3장 환

3.1 환의 정의와 보기

정의 3.1.1

환(ring)이란 다음의 공리들을 만족하는(보통 덧셈과 곱셈으로 쓰게 되는) 두 개의 연산을 갖는 공이 아닌 집합 R을 말한다.

모든 $a, b, c \in R$에 대해서,

(1) $a \in R$이고 $b \in R$면, $a+b \in R$. [덧셈에 대하여 닫힘]

(2) $a+(b+c)=(a+b)+c$. [덧셈의 결합 법칙]

(3) $a+b=b+a$. [덧셈의 교환 법칙]

(4) $\exists\, 0_R \in R \ s.t. \ a+0_R=a=0_R+a \quad \forall a \in R$. [덧셈의 항등원 또는 영원]

(5) $\forall a \in R$, 방정식 $a+x=0_R$이 R에서 해를 갖는다.

(6) $a \in R$이고 $b \in R$이면, $ab \in R$. [곱셈에 대하여 닫힘]

(7) $a(bc)=(ab)c$. [곱셈의 결합법칙]

(8) $a(b+c)=ab+ac$이고 $(a+b)c=ac+bc$. [분배법칙]

정의 3.1.2

가환환(commutative ring)은 다음의 공리를 만족하는 환 R이다.

(9) 임의의 $a, b \in R$에 대하여 $ab=ba$가 성립한다. [곱셈의 교환법칙]

정의 3.1.3

항등원이 있는 환(ring with identity)은 다음의 조건을 만족하는 원 1_R을 포함하는 환 R이다.

(10) 모든 $a \in R$에 대하여 $a1_R=a=1_Ra$가 성립한다. [곱의 항등원]

▌보기 3.1.1 ▌보통의 덧셈과 곱셈을 갖는 정수들 $\mathbb{Z}$는 항등원이 있는 가환환이다. ■

▌보기 3.1.2 ▌류들의 보통의 덧셈과 곱셈을 갖는 집합 $\mathbb{Z}_n$은 정리 2.2.3에 의하여, 항등원이 있는 가환환이다. ■

▌보기 3.1.3 ▌E는 보통의 덧셈과 곱셈을 갖는 짝수 정수들의 집합이라 하자. 두 짝수 정수들의 합과 곱은 역시 짝수이므로, 닫힘 (공리 (1)과 (6))이 성립한다. 0은 짝수 정수이므로, E는 덧셈의 항등원(공리 (4))을 갖는다. a가 짝수이면, $a+x=0$의 해$(-a)$는 역시 짝수이므로 공리

(5)가 성립한다. 나머지 공리들(결합성질, 교환성질, 분배성질)은 모든 E의 원들에 대하여 성립한다. 그러므로 E는 가환환이다. 그러나 E는 항등원이 있는 환이 아니다. 왜냐하면, 어떤 짝수인 정수 e도 모든 $a \in E$에 대하여 $ae = a = ea$인 성질을 갖지 않기 때문이다. ■

▌보기 3.1.4▐ 보통의 덧셈과 곱셈을 갖는 홀수 정수들의 집합은 환이 아니다. 왜냐하면, 공리 (1)이 성립하지 않는다. 두 홀수 정수의 합은 홀수가 아니다. ■

보기 3.1.4는 환의 부분집합이 환이 될 필요가 없음을 보여준

다.

환 R의 부분집합 S가 R에서의 덧셈과 곱셈에 대하여 자신이 환일 때, 우리는 S를 R의 부분환(subring) 이라 말한다. 부분환 S의 영원은 언제나 R의 영원 0_R과 같다(유제3.1.5-1).

공리 2, 3, 7과 8은 환 R의 모든 원에 대하여 성립한다. 그러므로 이 공리들은 반드시 임의의 부분집합 S의 원들에 대하여 성립한다. 그래서 S가 부분환임을 증명하기 위해 다음의 조건들만을 증명할 필요가 있다 :

S는 덧셈과 곱셈에 대하여 닫혀있고(공리 1과6);
$0_R \in S$ (공리 4);
$a \in S$일 때, 방정식 $a + x = 0_R$이 S 에서 해를 갖는다(공리 5).

사실, 환 R의 부분집합 S가 R의 부분환일 필요충분조건은
(i) 임의의 $a, b \in S$에 대하여 $a - b \in S$이고
(ii) 임의의 $a, b \in S$에 대하여 $ab \in S$이다.
이 S가 부분환임을 증명하기 위해 위의 두 조건들만을 보이면 된다. 증명은 예제 7.3.5와 유제 7.3.5를 이용하여 쉽게 증명할 수 있다.

▌보기 3.1.5▐ 아래의 표로 정의 되는 덧셈과 곱셈을 갖춘 집합

+	ㄱ	ㄴ	ㄷ	ㄹ
ㄱ	ㄱ	ㄴ	ㄷ	ㄹ
ㄴ	ㄴ	ㄱ	ㄹ	ㄷ
ㄷ	ㄷ	ㄹ	ㄱ	ㄴ
ㄹ	ㄹ	ㄷ	ㄴ	ㄱ

•	ㄱ	ㄴ	ㄷ	ㄹ
ㄱ	ㄱ	ㄱ	ㄱ	ㄱ
ㄴ	ㄱ	ㄱ	ㄴ	ㄴ
ㄷ	ㄱ	ㄱ	ㄷ	ㄷ
ㄹ	ㄱ	ㄱ	ㄹ	ㄹ

$T = \{ㄱ, ㄴ, ㄷ, ㄹ\}$는 환이다 :

여러분은 공리 (2), (7)과 (8)이 성립한다는 것을 알 수 있다.

원 ㄱ 은, 공리(4)에서 0_R로 표시되는 원인, 덧셈의 항등원이다. ㄱ은 수 0이 $\mathbb{Z}$에서와 같은 방법으로 행동 한다(이것이 표시법 0_R이 공리에서 사용되는 이유다). 그러나 이는 정수 0이 아니다 - 실제로, ㄱ은 어떤 종류의 수도 아니다. 그럼에도 불구하고, 우리는 ㄱ을 이환 T의 "영원"이라 부를 것이다. 공리5를 증명하기 위하여, 다음의 각 방정식

$$\text{ㄴ} + x = \text{ㄱ}, \quad \text{ㄹ} + x = \text{ㄱ},$$
$$\text{ㄷ} + x = \text{ㄱ}, \quad \text{ㄱ} + x = \text{ㄱ}$$

이 T에서 해를 가짐을 보여주어야만 한다. 이것은 덧셈표로부터 쉽게 보여 진다. 예로써, $x = \text{ㄴ}$은 $\text{ㄴ} + x = \text{ㄱ}$의 해 이다. 왜

냐면, $\text{ㄴ} + \text{ㄴ} = \text{ㄱ}$이기 때문이다. T는 가환환이 아님에 주목하라. 예로써 $\text{ㄴㄷ} = \text{ㄴ}$ 이고 $\text{ㄷㄴ} = \text{ㄱ}$이므로, $\text{ㄴㄷ} \neq \text{ㄷㄴ}$.■

보기 3.1.6 $M(\mathbb{R})$은 각 성분이 실수인 모든 2×2행렬들의 집합, 즉 $M(\mathbb{R})$은 모든 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

여기서 $a, b, c, d \in \mathbb{R}$, 꼴의 배열들로 이루어진다고 하자. $M(\mathbb{R})$의 두 원이 같다는 뜻을 다음과 같이 정의한다.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \Leftrightarrow a = r,\ b = s,\ c = t,\ d = u.$$

예로써,

$$\begin{pmatrix} 4 & 0 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 2+2 & 0 \\ 1-4 & 1 \end{pmatrix} \text{ 그러나, } \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} \neq \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}.$$

두 행렬의 덧셈은 다음과 같이 정의한다.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}.$$

예로써,

$$\begin{pmatrix} 3 & -2 \\ 5 & 1 \end{pmatrix} + \begin{pmatrix} 4 & 7 \\ 6 & 0 \end{pmatrix} = \begin{pmatrix} 3+4 & -2+7 \\ 5+6 & 1+0 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 11 & 1 \end{pmatrix}.$$

두 행렬의 곱셈은 다음과 같이 정의한다.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{pmatrix}.$$

예로써,

$$\begin{pmatrix} 2 & 3 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} 1 & -5 \\ 6 & 7 \end{pmatrix} = \begin{pmatrix} 2\cdot 1+3\cdot 6 & 2(-5)+3\cdot 7 \\ 0\cdot 1+(-4) & 0(-5)+(-4)7 \end{pmatrix}$$
$$= \begin{pmatrix} 20 & 11 \\ -24 & -28 \end{pmatrix}.$$

행렬곱셈에서 인수들의 순서를 바꾸는 것은 다른 답을 만들 수 있다.

$$\begin{pmatrix}1 & -5\\ 6 & 7\end{pmatrix}\begin{pmatrix}2 & 3\\ 0 & -4\end{pmatrix}=\begin{pmatrix}1\cdot 2+(-5)0 & 1\cdot 3+(-5)(-4)\\ 6\cdot 2+7\cdot 0 & 6\cdot 3+7(-4)\end{pmatrix}$$
$$=\begin{pmatrix}2 & 23\\ 12 & -10\end{pmatrix}.$$

그러므로 이 곱셈은 가환되지 않는다. 약간의 노력으로, 여러분은 $M(\mathbb{R})$이 항

등원이 있는 환임을 입증할 수 있다. 영원은 행렬 $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$이고 $X=\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}$는

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}+X=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

의 해이다. 곱셈의 항등원(공리 (10))은 행렬 $I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$이다. 예

컨대,

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}a\cdot 1+b\cdot 0 & a\cdot 0+b\cdot 1\\ c\cdot 1+d\cdot 0 & c\cdot 0+d\cdot 1\end{pmatrix}$$
$$=\begin{pmatrix}a & b\\ c & d\end{pmatrix}.$$

$M(\mathbb{R})$의 영이 아닌 두 원의 곱이 영원이 될 수 없음에 주목하

라. 예로써,

$$\begin{pmatrix}4 & 6\\ 2 & 3\end{pmatrix}\begin{pmatrix}-3 & -9\\ 2 & 6\end{pmatrix}=\begin{pmatrix}4(-3)+6\cdot 2 & 4(-9)+6\cdot 6\\ 2(-3)+3\cdot 2 & 2(-9)+3\cdot 6\end{pmatrix}$$
$$=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.\blacksquare$$

보기 3.1.7 $M(\mathbb{Z})$, $M(\mathbb{Q})$, $M(\mathbb{C})$와 $M(\mathbb{Z}_n)$은 각각 정수 $\mathbb{Z}$, 유리수 $\mathbb{Q}$, 복소수 $\mathbb{C}$와 환 $\mathbb{Z}_n$의 성질을 갖고 2×2 행렬들의 집합을 나타낸다고 하자. 보기 3.1.6에서와 같이 정의되는 덧셈과 곱셈과 함께 $M(\mathbb{Z})$, $M(\mathbb{Q})$, $M(\mathbb{C})$와 $M(\mathbb{Z}_n)$ $(n\geq 2)$은 모두 항등원이 있는

비가환환이다.■

보기 3.1.8 T는 $\mathbb{R}$에서 $\mathbb{R}$로의 모든 연속 함수들의 집합이라 하자. 미분적분학에서처럼, $f+g$와 fg는 각각 다음과 같이 정의된다.

$$(f+g)(x)=f(x)+g(x)\text{이고 } (fg)(x)=f(x)g(x).$$

미분적분학에서, 두 연속함수의 합과 곱이 연속이라는 것은 이미 증명되어 있다. 그래서 T는 덧셈과 곱셈에 관하여 닫혀있다(공리 (1)과 (6)). 여러분은 쉽사리 T가 항등원이 있는 가환환임을 입증할 수 있다. 영원은 모든 $x\in R$에 대하여 $h(x)=0$으로 주어지는 함수 h이다. 항등원은 모든 $x\in R$에 대하여 $e(x)=1$로 주어지는 함수 e이다. 다시 한 번 T의 영이 아닌 두 원의 곱

이 영원이 될 수 있다(3장 연습문제 1을 보라). ■

정의 3.1.4

정역(integral domain)은 다음의 공리를 만족하는 항등원 $1_R\neq 0_R$을 갖는 가환환 R이다.

