には単項イデアルではないイデアルが存在する。そのようなイデアルを用いると (1) の2式は各々さらに分解される。

$$A = (2, 1 + \sqrt{-5}), \quad B = (2, 1 - \sqrt{-5}), \quad C = (3, 1 + \sqrt{-5}), \quad D = (3, 1 - \sqrt{-5})$$

とする。

$AB \subset (4, 2(1 - \sqrt{-5}), 2(1 + \sqrt{-5}), 6) \subset (2)$ ,  $CD \subset (9, 3(1 - \sqrt{-5}), 3(1 + \sqrt{-5}), 6) \subset (3)$   
であり、また、

$2 = -2 \cdot 2 + (1 + \sqrt{-5})(1 - \sqrt{-5}) \in AB$ ,  $3 = 3 \cdot 3 - (1 + \sqrt{-5})(1 - \sqrt{-5}) \in CD$   
より  $(2) \subset AB$ ,  $(3) \subset CD$  であるから、

$$(2) = AB, \quad (3) = CD$$

となる。従って、(1) の第1式から

$$(6) = ABCD \quad (2)$$

という分解が得られる。他方、

$$AC \subset (6, 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) \subset (1 + \sqrt{-5}),$$

$$BD \subset (6, 2(1 - \sqrt{-5}), 3(1 - \sqrt{-5}), (1 - \sqrt{-5})^2) \subset (1 - \sqrt{-5})$$

であり、また、

$1 + \sqrt{-5} = -2(1 + \sqrt{-5}) + (1 + \sqrt{-5})3 \in AC$ ,  $1 - \sqrt{-5} = -2(1 - \sqrt{-5}) + (1 - \sqrt{-5})3 \in BD$   
より  $(1 + \sqrt{-5}) \subset AC$ ,  $(1 - \sqrt{-5}) \subset BD$  であるから、

$$(1 + \sqrt{-5}) = AC, \quad (1 - \sqrt{-5}) = BD$$

となる。従って、(1) の第2式から

$$(6) = ACBD \quad (3)$$

という分解が得られる。 $\mathbb{Z}[\sqrt{-5}]$  は可換環であるからイデアルの積も可換であり、(2) と (3) は同一の分解である。