A First Course In

Abstract Algebra

< Fraleigh 현대대수학 연습문제 풀이 >

- 제 7판 -

- J -

- 차 례-

※ 문제 1~6에서 주어진 복소수의 부분집합은 덧셈위에서 복소수의 군 C의 덧셈에 대한 부분군이 되는가를 결정하라.

문 1. R

풀 이

$R \subseteq C$이고 임의의 $a, b \in R$에 대하여 $a-b \in R$이므로 R은 군 C의 덧셈에 대한 부분군이 된다.

문 2. Q^+

풀 이

$Q^+ \subseteq C$이지만 $-1 = 1-2 \notin Q^+$이므로 Q^+는 군 C의 덧셈에 대한 부분군이 될 수 없다.

문 3. $7Z$

풀 이

$7Z \subseteq C$이고 임의의 $a, b \in 7Z$에 대하여 $x, y \in Z$가 존재해서 $a = 7x, b = 7y$를 만족한다.
그러면 $a-b = 7(x-y) \in 7Z$이 성립한다. 그러므로 $7Z$는 군 C의 덧셈에 대한 부분군이 된다.

문 4. 0을 포함한 순허수의 집합 iR

풀 이

$iR \subseteq C$이고 임의의 $a, b \in iR$에 대하여 $x, y \in R$이 존재해서 $a = ix, b = iy$를 만족한다.
그러면 $a-b = i(x-y) \in iR$이 성립한다. 따라서 iR는 군 C의 덧셈에 대한 부분군이 된다.

문 5. π**의 유리수 배의 집합** πQ

풀 이

πQ는 C의 부분집합임은 자명하다. 또한 πQ는 덧셈에 대한 연산에서 군을 이룬다.
따라서 πQ는 군 C의 덧셈에 대한 부분군이 된다.

문 6. 집합 $\{\pi^n | n \in Z\}$

풀 이

집합 $\{\pi^n | n \in Z\}$는 C의 부분집합임은 자명하다. 하지만 $0 = \pi - \pi \notin \{\pi^n | n \in Z\}$이다.
따라서 집합 $\{\pi^n | n \in Z\}$는 군 C의 덧셈에 대한 부분군이 될 수 없다.

문 7. 문제 1~6중에서 복소수의 부분집합은 곱셈위에서 복소수의 군 C의 곱셈에 대한 부분군이 되는가를 결정하라.

풀 이

(a) R인 경우 0을 포함한다. 이 경우에 0에 관하여 곱셈에 대한 항등원이 존재하지 않는다. 따라서 R은 군 C의 곱셈에 대한 부분군이 될 수 없다.
(b) Q^+인 경우는 C의 부분집합이며 곱셈 연산에 관하여 군을 이루므로 따라서 Q^+는 군 C의 곱셈에 대한 부분군이다.
(c) $7Z$인 경우 0을 포함한다. 따라서 $7Z$는 군 C의 곱셈에 대한 부분군이 될 수 없다.

(d) iR인 경우 0을 포함한다. 따라서 iR는 군 C의 곱셈에 대한 부분군이 될 수 없다.
(e) πQ인 경우 0을 포함한다. 따라서 πQ는 군 C의 곱셈에 대한 부분군이 될 수 없다.
(f) $\{\pi^n | n \in Z\}$는 C의 부분집합임은 자명하다. 또한 곱셈에 대하여 군을 이룬다. 그러므로 $\{\pi^n | n \in Z\}$는 군 C의 곱셈에 대한 부분군이다.

※ 문제 8~13에서, 실수를 원소로 갖는 $n \times n$인 가역행렬이 군 $GL(n, R)$의 부분군인가를 결정하라.

문 8. $M \equiv \{A = (a_{ij})_{n \times n} | \, |A| = 2, a_{ij} \in R\}$

풀 이

M이 일반선형군 $GL(n, R)$의 부분집합임은 자명하다. 또한 임의의 $A, B \in M$에 대하여 가역행렬이므로 $A^{-1} \in M$이다. 하지만 $|A^{-1}B| = |A^{-1}||B| = 2 \cdot 2 = 4 \notin M$이다. 그러므로 M은 곱셈에 대하여 일반선형군 $GL(n, R)$의 부분군이 될 수 없다.

문 9. $M \equiv \{A = (a_{ij})_{n \times n} | a_{ij} = 0 (i \neq j), a_{ij} \neq 0 (i = j)\}$

풀 이

- 생략함 -

문 10. $M \equiv \{A = (a_{ij})_{n \times n} | a_{ij} = 0 (i > j), a_{ij} \neq 0 (i \leq j)\}$

풀 이

- 생략함 -

문 11. $M \equiv \{A = (a_{ij})_{n \times n} | \, |A| = -1, a_{ij} \in R\}$

풀 이

곱셈에 관한 연산에 대하여 닫혀 있지 않다.
따라서 M은 일반선형군 $GL(n, R)$의 곱셈에 관하여 부분군이 될 수 없다.

문 12. $M \equiv \{A = (a_{ij})_{n \times n} | \, |A| = 1 \text{ or } -1, a_{ij} \in R\}$

풀 이

M이 일반선형군 $GL(n, R)$의 부분집합임은 자명하다. 또한, 임의의 $A, B \in M$에 대하여
$|A^{-1}| = \frac{1}{|A|} = 1 \text{ or } -1$이고 $|AB| = |A||B| = 1 \text{ or } -1$이므로 $A^{-1}, AB \in M$을 만족한다.
따라서 M은 일반선형군 $GL(n, R)$의 곱셈에 관하여 부분군이 될 수 있다.

문 13. $M \equiv \{A = (a_{ij})_{n \times n} | (A^T)A = I_n\}$

풀 이

M이 일반선형군 $GL(n, R)$의 부분집합임은 자명하다.
또한, 임의의 $A, B \in M$에 대하여 $(A^{-1})^T(A^{-1}) = (A^T)^{-1}(A^{-1}) = (A^T A)^{-1} = I_n^{-1} = I_n$이고
$(AB)^T(AB) = B^T A^T AB = B^T I_n B = B^T B = I_n$이므로 $A^{-1}, AB \in M$을 만족한다.
따라서 M은 일반선형군 $GL(n, R)$의 곱셈에 관하여 부분군이 될 수 있다.

※ 정의역을 R로 갖는 모든 실가 함수의 집합을 F라 하고 $\tilde{F}$를 R내의 모든 점에 0이 아닌 값을 함수로 구성된 F의 부분집합이라 하자. 문제 7~12에서 유도된 이항연산을 갖는 F의 주어진 부분집합이 (a) 덧셈에 대해 군 F의 부분군 (b) 곱셈에 대한 군 $\tilde{F}$의 부분군이 되는지를 결정하라.

문 14. 부분집합 $\tilde{F} \equiv \{f(x) \neq 0 | f \in F, x \in R\}$

풀 이

① (a)를 만족하지 않는다.
(∵ 항등함수 0이 존재하지 않는다.)
② (b)를 만족한다.
(∵ $\tilde{F}$는 $\tilde{F}$의 부분집합임에는 자명하다.
또한, 임의의 $f, g \in \tilde{F}$ $(x \in R)$에 대하여 $f(x) \neq 0$이므로 $f^{-1} = \frac{1}{f} \in F$이고 $f(x) \neq 0, g(x) \neq 0$이므로 $fg \in F$이다. 따라서 $\tilde{F}$는 곱셈에 대하여 군 $\tilde{F}$의 부분군이다.)

문 15. $A \equiv \{f \in F | f(1) = 0\}$

풀 이

① (a)를 만족한다.
(∵ A는 F의 부분집합임에는 자명하다. 또한, 임의의 $f, g \in A$ $(x \in R)$에 대하여
$f(1) = 0$이므로 $-f(1) = 0$이고, $f(1) = 0, g(1) = 0$이므로 $f(1) + g(1) = 0$이다.
따라서 $-f, f+g \in A$이다. 그러므로 A는 덧셈에 대하여 군 F의 부분군이다.)
② (b)를 만족하지 않는다.
(∵ $f \in A$에 대한 역원이 존재하지 않는다.)

문 16. $A \equiv \{f \in F | f(1) = 1\}$

풀 이

① (a)를 만족하지 않는다.
(∵ 덧셈의 연산에 관하여 닫혀있지 않다.)
② (b)를 만족한다.
(∵ A가 $\tilde{F}$의 부분집합임을 자명하다. 또한 임의의 $f, g \in A$ $(x \in R)$에 대하여
$f(1) = 1$이므로 $f^{-1}(1) = \frac{1}{f(1)} = 1$이므로 $f^{-1} \in A$이다. 그리고 $fg(1) = f(1)g(1) = 1$이므로 $fg \in A$이다.
따라서 A는 곱셈에 대하여 군 $\tilde{F}$의 부분군이다.)

문 17. $A \equiv \{f \in F | f(0) = 1\}$

풀 이

① (a)를 만족하지 않는다.
(∵ 덧셈에 관한 연산에 닫혀있지 않다.)
② (b)를 만족한다.
(∵ A가 $\tilde{F}$의 부분집합임을 자명하다. 또한 임의의 $f, g \in A$ $(x \in R)$에 대하여
$f(0) = 1$이므로 $f^{-1}(0) = \frac{1}{f(0)} = 1$이므로 $f^{-1} \in A$이다. 그리고 $fg(0) = f(0)g(0) = 1$이므로 $fg \in A$이다.
따라서 A는 곱셈에 대하여 군 $\tilde{F}$의 부분군이다.)

문 18. $A \equiv \{f \in F | f(0) = -1\}$

풀 이

① ⓐ를 만족하지 않는다.
(∵ 덧셈에 관한 연산에 닫혀있지 않다.)
② ⓑ를 만족하지 않는다.
(∵ 곱셈에 관한 연산에 닫혀있지 않다.)

문 19. F내의 모든 상수 함수들의 집합

풀 이

F내의 모든 상수 함수들의 집합을 A라 할 때
① ⓐ를 만족한다.
(∵ $A \simeq R$이므로 덧셈에 관하여 군을 이룬다.)
② ⓑ를 만족하지 않는다.
(∵ 0에 관한 역원이 존재하지 않는다.)

문 20. 다음에 주어진 많은 군 중에서 한 군이 다른 어떤 군의 부분군이 되는지의 모든 관계를 찾아 보아라.

G_1 = 덧셈에 대한 Z
G_2 = 덧셈에 대한 $12Z$
G_3 = 곱셈에 대한 Q^+
G_4 = 덧셈에 대한 R
G_5 = 곱셈에 대한 R^+
G_6 = 곱셈에 대한 $\{\pi^n | n \in Z\}$
G_7 = 덧셈에 대한 $3Z$
G_8 = 곱셈에 대한 6의 모든 정수배의 집합
G_9 = 곱셈에 대한 $\{6^n | n \in Z\}$

풀 이

덧셈에 관한 연산에서는 $12Z \leq 6Z \leq 3Z \leq Z \leq R$을 만족한다.
그러므로 $G_2 \leq G_8 \leq G_7 \leq G_{11} \leq G_4$의 관계를 만족한다.
한편, 곱셈에 관한 연산에서는 $Q^+ \leq R^+, \pi^n \leq R^+, 6^n \leq R^+$을 만족한다.
그러므로 $G_3 \leq G_5, G_6 \leq G_5, G_9 \leq G_5$의 관계를 만족한다.

문 21. 다음 각 순환군에서 적어도 5개의 원소를 써라.
ⓐ 덧셈에 대한 $25Z$

풀 이

$-50, -25, 0, 25, 50$

ⓑ 곱셈에 대한 $\left\{\left(\frac{1}{2}\right)^n | n \in Z\right\}$

풀 이

$-4, -2, 1, \frac{1}{2}, \frac{1}{4}$

(c) 곱셈에 대한 $\{\pi^n | n \in Z\}$

풀 이

$1, \pi, \pi^2, \pi^3, \pi^4$

※ 문제 22~24에서는 주어진 2차 정방행렬에 의해서 생성된 일반선형군 $GL(2, R)$의 순환 부분군의 모든 원소를 나타내시오.

문 22. $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$

풀 이

$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$이므로 위수 2인 순환군이다.

그러므로 $\left\{\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right\}$는 $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$에 의해 생성된 순환 부분군이다.

문 23. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

풀 이

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$이므로 따라서 $\left\{\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} | n \in Z^+\right\}$는 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$에 의해 생성된 순환 부분군이다.

문 24. $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$

풀 이

$\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix}$이므로 따라서 $\left\{\begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix} | n \in Z^+\right\}$는 $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$에 의해 생성된 순환 부분군이다.

문 25. $\begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$

풀 이

$\left\{\begin{bmatrix} 2^k & 0 \\ 0 & 2^k \end{bmatrix} | k\text{는 짝수}\right\} \cup \left\{\begin{bmatrix} 0 & (-2)^k \\ (-2)^k & 0 \end{bmatrix} | k\text{는 홀수}\right\}$는 $\begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$에 의해 생성된 순환 부분군이다.

문 26. 다음 군 중에서 순환군은 어느 것이며, 각 순환군에 대해서 그 군의 모든 생성원을 찾아라.

$G_1 = \langle Z, + \rangle$, $G_2 = \langle Q, + \rangle$, $G_3 = \langle Q^+, \cdot \rangle$, $G_4 = \langle 6Z, + \rangle$,

$G_5 =$**곱셈에 대한** $\{6^n | n \in Z\}$, $G_6 =$**덧셈에 대한** $\{a + b\sqrt{2} | a, b \in Z\}$

풀 이

순환군인 것은 G_1, G_4, G_5이고 이 때 생성원은 각각 $\langle 1 \rangle (= \langle -1 \rangle), \langle 6 \rangle (= \langle -6 \rangle), \langle 6 \rangle \left(= \left\langle \frac{1}{6} \right\rangle\right)$이다.

※ 문제 27~35에서 주어진 원소로 생성되는 군의 순환 부분군의 위수를 찾아라.

문 27. 3에 의해서 생성되는 Z_4의 부분군 (표 5.10 참조)

풀 이

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

3, 3+3=2, 3+3+3=1, 3+3+3+3=0 이므로 $|\langle 3 \rangle| = 4$이다.
따라서 3에 의해서 생성되는 Z_4의 부분군의 위수는 4이다.

문 28. c에 의해서 생성되는 V의 부분군 (표 5.11 참조)

풀 이

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

c, c*c=e, c*c*c=c 이므로 $|\langle c \rangle| = 2$이다.
따라서 c에 의해서 생성되는 V의 부분군의 위수는 2이다.

문 29. $\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$에 의해서 생성되는 U_6의 부분군

여기서, $U_n = \left\{x^n = 1 | \, x = \cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}\right\}$이다.

풀 이

$\left\langle \cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3} \right\rangle = \left\{\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}, \cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3}, 1\right\}$이므로 $\left\langle \cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3} \right\rangle$의 위수는 3이다. 따라서 $\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$에 의해서 생성되는 U_6의 부분군의 위수는 3이다.

문 30. $\cos\frac{4\pi}{5}+i\sin\frac{4\pi}{5}$에 의해서 생성되는 U_5의 부분군

풀 이

실제로 계산해보면 $\left\langle \cos\frac{4\pi}{5}+i\sin\frac{4\pi}{5} \right\rangle = U_5$이 성립하므로 $\cos\frac{4\pi}{5}+i\sin\frac{4\pi}{5}$에 의해서 생성되는 U_5의 부분군의 위수는 5이다.