(11) $a,\ b\in R$이고 $ab=0_R$이면, $a=0_R$ 또는 $b=0_R$이다.

조건 $1_R\neq 0_R$은 정역들 중에서 영환을 제외시키기 위해서 필요하다. 공리 (11)은 이것의 대우와 논리적으로 같다.

$$a\neq 0_R\text{이고 } b\neq 0_R\text{이면, } ab\neq 0_R\text{이다.}$$

보기 3.1.9 정수들의 환 $\mathbb{Z}$는 정역이다. p가 소수이면, 정리 2.3.1에 의하여 $\mathbb{Z}_p$ 역시 정역이다. ■

여러분은 $a,\ b\in\mathbb{Z}$이고 $b\neq 0$인 모든 분수 $\frac{a}{b}$들로 이루어지는 유리수들의 집합 $\mathbb{Q}$를 잘 알고 있을 것이다. 두 분수의 같음, 덧셈과 곱셈은 보통의 규칙에 의하여 주어진다.

$$\frac{a}{b}=\frac{r}{s}\ \text{iff}\ as=br,$$

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

$\mathbb{Q}$가 정역임을 증명하는 것은 쉽다. 그러나 $\mathbb{Q}$는 $\mathbb{Z}$에서 성립하지 않는 특별한 성질을 갖는다. $ax=1(a\neq 0)$ 꼴의 모든 방정식은 $\mathbb{Q}$에서 해를 갖는다. 그러므로 $\mathbb{Q}$는 다음 정의의 한 보기다.

정의 3.1.5

나눗셈환(division ring)은 다음의 공리를 만족하는 항등원 $1_R \neq 0_R$을 갖는 환 R이다.

(12) 각 $0_R \neq a \in R$에 대해서, 방정식 $ax = 1_R$과 $xa = 1_R$은 R에서 해를 갖는다.

체(field)는 나눗셈가환환을 말한다.

보기 3.1.10 보통의 덧셈과 곱셈을 갖는 실수들의 집합 $\mathbb{R}$은 체다. $\mathbb{R}$의 부분집합인 유리수들의 집합 $\mathbb{Q}$는 같은 연산을 갖는 체다. 우리는 $\mathbb{Q}$를 $\mathbb{R}$의 부분체(subfield)라 말한다. ■

보기 3.1.11 복소수들의 집합 $\mathbb{C}$는 $a+bi$ 꼴의 모든 수들로 이루어진다. 여기서 $a, b \in \mathbb{R}$이고 $i^2 = -1$이다. $\mathbb{C}$에서 같음은 다음과 같이 정의된다.

$$a+bi = r+si \text{ iff } a = r \text{이고 } b = s.$$

집합 $\mathbb{C}$는 다음 주어진 덧셈과 곱셈을 갖는 체다.

$$(a+bi)+(c+di) = (a+c)+(b+d)i,$$
$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i.$$

실수들의 체 $\mathbb{R}$은 $\mathbb{C}$의 부분체다. 왜냐하면, $\mathbb{R}$은 $a+0i$ 꼴의 모든 복소수들로
이루어지기 때문이다. $0 \neq a+bi \in \mathbb{C}$이면, 방정식 $(a+bi)x = 1$의 해는 $x = c+di$.여기서 $c = \dfrac{a}{(a^2+b^2)} \in \mathbb{R}$ 이고

$d = \dfrac{-b}{(a^2+b^2)} \in \mathbb{R}$(증명하라!). ■

보기 3.1.12 p가 소수이면, 정리 2.3.1에 대하여, Z_p는 체이다. ■

보기 3.1.13 $a, b \in \mathbb{R}$일 때, K는

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

꼴의 모든 2×2행렬들의 집합이라 하자. 여기서 $a, b \in \mathbb{R}$이다. 우리는 K가 체임을 주장한다. K에 속하는 임의의 두 행렬에 대하여,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}.$$

각 경우에 오른쪽변에 있는 행렬은 K에 속한다. 왜냐하면, (위 오른쪽에서 아래 왼쪽까지) 주대각선(main diagonal)을 따라서 있는 성분들은 서로의 음이기 때문이다. 그러므로 K는 덧셈과 곱셈에 관하여 닫혀있다. K는 가환환이다. 왜냐하면,

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

분명히 영행렬과 항등행렬 I는 K에 속한다.

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

면, $AX = I$의 해는 다음과 같음을 입증하라.

$$X = \begin{pmatrix} a/d & -b/d \\ b/d & a/d \end{pmatrix} \in K, \text{ 여기서 } d = a^2 + b^2. \quad \blacksquare$$

비가환 나눗셈환의 예

웨더번(Wedderburn)의 유명한 정리는 모든 유한 나눗셈환은 체임을 보여주기 때문에 이 보기는 반드시 무한집합이다.

보기 3.1.14 환 $M(\mathbb{C})$에서,

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

라 하자. 실수와 행렬의 곱은 다음 규칙으로 주어지는 행렬이다.

$$r\begin{pmatrix} t & u \\ v & w \end{pmatrix} = \begin{pmatrix} rt & ru \\ rv & rw \end{pmatrix}.$$

집합 H는 다음과 같은 꼴의 모든 행렬들로 이루어진다고 하자.

$$a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} bi & 0 \\ 0 & -bi \end{pmatrix} + \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix} + \begin{pmatrix} 0 & di \\ di & 0 \end{pmatrix}$$

$$= \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

여기서 $a, b, c, d \in \mathbb{R}$이다. 이때 H를 실사원수들의 집합이라고 한다. 그러면 행렬들의 보통의 덧셈과 곱셈에서, H는 비가환 나눗셈환이다. 상세한 내용에 대하여 3장 연습문제 3을 보라.

$\blacksquare$

보기 3.1.15 T는 카테시언곱 $\mathbb{Z}_6\times\mathbb{Z}$라 하자. T에서 덧셈은 다음 규칙으로 정의한다.

$$(a,\ z)+(a',\ z')=(a+a',\ z+z').$$

여기서 "+" 기호는 세 가지 방법으로 사용되고 있다. 등호의 오른쪽 변에 있는 첫째 좌표에서 +는 $\mathbb{Z}_6$에서 덧셈을 나타내고, 둘째 좌표에서 +는 $\mathbb{Z}$에서 덧셈을 나타내고, 등호의 왼쪽변에 있는 +는 정의되고 있는 T의 덧셈이다. $\mathbb{Z}_6$는 환이고 $a,\ a'\in\mathbb{Z}_6$이므로, 오른쪽변의 첫째좌표 $a+a'$는 $\mathbb{Z}_6$에 속한다. 비슷하게 $z+z'\in\mathbb{Z}$이다. 그러므로 T에서 덧셈은 닫혀있다. 곱셈

은 비슷하게 정의된다.

$$(a,\ z)(a',\ z')=(aa',\ zz').$$

예로써,

$$(3,\ 5)+(4,\ 9)=(3+4,\ 5+9)=(7,\ 14)$$

이고

$$(3,\ 5)(4,\ 9)=(3\cdot 4,\ 5\cdot 9)=(12,\ 45).$$

여러분은 손쉽게 T가 항등원이 있는 가환환임을 증명할 수 있다. 영원은 $(0,\ 0)$이고 곱의 항등원은 $(1,\ 1)$이다. 여기에서 다루어진 방법은 임의의 두 환이 주어졌을 때도 똑같이 일반적으

로 적용 될 수 있다. 다음의 정리를 보자. ■

정리 3.1.6

R과 S는 환이라 하자. 카테시언곱(Cartesian product) $R\times S$에서 덧셈과 곱셈을 다음과 같이 정의한다.

$$(r,\ s)+(r',\ s')=(r+r',\ s+s'),$$
$$(r,\ s)(r',\ s')=(rr',\ ss').$$

그러면 $R\times S$는 환이다. R과 S가 모두 가환환이면, $R\times S$역시 가환환이다. R과 S가 각각 항등원을 가지면, $R\times S$ 역시 항등원을 갖는다.

예제 | 3.1.1 다음의 각 명제가 참인지 거짓인지를 각각 T, F로 나타내라.

(1) 모든 체는 역시 환이다.

(2) 모든 환은 항등원을 갖는다.

(3) 어떤 체의 부분집합은 주어진 체의 두 연산에 대하여 환이지만 체가 아닐 수 있다.

(4) 환에 대한 분배법칙은 그리 중요하지 않다.

[풀이] (1) T (3) F

(3) T (4) F ■

유제 3.1.1 다음의 각 명제가 참인지 거짓인지를 각각 T, F로 나타내라.

(1) 체에서 곱셈은 가환한다.

(2) 체의 영 아닌 원들은 그 체에 있는 곱셈에 대하여 군을 이룬다.

(3) 모든 환에서 덧셈은 가환한다.

(4) 환에서 모든 원은 덧셈에 대한 역을 갖는다.

예제 | 3.1.2 $A=\left\{\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix} : r\in\mathbb{Q}\right\}$는 $M(\mathbb{R})$의 부분환인가? 항등원을 갖는가?

Tip 부분환의 정의 및 95~96쪽의 부분환임을 증명하는데 필요한 조건들을 다시 확인하고 보기 3.1.6을 참고한다.

[풀이] 임의로 $\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}\in A$를 택하자.

그러면

$$\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}+\begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}=\begin{pmatrix}0 & r+s\\ 0 & 0\end{pmatrix},\ \begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

$r+s\in\mathbb{Q}$. 그래서 $r,\ s\in\mathbb{Q}$이므로, $\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}+\begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}\in A$이고

$\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & s\\ 0 & 0\end{pmatrix}\in A$. 더욱이 $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\in A$이고 $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$은 $M(\mathbb{R})$의 영원이다. 또한 임의의 $\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}\in A$에 대하여 $\begin{pmatrix}0 & -r\\ 0 & 0\end{pmatrix}\in A$은 $\begin{pmatrix}0 & r\\ 0 & 0\end{pmatrix}+x=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$의 해이다. 그러므로 A는 $M(\mathbb{R})$의 부분환이다. 여기서 한편, $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\notin A$이므로 A는 항등원이 없다. 따라서 A는 항등원이 없는 $M(\mathbb{R})$의 부분환이다. ■

유제 3.1.2 다음의 두 개의 집합들 중 어느 것이 $M(\mathbb{R})$의 부분환인가? 어

느 것이 항등원을 갖는가?

(1) $\begin{pmatrix}a & a\\ b & b\end{pmatrix}$ 꼴의 모든 행렬들, 여기서 $a,\ b\in\mathbb{R}$.

(2) $\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$ 꼴의 모든 행렬들, 여기서 $a\in\mathbb{R}$.

예제 | 3.1.3 R과 S는 환이라 하자. 부분집합 $\overline{R}=\{(r,\ 0_s) : r\in R\}$은 $R\times S$의 부분환임을 보여라.

Tip 부분환의 정리 및 95~96쪽의 부분환임을 증명하는데 필요한 조건과 정리 3.1.6을 확인한다.

[풀이] 임의로 $(r,\ 0_s),\ (t,\ 0_s)\in\overline{R}$를 택한다. 그러면

$$(r,\ 0_s)+(t,\ 0_s)=(r+t,\ 0_s)\in\overline{R}$$

$$(r,\ 0_s)\cdot(t,\ 0_s)=(rt,\ 0_s)\in\overline{R}.$$

분명히 $(0_r,\ 0_s)\in\overline{R}$이고 $(0_r,\ 0_s)$는 $R\times S$의 영원이다. 한편 임의의 $(r,\ 0_s)\in\overline{R}$에 대하여, $(-r,\ 0_s)\in\overline{R}$는 $(r,\ 0_s)+x=(0_r,\ 0_s)$의 해이다. 따라서 $\overline{R}$는 $R\times S$의 부분환이다. ■

유 제 | 부분집합 $\overline{S}=\{(0_R,\ s):\ s\in S\}$은 $R\times S$의 부분환임을 보여라.

유 제 | R은 환이라 하자. $R^*=\{(r,\ r):r\in R\}$은 $R\times R$의 부분환임을 증명하라.

유 제 | $\mathbb{Z}[i]$는 집합 $\{a+bi:a,\ b\in\mathbb{Z}\}$를 나타내자. $\mathbb{Z}[i]$는 $\mathbb{C}$의 부분환임을 증명하라.

예제 | 3.1.4 $S=\{a,\ b,\ c\}$, $P(S)$는 S의 모든 부분집합들의 집합이고

$P(S)$의 원들을 다음과 같이 나타내자.

$$S=\{a,\ b,\ c\},\ D=\{a,\ b\},\ E=\{a,\ c\},\ F=\{b,\ c\},$$
$$A=\{a\},\ B=\{b\},\ C=\{c\},\ 0=\varnothing.$$

$P(S)$에서 덧셈과 곱셈은 다음 규칙으로 정의한다.

$$M+N=(M-N)\cup(N-M)\text{이고}\ \ MN=M\cap N.$$

$P(S)$에 대한 덧셈과 곱셈표를 만들어라.

[풀이]

+	0	S	A	B	C	D	E	F
0	0	S	A	B	C	D	E	F
S	S	0	F	E	D	C	B	A
A	A	F	0	D	E	B	C	S
B	B	E	D	0	F	A	S	C
C	C	D	E	F	0	S	A	B
D	D	C	B	A	S	0	F	E
E	E	B	C	S	A	F	0	D
F	F	A	S	C	B	E	D	0

•	0	S	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0
S	0	S	A	B	C	D	E	F
A	0	A	A	0	0	A	A	0
B	0	B	0	B	0	B	0	B
C	0	C	0	0	C	0	C	C
D	0	D	A	B	0	D	A	B
E	0	E	A	0	C	A	E	C
F	0	F	0	B	C	B	C	F

■

유제 3.1.4 다음 각각에 대한 덧셈과 곱셈표를 만들어라.

(1) $\mathbb{Z}_2 \times \mathbb{Z}_3$ (2) $\mathbb{Z}_3 \times \mathbb{Z}_3$

예제 3.1.5 E는 보통의 덧셈을 갖는 짝수 정수들의 집합이라 하자. E에서 새로운 곱셈 $*$를 규칙 "$a * b = \frac{ab}{2}$"로 정의한다. 여기서 오른쪽 변의 곱은 보통의 곱셈이다. 이 연산에서 E는 항등원이 있는 가환환임을 증명하라.

Tip 정의 3.1.1과 3.1.2와 3.1.3을 확인한다.

[풀이] E는 분명히 환의 조건 (1) ~ (5)를 만족한다. 임의로

$a, b \in E$를 택하자. 그러면 $a * b = \frac{ab}{2} \in \mathbb{Z}$ ($\because 4 | ab$이므로, $\frac{ab}{2}$는 짝수)이다. 그래서 E는 "$*$" 관해서 결합 성질을 만족한다. 한편 임의의 $a, b \in E$에 대하여,

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a.$$

그러므로 E는 "$*$"에 관하여 가환적이다. 이제 임의로 $a, b, c \in E$를 택하자.

그러면

$$a * (b+c) = \frac{a(b+c)}{2} = \frac{ab+ac}{2} = \frac{ab}{2} + \frac{ac}{2}$$

$$= a * b + a * c.$$

그래서 E는 분배성질을 만족한다. 마지막으로 항등원 $e \in E$가 존재한다고 가정하자. 그러면 임의의 $a \in E$에 대하여, $e * a = \frac{ea}{2} = a$이다. 그러므로 $e = 2 \in E$이다. 따라서 $(E, +, *)$는 항등원 2를 갖는 가환환이다. ■

유제 $\mathbb{Z}$에서 새로운 덧셈 $\oplus$과 곱셈 $\odot$을 $a \oplus b = a + b - 1$과 $a \odot b =$

$a+b-ab$로 정의한다. 여기서 각 등호의 오른쪽 변에 있는 연산들은 보통의 덧셈, 뺄셈과 곱셈이다. 이 연산들에서 $\mathbb{Z}$는 정역임을 증명하라.

유 제 $\mathbb{Z}$에서 새로운 덧셈과 곱셈을 $a\oplus b=a+b-1$과 $a\odot b=ab-(a+b)+2$로 정의한다. 이 연산들에서 $\mathbb{Z}$는 정역임을 증명하라.

유 제 $\mathbb{Q}$에서 새로운 덧셈과 곱셈을 $r\oplus s=r+s+1$이고 $r\odot s=rs+r+s$로 정의한다. 이 연산들에서 $\mathbb{Q}$는 항등원이

있는 가환환임을 증명하라. $\mathbb{Q}$는 정역인가?

3.2 환의 기본성질

정리 3.2.1

환 R의 임의의 원 a에 대하여, 방정식 $a+x=0_R$은 꼭하나의 해를 갖는다.

[증명] 공리 5에 의하여, 방정식 $a+x=0_R$은 적어도 하나의 해 u를 갖는다. v가 역시 하나의 해라 가정하자. 그러면 $a+u=0_R$이고 $a+v=0_R$이다. 그래서

$$v=o_R+v=(a+u)+v=(u+a)+v=u+(a+v)=u+0_R=u$$

가 성립한다. 따라서 u는 꼭하나의 해다. ■

$-a$는 $a+(-a)=0_R=(-a)+a$인 R의 꼭 하나의 해이다.

환에서, 이 정의는 한 원의 음의 개념과 일치한다. 더 중요한 것은, 이것은 임의의 환에서 "음"에 대한 의미를 제공한다.

▌보기 3.2.1 ▐ 환 $\mathbb{Z}_6$에서 방정식 $2+x=0$의 해는 4이다. 그래서 이 환

에서 $-2=4$이다. 비슷하게, $\mathbb{Z}_{14}$에서 $-9=5$이다. 왜냐하면, 5는 $9+x=0$의 해이기 때문이다. ■

이제 환에서 뺄셈은 다음의 규칙으로 정의된다.

$$b-a=b+(-a).$$

$\mathbb{Z}$와 다른 잘 알고 있는 환에서, 이것은 바로 보통의 뺄셈이다. 다른 환에서 우리는 새로운 연산을 갖는다.

보기 3.2.2 $\mathbb{Z}_6$에서 $1-2=1+(-2)=1+4=5$. ■

정리 3.2.2

환 R에서 $a+b=a+c$이면, $b=c$이다.

[증명] $a+b=a+c$의 양변에 $-a$를 더한다. 그러면

$$-a+(a+b)=-a+(a+c)$$
$$(-a+a)+b=(-a+a)+c \qquad \text{[덧셈의 결합성질]}$$
$$0_R+b=0_R+c. \qquad \text{[음의 정의]}$$

따라서 $b=c$. [항등원의 정의] ■

정리 3.2.3

a와 b는 환 R의 임의의 원이라 하자.

(1) $a\cdot 0_R=0_R=0_R\cdot a$.

(2) $a(-b)=-(ab)=(-a)b$.

(3) $-(-a)=a$. (4) $-(a+b)=(-a)+(-b)$.

(5) $-(a-b)=-a+b$. (6) $(-a)(-b)=ab$.

R이 항등원을 가지면,

(7) $(-1_R)a=-a$.

[증명] (1) $0_R+0_R=0_R$이므로 분배법칙에 의하여,

$$a\cdot 0_R+a\cdot 0_R=a(0_R+0_R)=a\cdot 0_R=a\cdot 0_R+0_R.$$

이 방정식의 첫 번째와 마지막 부분에 정리 3.2.2를 적용하면, $a\cdot 0_R=0_R$을 얻는다. $0_R\cdot a=0_R$의 증명도 비슷하다.

(2) 정의에 의하여, $-(ab)$는 방정식 $ab+x=0_R$의 꼭하나(unique)의 해다. 그래서 이 방정식의 임의의 다른 해는 $-(ab)$와 같아야 한다. 그런데 $x=a(-b)$는 해다. 왜냐하면, 분배법칙의 (1)에 의하여,

$$ab+a(-b)=a[b+(-b)]=a(0_R)=0_R.$$

그러므로 $a(-b)=-(ab)$이다. 다른 부분도 비슷하게 증명된다.

(3) 정의에 의하여, $-(-a)$는 $(-a)+x=0_R$의 꼭하나의 해다. $(-a)+a=0_R$이므로, a는 이 방정식의 해다. 따라서 유일성에 의하여, $-(-a)=a$.

(4) 정의에 의하여, $-(a+b)$는 $(a+b)+x=0_R$의 꼭하나의 해다. 한편,

$$\begin{aligned}(a+b)+[(-a)+(-b)] &= b+[a+(-a)]+(-b)\\ &= (b+0_R)+(-b)\\ &= b+(-b)=0_R.\end{aligned}$$

그래서 $(-a)+(-b)$, 역시 이 방정식의 해다. 따라서 유일성에 의하여, $-(a+b)=(-a)+(-b)$.

(5) 뺄셈의 정의 (4)와 (3)에 의하여,

$$-(a-b)=-(a+(-b))=-a+(-(-b))=-a+b.$$

(6) (3)과 (2)의 반복되는 사용에 의하여,

$$(-a)(-b)=[a(-b)]=-[-(ab)]=ab.$$

(7) (2)에 의하여, $(-1_R)(a)=-(1_Ra)=-(a)=-a$. ■

보통 계산을 할 때, 지수표시법(exponent notation)은, 이와 비

슷한 덧셈의 지수표시법(예컨대, $a+a+a=3a$)처럼 명확하게 편리하다. 이제 우리는 임의의 환에 대하여 이러한 개념들을 수행한다.