문 31. $\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2}$**에 의해서 생성되는** U_8**의 부분군**

풀 이

$\left\langle \cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2} \right\rangle = \left\{ \cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2}, \cos\pi+i\sin\pi, \cos\frac{\pi}{2}+i\sin\frac{\pi}{2}, 1 \right\}$이므로 $\left\langle \cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2} \right\rangle$의 위수는 4이다. 따라서 $\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2}$에 의해서 생성되는 U_8의 부분군의 위수는 4이다

문 32. $\cos\frac{5\pi}{4}+i\sin\frac{5\pi}{4}$**에 의해서 생성되는** U_8**의 부분군**

풀 이

실제로 계산해보면 $\left\langle \cos\frac{5\pi}{4}+i\sin\frac{5\pi}{4} \right\rangle = U_8$이 성립하므로 $\cos\frac{5\pi}{4}+i\sin\frac{5\pi}{4}$에 의해서 생성되는 U_8의 부분군의 위수는 8이다.

문 33. 아래의 행렬에 의해서 생성되는 역행렬을 갖는 4×4**의 행렬의 곱셈에 대한 군** G**의 부분군**

$$\begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix}$$

풀 이

$\left(\begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} \right)^2 = \begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} \begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix} = I_4$이 성립하므로 $\begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix}$에 의해서 생성되는 순환 부분군의 위수는 2이다.

문 34. 아래의 행렬에 의해서 생성되는 역행렬을 갖는 4×4**의 행렬의 곱셈에 대한 군** G**의 부분군**

$$\begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix}$$

풀 이

$\left(\begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} \right)^2 = \begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} \begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} = \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix}$ 이고 $\left(\begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} \right)^4 = \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix} = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix} = I_4$이다.

그러므로 $\begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix}$에 의해서 생성되는 순환 부분군의 위수는 4이다.

문 35. 아래의 행렬에 의해서 생성되는 역행렬을 갖는 4×4의 행렬의 곱셈에 대한 군 G의 부분군

$$\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}$$

풀 이

$\left(\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}\right)^2=\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&0&1&0\\0&1&0&0\end{bmatrix}$ 이고 $\left(\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}\right)^3=\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&0&1&0\\0&1&0&0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}=I_4$이다.

그러므로 $\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}$에 의해서 생성되는 순환 부분군의 위수는 3이다.

문 36.

(a) 비슷한 방법으로, 6개의 원소를 갖는 순환군 Z_6에 대한 표 5.25를 완성하라.

풀 이

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) (a)에서 주어진 군 Z_6의 부분군 $\langle 0\rangle,\langle 1\rangle,\langle 2\rangle,\langle 3\rangle,\langle 4\rangle,\langle 5\rangle$를 계산하라.

풀 이

$\langle 0\rangle=\{0\},\langle 1\rangle=\langle 5\rangle=\{0,1,2,3,4,5\},\langle 2\rangle=\langle 4\rangle=\{0,2,4\},\langle 3\rangle=\{0,3\}$

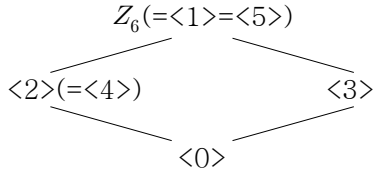
(c) 어느 원소가 (a)에서 주어진 군 Z_6에 대한 생성원인가?

풀 이

1과 5가 군 Z_6의 생성원이다.

(d) Z_6에 대한 이들 부분군의 $Lattice$ 도표를 작성하라. 뒤에 이들이 Z_6의 모든 부분군임을 보인 것이다.

풀 이



※ 문제 37과 38에서 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 37. A *subgroup* of a group G is a subset H of G that contains the identity element e of G and also contains the inverse of each of its elements.

풀 이

군 G의 부분집합 H가 군 G의 부분군이 되기 위한 필요충분조건은 다음을 만족해야 한다.
(1) 결합법칙이 성립해야 한다. 이는 H가 G의 부분집합이므로 자명하다.
(2) 항등원이 존재해야 한다. 이는 가정에 의하여 군 G의 항등원 e를 H가 포함한다.
(3) 역원이 존재해야 한다. 이 또한 가정에 의하여 만족한다.
(4) G의 이항연산에 관하여 닫혀 있어야 한다. 하지만 이는 위의 조건이 보장해 주지 못하고 있다.
따라서 G의 이항연산에 관하여 H가 닫혀 있음을 첨가 해 주어야 H가 G의 부분군임을 보장해 줄 수 있다.

문 38. 군 G가 *순환군* 일 필요충분조건은 $G=\{a^n | n\in Z\}$를 만족하는 $a\in G$가 존재하는 것이다.

풀 이

올바른 정의이다.

문 39. 참, 거짓을 판정하라.

(a) 모든 군에서 결합법칙이 성립한다.

풀 이 T

군에 대한 정의에 의하여 결합법칙이 성립함은 자명하다.

(b) 약분법칙을 만족하지 않는 군은 있을 수 있다.

풀 이 F

군에서 역원이 존재하고 그 연산은 닫혀 있으므로 반드시 소약법칙은 성립한다.

(c) 모든 군은 그 자신의 부분군이다.

풀 이 T

G를 군이라 하자. 그러면 G는 자기 자신의 부분집합이고 G가 군이므로 결합법칙이 만족하며 항등원과 역원이 존재한다. 따라서 G는 그 자신의 부분군이다.

(d) 모든 군은 꼭 두 개의 비진부분군(improper)을 가지고 있다.

풀 이 F

$G=\{e\}$인 자명군을 생각해 보자. 그러면 이 군의 부분군은 자신 하나 뿐임을 알 수 있다.

(e) 모든 순환군에서는 모든 원소가 생성원이다.

풀 이 F

Z_6은 덧셈 연산에 관하여 순환군을 이루지만 생성원으로 $1, 5$만을 갖는다. 다른 원소로 생성된 순환군은 이 군의 부분군이 된다.

(f) 순환군은 유일하게 하나의 생성원을 갖는다.

풀 이 F

Z_6은 덧셈 연산에 관하여 순환군을 이루지만 생성원으로 $1, 5$를 갖는다.
따라서 순환군은 유일하게 하나의 생성원을 갖는 것은 아니다.

(g) 덧셈에 대한 군이 되는 수의 집합은 곱셈에 대해서도 또한 군이 된다.

풀 이 F

$\langle Z, + \rangle$는 군이지만 $\langle Z, \cdot \rangle$는 군이 아니다.

(h) 부분군은 군의 부분집합이라고 정의해도 좋다.

풀 이 F

Z_4는 군이다 하지만 그 군의 부분집합 $\{2, 3\}$은 군이 아니다.
따라서 부분군을 군의 부분집합이라고 정의하면 이런 오류를 범할 가능성이 있다.
그러므로 부분군을 군의 부분집합이라고 정의하면 안 된다.

(i) Z_4는 순환군 이다.

풀 이 T

$\langle Z_4, + \rangle = \langle \langle 1 \rangle, + \rangle$로써 생성원 1이 존재한다. 따라서 Z_4는 순환군 이다.

(j) 모든 군의 부분집합은 유도된 이항연산에 대해서 부분군이다.

풀 이 F

모든 군의 부분집합은 유도된 이항연산에 대해서 결합법칙은 성립한다.
하지만 항등원, 역원이 항상 존재하는 것은 아니다.
따라서 이는 잘못된 명제이다. [(h) 참조]

문 40. 항등원 e를 갖는 어떤 군에서 이차방정식 $x^2 = e$가 세 개 이상의 해를 가질 수도 있음을 예로 들어라.

풀 이

클레인-V_4 군(=$\{e, \sigma, \tau, \rho\}$)을 생각해 보자.
여기서 $\sigma^2 = e, \tau^2 = e, \rho^2 = e, e^2 = e$을 만족한다.
따라서 $x^2 = e$를 만족하는 해는 4개 존재한다.

※ 문제 41과 42에서 $\phi: G \to G'$를 군 $\langle G, * \rangle$에서 군 $\langle G', *' \rangle$으로의 동형사상이라 하자.
Write out a proof to convince a skeptic of the intuitively clear statement.

문 41. H를 군 G의 부분군이라 하자. 그러면 $\phi(H) = \{\phi(h) | h \in H\}$가 G'의 부분군이다. 즉, 준동형사상은 부분군을 부분군으로 운반한다.

풀 이

$\phi(e) = e'$이므로 $\phi(H) \neq \varnothing$임은 자명하다. 단, e, e'는 각각 G, G'의 항등원이다.
또한 ϕ가 잘 정의되어 있으므로 $\phi(H) \subseteq \phi(G) = G'$임은 자명하다.
이제 임의의 $\phi(a), \phi(b) \in \phi(H)$에 대하여

$\phi(a)^{-1} *' \phi(b) = \phi(b) *' \phi(a)^{-1} = \phi(a^{-1}) *' \phi(b) = \phi(b) *' \phi(a^{-1}) = \phi(a^{-1} * b)$를 만족한다.
여기서 H가 부분군이고 a, b는 H의 원소이므로 $a^{-1} * b \in H$임을 알 수 있다.
따라서 $\phi(a)^{-1} *' \phi(b) \in \phi(H)$ 이다.
그러므로 $\phi(H)$는 G'의 부분군이다.

문 42. G가 순환군 이면 G' 또한 순환군 이다.

풀 이

$$\begin{aligned} G' &= \phi(G) \\ &= \{\phi(x) | \exists a \, s.t. \, x \in G = \langle a \rangle\} \\ &= \{\phi(x) | \exists i \in Z \, s.t. \, x = a^i\} \; (\because G\text{: 순환군}) \\ &= \{\phi(a^i) | \exists i \in Z\} \\ &= \{\phi(a)^i | \exists i \in Z\} \; (\because \phi\text{: 준동형사상}) \\ &= \langle \phi(a) \rangle \end{aligned}$$

따라서 G'는 순환군 이다.

문 43. 만약 H와 K가 가환군 G의 부분군이면 $\{hk | h \in H \text{ and } k \in K\}$는 G의 부분군이다.

풀 이

$S \equiv \{hk | h \in H \text{ and } k \in K\}$라 하자.
$e \in H$이고 $e \in K$이므로 $e \in S \neq \varnothing$ 임은 자명하다.
또한 H와 K가 G의 부분군이므로 $S = HK \subseteq G$ 이다.
이제 임의의 $x, y \in S$에 대하여
$h_1, h_2 \in H, k_1, k_2 \in K$가 존재해서 $x = h_1 k_1, y = h_2 k_2$가 성립한다.
또한 $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1}(h_1 k_1)(k_2^{-1} h_2^{-1}) = (h_1 h_2^{-1})(k_1 k_2^{-1}) \in HK$
($\because G$는 가환군이고 H, K는 G의 부분군이다.)
이 성립한다. 단, y^{-1}는 S에서 y의 역원이다.
따라서 S는 가환군 G의 부분군이다.

문 44. 다음 논법에서 잘못된 곳을 찾아라.
: "정리 5.14의 조건 2는 불필요하다. 왜냐하면 조건 1과 3으로부터 이것을 유도할 수 있기 때문이다. $a \in H$이면 조건 3에 의해서 $a^{-1} \in H$이고 조건 1에 의해서 $aa^{-1} = e$는 H의 원소이다. 따라서 조건 2가 증명된다."

풀 이

[정리5.14] 군 G의 부분집합 H가 G의 부분군일 필요충분조건은 다음 세 조건을 만족하는 것이다.
(1) H는 G의 이항연산에 관하여 닫혀 있어야 한다.
(2) G의 항등원 e가 H의 원소이어야 한다.
(3) 모든 $a \in H$에 대하여 또한 $a^{-1} \in H$이 참이어야 한다.

항등원이 존재한다는 가정하여 역원의 정의는 내릴수 있다. 즉, (2)를 만족하지 않는 상태에서 (3)의 참이라고 볼 수 없는데 위의 논법은 (3)이 참이라는 잘못된 가정에서 출발하는 모순을 보여주고 있다.

문 45. 군 G의 공집합이 아닌 부분집합 H가 G의 부분군일 필요충분조건은 모든 $a, b \in H$에 대하여 $ab^{-1} \in H$이다.

풀 이

(→) H가 G의 부분군이므로 임의의 $a, b \in H$에 대하여 $ab^{-1} \in H$는 자명하게 성립한다.
(←) 다음 조건에 의하여 H는 군 G의 부분군이 된다.
(1) 결합법칙이 성립한다. ($\because$ H가 군 G의 부분집합이므로 자명하게 성립한다.)
(2) 항등원이 존재한다. ($\because$ $H \neq \varnothing$이므로 임의의 $a \in H$에 대하여 $e = a \cdot a^{-1} \in H$가 성립한다.)
(3) 역원이 존재한다. ($\because$ 임의의 $e, a \in H$에 대하여 $a^{-1} = e \cdot a^{-1} \in H$이다.)
(4) 닫혀있다. ($\because$ 임의의 $a, b \in H$에 대하여 $b^{-1} \in H$이므로 $a \cdot b = a \cdot (b^{-1})^{-1} \in H$이다.)

문 46. 단 하나의 생성원을 갖는 순환군이 기껏해야 두 원소를 가질 수도 있음을 보여라.

풀 이

순환군은 Z 또는 Z_n과 동형이다. 그러므로 Z와 Z_n에 관하여 논하여도 충분하다.
(1) Z와 동형인 경우
Z의 생성원은 1과 -1 이다. 따라서 순환군의 생성원 또한 두 개 존재한다.
이는 위의 조건에 모순됨을 알 수 있다.
(2) Z_n과 동형인 경우
$Z_n = \langle 1 \rangle = \{1, 2, 3, \cdots, n\}$라 하자.
$a \in Z_n$에 대하여 a가 생성원이라 하자.
그러면 $|a| = \frac{n}{(a, n)} = 1$ 이다. 즉, $(a, n) = 1$이다.
$n \leq 2$이면 자명하게 하나의 생성원만 존재하고 원소 또한 많아야 두 개이다.
$n \geq 3$인 경우 $(1, n) = (n-1, n) = 1$이므로 적어도 두 개의 생성원 1과 $n-1$이 존재한다.
따라서 이 경우에는 위의 조건에 모순된다.
그러므로 (1)과 (2)에 의하여 단 하나의 생성원을 갖는 순환군은 $\{e\}$ 또는 Z_2와 동형이다.
즉, 기껏해야 두 원소만을 가질 수 있음을 알 수 있다.

문 47. G가 항등원 e를 갖는 가환군이면, 방정식 $x^2 = e$를 만족하는 모든 x의 집합은 G의 부분군 H를 형성함을 증명하라.

풀 이

$H \equiv \{x \in G \mid x^2 = e\}$라 하자. 이제 H가 가환군 G의 부분군임을 보인다.
$e^2 = e$이므로 $H \neq \varnothing$이고 $H \subseteq G$임은 자명하다.
이제 임의의 $a, b \in H$에 대하여 G가 가환군이므로 다음이 성립한다.
$(a \cdot b^{-1})^2 = (a \cdot b^{-1}) \cdot (a \cdot b^{-1}) = a^2 \cdot (b^{-1})^2 = a^2 \cdot (b^2)^{-1} = e \cdot e^{-1} = e$
따라서 $a \cdot b^{-1} \in H$이다. 그러므로 H는 가환군 G의 부분군이다.

문 48. 문제 47를 일반화하여 G가 항등원 e를 갖는 가환군이면, 고정된 양의 정수 $n \geq 1$에 대하여 방정식 $x^n = e$의 해의 집합 H는 G의 부분군임을 증명하라.

풀 이

$H \equiv \{x \in G | \, x^n = e \ (n \in Z^+)\}$라 하자.

$e^n = e$이므로 $H \neq \varnothing$이고 $H \subseteq G$ 임은 자명하다.