R은 환, $a\in R$이고 a는 양의 정수라 하자. 우리는 a^n을 다음과 같이 정의한다.

$$a^n = aaa\cdots a \ [n \text{ 인수}].$$

그러면 임의의 $a\in R$와 양의 정수 m과 n에 대하여,

$$a^m a^n = a^{m+n} \text{이고 } (a^m)^n = a^{mn}$$

임을 증명하는 것은 쉽다. R이 항등원을 갖고 $a\neq 0_R$라 하자. 우리는 a^0을 원 1_R이 되도록 정의한다. 이 경우에 위의 지수법칙은 모든 $m,\ n\geq 0$에 대하여 성립한다.

R은 환, $a\in R$이고 n은 양의 정수라 하자. 그러면 다음을 정의할 수 있다.

$$\begin{aligned}na &= a+a+a+\cdots+a \ [n\text{합}],\\ -na &= (-a)+(-a)+(-a)+\cdots+(-a) \ [n\text{합}].\end{aligned}$$

마지막으로 우리는 $0a=0_R$로 정의한다. 잘 알고 있는 환에서

이것은 전혀 새로운 것이 아니지만, 다른 환에서 이것은 정수 n과 환의 원 a의 '곱'에 의미를 준다.

보기 3.2.3 R은 환이고 $a, b \in R$라 하자. 그러면

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= aa+ab+ba+bb\\ &= a^2+ab+ba+b^2.\end{aligned}$$

여기에서 주의하라. $ab \neq ba$이면, 여러분은 가운데 항(term)들

을 결합할 수 없다. 그러나 R이 가환환이면 $ab = ba$이다. 그래서 우리는 잘 알고 있는 패턴을 갖는다.

$$\begin{aligned}(a+b)^2 &= a^2+ab+ba+b^2\\ &= a^2+ab+ab+b^2\\ &= a^2+2ab+b^2\end{aligned}$$

가환환에서 $n>2$인 $(a+b)^n$의 계산에 대하여, 0.5절에 있는 이항정리(Binomial Theorem)를 보라. ■

정리 3.2.4

R은 환이고 $a, b \in R$라 하자. 그러면 방정식 $a+x=b$는 꼭하나의 해 $x=b-a$를 갖는다.

[증명] $a+[b-a] = a+[b+(-a)] = a+[-a+b]$
$= [a+(-a)]+b = 0_R+b = b.$

그러면 $x=b-a$는 주어진 방정식의 해이다. 이제 w가 임의의 다른 해라 하자. 그러면 $a+w=b=a+(b-a)$이다. 그래서, 정리 3.2.2에 의하여, $w=b-a$. 따라서 $x=b-a$는 유일한 해다.■

환에서 곱셈의 방정식(multiplicative equation) $ax=b$는 해를 갖지 않을 수 있다.
예컨대, $4x=11$은 $\mathbb{Z}$에서 해를 갖지 않는다.
a가 나눗셈환(division ring) R의 영이 아닌 원이면, 공리 (12)에 의하여 방정식 $ax=1_R$은 해 u를 갖고 방정식 $xa=1_R$는 해 v를 갖는다. $au=1_R$이고 $va=1_R$인 사실을 사용하여, 우리는

$$u = 1_R u = (va)u = v(au) = v1_R = v$$

임을 알게 된다. 그래서 나눗셈환의 각 영이 아닌 원 a에 대하여, $au=1_R=ua$인 원 u가 존재한다. 우리는 이러한 상태를 설명하기 위하여 몇 가지 용어(terminology)가 필요하다.

정의 3.2.5

항등원이 있는 환 R의 원 a가 **단원(unit)**일 필요충분조건은 $u \in R$가 존재하여 $\exists\, au = 1_R = ua$이다. 이 경우에 원 u를 a의 **(곱셈의) 역(inverse)**이라 하고 a^{-1}로 쓰게 된다.

단원의 역에 대한 표시법은 실수에서 일반적 지수표시법의 모양으로 나타내진다. 실수에서는 $a^{-1} = 1/a$다. 위에서 알게 되었듯이 나눗셈환의 모든 영이 아닌 원은 단원이다. 더욱이 다른 환에서도 단원들이 존재한다.

보기 3.2.4 $\mathbb{Z}_{10}$에서 원 7은 단원이다. 왜냐하면, $7 \cdot 3 = 1 = 3 \cdot 7$이기 때문이다. 이 경우에 $7^{-1} = 3$이고 $3^{-1} = 7$이다. 더 일반적으로, 따름정리 2.3.1에 의하여,

a가 $\mathbb{Z}_n$에서 단원이다 $\Leftrightarrow$ $\mathbb{Z}$에서 $(a, n) = 1$. ■

보기 3.2.5 $\mathbb{Z}$에서 단원은 1과 -1뿐이다(왜?). 그러나 비가환환 $M(\mathbb{R})$에서 많은 단원이 있다. 예컨대,

$$\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}.$$

그래서 $\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$는 단원이다. 행렬 환에서 단원을 가역행렬(invertible matrix)이라 한다. ■

정리 3.2.6

R은 항등원이 있는 환이고, $a, b \in R$라 하자. a가 단원이면, 각 방정식 $ax = b$와 $ya = b$는 R에서 꼭하나의 해를 갖는다.

[증명] a는 단원이므로, $a^{-1} \in R$이고 $a\,a^{-1} = 1_R = a^{-1}\,a$이다. 그러면

$$a(a^{-1}\,b) = (a\,a^{-1})b = 1_R b = b$$

가 성립한다. 그래서 $x = a^{-1}\,b$는 $ax = b$의 해이다. $x = c$가 이 방정식의 다른 해라 하자. 그러면 $ac = b$이고

$$c = 1_R\,c = (a^{-1}a)c = a^{-1}(a\,c) = a^{-1}\,b.$$

그러므로 $x = a^{-1}b$는 유일한 해이다. 비슷한 방법으로, 우리는 $y = ba^{-1}$가 $ya = b$의 꼭하나의 해임을 보일 수 있다. ■

각 방정식은 꼭하나의 해를 갖는다. 그러나 비가환환에서 $ax = b$의 해가 $ya = b$의 해와 같지 않을 수 있다.

가끔 $\mathbb{Z}$에서 계산을 할 때 소거($a \neq 0$이고 $ab = ac$면 $b = c$)를 사용한다. 그러나 소거가 모든 환에서 허용되지는 않는다. 예컨대, $\mathbb{Z}_{12}$에서 $2 \cdot 4 = 2 \cdot 10$이지만 $4 \neq 10$이다. $\mathbb{Z}$는 정역이고 $\mathbb{Z}_{12}$는 정역이 아닌 것이 차이점이다.

정리 3.2.7

R은 항등원이 있는 가환환이라 하자. 그러면 R이 정역일 필요충분조건은 R에서 $ab = ac$일 때 $a \neq 0_R$이면 $b = c$이다.

[증명] ($\Rightarrow$) : R이 정역, $a \neq 0_R$이고 R에서 $ab = ac$라 가정하자. 그러면 $ab - ac = 0_R$이다. 또한 $a(b-c) = 0_R$이 성립한다. $a \neq 0_R$이고 R은 정역이므로, 공리 (11)에 의하여 $b - c = 0_R$, 즉 $b = c$이다.

($\Leftarrow$) : 소거 성질이 R에서 성립한다고 가정하자. R이 정역임을 증명하기 위하여, 우리는 공리 11이 성립하는 것만을 증명할 필요

가 있다. $ab = 0_R$라 가정하자.

$a = 0_R$이면 증명이 끝난다. 그러므로 $a \neq 0_R$이라 하면

$ab = 0_R = a0_R$이므로 소거법칙에 의해 $b = 0_R$이다. 따라서 $a = 0_R$ 또는 $b = 0_R$. 따라서 R은 정역이다. ■

따름정리 3.2.7

모든 체 R은 정역이다.

[증명] 모든 체는 항등원이 있는 가환환이다. 임의의 $a, b, c \in R$에 대하여 $ab = ac$이고 $a \neq 0_R$라 가정하자. 그러면 a는 단원이다. 그래서 $a^{-1} \in R$이 존재하여 $a^{-1}a = 1_R = a\,a^{-1}$이 성립한다.

$ab = ac$의 양변에 a^{-1}를 곱하면, $b = c$이다. 따라서 정리 3.2.7에 대하여, R은 정역이다. ■

일반적으로, 따름정리 3.2.7의 역은 성립하지 않는다($\mathbb{Z}$는 정역

이지만 체가 아니다). 그러나 유한인 경우에는 성립한다.

정리 3.2.8 ∗1998년도 임용고시 문제

모든 유한 정역 R은 체이다.

[증명] R은 항등원이 있는 가환환 이므로, 우리는, 각 $0_R \neq a \in R$에 대하여, 방정식 $ax = 1_R$이 해를 가짐을 보이면 된다.

$a_1, a_2, \cdots, a_n$은 R의 서로 다른 원이라 하고 $a_t \neq 0_R$라 가정하자. $a_t x = 1_R$이 해를 가짐을 보이기 위하여 $a_t a_1, a_t a_2, a_t a_3, \cdots, a_t a_n$

을 생각한다. $a_i \neq a_j$이면, $a_t a_i \neq a_t a_j$(왜냐하면 $a_t a_i = a_t a_j$라면, 소거 성질에 의하여, $a_i = a_j$이기 때문이다). 그래서 $a_t a_1, a_t a_2, a_t a_3, \cdots, a_t a_n$은 R의 n개의 서로 다른 원이다. 그러나 R은 모두 꼭 n개의 원을 갖는다. 그러므로 $1 \in \{a_t a_1, a_t a_2, a_t a_3, \cdots, a_t a_n\}$이다. 따라서 적당한 j가 존재하여 $a_t a_j = 1_R$ 이다. 그러므로 방정식 $a_t x = 1_R$은 해를 갖는다. 따라서 R은 체이다.

■

우리는 약간의 편리한 용어를 소개하고 이 장을 끝낸다.

정의 3.2.9

가환환 R의 영이 아닌 원 a가 있다 하자. 영이 아닌 원소 $b \in R$가 존재하여 $ab = 0_R$이면 a를 영인자(zero divisor)라 한다.

예로써, 3은 $\mathbb{Z}_6$에서 영인수이다. 왜냐하면, $3 \cdot 2 = 0$이기 때문이다. 0_R은 영인자가 아님에 주의하라. 정역은 영인자를 소유하지 않는 영환이 아닌, 항등원이 있는 가환환이다. 어떠한 단원도 영인자가 아니다(예제 3.2.3). 그러나 영인자가 아닌 원이 단원일 필요는 없다(예컨대, 2는 $\mathbb{Z}$에서 영인자도 단원도 아니다).

그림 3.2.1은 환들 사이의 관계를 나타낸다.

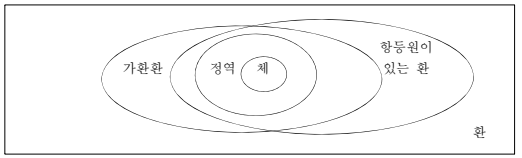
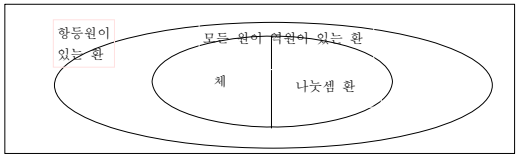


그림 3.2.1



예제 | 3.2.1 **환 R의 원 e가 $e^2=e$을 만족하면 멱등원(idempotent element)이라 한다.**

(1) 환 $M(\mathbb{R})$에 속하는 멱등원 4개만 구하라(4개 이상 있다).

(2) $\mathbb{Z}_{12}$에 속하는 모든 멱등원을 구하라.

[풀이] (1) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(\mathbb{R})$이 멱등원이라 하자. 그러면

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a^2+bc & ab+ad \\ ac+cd & bc+d_2 \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

그래서

$$a^2+bc=a \ \ldots ①$$
$$ab+ad=b \ \ldots ②$$
$$ac+cd=c \ \ldots ③$$
$$bc+d^2=d \ \ldots ④$$

식 ①, ②, ③, ④를 연립하여 $a,\ b,\ c,\ d$를 구하면,

$$(a,\ b,\ c,\ d)=(0,\ 0,\ 0,\ 0),\ (1,\ 0,\ 0,\ 1),\ (0,\ 1,\ 0,\ 1),$$
$$(0,\ 0,\ 0,\ 1).$$

따라서 $M(\mathbb{R})$의 4개의 멱등원은

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

(2) $a^2=a$가 되는 $a\in\mathbb{Z}_{12}$를 구하면 $a=0,\ 1,\ 4,\ 9$. 따라서 $\mathbb{Z}_{12}$의 멱등원은 $0,\ 1,\ 4,\ 9$. ■

유 제 R을 실함수의 집합이라고 하고 $f,\ g\in R$에서 모든 실수 x에 대해서

$$(f+g)(x)=f(x)+g(x),\ \ (f\cdot g)(x)=f(x)g(x)$$

로 덧셈과 곱셈을 정의한다.

(1) $(R,\ +,\ \cdot)$은 환이 됨을 보여라

(2) R에서 모든 멱등원을 구하여라.

유 제 $R=\{f \mid f:[0,\ 1]\to R,\ f$는 연속함수$\}$, R에서의 연산 $+,\ \cdot$은 유제 3.2.1-1과 같다. R에서의 멱등원을 구하여라.

정역 정역R에 속하는 멱등원은 0_R과 1_R뿐임을 증명하라.

Tip 멱등원의 정의와 정리 3.2.7을 확인한다.

[풀이] e는 0_R이 아닌 정역 R의 멱등원이라 하자. 그러면

$$e^2 = e = e \cdot 1_R.$$

그러므로 $e = 1_R$이다. 따라서 멱등원은 0_R과 1_R뿐이다. ■

유 제 e는 환 R의 멱등원이고 $x \in R$라 하자.
$(xe - exe)^2 = 0_R$임을 증명하라.

유 제 R은 1을 갖는 환이고, r을 멱등원이라 하자.
(1) $1 - r$도 멱등원이다.
(2) r 또는 $1 - r$은 영인수이다.

Tip
정의 3.2.5와 3.2.9를 확인한다.

예제 | 3.2.3 가환환의 단원은 영인수가 될 수 없음을 증명하라.

[풀이] R은 가환환이고 $u \in R$는 임의의 단원이라 하자. u가 영인수라 가정하자. 그러면 $0_R \neq b \in R$가 존재하여 $ub = 0_R$이다. u는 단원이므로 $v \in R$이 존재하여 $uv = 1_R = vu$이다. 그래서 $v(ub) = v0_R = 0_R$이다. 그런데 $v(ub) = (vu)b = 1_R b = b$이므로 $b = 0_R$이 된다. 이것은 $b \neq 0_R$라는 사실에 모순이다. 따라서 u는 영인자가 아니다. ■

유 제 R은 항등원이 있는 가환환이고 $a \in R$라 하자. $a^2 = 1_R$이고

$a \neq \pm 1_R$이면, $a + 1_R$과 $a - 1_R$은 영인수임을 증명하라.

유 제 R은 가환환이고 $a \in R$라 하자. $a \neq 0_R$이고 a는 영인수가 아니라 가정하자. R에서 $ab = ac$이면, $b = c$임을 증명하라.

예제 | 3.2.4 환의 원 a가 적당한 양의 정수 n이 존재하여 $a^n = 0_R$을 만족하면 멱영원(nilpotent element)이라 한다. 0_R이 아닌 멱영원이 환 R에 존재하지 않을 필요충분조건은 방정식 $x^2 = 0_R$의 0_R이 아닌 해가 존재하지 않는 것이다. 이를 증명하라.

[풀이] ($\Rightarrow$) : R의 0이 아닌 원소 $a \in R$는 멱영원이 아니라는 것이므로 모든 n에 대하여 $a^n \neq 0$이 아니다. 따라서 $n = 2$일 때, 즉, 방정식 $x^2 = 0_R$의 영이 아닌 해는 존재하지 않는다. 따라서 $x^2 = 0_R$의 해는 0_R뿐이다.

($\Leftarrow$) : 필요조건이 성립하고 충분조건이 성립하지 않는다고 가정하자. 영이 아닌 한 원소 $a \in R$가 있어 자연수 k가 $a^k = 0$를 만족하는 가장 작은 수라 하자. 즉, $a^i \neq 0$, $i < k$이다. 만약 $k = 2$이면 $a^2 = 0_R$이고 이 말은 a가 $x^2 = 0_R$의 근이라는 뜻이므로 $a = 0_R$이다. 그러므

로 $k>2$이다.

$i)$ k가 짝수일 때,

$$a^k=(a^{k/2})^2=0_R$$

이 되므로 가정에 의해 $a^{k/2}=0_R$이다. $k/2<k$이므로 $a^i\neq 0,\ i<k$이라는 것에 모순이다.

$ii)$ k가 홀수일 때,

$$0_R=0_R\cdot a=a^k\cdot a=a^{k+1}=(a^{(k+1)/2})^2$$

이 되므로 가정에 의해 $a^{(k+1)/2}=0_R$이다.

$(k+1)/2<k$ 이므로 $a^i\neq 0,\ i<k$이라는 것에 모

순이다.

■

유 제 R은 1을 갖는 가환환이고 $x\in R$은 멱영원이라 하자. 다음을 증명하여라.

(1) $1+x$은 단원이다.

(2) a가 멱영원, u가 단원이면 $a+u$도 단원이다.

유 제 $\mathbb{Z}_4\times\mathbb{Z}_6$에서 단원, 영인수, 멱등원, 멱영원을 모두 구하여라.

예제 | 3.2.5 R은 항등원이 있는 환이고 $a\in R$라 하자. $a^2=0_R$이면, $a+1_R$과 $a-1_R$은 단원임을 증명하라.

[풀이] $a^2=0_R$이므로

$-1=0_R-1=a^2-1=(a+1)(a-1)=(a-1)(a+1)$이다.

$1=-(a+1)(a-1)=-(a-1)(a+1)$이 되므로 $a+1_R$과 $a-1_R$은 단원이다. ■

(i) 임의의 $n\in\mathbb{Z}^+$에 대하여, $n1\neq 0$. 따라서 $\mathbb{Z}$의 표수는 0이다.

(ii) 분명히 $\mathbb{Z}_n$에서 n은 $n1=0$인 최소의 양의 정수이다. 그러므로 $\mathbb{Z}_n$의 표수는 n이다.

(iii) $\mathbb{Z}_4\times\mathbb{Z}_6$의 표수가 n이라 하자.

그러면 $n(1,\ 1)=(n1,\ n1)=(0,\ 0)$. (*)

그런데 (ii)에 의하여, $\mathbb{Z}_4$와 $\mathbb{Z}_6$의 표수는 각각 4와 6이다. 그러므로, (*)가 성립하려면, n은 4와 6의 최소공배수이다. 따라서 $n=12$는 $\mathbb{Z}_4\times\mathbb{Z}_6$의 표수이다.

유제 3.2.5 R은 표수 $n>0$의 항등원이 있는 환이라 한다.

(1) 모든 $a\in R$에 대하여 $na=0_R$임을 증명하라.

(2) R이 정역이면 n은 소수임을 증명하라.

예제 3.2.7 다음 각 명제가 참 또는 거짓인지를 말하라.

(1) 항등원이 있는 환은 적어도 두 개의 단원을 갖는다.

(2) n이 소수가 아니면, $n\mathbb{Z}$는 영인수를 갖는다.

(3) 모든 체는 정역이다.

[풀이] (1) F (2) F (3) T ■

유제 3.2.7 다음 각 명제가 참 또는 거짓인지를 말하라.

(1) 항등원이 있는 모든 환은 많아야 두 개의 단원을 갖는다.

(2) 두 정역의 직곱은 다시 정역이다.

(3) $n\mathbb{Z}$는 $\mathbb{Z}$의 부분정역이다.

(4) $\mathbb{Z}$는 $\mathbb{Q}$의 부분체이다.

3.3 동형사상

▌보기 3.3.1 ▐ $\mathbb{Z}_{10}$ 의 부분집합 $S=\{0,2,4,6,8\}$을 생각하자. $\mathbb{Z}_{10}$의 덧셈과 곱셈표로부터 알 수 있듯이, S는 가환환이다:

+	0	6	2	8	4
0	0	6	2	8	4
6	6	2	8	4	0
2	2	8	4	0	6
8	8	4	0	6	2
4	4	0	6	2	8

•	0	6	2	8	4
0	0	0	0	0	0
6	0	6	2	8	4
2	0	2	4	6	8
8	0	8	6	4	2
4	0	4	8	2	6

이 표들을 신중하게 조사하게 되면, S는 5개의 원을 갖는 체이고 곱셈의 항등원은 6임을 알게 된다. ■

우리는 S가 이 원소들의 표시를 제외하고 체 $\mathbb{Z}_5$와 "본질적으로 같다 "는 것을 알 수 있다. $\mathbb{Z}_5$에 대한 덧셈과 곱셈표를 만들어라. S의 원들과 어떠한 가능한 혼돈도 피하기 위하여, $\mathbb{Z}_5$의 원들을 $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$로 나타낸다. 다음에 계획(Scheme)에 따라서 $\mathbb{Z}_5$의 원들에 다음과 같이 다시 이름을 붙인다 :

$\bar{0}$은 0으로, $\bar{1}$은 6으로, $\bar{2}$는 2로, $\bar{3}$은 8로, $\bar{4}$는 4로 붙인다.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

"R과 S가 동형이다"는 직관적인 생각에 두 가지 관점이 있다 : 다시 이름을 붙이고 표들을 비교하는 것. 다시 이름을 붙이는 것은 R의 모든 원들이 S의 꼭 하나의 원 (R의 새로 붙여진 이름)과 짝지어짐을 의미한다. 다른 말로 하면, 각 $r \in R$에 이것의 새로 붙여진 이름 $f(r) \in S$을 할당하는 함수 $f : R \to S$가 존재한다. 위의 보기에서, 우리는 다음과 같이 주어지는 이름을 다시 붙이는 함수 $f : \mathbb{Z}_5 \to S$를 사용하였다 :

$$f(\bar{0}) = 0,\ f(\bar{1}) = 6,\ f(\bar{2}) = 2,\ f(\bar{3}) = 8,\ f(\bar{4}) = 4.$$

이와 같은 함수는 다음의 특별한 성질들을 가져야만 한다.

(i) R의 다른 원들은 다른 새로 붙여진 이름을 얻어야만 한다.

$$R\text{에서 } r \neq r' \text{이면, } S\text{에서 } f(r) \neq f(r').$$

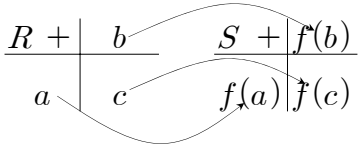
(ii) S의 각 원은 R의 어떤 원의 붙여진 이름이어야만 한다.

$$\forall\ s \in S,\ \exists\ r \in R \quad s.t. \quad f(r) = s.$$

명제 (i)과 (ii)는 간단히 함수 f가 단사(injective)이고 동시에 전사(surjective)이어야만 한다. 즉 f는 전단사 함수(bijection)이어야만 한다고 말한다.