이제 임의의 $a, b \in H$에 대하여 $a^n = e, b^n = e$이고

$$\begin{aligned}(a \cdot b^{-1})^n &= (a^n) \cdot (b^{-1})^n \ (\because G\text{: 가환군}) \\ &= (a^n) \cdot (b^n)^{-1} \ (\because \text{역원의 성질}) \\ &= e \cdot e^{-1} \ (\because \ a, b \in H \ ) \\ &= e\end{aligned}$$

따라서 $a \cdot b^{-1} \in H$이다. 그러므로 H는 가환군 G의 부분군이다.

문 49. G가 항등원 e를 갖는 유한군이고 $a \in G$이면, $a^n = e$가 되는 $n \in Z^+$가 존재함을 보여라.

풀 이

임의의 $a \in G$에 대하여 $i, j \in Z \, (i > j)$가 존재하여 $a^i = a^j$이다.

($\because$ i,j가 존재하지 않는다면 G가 유한군임에 모순된다.)

그러면 소약법칙에 의하여 다음이 성립한다.

$a^i = a^j \Leftrightarrow a^{i-j} = e$

이제 $n = i - j$이라 하자. 그러면 $a^n = e$임을 알 수 있다.

그러므로 $a^n = e$가 되는 $n \in Z^+$가 존재함을 알 수 있다.

문 50. 군 G의 공집합이 아닌 유한집합 H가 G의 이항연산에 대해 닫혀 있다고 하면 H가 G의 부분군임을 보여라.

풀 이

H가 G의 부분집합이므로 결합법칙이 성립함을 자명하다.

그리고 가정에 의하여 G의 연산에 관하여 닫혀 있다.

이제 항등원과 역원의 존재성만 보이면 충분하다.

H가 유한집합이므로 $H = \{a_1, a_2, a_3, \cdots, a_n\}$라 하자.

임의의 $a \in H$에 대하여 $aH = \{aa_1, aa_2, aa_3, \cdots, aa_n\}$이다.

조건에 의하여 G의 이항연산에 대하여 닫혀 있으므로 $aH \subseteq H$가 성립한다.

이제 $aa_i = aa_j$라면 $a \in H \subseteq G$이므로 소약 법칙에 의하여 $a_i = a_j$임을 알 수 있다. 즉, $i = j$이다.

따라서 $i \neq j$이면 $aa_i \neq aa_j$이므로 $|aH| = |H|$이다.

그러면 $aa_s = a$를 만족하는 s가 존재함을 알 수 있다.

그러므로 a의 항등원은 $e = a_s$이 존재한다. 단, e는 G의 항등원

마찬가지로 $aa_t = a_s = e$를 만족하는 t가 존재한다.

그러므로 a의 역원은 $a^{-1} = a_t$이 존재한다.

문 51. G**는 군이고** a**는** G**의 하나의 고정된 원소이다.**
$H_a = \{x \in G \mid xa = ax\}$**가** G**의 부분군임을 보여라.**

풀 이

우선 $ea = a = ae$이므로 $e \in H_a \neq \varnothing$ 이다. 또한 $H_a \subseteq G$임은 자명하다.

이제 임의의 $x_1, x_2 \in H_a$에 대하여

$$\begin{aligned}(x_1x_2)a &= x_1(x_2a) \ (\because \text{ 결합법칙})\\ &= x_1(ax_2) \ (\because \ x_2 \in H_a \ )\\ &= (x_1a)x_2 \ (\because \text{ 결합법칙})\\ &= (ax_1)x_2 \ (\because \ x_1 \in H_a \ )\\ &= a(x_1x_2) \ (\because \text{ 결합법칙})\end{aligned}$$

이 성립한다. 따라서 $x_1x_2 \in H_a$ 이다.

또한 $x_1a = ax_1 \Rightarrow x_1^{-1}(x_1a)x_1^{-1} = x_1^{-1}(ax_1)x_1^{-1} \Rightarrow ax_1^{-1} = x_1^{-1}a$ 이 성립한다.

따라서 $x_1^{-1} \in H_a$ 이다.

그러므로 H_a는 G의 부분군이다.

문 52. 문제 51을 일반화하여 S**를 군** G**의 어떤 부분집합이라 하자.**
(a) $H_S = \{x \in G \mid \forall s \in S \ s.t. \ xs = sx\}$**가** G**의 부분군임을 보여라.**

풀 이

우선 임의의 $s \in S$에 대하여 $es = s = as$이므로 $e \in H_S \neq \varnothing$ 이다. 또한 $H_S \subseteq G$임은 자명하다.

이제 임의의 $x_1, x_2 \in H_S$와 임의의 $s \in S$에 대하여

$$\begin{aligned}(x_1x_2)s &= x_1(x_2s) \ (\because \text{ 결합법칙})\\ &= x_1(sx_2) \ (\because \ x_2 \in H_S \ )\\ &= (x_1s)x_2 \ (\because \text{ 결합법칙})\\ &= (sx_1)x_2 \ (\because \ x_1 \in H_S \ )\\ &= s(x_1x_2) \ (\because \text{ 결합법칙})\end{aligned}$$

이 성립한다. 따라서 $x_1x_2 \in H_S$ 이다.

또한 $x_1s = sx_1 \Rightarrow x_1^{-1}(x_1s)x_1^{-1} = x_1^{-1}(sx_1)x_1^{-1} \Rightarrow sx_1^{-1} = x_1^{-1}s$ 이 성립한다.

따라서 $x_1^{-1} \in H_S$ 이다.

그러므로 H_S는 G의 부분군이다.

(b) (a)에서의 부분군 H_G**는** G**의 중심 이라 한다.** H_G**가 가환군임을 보여라.**

풀 이

$H_G \equiv \{x \in G \mid \forall g \in G \ s.t. \ xg = gx\}$라 하자.

(a)에 의하여 군임은 자명하게 보일 수 있다. 이제 가환임을 보이면 충분하다.

임의의 $a \in H_G$와 임의의 $b \in H_G \subseteq G$ 에 대하여 가정에 의하여 다음이 성립한다.

$ab = ba$

따라서 H_G는 가환이다.

문 53. H**를 군** G**의 부분군이라 하자.** $a,b\in G$**에 대하여** $a\sim b$**일 필요충분조건은** $ab^{-1}\in H$**이라 하자. 그러면** $\sim$**은** G**위에서 동치관계임을 보여라.**

풀 이

① $a\sim a \Leftrightarrow e=a\cdot a^{-1}\in H$ ($\because$ 항등원의 존재)

② $a\sim b \Leftrightarrow a\cdot b^{-1}\in H$ 이면 $b\cdot a^{-1}=(a\cdot b^{-1})^{-1}\in H$ 이므로 $b\sim a$이다. ($\because$역원이 존재)

③ $a\sim b \Leftrightarrow a\cdot b^{-1}\in H$ 이고 $b\sim c \Leftrightarrow b\cdot c^{-1}\in H$ 이면 $a\cdot c^{-1}=(a\cdot b^{-1})(b\cdot c^{-1})\in H$이므로 $a\sim c$이다.
($\because$닫혀 있음)
따라서 $\sim$은 G위에서 동치관계 이다.

문 54. 집합 H**와** K**에 대해서 교집합** $H\cap K$**를** $H\cap K=\{x|x\in H \text{ and } x\in K\}$**로 정의한다. 만약** $H\leq G$ **이고** $K\leq G$**이면** $H\cap K\leq G$**임을 보여라.**

풀 이

$e\in H$이고 $e\in K$이므로 $e\in H\cap K\neq\varnothing$ 이고 $H\cap K\subseteq G$ 임은 자명하다.
이제 임의의 $a,b\in H\cap K$에 대하여
$a,b\in H$이고 $a,b\in K$ 이므로 H,K가 G의 부분군이라는 가정에 의해 $a\cdot b^{-1}\in H$이고 $a\cdot b^{-1}\in K$ 을 만족한다. 따라서 $a\cdot b^{-1}\in H\cap K$이다.
그러므로 $H\cap K$ 또한 G의 부분군이다.

문 55. 모든 순환군은 가환임을 보여라.

풀 이

임의의 순환군 G에 대하여 적당한 원소 a가 존재하여 $G=\langle a\rangle$를 만족한다.
이제 임의의 $x,y\in G=\langle a\rangle$에 대하여 적당한 $n,m\in Z$이 존재하여 $x=a^n, y=a^m$를 만족한다.
그러면 $x\cdot y=(a^n)\cdot(a^m)=a^{n+m}=a^{m+n}=(a^m)\cdot(a^n)=y\cdot x$ 이 성립한다.
따라서 모든 순환군은 가환이다.

문 56. G**를 군이라 하고** $G_n=\{g^n|g\in G\}$ **라 하자.** G_n**이** G**의 부분군이 되자면** G**에 무슨 조건이 필요한가?**

풀 이

항등원이 존재해야 한다. 즉, $e=g^m$이 되는 m이 존재해야 한다.
또한 n의 범위를 명백히 해 줘야 한다. 즉, $n\in Z$

문 57. 비자명 진부분군을 갖지 않는 군은 순환군임을 보여라.

풀 이

$G=\{e\}$이면 자명하다. 그러면 $|G|>1$인 경우에 대하여 G를 비자명 진부분근을 갖지 않는 군이라 하자. 그러면 $a\neq e$인 임의의 $a\in G$에 대하여 $\langle a\rangle$가 G의 부분군임에는 자명하다. 하지만 가정에서 G가 비자명 진부분군을 갖지 않기 때문에 $G=\langle a\rangle$일 수 밖에는 없다. 따라서 G는 생성원 a가 존재한다. 그러므로 G는 순환군이다.

※ 문제 1~4에서 n을 m으로 나눌 때 호제법에 따라 몫과 나머지를 구하라.

문 1. $n=42, m=9$

풀 이

$42=4\cdot 9+6$ 이므로 따라서 몫은 4이고 나머지는 6이다.

문 2. $n=-42, m=9$

풀 이

$-42=(-5)\cdot 9+3$ 이므로 따라서 몫은 -5이고 나머지는 3이다.

문 3. $n=-50, m=8$

풀 이

$-50=(-7)\cdot 8+6$ 이므로 따라서 몫은 -7이고 나머지는 6이다.

문 4. $n=50, m=8$

풀 이

$50=6\cdot 8+2$ 이므로 따라서 몫은 6이고 나머지는 2이다.

※ 문제 5~7에서 두 정수의 최대 공약수를 구하여라.

문 5. 32와 24

풀 이

유클리드 호제법에 의하여 다음이 성립한다.

$32=1\cdot 24+8$
$24=3\cdot 8+0$

따라서 $(32,24)=8$이다.

문 6. 48과 88

풀 이

유클리드 호제법에 의하여 다음이 성립한다.

$88=1\cdot 48+40$
$48=1\cdot 40+8$
$40=5\cdot 8+0$

따라서 $(88,48)=8$이다.

문 7. 360과 420

풀 이

유클리드 호제법에 의하여 다음이 성립한다.

$420=1\cdot 360+60$
$360=6\cdot 60+0$

따라서 $(360,420)=60$이다.

※ 문제 8~11에서 주어진 위수를 갖는 순환군의 생성원의 개수를 구하여라.

문 8. 5

풀 이

5를 위수로 갖는 순환군의 생성원의 개수를 오일러 ϕ함수를 이용하면 $\phi(5)=5-1=4$ 이다.

문 9. 8

풀 이

8를 위수로 갖는 순환군의 생성원의 개수를 오일러 ϕ함수를 이용하면 $\phi(8)=8(1-\frac{1}{2})=4$ 이다.

문 10. 12

풀 이

12를 위수로 갖는 순환군의 생성원의 개수를

오일러 ϕ함수를 이용하면 $\phi(12)=\phi(4)\phi(3)=4(1-\frac{1}{2})(3-1)=4$ 이다.

문 11. 60

풀 이

60를 위수로 갖는 순환군의 생성원의 개수를

오일러 ϕ함수를 이용하면 $\phi(60)=\phi(2^2)\phi(3)\phi(5)=2\cdot2\cdot4=16$ 이다.

※ 자기 자신으로의 군 동형사상을 군 자기동형사상이라고 한다.
다음 문제 12~16에서 주어진 군의 자기동형사상의 개수를 찾아라.

문 12. Z_2

풀 이

$\phi: Z_2 \to Z_2$ 를 자기 동형사상이라 하자.

Z_2의 생성원 1에 대하여 $\phi(1)=1$ 또는 $\phi(1)=0$이다.

① $\phi(1)=0$ 인 경우

$\phi(n)=n\cdot\phi(1)=0$이므로 $im\phi \neq Z_2$이다. 이는 가정에 모순된다.

② $\phi(1)=1$ 인 경우

$\phi(n)=n\cdot\phi(1)=n$이고 이때 ϕ는 동형사상임에 자명하다.

따라서 Z_2의 자기동형사상의 개수는 1개 이다.

문 13. Z_6

풀 이

$\phi: Z_6 \to Z_6$ 를 자기 동형사상이라 하자.

Z_2의 생성원 1, 5에 대하여 $\phi(1)=0$ 또는 $\phi(1)=1$ 또는 $\phi(1)=5$ 이다.

① $\phi(1)=0$ 인 경우

$\phi(n)=n\cdot\phi(1)=0$이므로 $im\phi \neq Z_6$이다. 이는 가정에 모순된다.

② $\phi(1)=1$ 인 경우

$\phi(n)=n\cdot\phi(1)=n$이고 이때 ϕ는 동형사상임에 자명하다.
③ $\phi(1)=5$
$\phi(n)=n\cdot\phi(1)=5n$이고 이때 ϕ는 동형사상임에 자명하다.
따라서 Z_6의 자기동형사상의 개수는 2개 이다. 즉, 생성원의 개수와 같음을 알 수 있다.

문 14. Z_8

풀 이

위와 비슷한 방법으로 하면 Z_8의 자기동형사상의 개수는 4개이다.
즉, $\phi(n)=n, \phi(n)=3n, \phi(n)=5n, \phi(n)=7n$ 이 있다.

문 15. Z

풀 이

Z의 자기동형사상의 개수는 2개이다.
즉, $\phi(n)=n$ 또는 $\phi(n)=-n$ 이 있다.

문 16. Z_{12}

풀 이

Z_{12}의 자기동형사상의 개수는 4개이다.
즉, $\phi(n)=n, \phi(n)=5n, \phi(n)=7n, \phi(n)=11n$ 이 있다.

※ 문제 17~21에서 주어진 순환군의 원소의 개수를 구하라.

문 17. 25에 의해서 생성되는 Z_{30}의 순환 부분군

풀 이

$|\langle 25\rangle|=\dfrac{|Z_{30}|}{(25,30)}=\dfrac{30}{5}=6$ 이므로 원소의 개수는 6개이다.

문 18. 30에 의해서 생성되는 Z_{42}의 순환 부분군

풀 이

$|\langle 30\rangle|=\dfrac{|Z_{42}|}{(30,42)}=\dfrac{42}{6}=7$ 이므로 원소의 개수는 7개이다.

문 19. 0이 아닌 복소수의 곱셈에 대한 군 C^*의 순환 부부군 $\langle i\rangle$

풀 이

$\langle i\rangle=\{1,-1,i,-i\}$이므로 원소의 개수는 4개이다.

문 20. $\dfrac{1+i}{\sqrt{2}}$에 의해서 생성되는 문제 19의 군 C^*의 순환 부분군

풀 이

$\left\langle\dfrac{1+i}{\sqrt{2}}\right\rangle=\left\{\dfrac{1+i}{\sqrt{2}},\dfrac{1-i}{\sqrt{2}},\dfrac{-1+i}{\sqrt{2}},\dfrac{-1-i}{\sqrt{2}},1,-1,i,-i\right\}$이므로 원소의 개수는 8개이다.

문 21. $1+i$**에 의해서 생성되는 문제 19의 군** C^***의 순환 부분군**

풀 이

$(1+i)^n = 1$를 만족하는 $n \in Z^+$이 존재하지 않는다. 따라서 무한위수를 갖는 순환군이다. 그러므로 원소의 개수는 무한히 많다.