그러나 전단사 함수(다시 이름을 붙이는 계획) f는, R의 표들이 f가 적용될때 S의 표들이 되지 않는 한, 동형사상

(isomorphism)이 아닐 것이다. 이 경우에, R에서 $a+b=c$면, R과 S의 표들은 다음과 같이 보여야만 한다 :



표는 $f(a)+f(b)=f(c)$임을 보여준다. 그러나 $a+b$와 c는 R의 같은 원이다. 그래서 $f(a+b)=f(c)$이 된다. 그러므로

$$f(a+b) = f(a)+f(b).$$

이것은 f가 R의 덧셈표를 S의 덧셈표로 바꾸기 위하여 만족해

야만 하는 조건이다. 곱셈표들에 대하여 f에 대한 비슷한 조건은 $f(ab)=f(a)f(b)$이다. 이제 우리는 동형사상에 대한 공식적인 정의를 말할 수 있다.

정의 3.3.1

집합 R과 S가 환이라 하자. 함수 $f: R \to S$가 존재하여 다음을 만족하면 환 R이 환 S와 동형이라고 하고 $R \cong S$로 쓴다.

(i) f는 단사

(ii) f는 전사

(iii) $f(a+b)=f(a)+f(b)$이고 $f(ab)=f(a)f(b)\ \forall\ a,\ b \in R$.

이 경우에, 함수 f를 **동형사상**(isomorphism)이라 한다. 조건 (iii)을 만족하지만 단사 또는 전사일 필요가 없는 함수를 **준동형사상**(homomorphism)이라 한다.

주목 동형사상이기 위하여, 함수는 정의 3.3.1에 있는 세 가지 모든 조건을 만족해야만 한다. 함수가 세 조건들 중의 임의의 두 조건을 만족하지만, 나머지를 만족하지 않을 수 있다. 3장 연습문제 12를 보라.

주목 정의 3.3.1에서 조건 (3)은 틀림없이 기호들의 교묘한 처리(maniqulation)가 아니다. $f(x)=x+2$로 주어진 함수 $f: R \to R$와 같은, 많은 함수들은 간단히 준동형사상이 아니다. f는 조건 (3)을 만족하지 않는다. 왜냐하면, 예로써,

$f(3+4)=f(7)=9$이지만 $f(3)+f(4)=5+6=11$이고,

$f(3\cdot 4)=f(12)=14$이지만 $f(3)f(4)=5\cdot 6=30$이다.

보기 3.3.2 보기 3.1.13에서, 우리는 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ 꼴의 모든 2×2 행렬들의 체 K를 생각하였다. 여기서 $a,\ b \in R$이다. 우리는 K가 복소수들의 체 $\mathbb{C}$와 동형임을 주장한다. 이것을 증명하기 위하여, 함수 $f: K \to \mathbb{C}$를 규칙 $f\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=a+bi$로 정의한다. f가 단사임을 보이기 위하여 $f\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=f\begin{pmatrix} r & s \\ -s & r \end{pmatrix}$이라 가정하자. 그러면 f의 정의에 의하여, $\mathbb{C}$에서 $a+bi=r+si$이다. $\mathbb{C}$에서 같음의 법

칙에 의하여, $a=r$이고 $b=s$이다. 그래서 K에서

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} r & s \\ -s & r \end{pmatrix}.$$

그러므로 f는 단사이다. 분명히, 임의의 복소수 $a+bi$에 대하여

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K \text{이고 } f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a+bi.$$

그러므로 f는 전사이다. 마지막으로, 임의의 $A, B \in K$에 대하여 우리는 $f(A+B)=f(A)+f(B)$이고 $f(AB)=f(A)f(B)$임을 보여야만 한다.

$$f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] = f\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}$$
$$= (a+c)+(b+d)i$$
$$= (a+bi)+(c+di)$$
$$= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + f\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

이고

$$f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] = f\begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$
$$= (ac-bd)+(ad+bc)i$$

$$= (a+bi)(c+di)$$
$$= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} f\begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

그러므로 f는 동형사상이다. 따라서 $K \cong \mathbb{C}$. ■

보기 3.3.3 $f: \mathbb{C} \to \mathbb{C}$는 $f(a+bi)=a-bi$로 주어지는 복소수의 켤레사상(conjugation mapping)이라 하자. 그러면

$$f[(a+bi)+(c+di)] = f[(a+c)+(b+d)i]$$
$$= (a+c)-(b+d)i$$
$$= (a-bi)+(c-di)$$

$$= f(a+bi)+f(c+di),$$
$$f[(a+bi)(c+di)] = f[(ac-bd)+(ad+bc)i]$$
$$= (ac-bd)-(b+d)i$$
$$= (a-bi)(c-di)$$
$$= f(a+bi)f(c+di).$$

그래서 f는 준동형사상이다. 여러분은 쉽게 f가 전단사임을 보여줄 수 있다(3장의 연습문제 13). 따라서 f는 동형사상이다.

■

정리 3.3.2

$f : R \to S$는 환들의 준동형사상이라 하자. 그러면

(1) $f(0_R) = 0_S$.

(2) $f(-a) = -f(a),\ \forall\ a \in R$.

R과 S가 항등원을 갖고 f가 동형사상이면,

(3) $f(1_R) = 1_S$.

[증명] (1) f는 준동형사상이고 R에서 $0_R + 0_R = 0_R$이므로, S에서

$$f(0_R) + f(0_R) = f(0_R + 0_R) = f(0_R).$$

양쪽 끝에서 $f(0_R)$을 빼면, $f(0_R) = 0_S$.

(2) $$f(a) + f(-a) = f(a + (-a)) = f(0_R) = 0_S.$$

그래서 $f(-a)$는 $f(a) + x = 0_S$의 해이다. 정리 3.2.1에 의하여, 이 방정식의 유일한 해는 $-f(a)$이다. 따라서 유일성에 의하여, $f(-a) = -f(a)$이다.

(3) f는 전사이므로 $r \in R$이 존재하여 $1_S = f(r)$이다. 따라서

$$f(1_R) = f(1_R) \cdot 1_S = f(1_R)f(r) = f(1_R r) = f(r) = 1_S. \quad \blacksquare$$

보기 3.3.4 $\mathbb{Z}_{12}$에서 환 $\mathbb{Z}_3 \times \mathbb{Z}_4$로의 동형사상 f가 존재한다고 가정하자. 그러면 정리 3.3.2에 의하여, $f(1) = (1,\ 1)$이고 f는 준동형사상이므로, f는 다음을 만족 해야만 한다.

$$f(2) = f(1+1) = f(1) + f(1) = (1,\ 1) + (1,\ 1) = (2,\ 2),$$
$$f(3) = f(2+1) = f(2) + f(1) = (2,\ 2) + (1,\ 1) = (0,\ 3),$$
$$f(4) = f(3+1) = f(3) + f(1) = (0,\ 3) + (1,\ 1) = (1,\ 0).$$

이 방법을 계속하는 것은 f가 동형사상이면, f는 다음과 같은 전단사함수임을 보여준다.

$$f(1) = (1,\ 1),\ f(4) = (1,\ 0),\ f(7) = (1,\ 3),\ f(10) = (1,\ 2),$$

$$f(2) = (2,\ 2),\ f(5) = (2,\ 1),\ f(8) = (2,\ 0),\ f(11) = (2,\ 3),$$
$$f(3) = (0,\ 3),\ f(6) = (0,\ 2),\ f(9) = (0,\ 1),\ f(0) = (0,\ 0).$$

여기까지에 이르러 우리가 보여주었던 모든 것은 이 전단사함수 f가 유일한 가능한 동형사상이다. 이 f가 실제로 동형사상임을 보이기 위하여, 우리는 이것이 준동형사상임을 입증해야 한다. 이것은 (지루한) 덧셈과 곱셈표를 만들거나 또는 f의 규칙이 다음의 방법

$$f([a]_{12}) = ([a]_3,\ [a]_4)$$

으로 설명될 수 있음을 관찰함으로써 입증될 수 있다. 여기서

$[a]_{12}$는 $\mathbb{Z}_{12}$에 속하는 정수 a의 합동류를 나타내고, $[a]_3$은 $\mathbb{Z}_3$에 속하는 a의 합동류 그리고 $[a]_4$는 $\mathbb{Z}_4$에 속하는 a의 합동류를 나타낸다(이 마지막 명제가 옳다는 것을 입증하자). 그러면

$$\begin{aligned} f([a]_{12}+[b]_{12}) &= f([a+b]_{12}) && [\mathbb{Z}_{12}\text{에서 덧셈의 정의}] \\ &= ([a+b]_3,\ [a+b]_4) && [f\text{의 정의}] \\ &= ([a]_3+[b]_3,\ [a]_4+[b]_4) && [\mathbb{Z}_3\text{과 } \mathbb{Z}_4\text{에서 덧셈의 정의}] \\ &= ([a]_3,\ [a]_4)+([b]_3,\ [b]_4) && [\mathbb{Z}_3\times\mathbb{Z}_4\text{에서 덧셈의 정리}] \\ &= f([a]_{12})+f([b]_{12}). && [f\text{의 정의}] \end{aligned}$$

덧셈 대신에 곱셈을 사용하는 일치하는 주장을 하게 되면, $f([a]_{12}[b]_{12})=f([a]_{12})f([b]_{12})$임을 보여줄 수 있다. 따라서 f는 동형사상이고 $\mathbb{Z}_{12}\cong\mathbb{Z}_3\times\mathbb{Z}_4$. ■

보기 3.3.5 $\mathbb{Z}_6$는 $\mathbb{Z}_{12}$ 또는 $\mathbb{Z}$와 동형이 아니다. 왜냐면, 6개 원으로된 집합 $\mathbb{Z}_6$에서 더 큰 집합 $\mathbb{Z}_{12}$ 또는 $\mathbb{Z}$로의 전사함수(또는 더 큰 집합 $\mathbb{Z}_{12}$ 또는 $\mathbb{Z}$에서 $\mathbb{Z}_6$으로의 단사함수)를 가질 수 없기 때문이다.

■

두 무한환 또는 같은 원의 개수를 갖는 두 유한환이 동형이 아님을 보이기 위하여, 간접증명방법을 사용하는 것이 보통 가장 좋다.

보기 3.3.6 두 환 $\mathbb{Z}_4$와 $\mathbb{Z}_2\times\mathbb{Z}_2$는 동형이 아님을 보여라.

[풀이] 이것을 보이기 위하여, 동형사상 $f:\mathbb{Z}_4\to\mathbb{Z}_2\times\mathbb{Z}_2$가 존재한다고 가정하자. 그러면 정리 3.3.2에 의하여,

$$f(0)=(0,\ 0)\text{이고 } f(1)=(1,\ 1).$$

더욱이,

$$f(2)=f(1+1)=f(1)+f(1)=(1,\ 1)+(1,\ 1)=(0,\ 0).$$

f는 단사이고 $f(2)=f(0)$이므로, 이것은 모순이다. 따라서 동형사상은 존재할 수 없다. ■

같은 크기의 두 환이 동형이 아님을 증명하는 대부분의 공통의 방법은 동형사상에 의하여 보존되는 성질을 생각하는 것이다. R이 하나의 성질을 갖고 R이 S와 동형이면, S는 반드시 R과 같은 성질을 갖는다. 하나의 환이 이와 같은 성질을 갖고 다른 환이 이 성질을 갖지 않으면, 두 환은 동형이 아니다.

보기 3.3.7 가환환은 비가환환과 동형이 아니다. 왜냐하면, 가환성질은 동형사상에 의하여 보존되기 때문이다. 이제 이 사실을 입증한다. R은 가환환이고 S는 비가환환이라하고 동형사상 $f: R \to S$가 존재한다고 가정하자. $c, d \in S$를 임의로 택하자. 그러면 f는 전사이므로, $a, b \in R$이 존재하여 $f(a) = c$이고 $f(b) = d$가 성립한다. R에서 $ab = ba$이고 f는 준동형사상이므로,

$$cd = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = dc.$$

그래서 S는 가환환이다. 이것은 모순이다. 따라서 R과 S는 동형이 아니다. ■

보기 3.3.8 $f: R \to S$는 항등원이 있는 환들의 동형사상 이라하자. a가 R의 단원이면, $u \in R$가 존재하여 $au = 1_R = ua$이다. 그러면 정리 3.3.2에 의하여 $f(a)f(u) = f(au) = f(1_R) = 1_S$이고 비슷하게 $f(u)f(a) = 1_S$이다. 그러므로 $f(a)$는 S의 단원이다. 따라서 단원이라는 성질은 동형사상에 의하여 보존된다. 환 $\mathbb{Z}_8$은 4개의 단원(따름정리 2.3.1에 의하여, 1, 3, 5, 7)을 갖는다. 그래서 $\mathbb{Z}_8$에서 다른 환으로의 임의의 동형사상은 이 4개의 단원들을 다른 환의 단원들로 대응시킬 것이다. $\mathbb{Z}_8$는 $\mathbb{Z}_4 \times \mathbb{Z}_2$와 동형이 아니다. 왜냐하면, $\mathbb{Z}_4 \times \mathbb{Z}_2$는 두 개의 단원 $(1, 1)$과 $(3, 1)$만

을 갖기 때문이다. 여러분은 쉽사리 이 사실을 증명할 수 있다. 비슷하게, $\mathbb{Z}$는 $\mathbb{Q}$, $\mathbb{R}$과 $\mathbb{C}$와 동형이 아니다. 왜냐하면, $\mathbb{Z}$는 꼭 두 개의 단원(1과 -1)을 갖고, 반면에 체 $\mathbb{Q}$, $\mathbb{R}$과 $\mathbb{C}$의 모든 영이 아닌 원은 단원이기 때문이다. ■

예제 | 3.3.1 R은 환이고 R^*는 (a, a) 꼴의 모든 원들로 이루어지는 $R \times R$의 부분환이라 하자. $f(a) = (a, a)$로 주어지는 함수 $f: R \to R^*$는 동형사상임을 증명하라.

Tip 동형사상의 정의를 확인한다.

[풀이] (1) 임의의 $a, b \in R$에 대하여 $f(a) = f(b)$라 가정하자.

그러면 $(a, a) = (b, b)$이다. 그래서 $a = b$이 된다. 그러므로 f는 단사이다.

(2) f가 전사임은 분명하다.

(3) 임의의 $a, b \in R$에 대하여,

$$f(a+b) = (a+b, a+b) = (a, a) + (b, b) = f(a) + f(b),$$
$$f(ab) = (ab, ab) = (a, a)(b, b) = f(a)f(b).$$

그래서 f는 준동형사상이다. 따라서 f는 동형사상이다. ■

유제 | R과 S는 환이고 $\overline{R}$는 $(a, 0_S)$ 꼴의 원들로 이루어진 $R \times S$의

부분환이라 하자. $f(a)=(a,\ 0_S)$로 주어지는 함수 $f: R\to\overline{R}$는 동형사상임을 보여라.

유 제 실수들의 체 $\mathbb{R}$은 $\begin{pmatrix}0 & 0\\ 0 & a\end{pmatrix}$ 꼴의 모든 2×2행렬들의 환과 동형임을 증명하라. 여기서 $a\in\mathbb{R}$이다.

[도움말: $f(a)=\begin{pmatrix}0 & 0\\ 0 & a\end{pmatrix}$로 주어지는 함수 f를 생각하라]

유 제 $\mathbb{Q}(\sqrt{2})=\{r+s\sqrt{2}\ ;r,\ s\in\mathbb{Q}\}$라 하자. $f(a+b\sqrt{2})=a-b\sqrt{2}$로 주어지는 함수 $f:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2})$는 동형사상

임을 증명하라.

예제 | 3.3.2 $\mathbb{Z}^*$는 유제 3.1.5-1에서 정의된 $\oplus$과 $\odot$ 연산을 갖는 정수들의 환이라 하자. $\mathbb{Z}\cong\mathbb{Z}^*$임을 증명하라.

Tip 동형의 정의와 정리 3.3.2를 확인한다.

[풀이] $\mathbb{Z}^*$에서 (곱셈)항등원은 분명히 0이다. 동형사상 $f:\mathbb{Z}\to\mathbb{Z}^*$가 존재한다고 가정하자. 그러면 $f(1)=0(\because 1\in\mathbb{Z}$은 항등원)이다.

그래서

$$f(2)=f(1+1)=f(1)\oplus f(1)=0\oplus 0=0+0-1=-1,$$

$$f(3)=f(2+1)=f(2)\oplus f(1)=-1\oplus 0=-1+0-1=-2,$$
$$f(4)=f(3+1)=f(3)\oplus f(1)=-2\oplus 0=-2+0-1=-3,$$
$$\vdots$$

이제 함수 $f:\mathbb{Z}\to\mathbb{Z}^*$를 다음과 같이 정의한다.

$$f(n)=-n+1\quad\forall n\in\mathbb{Z}.$$

(1) 임의의 $n,\ m\in\mathbb{Z}$에 대하여, $f(n)=f(m)$라 가정하자. 그러면 $-n+1=-m+1$. 그래서 $n=m$. 그러므로 f는 단사이다.

(2) 임의로 $n\in\mathbb{Z}^*$을 택하고 $m=-n+1$이라 하자. 그러면 $m\in\mathbb{Z}$이고

$$f(m)=-m+1=-(-n+1)+1=n.$$

그래서 f는 전사이다.

(3) 임의로 $n,\ m\in\mathbb{Z}$을 택하자. 그러면

$$\begin{aligned}f(n+m)&=-(n+m)+1\\&=(-n+1)+(-m+1)-1\\&=(-n+1)\oplus(-m+1)\\&=f(n)\oplus f(m),\end{aligned}$$

$$\begin{aligned}f(nm)&=-(nm)+1\\&=-(n+1)+(-m+1)-(nm-n-m+1)\end{aligned}$$

$$= (-n+1)+(-m+1)-(-n+1)(-m+1)$$
$$= (-n+1)\odot(-m+1)$$
$$= f(n)\odot f(m).$$

그러므로 f는 준동형사상이다. 따라서 $\mathbb{Z} \cong \mathbb{Z}^*$. ■

유 제 $\overline{\mathbb{Z}}$는 유제 3.1.5-2에서 정의된 $\oplus$과 $\odot$ 연산을 갖는 정수들의 환이라 하자. $\overline{\mathbb{Z}} \cong \mathbb{Z}$임을 증명하라.

유 제 $\mathbb{R}\times\mathbb{R}$은 3장 연습문제 6번의 체라 하자. $\mathbb{R}\times\mathbb{R} \cong \mathbb{C}$임을 보여

라. 여기서 $\mathbb{C}$은 복소수들의 체이다.

예 제 | 3.3.3 (1) $f: R\to S$와 $g: S\to T$가 환준동형사상이면, $g\circ f: R\to T$는 환준동형사상임을 보여라.

(2) f와 g가 환동형사상이면, $g\circ f$역시 환동형사상임을 보여라.

[풀이] (1) 임의로 $a, b\in R$을 택하자. 그러면

$$g\circ f(a+b) = g(f(a+b)) \qquad (\text{합성함수의 정의})$$
$$= g(f(a)+f(b)) \qquad (\because f\text{가 준동형사상})$$

$$= g(f(a))+g(f(b)) \quad (\because g\text{가 준동형사상})$$
$$= g\circ f(a)+g\circ f(b),$$

$$g\circ f(ab) = g(f(ab))$$
$$= g(f(a)f(b))$$
$$= g(f(a))g(f(b))$$
$$= g\circ f(a)\ g\circ f(b).$$

따라서 $g\circ f$는 준동형사상이다.

(2) (1)에 의하여 $g\circ f$는 준동형사상이다. 또한 f와 g가 전단사이므로, $g\circ f$는 전단사이다. 따라서 동형사상이다. ■

유제 | 3.3.3 $f: R\to S$는 환들의 동형사상이고 $g: S\to R$는 (들어가기 0.4에서 정의된) f의 역함수라 하자. 그러면 g 역시 동형사상임을 보여라.

[도움말: $g(a+b)=g(a)+g(b)$임을 보이기 위하여 f의 왼쪽과 오른쪽변의 상을 생각하고 f가 준동형사상이고 $g\circ f$는 항등함수라는 사실을 사용하라.]

예 제 | 3.3.4 동형사상에 의하여 보존되는 성질들을 사용하여 첫 번째 환과 두 번째 환이 동형이 아님을 보여라.

Tip
동형사상에 대하여 보존되는 성질들이 어떤 것들인 지 확인한다(정리 3.3.2의 뒤에 나오는 각 보기들과 설명을 다시 확인한다).

(1) E와 $\mathbb{Z}$, 여기서 E는 짝수정수의 집합.

(2) $\mathbb{Z}_4\times\mathbb{Z}_{14}$와 $\mathbb{Z}_{16}$

(3) $\mathbb{Z}\times\mathbb{Z}_2$와 $\mathbb{Z}$

[풀이](1) $\mathbb{Z}$는 항등원 1을 갖지만 E는 항등원을 갖지 않는다.

(2) 두 환이 다른 원의 개수를 갖는다. 그러므로 $\mathbb{Z}_4\times\mathbb{Z}_{14}$에서 방정식 $\mathbb{Z}_{16}$으로의 단사함수가 존재할 수 없다.

(3) $f:\mathbb{Z}\times\mathbb{Z}_2\to\mathbb{Z}$를 동형사상이라하자. 그러면 정리 3.3.2에 의하여 $f((0,0))=0$이다. 또한

$$0=f((0,0))=f((0,1)+(0,1))=f((0,1))+f((0,1))=2f((0,\ 1))$$

이므로 $f((0,\ 1))=0$이므로 f가 단사라는 것에 모순이다. 따라서 이러한 동형사상은 존재하는 것이 불가능하다. ■

유제 | 3.3.4 동형사상에 의하여 보존되는 성질들을 사용하여 첫 번째 환과 두 번째 환이 동형이 아님을 보여라.