※ 문제 22~24에서 주어진 군의 모든 부분군을 구하고 그 부분군에 대한 $lattice$ **도표를 그려라.**

문 22. Z_{12}

풀 이

주어진 군의 모든 부분군은 다음과 같다.

① $Z_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$

② $< 2 > = < 10 > = \{0, 2, 4, 6, 8, 10\}$

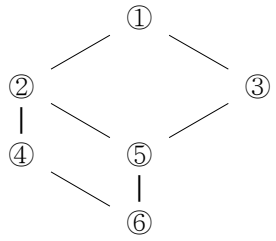
③ $< 3 > = < 9 > = \{0, 3, 6, 9\}$

④ $< 4 > = < 8 > = \{0, 4, 8\}$

⑤ $< 6 > = \{0, 6\}$

⑥ $\{0\}$

위의 부분군에 대한 $lattice$ 도표는 다음과 같다.



문 23. Z_{36}

풀 이

- 생략함 -

문 24. Z_8

풀 이

- 생략함 -

※ 문제 25~29에서 주어진 군의 모든 부분군의 위수를 구하라.

문 25. Z_6

풀 이

$|\{0\}| = 1$, $|\langle 1 \rangle| = |\langle 5 \rangle| = \dfrac{|Z_6|}{(1,6)} = \dfrac{6}{(1,6)} = \dfrac{6}{1} = 6$,

$|\langle 2 \rangle| = |\langle 4 \rangle| = \dfrac{|Z_6|}{(2,6)} = \dfrac{6}{(2,6)} = \dfrac{6}{2} = 3$, $|\langle 3 \rangle| = \dfrac{|Z_6|}{(3,6)} = \dfrac{6}{(3,6)} = \dfrac{6}{3} = 2$

간략히 설명하면, $|Z_6| = 6$이고 $\tau(6) = \tau(2 \cdot 3) = (1+1)(1+1) = 4$이므로 부분군은 4개이다. 이 때 위수는 1, 2, 3, 6 이다.

문 26. Z_8

풀 이

실제로 부분군을 구하는 것은 Z_8이 순환군이므로 각각의 원소가 생성하는 군을 생각하면 충분하다. 그러므로 생략한다. 간략히 설명하면, $|Z_8|=8$이고 $\tau(8)=\tau(2^3)=(3+1)=4$이므로 부분군은 4개이다. 또한 이 때 위수는 1, 2, 4, 8이다.

문 27. Z_{12}

풀 이

- 생략함 -

문 28. Z_{20}

풀 이

- 생략함 -

문 29. Z_{17}

풀 이

- 생략함 -

※ 문제 30과 31에서 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 30. 군 G의 원소가 *위수* $n\in Z^+$를 갖을 필요충분조건은 $a^n=e$를 만족하는 것이다.

풀 이

$a^n=e$를 만족하는 최소의 양의 정수라고 바꿔야 옳은 정의이다.

문 31. 두 양의 정수의 *최대공약수*는 그들 둘을 나눌 수 있는 가장 큰 양의 정수이다.

풀 이

옳은 정의이다.

문 32. 참, 거짓을 판정하라.

(a) 모든 순환군은 가환이다.

풀 이 T

임의의 순환군 G에 대하여 $\exists a\in G\ s.t.\ G=\langle a\rangle$

임의의 $x,y\in\langle a\rangle$에 대하여 $n,m\in Z$가 존재하여 $x=a^n, y=a^m$을 만족하고

이 때 $x\cdot y=(a^n)(a^m)=a^{n+m}=a^{m+n}=(a^m)(a^n)=y\cdot x$ 가 성립한다.

따라서 모든 순환군은 가환임을 알 수 있다.

(b) 모든 가환군은 순환적이다.

풀 이 F

(반례) $klein-V_4$군은 가환이지만 순환적이지는 않다.

(c) 덧셈에 대한 군 Q는 순환군이다.

풀 이 F

Q가 순환적이라고 가정하자.

그러면 $\exists a \in G \; s.t. \; G = \langle a \rangle = \{ka | k \in Z\}$ 이다.

이제 $n < m$인 임의의 $\frac{na}{m} \in Q$에 대하여 $k \cdot a = \frac{na}{m} \Leftrightarrow k = \frac{n}{m}$ 을 만족한다.

이는 k가 정수임에 모순된다.

따라서 Q는 순환적이지 않다.

(d) 모든 순환군의 모든 원소는 그 군을 생성한다.

풀 이 F

(반례) Z_4는 순환군임에는 자명하다. 하지만 $\langle 2 \rangle = \{0, 2\} \neq Z_4$이다.

(e) 모든 유한 위수 > 0 를 갖는 가환군은 적어도 하나 존재한다.

풀 이 T

임의의 유한 위수 n을 갖는 순환군 Z_n은 존재함은 자명하다. 또한 순환군은 가환군임은 자명하게 알고 있다. 따라서 위의 명제는 참임을 알 수 있다.

(f) 위수가 4보다 적거나, 같은 모든 군은 순환적이다.

풀 이 F

(반례) $klein - V_4$는 위수가 4이지만 순환적이지는 않다.

(g) Z_{20}의 모든 생성원은 소수이다.

풀 이 F

(반례) Z_{20}의 생성원은 1, 3, 7, 9, 11, 17, 19이지만 여기서 9는 소수가 아니다.

(h) G와 G'를 군이라 하자. 그러면 $G \cap G'$ 또한 군이다.

풀 이 F

e, e'를 각각 G, G'의 항등원이라 하자. $e = e'$이면 자명하다.

그러므로 $e \neq e'$이라 하자. 만약 $G \cap G'$이 군이라면 항등원 e''이 존재한다.

또한 $G \cap G'$는 각각 G, G'의 부분군이므로 $e = e'' = e'$를 만족한다. 이는 모순이다.

따라서 $e \neq e'$인 군 G, G'에 대해서는 $G \cap G'$ 또한 군이라고 할 수 없다.

(i) H와 K를 군 G의 부분군이라 하자. 그러면 $H \cap K$는 군이다.

풀 이 T

$e \in H$이고 $e \in K$이므로 $e \in H \cap K \neq \varnothing$ 이고 $H \cap K \subseteq G$ 임은 자명하다.

이제 임의의 $a, b \in H \cap K$에 대하여

$a, b \in H$이고 $a, b \in K$ 이므로 H, K가 G의 부분군이라는 가정에 의해 $a \cdot b^{-1} \in H$이고 $a \cdot b^{-1} \in K$ 을 만족한다. 따라서 $a \cdot b^{-1} \in H \cap K$이다.

그러므로 $H \cap K$ 또한 G의 부분군이다.

(j) 위수가 2보다 큰 모든 순환군은 적어도 2개의 서로 다른 생성원을 갖는다.

풀 이 T

군 G를 위수 $n(>2)$인 임의의 순환군이라 하자.

$a \in G$에 대하여 $|\langle a \rangle| = \frac{n}{(a,n)}$ 임은 자명하다.

그러면 a가 군 G의 생성원일 필요충분조건은 $(a,n)=1$이다.

여기서 $n>2$이므로 적어도 $(1,n)=(n-1,n)=1$임을 안다.

따라서 적어도 2개의 서로 다른 생성원을 갖는다.

※ 문제 33~37에서 주어진 성질을 갖는 군의 예를 들든지 또는 그런 예가 존재하지 않는다면 이유를 설명하라.

문 33. 순환하지 않는 유한군

풀 이

$klein-V_4$ **또는** S_3

문 34. 순환하지 않는 무한군

풀 이

Q **또는** R

문 35. 단 하나의 생성원을 갖는 순환군

풀 이

$\{e\}$ **또는** Z_2

문 36. 4개의 생성원을 갖는 무한 순환군

풀 이

무한 순환군은 Z와 동형이다. 하지만 Z는 2개의 생성원 1, -1만을 갖는다. 이는 모순이다.

따라서 4개의 생성원을 갖는 무한 순환군은 존재하지 않는다.

문 37. 4개의 생성원을 갖는 유한 순환군

풀 이

Z_5 **또는** Z_8

※ C에 속하는 1의 n제곱근의 곱셈에 대한 순환군 U_n의 생성원을 1의 원시적 n제곱근이라 부른다. 문제 38~41에서 주어진 n의 값에 대하여 1의 원시적 n제곱근을 구하라.

즉, $U_n = \left\{ \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \mid n \in N \right\}$

문 38. $n=4$

풀 이

$\{1,-1,i,-i\}$

문 39. $n=6$

풀 이

$\left\{\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -1, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, \frac{1}{2}-\frac{\sqrt{3}}{2}i, 1\right\}$

문 40. $n=8$

풀 이

- 생략함 -

문 41. $n=12$

풀 이

- 생략함 -

문 42.

풀 이

- 생략함 -

문 43.

풀 이

- 생략함 -

문 44. G를 생성원 a를 갖는 순환군이고 G'를 G와 동형인 군이라 하자. $\phi: G \to G'$가 동형사상이면 임의의 $x \in G$에 대하여 $\phi(x)$는 $\phi(a)$의 값에 의하여 완전히 결정됨을 보여라.
즉, 두 동형사상 $\phi: G \to G', \psi: G \to G'$이 $\phi(a)=\psi(a)$를 만족하면
임의의 $x \in G$에 대하여 $\phi(x)=\psi(x)$를 만족함을 보여라.

풀 이

임의의 $x \in G$에 대하여 적당한 $n \in Z$가 존재해서 $x=a^n$을 만족한다.
그러면 $\phi: G \to G'$가 동형사상이므로 $\phi(x)=\phi(a^n)=\{\phi(a)\}^n$을 만족한다.
따라서 $\phi(x)$는 $\phi(a)$의 값에 의하여 결정된다.
즉, 두 동형사상 $\phi: G \to G', \psi: G \to G'$이 $\phi(a)=\psi(a)$이면
또한 $\phi(x)=\phi(a^n)=\{\phi(a)\}^n=\{\psi(a)\}^n=\psi(a^n)=\psi(x)$가 성립하여 $\phi(x)=\psi(x)$임을 알 수 있다.

문 45. r과 s를 양의 정수라 하자. $\{nr+ms \mid n, m \in Z\}$이 군 Z의 부분군임을 보여라.

풀 이

$H \equiv \{nr+ms \mid n, m \in Z\}$라 하자.
$n=s, m=-r$ 일 때, $0=s \cdot r+(-r) \cdot s \in H$임을 알 수 있다. 그러므로 $H \neq \varnothing$이다.
또한 $H \subseteq Z$임은 자명하다.
이제 임의의 $x, y \in H$에 대하여
$n_1, n_2, m_1, m_2 \in Z$가 존재해서 $x=n_1 \cdot r+m_1 \cdot s$, $y=n_2 \cdot r+m_2 \cdot s$를 만족한다.
그리고 $x-y=(n_1 \cdot r+m_1 \cdot s)-(n_2 \cdot r+m_2 \cdot s)=(n_1-n_2) \cdot r+(m_1-m_2) \cdot s \in H$
($\because$ n_1-n_2 , $m_1-m_2 \in Z$)
이다. 따라서 H는 Z의 부분군이다.

문 46. a와 b를 군 G의 원소라 하자. ab가 유한위수 n을 갖는다면 ba 또한 위수 n을 갖음을 보여라.

풀 이

$|ab|=n, |ba|=k$라고 하자.

$(ba)^n = b(ab)^{n-1}a = a^{-1}ab(ab)^{n-1}a = a^{-1}(ab)^n a = a^{-1}\cdot e\cdot a = e$이므로 따라서 $k|n$ 이다.

한편 $(ab)^k = a(ba)^{k-1}b = b^{-1}ba(ba)^{k-1}b = b^{-1}(ba)^k b = b^{-1}\cdot e\cdot b = e$이므로 따라서 $n|k$ 이다.

그러므로 $k=n$이다. 즉, ab가 유한위수 n을 갖는다면 ba 또한 위수 n을 갖는다.

문 47. r와 s를 양의정수라 하자.

(a) 어떤 순환군이 생성원으로서 r와 s의 최소공배수를 정하라.

풀 이

$[r,s] \equiv \frac{rs}{(r,s)}$ 단, $[r,s]$는 r와 s의 최소공배수이고 (r,s)는 r와 s의 최대공약수이다.

(→ 정확하게 문제가 요구하고 있는 것이 뭔지 이해가 안됨 ㅜ)

(b) r과 s의 최소공배수는 어떤 조건하에서 rs가 되는가?

풀 이

$(r,s)=1$ 즉, r과 s의 최대 공약수가 1일 때 최소공배수는 rs이다.

(c) (b)를 일반화하여 r과 s의 최대공약수와 최소공배수의 곱은 rs임을 보여라.

풀 이

$rs = [r,s]\times(r,s)$이므로 최대공약수와 최소공배수의 곱은 rs임을 알 수 있다.

문 48. 단지 유한개의 부분군을 갖는 군은 유한군이어야 함을 보여라.

풀 이

군 G가 유한군이면 라그랑지 정리에 의하여 단지 유한개의 부분군을 갖는 것은 자명한 사실이다.

이제 군 G가 무한군일 때 유한개의 부분군이 존재하지 않음을 보이면 충분하다.

군 G가 무한군일 때, 임의의 $a\in G$에 대하여 $\langle a\rangle$ 또한 무한이다. 그리고 $a\neq b$인 $a,b\in G$에 대하여 $<a> \neq <b>$임은 자명하다. 그러므로 적어도 군 G의 원소에 의하여 생성된 순환 부분군의 개수만큼은 부분군이 존재한다. 하지만 원소의 개수가 무한이므로 단지 유한개의 부분군이 존재하지는 않는다.

문 49. 정리 6.6의 다음 "역"이 참이 아님을 반례를 들어 보아라. "만약 군 G의 모든 진부분군이 순환적이면 G도 순환적이다."

풀 이

$klein-V_4 = \{1,\sigma,\tau,\rho\}$라 하자.

그러면 진부분군은 $\{1\},\{1,\tau\},\{1,\rho\},\{1,\tau\}$로써 모두 순환적이다.

하지만 V_4는 순환적이지 않다.

문 50. G가 군이고 $a\in G$가 위수 2인 순환부분군을 생성하고 이것이 그런 원소로는 유일한 것이라고 가정하자. 모든 $x\in G$에 대하여 $ax=xa$임을 보여라.

[기교: $(xax^{-1})^2$을 고려하여라.]

풀 이

모든 $x\in G$에 대하여

$(x\cdot a\cdot x^{-1})^2=(x\cdot a\cdot x^{-1})(x\cdot a\cdot x^{-1})=x\cdot a\cdot e\cdot a\cdot x^{-1}=x\cdot a^2\cdot x^{-1}=x\cdot x^{-1}=e$ 를 만족한다.

그러면 $x\cdot a\cdot x^{-1}$의 위수는 라그랑지 정리에 의하여 1 또는 2이다.

하지만 위수가 1이면 $a=e$가 되어 a의 위수가 2인 가정에 모순된다.

한편, 가정에 의하여 위수 2인 원소는 유일하므로 $a=x\cdot a\cdot x^{-1}$이 성립한다.

즉, $a\cdot x=x\cdot a$이다.

따라서 모든 $x\in G$에 대하여 $ax=xa$ 이다.

문 51. p와 q가 소수일 때, 순환군 Z_{pq}의 생성원의 개수를 구하라.

풀 이

오일러 ϕ함수에 의하여 순환군 Z_{pq}의 생성원의 개수는 다음과 같다.

$p=q$ 이면 $\phi(pq)=\phi(p^2)=p^2\left(1-\frac{1}{p}\right)$이고 $p\neq q$이면 $\phi(pq)=\phi(p)\phi(q)=(p-1)(q-1)$이다.

문 52. p가 소수일 때, 순환군 Z_{p^r}의 생성원의 개수를 구하라. 단, r는 1이상인 정수이다.

풀 이

오일러 ϕ함수에 의하여 순환군 Z_{p^r}의 생성원의 개수는 $\phi(p^r)=p^r\left(1-\frac{1}{p}\right)$이다.

문 53. 위수 n인 유한 순환군 G에서 방정식 $x^m=e$는 n을 나누는 각 양의 정수 m에 대하여 G내에서 정확히 m개의 해 x를 가짐을 보여라.

풀 이

① 아시다시피 $\left|a^{\frac{n}{m}}\right|=\frac{n}{\left(n,\frac{n}{m}\right)}=m$ 이다.

그러므로 $0\le t\le m-1$인 임의의 t에 대하여 $\left(a^{\frac{n}{m}\times t}\right)^m=(a^n)^t=e^t=e$ 이 성립한다. 즉, $a^{\frac{n}{m}\times t}$는 군 G에서 방정식 $x^m=e$의 해이다. 게다가 만약 $0\le s\le t\le m-1$인 s,t가 존재해서 $a^{\frac{n}{m}\times t}=a^{\frac{n}{m}\times s}$를 만족한다면 소약법칙에 의하여 $\left(a^{\frac{n}{m}}\right)^{(t-s)}=e$ 이고 $0\le t-s\le m-1$이다. 그러므로 $t-s=0$이다.

즉, $0\le t\le m-1$인 임의의 t에 대하여 $a^{\frac{n}{m}\times t}$는 모두 서로 구별되는 방정식 $x^m=e$의 영점이다. 따라서 G에서 방정식 $x^m=e$의 해 x는 적어도 m개를 갖는다.

② $x^m=e$의 해를 $x=a^s$라고 가정하자. 그러면

$$(a^s)^m=a^{sm}=e\Rightarrow n|sm\Rightarrow\frac{n}{m}|s\Rightarrow s=\frac{n}{m}\times t$$

를 만족하고 이는 군 G에서 $x^m=e$의 해 x가 많아야 m개 있음을 의미한다.

①, ②로부터 $x^m=e$의 해는 정확히 m개 존재한다.

문 54. 문제 53을 참고로 하여 $1<m<n$이고 m이 n을 나누지 않는 경우는 어떠한가?

풀 이

위의 가정 하 에서는 $x^m=e$를 만족하는 m이 존재할 수 없다.
만약 존재한다면 n이 위수라는 정의에 모순되기 때문이다.

문 55. p가 소수이면 Z_p는 비자명 진부분 군을 갖지 않음을 보여라.

풀 이

비자명 진부분군을 갖는다고 가정하고 이를 H라 하자. 즉, $\{e\}\subsetneq H\subsetneq Z_p$ 이다.
그러면 H의 위수는 라그랑지 정리에 의하여 Z_p의 위수 p를 나눈다.
따라서 H의 위수는 p또는 1이다. 이는 모순이다.
그러므로 Z_p는 비자명 진부분군을 갖지 않는다.

[다른 풀이]
Z_p는 순환군이므로 부분군 또한 순환군임에는 자명하다.
그러므로 모든 원소에 대해 생성되는 순환군이 존재하는지 그리고 그 때 생성되는 순환 부분군이 비자명 진부분군인지 보여주면 충분하다.
$1<a<p$인 임의의 $a\in Z_p$에 대하여

$\langle a\rangle\subset Z_p$임에는 자명하다. 또한 $|\langle a\rangle|=\frac{p}{(a,p)}$이고 $(a,p)=1$이므로 $|\langle a\rangle|=p$이다.
따라서 $\langle a\rangle=Z_p$ 이다. 그러므로 Z_p는 비자명 진부분군을 갖지 않는다.

문 56. G가 가환군이면 H와 K를 $|H|=r$이고 $|K|=s$인 유한 순환부분군이라 하자.
(a) r과 s가 서로소이면, G가 위수 rs를 갖는 순환 부분군을 가짐을 보여라.

풀 이

H,K가 각각 순환군이므로 생성원a,b가 존재해서 $H=\langle a\rangle, K=\langle b\rangle$를 만족한다.
또한 각각의 위수가 r,s이므로 $a^r=e, b^s=e$를 만족한다. 단, e는 G의 항등원이다.

이제 $\langle ab\rangle$의 위수가 rs임을 보인다.
우선 $|\langle ab\rangle|=k$ 라 하자.
$(ab)^{rs}=(a)^{rs}\cdot(b)^{rs}=(a^r)^s\cdot(b^s)^r=e^s\cdot e^r=e$ ($\because G$: 가환군) 이므로 $k|rs$이다.
역으로, $(ab)^k=e\Rightarrow a^k=(b^{-1})^k$ 을 만족한다.
가정에 의하여 r과 s가 서로소이므로 $<a>\cap<b>=\{e\}$이고
그러면 $a^k=e, b^k=e\,(\Leftrightarrow(b^{-1})^k=e)$이다. 그러므로 $r|k$이고 $s|k$이다. 즉, $rs|k$이다.
따라서 군 G는 위수 rs인 순환부분군 $<ab>$를 갖는다.

[다른 풀이]
이제 $\langle ab\rangle$의 위수가 rs임을 보인다.
우선 $|\langle ab\rangle|=k$ 라 하자.
$(ab)^{rs}=(a)^{rs}\cdot(b)^{rs}=(a^r)^s\cdot(b^s)^r=e^s\cdot e^r=e$ ($\because G$: 가환군) 이므로 $k|rs$이다.
역으로, $(ab)^k=e\Rightarrow a^k=(b^{-1})^k$ 을 만족한다.
즉, $|a^k|=|(b^{-1})^k|=|b^k|$이다.
($\because$ $|a|=n, |a^{-1}|=m$이라 하자.

그러면 $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$이므로 $m|n$이다.

역으로 $a^m = \{(a^{-1})^{-1}\}^m = \{(a^{-1})^m\}^{-1} = e^{-1} = e$이므로 $n|m$이다.

따라서 $|a^{-1}| = |a|$ 이다.)

$$|a^k| = \frac{r}{(k,r)} = \frac{s}{(k,s)} = |b^k|$$

$\Rightarrow r\cdot(k,s) = s\cdot(k,r)$

$\Rightarrow r|s\cdot(k,r)$ 이고 $s|r\cdot(k,s)$

$\Rightarrow (r,s) = 1$이므로 $r|(k,r)$ 이고 $s|(k,s)$

$\Rightarrow (k,r)|k$ 이고 $(k,s)|k$이므로 $r|k$이고 $s|k$

$\Rightarrow [r,s]|k$

$\Rightarrow (r,s) = 1$이므로 $[r,s] = rs|k$

따라서 군 G는 위수 rs인 순환부분군 $< ab >$를 갖는다.

⑹ ⓐ를 일반화해서 G가 r과 s의 최소공배수인 위수를 가는 순환 부분군을 포함함을 증명한다.

풀 이

H, K가 각각 순환군이므로 생성원a, b가 존재해서 $H = \langle a \rangle, K = \langle b \rangle$를 만족한다.

또한 각각의 위수가 r, s이므로 $a^r = e, b^s = e$를 만족한다. 단, e는 G의 항등원이다.

$(r,s) = d$라 하고 이 때 $r = pd,\ s = dq$라고 하자. 즉, $[r,s] = \frac{rs}{d} = rq = sp$이다.

그러면 $(r,q) = 1$ 또는 $(s,p) = 1$이다.

(만약 $(r,q) \neq 1$ 이고 $(s,p) \neq 1$ 이면 $(p,q) \neq 1$이므로 d가 최대공약수임에 모순된다.)

단, $[r,s]$는 r와 s의 최소공배수이고 (r,s)는 r와 s의 최대공약수이다.

① $(r,q) = 1$인 경우

$|a| = r$이고 $|b^d| = \frac{s}{(s,d)} = \frac{s}{d} = q$ 이므로 ⓐ에 의하여 위수 $rq(=[r,s])$인 순환부분군 $\langle ab^d \rangle$가 존재함을 알 수 있다.

② $(s,p) = 1$인 경우

$|a^d| = \frac{r}{(r,d)} = \frac{r}{d} = p$ 이고 $|b| = s$ 이므로 ⓐ에 의하여 위수 $sp(=[r,s])$인 순환부분군 $\langle a^d b \rangle$가 존재함을 알 수 있다.

실제로 $G = Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$H = \langle 2 \rangle = \{0,2,4,6,8,10\}$ 이고 $K = \langle 3 \rangle = \{0,3,6,9\}$라 하자.

그러면 $(6,4) = 2$이고 $(4, \frac{6}{2}) = 1$이므로 $Z_{12} = \langle 1 \rangle = \langle 7 \rangle = \langle 2\cdot 2 + 3 \rangle$이다.

$\langle 2 + 2\cdot 3 \rangle$은 경우는 성립하지 않는다. 이유인 즉, $(6, \frac{4}{2}) \neq 1$이기 때문이다.

참고로 위의 증명에서의 연산은 곱셈연산이고 예로 든 연산은 덧셈연산이다.

※ 문제 1~5에서 S_6의 다음 치환에 대한 주어진 곱을 계산하라.

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix},\mu=\begin{pmatrix}1&2&3&4&5&6\\5&2&4&3&1&6\end{pmatrix}$$

문 1. $\tau\cdot\sigma$

풀 이

순환치환의 곱으로 나타내면 다음과 같다.

$\sigma=(134562),\tau=(1243)(56),\mu=(15)(34)$

그러면 $\sigma\cdot\tau=(1243)(56)(134562)=(46)$이다.

따라서 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&6&5&4\end{pmatrix}$ 이다.

문 2. $\tau^2\cdot\sigma$

풀 이

$\tau^2\sigma=(1243)(56)(1243)(56)(134562)=(124563)$이다.

따라서 $\tau^2\cdot\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&5&6&3\end{pmatrix}$ 이다.

문 3. $\mu\cdot\sigma^2$

풀 이

$\mu\cdot\sigma^2=(15)(34)(146)(352)=(13)(2465)$이다.

따라서 $\mu\cdot\sigma^2=\begin{pmatrix}1&2&3&4&5&6\\3&4&1&6&2&5\end{pmatrix}$ 이다.

문 4. $\sigma^{-2}\cdot\tau$

풀 이

$\sigma^2=(146)(352)$이므로 $\sigma^{-2}=(253)(641)$이다.

그러면 $\sigma^{-2}\cdot\tau=(253)(641)(1243)(56)=(1542)(36)$ 이다.

따라서 $\sigma^{-2}\cdot\tau=\begin{pmatrix}1&2&3&4&5&6\\5&1&6&2&4&3\end{pmatrix}$ 이다.

문 5. $\sigma^{-1}\tau\sigma$

풀 이

$\sigma^{-1}=(265431)$이므로 $\sigma^{-1}\tau\sigma=(265431)(1243)(56)(134562)=(1263)(45)$ 이다.

따라서 $\sigma^{-1}\cdot\tau\cdot\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&5&4&3\end{pmatrix}$ 이다.

※ 문제 6~9에서 앞의 문제 1에서 정의된 치환 σ, τ 와 μ에 대해서 다음을 계산하라.
즉, $\sigma = (134562), \tau = (1243)(56), \mu = (15)(34)$

문 6. $|\langle\sigma\rangle|$

풀 이

$|\langle\sigma\rangle| = |(134562)| = 6$ 이다.

문 7. $|\langle\tau^2\rangle|$

풀 이

$|\langle\tau^2\rangle| = |(14)(23)| = 2$ 이다.

문 8. σ^{100}

풀 이

$\sigma^6 = (12)(21)$이므로 $\sigma^{100} = (\sigma^6)^{16}(\sigma^4) = \sigma^4 = (164)(253)$이다.

따라서 $\sigma^{100} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$ 이다.

문 9. μ^{100}

풀 이

$\mu^2 = (12)(21)$이므로 $\mu^{100} = (\mu^2)^{50} = (12)(21) = (1)$이다.

따라서 $\mu^{100} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ 이다.

문 10. Partition the following collection of groups into subcollections of isomorphic groups. Here a superscript means all nonzero elements of the set.

Z under addition	S_2
Z_6	R^* under multiplication
Z_2	R^+ under multiplication
S_6	Q^* under multiplication
$17Z$ under addition	C^* under multiplication
Q under addition	the subgroup $\langle\pi\rangle$ of R^* under multiplication
$3Z$ under addition	the subgroup G of S_5 generated by $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$
R under addition	

풀 이

- 생략함 -

※ A를 집합이라 하고 $\sigma \in S_A$라 하자. 주어진 $a \in A$에 대해 집합 $O_{a,\sigma} = \{\sigma^n(a) \mid n \in Z\}$를 σ에 대한 궤도라 한다. 문제 11~13에서 앞의 문제 1에서 정의된 치환에 대한 1의 궤도를 구하라.
즉, $\sigma = (134562), \tau = (1243)(56), \mu = (15)(34)$

문 11. σ

풀 이

$O_{1,\sigma} = \{\sigma^n(1) \mid n \in Z\} = \{3\ 4\ 5\ 6\ 2\ 1\}$

문 12. τ

풀 이

$O_{1,\tau} = \{\tau^n(1) \mid n \in Z\} = \{1\ 2\ 4\ 3\}$

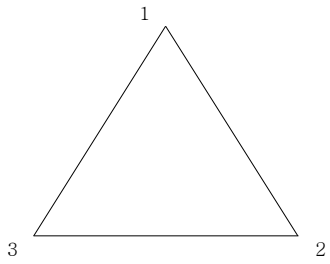
문 13. μ

풀 이

$O_{1,\mu} = \{\sigma^n(1) \mid n \in Z\} = \{1\ 5\}$

문 14. 표 8.8에서 S_3의 여섯 원소의 이름으로 $\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3$를 사용하였다. 혹자는 이들 원소를 기호 $\epsilon, \rho, \rho^2, \phi, \rho\phi, \rho^2\phi$를 사용하기도 하는데 ϵ는 항등원 ρ_0이며, ρ는 우리의 ρ_1, 그리고 ϕ는 우리의 μ이다. 기하학적으로 그들의 6가지 표현이 S_3의 모든 원소를 나타내줌을 보여라.

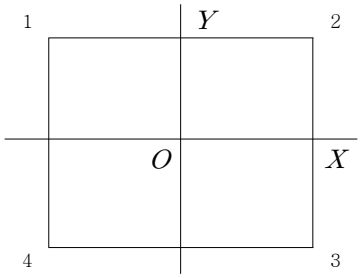
풀 이



ρ는 위의 정삼각형의 내심을 중심으로 120도 회전변환이고 ϕ는 꼭지점 3과 변12의 중점을 이은 선분을 중심으로 하는 대칭변환이라 하면 $\epsilon, \rho, \rho^2, \phi, \rho\phi, \rho^2\phi$이 S_3의 원소 $\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3$를 나타내 줌을 확인할 수 있다.
실제로 $\rho_0 = (1) = \epsilon, \rho_1 = (1\ 2\ 3) = \rho, \rho_2 = (1\ 3\ 2) = \rho^2, \mu_1 = (1\ 2) = \phi, \mu_2 = (2\ 3) = \rho\phi, \mu_3 = (1\ 3) = \rho^2\phi$ 임을 알 수 있다.

문 15. 문제 14를 참고로 해서, 표 8.12에서의 D_4의 8가지 원소에 대하여 다른 표현을 유도해 보자.

풀 이



$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau_1, \tau_2, \tau_3, \tau_4\} = \{1, \sigma, \sigma^2, \sigma^3, \tau(=\tau_1), \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$

문 16. 집합 $\{\rho \in S_4 | \sigma(3) = 3\}$의 원소의 수를 구하라.