(1) $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$과 $M(\mathbb{R})$

(2) $\mathbb{Q}$와 $\mathbb{R}$

(3) $\mathbb{Z}_4\times\mathbb{Z}_4$와 $\mathbb{Z}_{16}$

예제 | 3.3.5 T는 $\mathbb{R}$에서 $\mathbb{R}$로의 연속함수들의 환이라 하자. $f\in T$이고 $f^2=f$이면, f는 상수함수 $f(x)=0$ 또는 상수함수 $f(x)=1$임을 보여라.

[풀이] 임의로 $a\in\mathbb{R}$를 택하자. 그러면 $f^2(a)=f(a)f(a)=f(a)$이다. 그래서

$$f(a)=(f(a)-1)=0.$$

그러므로

$$f(a)=0 \text{ 또는 } f(a)=1.$$

따라서 f는 상수함수 $f=\underline{0}$ 또는 $f=\underline{1}$이다. ■

유제 | 3.3.5 예제 3.3.5의 환 T는 $\mathbb{R}\times\mathbb{R}$과 동형이 아님을 증명하라.

[도움말 $\mathbb{R}\times\mathbb{R}$에서 $x^2=x$의 4개의 해를 구하고 예제 3.3.5를 사용하라]

예제 | 3.3.6 $m,\ n\in\mathbb{Z},\ (m,\ n)=1$이고 $f:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$은 $f([a]_{mn})=([a]_m,\ [a]_n)$으로 주어지는 함수라 하자(표시법은 보기 3.3.4에서와 같음).

(1) 함수 f는 잘 정의(well-defined)된다. 즉, $\mathbb{Z}_{mn}$에서 $[a]_{mn}$

$= [b]_{mn}$이면, $\mathbb{Z}_m$에서 $[a]_m = [b]_m$이고 $\mathbb{Z}_n$에서 $[a]_n = [b]_n$임을 보여라.

(2) f는 동형사상임을 증명하라.

[도움말: 보기 3.3.4의 증명을 각색하고, f가 전단사함수임을 증명하는 것이 여기에서 추가로 처리할 차이점이다.]

[풀이] (1) $[a]_{mn} = [b]_{mn}$라 가정하자. 그러면 $a \equiv b \pmod{mn}$이므로 ($(m, n) = 1$이므로 삭제) $a \equiv b \pmod{m}$이고 $a \equiv b \pmod{n}$이다. 따라서 $[a]_m = [b]_m$이고 $[a]_n = [b]_n$. 그러므로 f는 잘 정의된다.

(2) (i) 임의로 $[a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}$을 택하자. 그러면

$$\begin{aligned} f([a]_{mn}[b]_{mn}) &= f([ab]_{mn}) \\ &= ([ab]_m, [ab]_n) \\ &= ([a]_m[b]_m, [a]_n[b]_n) \\ &= ([a]_m, [a]_n)([b]_m, [b]_n) \\ &= f([a]_{mn})f([b]_{mn}), \end{aligned}$$

$$\begin{aligned} f([a]_{mn} + [b]_{mn}) &= f([a+b]_{mn}) \\ &= ([a+b]_m, [a+b]_n) \\ &= ([a]_m + [b]_m, [a]_n + [b]_n) \end{aligned}$$

$$= ([a]_m, [a]_n) + ([b]_m, [b]_n)$$
$$= f([a]_{mn}) + f([b]_{mn}).$$

그래서 f는 준동형사상이다.

(ii) 임의의 $[a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}$에 대하여 $f([a]_{mn}) = f([b]_{mn})$라 가정하자. 그러면

$$([a]_m, [a]_n) = ([b]_m, [b]_n).$$

그래서

$$[a]_m = [b]_m, \quad [a]_n = [b]_n.$$

$(m, n) = 1$이므로, $[a]_{mn} = [b]_{mn}$이다. 그러므로 f는 단사함수이다.

(iii) 임의로 $([a]_m, [a]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$을 택하자. 그러면 분명히 $[a]_{mn} \in \mathbb{Z}_{mn}$이다. 더욱이 $f([a]_{mn}) = ([a]_m, [b]_n)$. 그래서 f는 전사함수이다.

따라서 f는 동형사상이다. ■

유제 3.3.6 $(m, n) \neq 1$이면, $\mathbb{Z}_{mn}$는 $\mathbb{Z}_m \times \mathbb{Z}_n$과 동형이 아님을 증명하라.

증명 : 임의의 $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ 에 대하여 f가 동형사상이 되기 위

하여는 $f(1)=(1,1)$이 되어야 한다. 따라서 $f(2)=(2,2)$, ... 이 되어야 한다. 그런데 $(m,n)\neq 1$이므로 $m=m_1d$이고 $n=n_1d$라 하면 $m_1n_1d\not\equiv 0 \pmod{mn}$, $nm_1\equiv 0 \pmod{n}$이고 $n_1m\equiv 0 \pmod{m}$이므로 $f(0)\neq f(m_1n_1d)=(m_1n_1d,\, m_1n_1d)=(mn_1,\, nm_1)=(0,0)$이다. 따라서 $f(0)=(0,0)$이 되어야 하는 것에 모순이 된다.

간단히 반례를 들면 $m=4$, $n=2$이라 하자. $5\equiv 1 \pmod{4}$이고 $5\equiv 1 \pmod{2}$이지만 $5\not\equiv 1 \pmod{8}$이다.

유제 3.3.7 $a\equiv b \pmod{[m,n]}$일 필요충분조건은 $a\equiv b \pmod{m}$이고 $a\equiv b \pmod{n}$인 것이다. 여기서 $[m,n]$은 m과 n의 최소공해수이다.

증명] $\Rightarrow$] $a\equiv b \pmod{[m,n]}$이므로 $[mn]|a-b$이다. 따라서 $m|a-b$이고 $n|a-b$이다. 그러므로 $a\equiv b \pmod{m}$이고 $a\equiv b \pmod{n}$인 것이다.

$\Leftarrow$] $m|a-b$이고 $n|a-b$이므로 $a-b=nk_1$이고 $a-b=mk_2$라 하자. $(m,n)=d$라 하면 적당한 정수 m_1과 n_1이 존재하여 $m=dm_1$이고 $n=dn_1$, $(m_1,n_1)=1$이라 할 수 있고 $[m,n]=n_1m_1d$이다.

$a-b=nk_1=dn_1k_1=dm_1k_2$이고 $(m_1,n_1)=1$이므로 $n_1|k_2$이어야만 한다. 즉, $k_2=n_1k'_2$이다. 따라서 $a-b=dm_1n_1k'_2=[m,n]k'_2$이므로 $[mn]|a-b$이다. 그러므로 $a\equiv b \pmod{[m,n]}$이다.

여기서 $(m,n)=1$이면 $[m,n]=mn$이다.

3장 연습문제

1. T는 $\mathbb{R}$에서 $\mathbb{R}$로의 연속함수들의 환이고 f와 g는 각각 다음과 같이 주어진다고 하자.

$$f(x)=\begin{cases}0 & (x\le 2)\\ x-2 & (2<x)\end{cases},\quad g(x)=\begin{cases}2-x & (x\le 2)\\ 0 & (2<x)\end{cases}.$$

$f,\, g\in T$이고 $fg=0_T$임을 보여라. 그러므로 T는 정역이 아니다.

2. d는 완전제곱이 아닌 정수라 하자. $\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d}\,:a,\, b\in\mathbb{Q}\}$는 $\mathbb{C}$의 부분체임을 증명하라.

3. H는 실사원수들의 집합이고 1, i, j, k는 보기 3.1.14에서 정의된 행렬들이라 하자.

(1) 다음을 각각 증명하라.

$$\mathrm{i}^2=\mathrm{j}^2=\mathrm{k}^2=-1,\quad \mathrm{ij}=-\mathrm{ji}=\mathrm{k},$$
$$\mathrm{jk}=-\mathrm{kj}=\mathrm{i},\quad \mathrm{ki}=-\mathrm{ik}=\mathrm{j}.$$

(2) H는 항등원이 있는 비가환환임을 증명하라.

(3) H는 나눗셈환임을 증명하라.

[도움말: $M=\mathrm{a1}+\mathrm{bi}+\mathrm{cj}+\mathrm{dk}$ 방정식 $Mx=1$의 해는 행렬 $ta\mathbf{1}-\mathrm{tbi}-\mathrm{tcj}-\mathrm{tdk}$임을 입증하라. 여기서 $t=1/(a^2+b^2+c^2+d^2)$이다.]

(4) 방정식 $x^2=-1$은 H에서 무한히 많은 해를 가짐을 보여라.

[도움말: $\mathrm{a1}+\mathrm{bi}+\mathrm{cj}+\mathrm{dk}$ 꼴의 사원수를 생각하자. 여기서 $b^2+c^2+d^2=1$이다.]

4. 증명하거나 거짓임을 증명하라

(1) R과 S가 정역이면, $R\times S$는 정역이다.

(2) R과 S가 체이면, $R\times S$는 체이다.

5. 집합 $\mathbb{Z}\times\mathbb{Z}$는 정리 3.1.6에서와 같은 덧셈을 갖고 새로운 곱셈은 다음의 규칙으로 주어진다고 하자.

$$(a,\ b)(c,\ d)=(ac+2bd,\ ad+bc).$$

이 연산들에서 $\mathbb{Z}\times\mathbb{Z}$는 항등원이 있는 가환환임을 증명하라.

6. $\mathbb{R}\times\mathbb{R}$은 정리 3.1.6에서와 같은 덧셈을 갖고 새로운 곱셈은

$$(a,\ b)(c,\ d)=(ac-bd,\ ad+bc)$$

로 주어진다. 이 연산들에서 $\mathbb{R}\times\mathbb{R}$은 체임을 증명하라.

7. S는 환 R의 공이 아닌 부분집합이라 하자. 그러면

$$S\text{가 } R\text{의 부분환이다} \iff \forall\, a,\ b\in S,\ a-b,\ ab\in S.$$

이를 증명하라.

8. (1) S가 환 R의 부분환이면, $0_S=0_R$임을 증명하라.

[도움말: $a\in S$에 대하여, 방정식 $a+x=a$를 생각하라.]

(2) S는 환 R의 부분환이라 하자. R과 S가 항등원을 갖는다면 1_S가 1_R과 같지 않을 수 있음을 보이기 위하여 보기를 주라.

(3) S가 체 R의 부분체면, $1_S=1_R$임을 증명하라.

9. 불환(Boolean ring)은 모든 $x\in R$에 대하여 $x^2=x$인 항등원이 있는 환 R을 말한다. R이 불환이면, 다음이 성립함을 증명하라.

(1) 모든 $a\in R$에 대하여, $a+a=0_R$.

[도움말: $(a+a)^2$을 전개하라.]

(2) R은 가환환이다.

[도움말 $(a+b)^2$을 전개하라]

10. $\mathbb{Z}_n$의 영 아닌 원이 영인수이다 $\Leftrightarrow$ 이 원이 단원이 아니다. 이를 증명하라.

11. R은 환, $a \in R$이고 $S = \{r \in R : ra = 0_R\}$라 하자. 그러면 S는 R의 부분환임을 증명하라.

12. $f(a) = [a]$로 주어지는 함수 $f : Z \to Z_n$는 전사인 준동형사상이지만 동형사상이 아님을 보여라.

13. 복소수 켤레사상 $f : \mathbb{C} \to \mathbb{C}$는 전단사함수임을 보여라.

14. R은 항등원이 있는 환이고 $f : R \to S$는 환들의 전사준동형사상이라 하자. S는 항등원을 갖고 $f(1_R) = 1_S$임을 증명하라.