풀 이

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \square & \square & 3 & \square \end{pmatrix}$의 개수를 찾아보면 충분하다. 따라서 $6(=3!)$개 이다.

문 17. 집합 $\{\rho \in S_5 | \sigma(2) = 5\}$의 원소의 수를 구하라.

풀 이

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \square & 5 & \square & \square & \square \end{pmatrix}$의 개수를 찾아보면 충분하다. 따라서 $24(=4!)$개 이다.

문 18. 예제 8.7의 군 S_3에 대하여

(a) S_3의 순환 부분군 $\langle \rho_1 \rangle, \langle \rho_2 \rangle$와 $\langle \mu_1 \rangle$을 구하라.

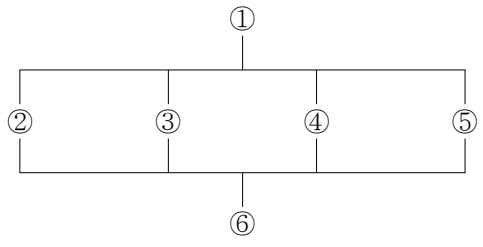
풀 이

$\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\} = \langle \rho_2 \rangle$, $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$

(b) S_3의 모든 부분군(진 그리고 비진)을 구하고 이들에 대한 Lattice 도표를 그려라.

풀 이

① S_3 ② $\langle \rho_1 \rangle$ ③ $\langle \mu_1 \rangle$ ④ $\langle \mu_2 \rangle$ ⑤ $\langle \mu_3 \rangle$ ⑥ $\{\rho_0\}$



문 19. Verify that the subgroup diagram for D_4 shown in Fig. 8.13 is correct by finding all (cyclic) subgroups generated by one element then all subgroups generated by two elements, etc.

풀 이

① 하나의 생성원에 의하여 생성되는 부분군 : $\{\rho_0\}$, $\langle\rho_1\rangle(=\langle\rho_3\rangle)$, $\langle\mu_1\rangle$, $\langle\mu_2\rangle$, $\langle\delta_1\rangle$, $\langle\delta_2\rangle$, $\langle\rho_2\rangle$

② 두 개의 생선원에 의하여 생성되는 부분군 :

$$\langle\rho_1,\mu_1\rangle=\langle\mu_1,\delta_1\rangle=\langle\mu_1,\delta_2\rangle=\langle\mu_2,\delta_1\rangle=\langle\mu_2,\delta_2\rangle=D_4,\ \langle\rho_2,\mu_1\rangle,\ \langle\rho_2,\delta_1\rangle$$

③ Lattice 도표 그리는 것은 생략함.

④ 따라서 $Fig 8.13$에서 주어진 부분군의 다이어그램은 옳은 표현이다.

문 20. $\rho=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}$에 의해 생성되는 S_5의 순환부분군에 대한 곱셈 연산표를 만들어라. 이 때, 여섯 개의 원소를 $\rho,\rho^2,\rho^3,\rho^4,\rho^5$ 그리고 $\rho^0=\rho^6$라 하면 이 군은 S_3와 동형인가?

풀 이

$\rho=(1\,2\,4)(3\,5)$이므로

$\rho^2=(1\,2\,4)(3\,5)(1\,2\,4)(3\,5)=(1\,4\,2)$

$\rho^3=(3\,5)$

$\rho^4=(1\,2\,4)$

$\rho^5=(1\,4\,2)(3\,5)$

$\rho^6=(1)$

따라서 $\langle\rho\rangle=\{(1\,2\,4)(3\,5),(1\,4\,2)(3\,5),(1\,4\,2),(1\,2\,4),(3\,5),(1)\}$이고

이들 각각의 원소의 위수는 6, 6, 3, 3, 2, 1이다.

이는 S_3의 원소의 위수와는 다름을 알 수 있다.

따라서 S_3와 동형이 아니다.

문 21.

(a) 여섯 개의 행렬 $\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}1&0&0\\0&0&1\\1&0&0\end{bmatrix},\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix},\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix},\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix},\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$은 행렬의 곱셈에 대하여 군을 이룸을 증명하라. [힌트: 이들 행렬의 모든 곱을 계산하지 말고 열 벡터 $\begin{bmatrix}1\\2\\3\end{bmatrix}$에 여섯 개의 각 행렬을 왼쪽에 곱하면 어떻게 변형되는가를 생각하라.]

풀 이

위의 여섯 개의 행렬에 열 벡터 $\begin{bmatrix}1\\2\\3\end{bmatrix}$를 각 행렬의 왼쪽에 곱하면 다음과 같은 치환을 얻을 수 있다.

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

이는 S_3와 동형임에 자명하다. 따라서 6개의 행렬은 곱셈의 연산에 관하여 군을 이룬다.

(→ 구체적으로 군을 이룸을 보여야겠지만 간접적으로 증명함.)

(b) 이 절에서 연구한 군 중에서 어느 것이 이 여섯 행렬의 군과 동형인가?

풀 이

S_3와 동형이다.

문 22. 문제 21를 하고 난 뒤에 D_4와 동형되는 치환의 곱에 대해 군을 형성하는 여덟 개의 행렬을 써라.

풀 이

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix},\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix},\begin{bmatrix}0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1\end{bmatrix},\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix},\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix},\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix},\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}$$

문 23~ 27 - 생략함 -

※ 28, 29에서, correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 28. A *permutation* of a set S is a one-to-one map from S to S.

풀 이

전사사상임이 추가되어야 한다. 치환은 S에서 S로의 전단사사상이기 때문이다.

문 29. *The left regular representation* of a group G is the map of G into S_G whose value at $G \in g$ is the permutation of G that carries each $x \in G$ into g_x

풀 이

옳은 정의이다.

※ 문제 30~34에서 주어진 함수가 R위에서 치환인가를 결정하라.

문 30. $f_1(x) = x+1$로 정의된 $f_1 : R \to R$

풀 이

f_1이 전단사 함수이므로 치환이다.

문 31. $f_2(x) = x^2$로 정의된 $f_2 : R \to R$

풀 이

f_2가 전사 및 단사가 아니므로 치환이 아니다.

문 32. $f_3(x) = -x^3$로 정의된 $f_3 : R \to R$

풀 이

f_3가 전단사 함수이므로 치환이다.

문 33. $f_4(x) = e^x$로 정의된 $f_4 : R \to R$

풀 이

f_4는 단사사상이지만 전사사상이 아니므로 치환이 아니다.

문 34. $f_5(x) = x^3 - x^2 - 2x$로 정의된 $f_5 : R \to R$

풀 이

f_5는 전사사상이지만 단사사상이 아니므로 치환이 아니다.

문 35. 참과 거짓을 판정하라.

(a) 모든 치환은 1-1 함수이다.

풀 이 T

임의의 치환은 전단사 함수이다. 그러므로 1-1함수이다.

(b) 함수가 치환이 되기 위한 필요충분조건은 1-1이다.

풀 이 F

(반례) [문제 33]은 1-1 이지만 치환이 아니다.

(c) 유한집합에서 자기 자신 위로 대응하는 함수는 1-1이어야 한다.

풀 이 T

X를 유한집합이라 하자. 그리고 f를 X에서 X위로의 사상이라고 하자.
이제 f가 1-1 함수가 아니라고 가정하자.
그러면 $x_1 \neq x_2$에 대하여 $f(x_1)=f(x_2)$인 $x_1, x_2 \in X$가 존재한다.
따라서 $|f(X)|<|X|<\infty$ 임을 알 수 있다. 이는 $f(X)=X$인 가정에 모순이다.
그러므로 1-1함수이다.

(d) 임의의 군 G는 S_G의 부분군과 동형이다.

풀 이 F

(반례) $G=\{e, a, a^2\}$이라 할 때, $S_G=\{(e),(e\ a),(e\ a^2),(a\ a^2),(e\ a\ a^2),(e\ a^2\ a)\}$이고 이 때 위수가 3인 부분군은 $A_3=\{(e),(e\ a\ a^2),(e\ a^2, a)\}$로 유일하다. 하지만 G와 A_3는 동형이 아니다.
만약 동형이라고 가정하면, G의 각각의 원소들의 위수 1, 3, 3과 A_3의 각각의 원소들의 위수 1, 2, 2는 같아야 한다. 하지만 다르다. 그러므로 모순이다.
따라서 위의 명제는 잘못된 명제이다.

(e) 가환군의 모든 부분군은 가환이다.

풀 이 T

H를 군 G의 부분군이라 하자. 그러면 임의의 $a, b \in H \subseteq G$이므로 $a \cdot b = b \cdot a$ 가 성립한다.
따라서 H또한 가환이다.

(f) 군의 모든 원소는 그 군의 순환 부분군을 생성한다.

풀 이 T

임의의 $a \in G$에서 $\langle a \rangle$가 군 G의 부분군임을 보이면 충분하다.
임의의 $x, y \in \langle a \rangle$에 대하여 $i, j \in Z$가 존재하여 $x=a^i, y=a^j$를 만족한다.
$x \cdot y^{-1} = a^i \cdot a^{-j} = a^{i-j} \in \langle a \rangle$ ($\because\ i-j \in Z$)
따라서 모든 원소는 그 군의 순환 부분군을 생성한다.

(g) 대칭군 S_{10}은 10개의 원소를 갖는다.

풀 이 F

$10!$개의 원소를 갖는다.

(h) 대칭군 S_3는 순환군이다.

풀 이 F

[문제 18]을 참조하면
S_3의 각 원소에 대하여 S_3가 순환군이기 위한 생성원이 존재하지 않음을 확인할 수 있다.
따라서 순환군이 아니다.

(i) 어떤 n에 대해서도 S_n은 순환군이 아니다.

풀 이 F

(반례) $n=2$일 때, $S_2=\{(1),(1,2)\}=\langle(1,2)\rangle$는 순환군이다.

(j) 모든 군은 어떤 치환군과 동형이다.

풀 이 T

Cayley's 정리의 의하여 참인 명제이다.

문 36. 비가환군의 모든 진부분군은 가환군일 수 있음을 예로 들어 증명하라.

풀 이

D_4는 비가환군이다.
하지만 이 군의 모든 진부분군 $\{\rho_0\},\langle\mu_1\rangle,\langle\mu_2\rangle,\langle\rho_2\rangle,\langle\delta_1\rangle,\langle\delta_2\rangle,\langle\rho_2,\mu_1\rangle,\langle\rho_1\rangle,\langle\rho_2,\delta_1\rangle$는 모두 가환군이다.

문 37. Let A be a nonempty set. What type of algebraic structure mentioned previously in the text is given by the set all functions mapping A into itself under funtion compositon?

풀 이

- 생략함 -

문 38. Indicate schematically a Cayley diagraph for D_n using a generating set consisting of a rotation through $\frac{2\pi}{n}$ radians and a reflection (mirror image). See Ex44.

풀 이

- 생략함 -

※ 문제 40~43에서 A를 하나의 집합, B를 부분 집합이라 하고 b를 B의 특정한 원소라 하자. 주어진 집합이 유도된 연산에 대해 S_A부분군이 되는가를 결정하라.

문 40. $H\equiv\{\sigma\in S_A\,|\,\sigma(b)=b\}$

풀 이 Yes

$\forall\sigma,\tau\in H\ s.t.\ \sigma\cdot\tau^{-1}(b)=\sigma(b)=b$
따라서 $\sigma\cdot\tau^{-1}\in H$이다. 그러므로 H는 S_A의 부분군이다.

문 41. $H \equiv \{\sigma \in S_A | \sigma(b) \in B\}$

풀 이 No

$A = \{a, b, c\}$, $B = \{b, c\}$라 하자.
그러면 $\sigma(b) = c, \mu(b) = b$인 $\sigma, \mu \in S_A$에 대하여 $\mu\sigma(b) = \mu(c) \notin B$이다.
따라서 연산에 닫혀있음을 보장해 주지 못한다.

문 42. $H \equiv \{\sigma \in S_A | \sigma[b] \subseteq B\}$

풀 이 No

$A = Z, B = Z^+$라 하자.
$\sigma : A \to A, \sigma[n] = n+1$이라 하자. 그러면 위의 조건을 만족하여 σ가 존재한다.
하지만 $\sigma^{-1}[1] = 0$으로 B의 부분집합이 아니다.
즉, 연산에 대하여 역원의 존재성을 항상 보장해 주지 못한다.

문 43. $H \equiv \{\sigma \in S_A | \sigma[b] = B\}$

풀 이 Yes

문 44. 예제 8.7, 8.10와 비슷하게 $n \geq 3$일 때 정 n각형을 생각하자. 그런 두 개의 n각형에서 하나를 다른 하나에 포갤 수 있는 각 방법은 꼭지점의 어떤 치환에 대응한다. 이 치환의 집합은 치환의 곱에 대해 n차 이면체군(nth dihedral group)이라 불리는 군이 된다. 이 군 D_n의 위수를 구하라. 기하학적으로 이 군은 전체군의 꼭 반의 원소 개수를 갖는 부분군을 갖는다는 것을 설명하라.

풀 이

$D_n = \{1, \sigma, \sigma^2, \cdots, \sigma^n, \sigma\tau, \sigma\tau^2, \cdots, \sigma\tau^n\}$이므로 $|D_n| = 2n$이다.
또한 순환군 $\langle\sigma\rangle$는 위수가 n으로 전체군의 꼭 반의 원소 개수를 갖는 부분군임을 알 수 있다.
기하학적인 설명은 생략하며 문제14와 15를 참조

문 45. 어떤 정육면체에 꼭 들어 가는 정육면체를 생각하자. 예제 8.8과 8.10에서 처럼 한 정육면체를 다른 정육면체 속에 넣을 수 있는 방법은 정육면체의 꼭지점의 어떤 대칭군에 대응된다. 이 군이 group of rigid motion of the cube 이다. (12장에서 공부한 정육면체의 대칭군과 혼돈해서는 안된다.) 이 군에는 원소가 몇 개 있는가? 이 군은 적어도 3개의 위수가 4인 부분군을 가짐과 적어도 4개의 위수가 3인 부분군을 가짐을 기하학적으로 설명하라.

풀 이

① 24개의 원소를 갖는다.
② 3개의 위수가 4인 부분군과 적어도 4개의 위수가 3인 부분군을 가짐을 기하학적으로 보이는 것은 생략한다.

문 46. $n \geq 3$**에 대해서** S_n**은 가환군이 아님을 증명하라.**

풀 이

$n \geq 3$인 S_n에 대하여

$(2\,3)(1\,3), (1\,3)(2\,3) \in S_n$은 $(2\,3)(1\,3) = (1\,2\,3) \neq (1\,3\,2) = (1\,3)(2\,3)$이므로 비가환이다.

따라서 $n \geq 3$에 대해서 S_n은 가환군이 아니다.

문 47. 문제 46를 확장하여 $n \geq 3$**일 때 모든** $\gamma \in S_n$**에 대해서** $\sigma\gamma = \gamma\sigma$**를 만족하는 유일한 원소** σ**는 항등치환인** $\sigma = \iota$**이다.**

풀 이

$\sigma = \iota$이면 임의의 모든 $\gamma \in S_n$에 대해서 $\sigma\gamma = \gamma\sigma$을 만족함은 자명하다.

이제 $\sigma \neq \iota$라고 가정하여 모순됨을 보이자.

$\sigma(l) = m\ (l \neq m)$이라 하자.

$n \geq 3$이므로 $\exists k \in \{1, 2, 3, \cdots, n\}\ s.t.\ k \neq l, m$

$\tau = (k, m) \in S_n$이라 하자. 그러면 $\sigma \cdot \tau(l) = \sigma(l) = m \neq k = \tau(m) = \tau \cdot \sigma(l)$ 을 만족한다.

이는 모순이다. 따라서 위의 조건을 만족하는 유일한 원소 σ는 항등치환인 $\sigma = \iota$이다.

문 48. 문제 11에서 정의한 개념을 참고로, 모든 $a, b \in A$**에 대하여** $O_{a,\sigma}$**와** $O_{b,\sigma}$**가 공통인 원소를 갖는다면** $O_{a,\sigma} = O_{b,\sigma}$**임을 보여라.** (단, $O_{a,\sigma} = \{\sigma^n(a) \mid n \in Z\}$), $\sigma \in S_A$

풀 이

$c \in O_{a,\sigma} \cap O_b, \sigma$이라 하자.

그러면 $\exists n, m \in Z\ s.t.\ c = \sigma^n(a) = \sigma^m(b)$

$\sigma^{n-m}(a) = \sigma^{-m} \cdot \sigma^n(a) = \sigma^{-m}(c) = b$ 이므로 따라서 $\sigma^k(b) = \sigma^{k+n-m}(a) \in O_{a,\sigma}$이 성립한다.

즉, $O_{b,\sigma} \subseteq O_{a,\sigma}$이다.

역으로 $\sigma^{m-n}(b) = \sigma^{-n} \cdot \sigma^m(b) = \sigma^{-n}(c) = a$ 이므로 따라서 $\sigma^l(a) = \sigma^{l+m-n}(b) \in O_{b,\sigma}$이 성립한다.

즉, $O_{a,\sigma} \subseteq O_{b,\sigma}$ 이다.

따라서 모든 $a, b \in A$에 대하여 $O_{a,\sigma}$와 $O_{b,\sigma}$가 공통인 원소를 갖는다면 $O_{a,\sigma} = O_{b,\sigma}$이다.

문 49. 만약 A**가 집합이고, 모든** $a, b \in A$**에 대하여** $\sigma(a) = b$**인** $\sigma \in H$ **가 존재할 때,** S_A**의 부분군** H**는** A **위에서 이동적이라 한다. 만약** A**가 공집합이 아닌 유한집합이면** $|H| = |A|$**이며** A**위에서 이동적인** S_A**의 유한 순환부분군** H**가 존재함을 보여라.**

풀 이

$|A| = n$이라 하자. 그러면 $A \simeq \{1, 2, 3, \cdots, n\} \equiv B$이다.

이제 $(1\,2\,3\,4\,\cdots\,n) \in S_B$에 대하여 $|\langle(1\,2\,3\,4\,\cdots\,n)\rangle| = n$임은 자명하다.

그러므로 $|H| = |B| = |A|$이며 A위에서 이동적인 S_A의 유한 순환부분군 H가 존재함을 알 수 있다.

[다른 풀이]

$A = \{a_1, a_2, \cdots, a_n\}$이라 하자. 또한 $\sigma = (a_1\,a_2\,a_3\,\cdots\,a_n)$라 하자.

그러면 $i > j$이고 $a_i \neq a_j$인 $a_i, a_j \in A$에 대하여 $\sigma^{i-j}(a_i) = a_j$를 만족한다.

따라서 순환부분군 $\langle\sigma\rangle$이 A위에서 이동적임을 의미한다.

즉, $|\langle\sigma\rangle| = n = |A|$

문 50. 문제 11과 49에서의 정의를 참고로, $\sigma \in S_A$에 대하여 $\langle \sigma \rangle$가 A위에서 이동적일 필요충분조건은 어떤 적당한 $a \in A$에 대해서 $O_{a,\sigma} = A$임을 보여라.

풀 이

$\langle \sigma \rangle$가 A 위에서 이동적 이라 하자. 그러면 $O_{a,\sigma} = \{\sigma^n(a) \mid n \in Z\}$는 A의 모든 원소를 포함해야 한다. 즉, $O_{a,\sigma} = A$이다. 역으로 어떤 적당한 $a \in A$에 대해서 $O_{a,\sigma} = \{\sigma^n(a) \mid n \in Z\} = A$라 하자.
임의의 $b, c \in A$에 대하여 $\exists n, m \; s.t. \; b = \sigma^n(a), c = \sigma^m(a)$. 그러면 $\sigma^{n-m}(b) = \sigma^n \cdot \sigma^{-m}(b) = \sigma^n(a) = c$ 을 만족한다. 따라서 $\langle \sigma \rangle$는 A위에서 이동적 이다.

문 51. (78페이지의 주의를 보라.) G를 이항연산 $*$를 갖는 군이라 하자. G'를 같은 집합 G로 두고, G'위에 이항연산 $*'$를 모든 $x, y \in G$에 대하여 $x *' y = y * x$로 정의한다.

(a) (G'가 $*'$에 대해 군이 된다는 직관적 논법) 강의실 앞쪽 벽이 투명한 유리로 되어 있고, $*$에 대한 G의 모든 가능한 곱 $a * b = c$와 $*$하에서 G에 대한 모든 가능한 결합 $a * (b * c) = (a * b) * c$를 매직으로 벽 위에 썼다고 가정하자. 앞쪽 방에서 벽의 다른 쪽을 보았을 때 무엇을 보게 될 것인가?

풀 이

- 생략함 -

(b) G'가 $*'$에 대해 군이 됨을 $*'$의 수학적 정의에서 보여라.

풀 이

- 생략함 -

문 52. Let G be a group. Prove that the permutation $\rho_a : G \to G$, where $\rho_a(x) = xa$ for $a \in G$ and $x \in G$ do form a group isomorphic to G

풀 이

- 생략함 -

문 53. A permutation matrix is one that can be obtained from an identity matrix by recordering its rows. If P is $n \times n$ permutation matrix and A is any $n \times n$ matrix and $C = PA$. then C can be obtained form A by making precisely the same recording of the rows of A as the recording of the rows which produced P form I_n.

(a) Show that every finite group of order n is isomorphic to a group consisting of $n \times n$ permutation matrices under matrix multiplication.

풀 이

- 생략함 -

(b) For each of the four elements e, a, b and c in the Table 5.11 for the group V give a specific 4×4 matrix that corresponds to it under such an isomorphism.

풀 이

- 생략함 -

※ 문제 1~6에서 주어진 치환이 모든 궤도들을 구하라.

문 1. $\begin{pmatrix}1&2&3&4&5&6\\5&1&3&6&2&4\end{pmatrix}$

풀 이

$(1\,5\,2)(4\,6)$

문 2. $\begin{pmatrix}1&2&3&4&5&6&7&8\\5&6&2&4&8&3&1&7\end{pmatrix}$

풀 이

$(1\,5\,8\,7)(2\,6\,3)$

문 3. $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&5&1&4&6&8&7\end{pmatrix}$

풀 이

$(1\,2\,3\,5\,4)(7\,8)$

문 4. $\sigma : Z \to Z$, 단, $\sigma(n) = n+1$이다.

풀 이

$Z = \langle 1 \rangle$

문 5. $\sigma : Z \to Z$, 단 $\sigma(n) = n+2$이다.

풀 이

$\{2n \mid n \in Z\}, \{2n+1 \mid n \in Z\}$

문 6. $\sigma : Z \to Z$, 단 $\sigma(n) = n-3$이다.

풀 이

$\{3n \mid n \in Z\}, \{3n+1 \mid n \in Z\}, \{3n+2 \mid n \in Z\}$

※ 문제 7~9에서 $\{1,2,3,4,5,6,7,8\}$에서의 주어진 순환치환의 곱을 계산하라.

문 7. $(1,4,5)(7,8)(2,5,7)$

풀 이

$\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&3&5&8&6&2&7\end{pmatrix}$

문 8. $(1,3,2,7)(4,8,6)$

풀 이

$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&7&2&8&5&4&1&6\end{pmatrix}$

문 9. $(1,2)(4,7,8)(2,1)(7,2,8,1,5)$

풀 이

$\begin{pmatrix}1&2&3&4&5&6&7&8\\5&4&3&7&8&6&2&1\end{pmatrix}$

문제 10~12에서 $\{1,2,3,4,5,6,7,8\}$에서의 치환을 순환치환의 곱으로 표현하고 호환의 곱으로도 나타내어라.

문 10. $\begin{pmatrix}1&2&3&4&5&6&7&8\\8&2&6&3&7&4&5&1\end{pmatrix}$

풀 이

$(1\,8)(2\,6\,4)(5\,7)=(1\,8)(2\,4)(2\,6)(5\,7)$

문 11. $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}$

풀 이

$(1\,3\,4)(2\,6)(5\,8\,7)=(1\,4)(1\,3)(2\,6)(5\,7)(5\,8)$

문 12. $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&7&2&5&8&6\end{pmatrix}$

풀 이

$(1\,3\,4\,7\,8\,6\,5\,2)=(1\,2)(1\,5)(1\,6)(1\,8)(1\,7)(1\,4)(1\,3)$

문 13. Recall that element a of a group G with identity element e has order $r>0$ if $a^r=e$ and no smaller positive power of a is the identity. Consider the group S_8.

(a) What is the order of the cycle $(1\,4\,5\,7)$

풀 이

$|(1\,4\,5\,7)|=4$

(b) State a theorem suggested by part (a).

풀 이

순환치환의 위수는 그 순환치환의 궤도의 길이와 같다.

(c) What is the order of $\sigma=(4\,5)(2\,3\,7)$? of $\gamma=(1\,4)(3\,5\,7\,8)$?

풀 이

$|\sigma|=(2,3)=6$, $|\gamma|=(2,4)=4$

(d) Find the order of each of the permutations given in Ex 10~12 by looking at its decompostion inti a product of disjoint cycles.

풀 이

$|(1\,8)(2\,3\,6)(5\,7)|=(2,3,2)=6$,
$|(1\,3\,4)(2\,6)(5\,8\,7)|=(3,2,3)=6$
$|(1\,3\,4\,7\,8\,6\,5\,2)|=8$

※ In Ex 14~18, find the maximum possible order for an element of S_n for the given value of n.

문 14. $n=5$

풀 이

최대 위수는 6이다.
궤도 2인 순환치환과 궤도 3인 순환치환의 곱으로 표현될 때 최대의 위수를 갖는다.
실제로, $|(1\,2)(3\,4\,5)|=6$이다.

문 15. $n=6$

풀 이

최대 위수는 6이다.
궤도 6인 순환치환 또는 궤도 2인 순환치환과 궤도 3인 순환치환의 곱으로 표현될 때 최대위수를 갖는다. 실제로, $|(1\,2\,3\,4\,5\,6)|=6$이다.

문 16. $n=7$

풀 이

최대 위수는 12이다.
궤도 3인 순환치환과 궤도 4인 순환치환의 곱으로 표현될 때 최대위수를 갖는다.
실제로, $|(1\,2\,3)(4\,5\,6\,7)|=12$이다.

문 17. $n=10$

풀 이

최대 위수는 30이다.
궤도 2인 순환치환과 궤도 3인 순환치환 그리고 궤도 5인 순환치환의 곱으로 표현될 때 최대위수를 갖는다. 실제로, $|(1\,2)(3\,4\,5)(6\,7\,8\,9\,10)|=30$이다.

문 18. $n=15$

풀 이

최대 위수는 105이다.
궤도 3인 순환치환과 궤도 5인 순환치환 그리고 궤도 7인 순환치환의 곱으로 표현될 때 최대위수를 갖는다. 실제로, $|(1\,2\,3)(4\,5\,6\,7\,8)(9\,10\,11\,12\,13\,14\,15)|=105$이다.

문 19. Figure 9.22 shows a Cayley diaraph for the alternating group A_4 using the generating set $S=\{(1\,2\,3),(1\,2)(3\,4)\}$. continue labeling the other nine vertices with elements of A_4 expressed as a product of disjoint cycles.

풀 이

- 생략함 -

※ 문제 20~22에서, correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 20. For a permutation σ of a set A. an *orbit* of σ is a nonempty minimal subset of A that is mapped into itself by σ.

풀 이

(번역) 집합 A의 치환 σ에 대하여 σ의 *궤도*는 σ에 의하여 자기 자신으로 사상되는 A의 최소의 공집합이 아닌 부분집합이다.??

문 21. A *cycle* is a permutation having only one orbit.

풀 이

순환치환은 2개 이상의 원소를 갖는 궤도가 많아야 하나인 치환이다.

문 22. The alternating group is the group of all even permutations.

풀 이

교대군은 모든 우치환들의 집합이므로 옳은 정의이다.

문 23. 참, 거짓을 판정하라.

(a) 모든 치환은 순환치환이다.

풀 이 F

(반례) S_5에서 $(1\,2)(3\,4\,5)$는 치환이지만 순환치환은 아니다.

(b) 모든 순환치환은 치환이다.

풀 이 T

정의에 의하여 옳은 명제이다.

(c) 우치환과 기치환의 정의는 정리 9.15에 앞서 잘 정의될 수 있었다.

풀 이 F

임의의 치환을 우치환과 기치환으로 둘 다 표현할 수 있다면 우치환과 기치환의 정의는 혼동을 야기한다. 따라서 정리 9. 15에 의하여 우치환과 기치환의 정의는 잘 정의될 수 있었다.

(d) 기치환은 포함하는 S_9의 모든 비자명 부분군 H는 호환을 포함한다.

풀 이 F

(반례) $\sigma=(1\,2)(3\,4)(5\,6)$는 기치환이지만 $H=\{\sigma,\sigma^2\}=\langle\sigma\rangle$로써 호환을 포함하지는 않는다.

(e) A_5는 120개의 원소를 갖고 있다.

풀 이 F

$|A_5|=\frac{5!}{2}=60$

(f) $n \geq 1$일 때, S_n은 순환군이 아니다.

풀 이 F

(반례) $n=2$일 때, $S_2 = \{(1), (1\,2)\} = \langle (1\,2) \rangle$로써 생성원 $(1\,2) \in S_2$가 존재한다.
따라서 순환군이다.

(g) A_3는 가환군이다.

풀 이 T

$A_3 = \{(1), (1\,2\,3), (1\,3\,2)\} = \langle (1\,2\,3) \rangle$로써 순환군이다.
그러므로 가환군이다.

(h) S_7은 8을 고정시키는 S_8의 모든 원소의 부분군과 동형이다.

풀 이 T

$\phi : S_7 \to S_8^*$, $\phi(\sigma) = (8)\sigma$ 라 하자. 단, S_8^*는 S_8에서 8을 고정시킨 것이다.
그러면 ϕ는 동형사상임에 자명하다. 따라서 위의 명제는 참인 명제이다.

(i) S_7은 5를 고정시키는 S_8의 모든 원소들의 부분군과 동형이다.

풀 이 T

$\phi : S_7 \to S_8^{**}$, $\phi(\sigma) = (5\,8)\sigma$ 라 하자. 단, S_8^{**}는 S_8에서 5을 고정시킨 것이다.
그러면 ϕ는 동형사상임에 자명하다. 따라서 위의 명제는 참인 명제이다.

(j) S_8에서 기치환은 S_8의 부분군을 이룬다.

풀 이 F

기치환 간의 연산은 우치환이다. 즉, 닫혀있지 않다.
그러므로 부분군이 될 수 없다.

문 24. 예제 8.7에 있는 S_3의 치환 중 어느 것이 우치환인가? 그리고 교대군 A_3를 표로 나타내시오.

풀 이

$S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$에서 우치환인 것은 $(1), (1\,2\,3), (1\,3\,2)$이다.
이 때, 교대군 $A_3 = \{(1), (1\,2\,3), (1\,3\,2)\} = \langle (1\,2\,3) \rangle$으로 순환군이다.
- 표로 나타내는 것은 생략함! -

문 25. $n \geq 3$일 때, S_n에 대하여 다음 사실을 증명하라.

(a) S_n내의 모든 치환은 기껏해야 $n-1$개의 호환의 곱으로 나타낼 수 있다.

풀 이

$n \geq 3$일 때, S_n에서 임의의 순환치환 $(i_1\, i_2 \cdots i_r)$는 $(i_1\, i_r) \cdots (i_1\, i_2)$의 $r-1$개의 호환의 곱으로 나타낼 수 있다. 그리고 임의의 치환 $\sigma \in S_n$은 유한개의 순환치환의 곱으로 나타낼 수 있다. 이 때, $\tau_1, \cdots, \tau_k$를 유한개의 순환치환이라 하고 $\sigma = \tau_1 \cdot \tau_2 \cdot \cdots \cdot \tau_k$을 만족한다고 하자. 그러면 σ는 위의 결과에 의하여 $n-k (1 \leq i \leq k)$개의 호환의 곱으로 나타낼 수 있다. 따라서 S_n내의 모든 치환은 많아야 $n-1$개의 호환의 곱으로 나타낼 수 있다.

(b) 순환치환이 아닌 S_n에 속하는 모든 치환은 기껏해야 $n-2$개의 호환의 곱으로 나타낼 수 있다.

풀 이

임의의 치환 $\sigma \in S_n$이 순환치환이 아니면 σ는 2개 이상의 원소를 갖는 궤도가 2개 이상이 존재한다. 즉, σ는 순환치환의 2개 이상의 곱으로 이루어져 있다. 따라서 (a)에 의하여 σ는 $n-k$의 곱으로 이루어져 있으므로 많아야 $n-2$개의 호환의 곱으로 이루어져 있음을 알 수 있다.

(c) S_n에 속하는 모든 기치환은 $2n+3$개의 호환의 곱으로 쓸 수 있으며 모든 우치환은 $2n+8$개의 호환의 곱으로 표시된다.

풀 이

① $\sigma \in S_n$를 임의의 기치환이라 하고, σ의 호환의 개수를 s라 하자.
그러면 (a)에 의하여 $s \le n-1$를 만족한다.
여기서, s는 홀수이고 $2n+3$도 홀수이므로 $2n+3-s$는 짝수이다.
이 때, 항등치환은 짝수개의 호환의 곱이므로 다음을 만족한다.
$\sigma = \sigma(1) = \sigma(1\,2)(1\,2)\cdots(1\,2)$ 단, $(1\,2)\cdots(1\,2)$는 $2n+3-s$개의 곱이다.
따라서 σ는 $2n+3$개의 호환의 곱으로 쓸 수 있다.
② $\tau \in S_n$를 임의의 우치환이라 하고, τ의 호환의 개수를 t라 하자.
그러면 (a)에 의하여 $t \le n-1$를 만족한다.
여기서, t는 짝수이고 $2n+8$도 짝수이므로 $2n+8-t$는 짝수이다.
이 때, 항등치환은 짝수개의 호환의 곱이므로 다음을 만족한다.
$\tau = \tau(1) = \tau(1\,2)(1\,2)\cdots(1\,2)$ 단, $(1\,2)\cdots(1\,2)$는 $2n+8-t$개의 곱이다.
따라서 τ는 $2n+8$개의 호환의 곱으로 쓸 수 있다.

문 28.

(a) 만약 i와 j가 σ의 서로 다른 궤도에 속하고 $\sigma(i) = j$이면 $(i,j)\sigma$의 궤도는 σ의 궤도 개수보다 하나 적음을 그림 9.16처럼 그려서 설명하라.

풀 이

- 생략함 -

(b) 또한 $\sigma(j) = j$일 때 (a)를 반복하라.

풀 이

- 생략함 -

문 29. $n \geq 2$**일 때** S_n**의 모든 부분군** H**에 대하여** H**에 속하는 모든 치환이 우치환이거나 혹은** H**의 꼭 반이 우치환임을 보여라.**

풀 이

① H가 기치환을 갖지 않는 경우 S_n은 유한집합이므로 H가 닫혀있음을 보이면 충분하다.
실제로 (우치환)+(우치환)=(우치환)으로 닫혀 있다.
따라서 H는 우치환으로만 이루어진 S_n은 부분군이다.
② H가 기치환을 포함한다고 하자. 즉, $\sigma \in H$를 기치환이라 하자.
$\phi : H \to H, \phi(\mu) = \sigma\mu$ ($\mu \in H$)라 하자.
$\phi(\mu_1) = \phi(\mu_2) \Leftrightarrow \sigma\mu_1 = \sigma\mu_2 \Leftrightarrow \mu_1 = \mu_2$ ($\because$ 소약법칙)
또한 임의의 $\mu \in H$ 에 대하여 $\sigma^{-1}\mu \in H$가 존재해서 $\phi(\sigma^{-1}\mu) = \sigma(\sigma^{-1}\mu) = \mu$를 만족한다.
따라서 ϕ는 자기동형사상이다.
σ는 기치환이므로 ϕ는 우치환을 기치환 하나로, 기치환은 우치환 하나로 유일하게 대응된다.
따라서 ϕ는 H의 우치환의 집합을 H의 기치환의 집합으로 1-1대응된다.
즉, H는 같은 수의 우치환과 기치환을 갖는다.
그러므로 H가 기치환을 갖는다면 우치환의 수와 기치환의 수는 같다.

문 30. σ**가 집합** A**의 치환이라 하고** $\sigma(a) \neq a$**이면** σ**가** $a \in A$**를 움직인다고 한다. 만약** A**가 유한집합이면 길이가** n**인 순환치환** $\sigma \in S_A$**에 의해서 몇 개의 원소가 움직이는가?**

풀 이 움직인다.
A가 유한집합이라 하자. $\sigma = (i_1\, i_2 \cdots i_n) \in S_A$라 하자.
그러면 각각의 $1 \leq j \leq n-1$일 때, $\sigma(i_j) = i_{j+1}$을 만족한다.
또한 $j = n$일 때, $\sigma(i_n) = i_1$이다.
따라서 길이가 n인 순환치환 $\sigma \in S_A$에 의하여 n개의 원소가 이동된다.

문 31. A**가 무한집합이라 하자.** A**의 유한개의 원소만을 움직이는(문제 30 참조) 모든** $\sigma \in S_A$**의 집합을** H**라 하면,** H**가** S_A**의 부분군임을 보여라.**

풀 이

항등치환은 유한개의 원소를 움직이다. 따라서 H는 공집합이 아니다.
또한 H의 임의의 두 원소 σ, μ에 대하여 각각 s, t개의 원소를 움직인다고 하자.
그러면 $\sigma\mu$는 최대 $s+t$개의 원소를 움직일 수 있다. 따라서 $\sigma\mu$는 H의 원소이다.
그리고 σ가 s개의 원소를 움직이면 σ^{-1} 또한 s개의 원소를 움직이다. 따라서 σ^{-1} 또한 H의 원소이다.
그러므로 H는 S_A의 부분군이다.

문 32. A**가 무한집합이라 하고,** A**의 원소를 기껏해야 50개 움직이는 모든** $\sigma \in S_A$**의 집합을** K**라 하자.** K**는** S_A**의 부분군인가? 그 이유는?**

풀 이 아니다.
S_A의 연산에 관하여 K는 닫혀있지 않다.
(반례) $A = Z$라 하자.
$(1\,2\,3\,4 \cdots 49)$와 $(50\,51\,52)$는 각각 49개와 3개를 움직이는 치환이다. 그러므로 K의 원소이다.
하지만 $(1\,2\,3\,4 \cdots 49)(50\,51\,52)$는 52개의 원소를 움직이다. 따라서 K의 원소가 아니다.

문 33. 고정된 $n \geq 2$에 대하여 S_n을 생각해 보고 σ를 고정된 기치환이라 하자. S_n에 속하는 모든 기치환은 σ와 A_n에 속하는 적당한 우치환과의 곱임을 보여라.

풀 이

임의의 기치환 $\mu \in S_n$에 대하여 기치환 $\sigma \in S_n$이 고정되었을 때, $\sigma^{-1} \in S_n$ 또한 기치환이고 $\mu\sigma^{-1} \in S_n$는 우치환이다. 따라서 $\mu\sigma^{-1} \in A_n$이다. 이제 $\mu = (\mu\sigma^{-1})\sigma$이므로 따라서 임의의 기치환은 고정된 기치환 $\sigma \in S_n$와 어떤 우치환에 의하여 나타낼 수 있다.

문 34. σ가 홀수의 길이를 갖는 순환치환이면 σ^2도 순환치환임을 보여라.

풀 이

$\sigma = (a_1\, a_2\, a_3 \cdots a_{2k+1})$인 길이 $2k+1$인 순환치환이라 하자. 즉, $i \neq j$이면 $a_i \neq a_j$이다.

그러면 $\sigma^2 = (a_1\, a_2\, a_3 \cdots a_{2k+1})(a_1\, a_2\, a_3 \cdots a_{2k+1}) = (a_1\, a_3 \cdots a_{2k+1}\, a_2\, a_4 \cdots a_{2k})$이다.

따라서 σ^2 또한 길이 $2k+1$인 순환치환임을 알 수 있다.

문 35. 문제 34에서 제시된 방법에 따라 n과 r로 표현되는 조건 하나로 다음의 내용이 하나의 정리가 되로록 완성하라. "σ가 길이 n인 순환치환일 때, σ^r도 순환일 필요충분조건은 … ."

풀 이

$(n, r) = 1$

문 36. G가 군이고 a를 G의 한 원소라 하자. $g \in G$에 대해서 $\lambda_a(g) = ag$로 정의되는 사상 $\lambda_a : G \to G$는 집합 G의 치환임을 보여라.

풀 이

① $\lambda_a(g_1) = \lambda_a(g_2) \Leftrightarrow ag_1 = ag_2$

$\Leftrightarrow g_1 = g_2$ ($\because$군의 소약법칙)

따라서 λ_a는 단사사상이고 잘 정의되어 있는 사상이다.

② 임의의 $g \in G$에 대하여 $a^{-1}g \in G$가 존재해서 $g = a(a^{-1}g) = \lambda_a(a^{-1}g)$를 만족한다.

따라서 λ_a는 전사사상이다.

③ ①과 ②에 의하여 λ_a는 전단사사상이므로 집합 G의 치환이다.

문 37. 문제 36를 참고로 하여 $H = \{\lambda_a | a \in G\}$는 S_G의 부분군임을 보여라.
단, S_G는 G의 모든 치환의 군이다.

풀 이

① $\lambda_e \in H \neq \varnothing$임이 자명하다.

② 임의의 $\lambda_a, \lambda_b \in H$에 대하여 $(\lambda_a\lambda_b)(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) = (ab)g = \lambda_{ab}(g)$를 만족한다.

여기서 $ab \in G$이므로 따라서 $\lambda_a\lambda_b = \lambda_{ab} \in H$이다.

③ 임의의 $\lambda_a \in H$에 대하여 $a^{-1} \in G$이므로 따라서 $\lambda_a^{-1} = \lambda_{a^{-1}} \in H$ 이다.

따라서 H는 S_G의 부분군이다.

문 38. 8장의 문제 49를 참고로 하여 문제 37의 H는 집합 G위에서 이동적임을 보여라.
[힌트: 4장에 있는 정리에서 즉시 얻을 수 있는 따름정리이다.]

풀 이

임의의 $a, b \in G$에 대하여 $\lambda_c(a) = b$를 만족하는 $\lambda_c \in H$가 존재함을 보이면 충분하다.

이제 $ac = b$를 만족하는 c를 선택하자. 즉, $c = ba^{-1}$이다.
그러면 위의 조건을 만족시킨다.
따라서 H는 집합 G위에서 이동적이다.

문 39. S_n은 $\{(1,2),(1,2,\cdots,n)\}$에 의해서 생성됨을 보여라.

[힌트: r을 움직일 때 $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}$은 호환 $(1,2),(2,3),(3,4),\cdots,(n-1,n),(n,1)$을 만들게 됨을 보이고, 모든 호환은 이들 호환의 곱임을 보인다.]

풀 이

$r=0$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r} = (1,2)$
$r=1$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r} = (1,2,\cdots,n)(1,2)(1,2,\cdots,n)^{n-1} = (2,3)$
$r=2$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r} = (1,2,\cdots,n)^2(1,2)(1,2,\cdots,n)^{n-2} = (3,4)$
$\vdots$
$r=n-1$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r} = (1,2,\cdots,n)^{n-1}(1,2)(1,2,\cdots,n)^1 = (n,1)$
임을 알 수 있다.
또한 임의의 호환 (i,j)에 대하여
$(i,j) = (i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j)(j-2,j-1)\cdots(i+1,i+2)(i,i+1)$이 성립한다.
임의의 치환은 유한개의 순환치환의 곱으로 나타낼 수 있으며 순환치환은 유한개의 호환의 곱으로 나타낼 수 있다. 즉, 임의의 치환은 유한개의 호환의 곱으로 나타낼 수 있다.
따라서 S_n상의 임의의 치환은 각각의 r에 대하여 $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}$의 유한번의 곱에 의하여 나타낼 수 있다. 따라서 $S_n = \{(1,2),(1,2,3,\cdots,n)\}$이다.

문 1. Z의 부분군 $4Z$에 대한 잉여류를 구하라.

풀 이

$4Z, 4Z+1, 4Z+2, 4Z+3$

문 2. $2Z$의 부분군 $4Z$에 대한 모든 잉여류를 구하라.

풀 이

$4Z, 2+4Z$

문 3. Z_{12}의 부분군 $\langle 2\rangle$에 대한 모든 잉여류를 구하라.

풀 이

$\langle 2\rangle, 1+\langle 2\rangle$

문 4. Z_{12}의 부분군 $\langle 4\rangle$에 대한 모든 잉여류를 구하라.

풀 이

$\langle 4\rangle, 1+\langle 4\rangle, 2+\langle 4\rangle, 3+\langle 4\rangle$

문 5. Z_{36}의 부분군 $\langle 18\rangle$에 대한 모든 잉여류를 구하라.

풀 이

$\langle 18\rangle, 1+\langle 18\rangle, 2+\langle 18\rangle, \cdots, 17+\langle 18\rangle$

문 6. 표 8.12에서 주어진 군 D_4의 부분군 $\{\rho_0, \mu_2\}$에 대한 모든 좌잉여류를 구하라.

풀 이

$\{\rho_0, \mu_2\} = \mu_2\{\rho_0, \mu_2\}$

$\rho_1\{\rho_0, \mu_2\} = \{\rho_1\rho_0, \rho_1\mu_2\} = \{\rho_1, \delta_2\} = \delta_2\{\rho_0, \mu_2\}$

$\rho_2\{\rho_0, \mu_2\} = \{\rho_2, \mu_1\} = \mu_1\{\rho_0, \mu_2\}$

$\rho_3\{\rho_0, \mu_2\} = \{\rho_3, \delta_1\} = \delta_1\{\rho_3, \delta_1\}$

따라서 군 D_4의 부분군 $\{\rho_0, \mu_2\}$에 대한 좌잉여류는 $\{\{\rho_0, \mu_2\}, \{\rho_1, \delta_2\}, \{\rho_2, \mu_1\}, \{\rho_3, \delta_1\}\}$이다.

문 7. 앞의 연습문제를 반복해서 이번에는 우잉여류를 구하라. 이들은 좌잉여류와 같은가?

풀 이

$\{\rho_0, \mu_2\} = \{\rho_0, \mu_2\}\mu_2$

$\{\rho_0, \mu_2\}\rho_1 = \{\rho_1, \delta_1\} = \{\rho_0, \mu_2\}\delta_1$

$\{\rho_0, \mu_2\}\rho_2 = \{\rho_2, \mu_1\} = \{\rho_0, \mu_2\}\mu_1$

$\{\rho_0, \mu_2\}\rho_3 = \{\rho_3, \delta_2\} = \{\rho_3, \mu_2\}\delta_2$

따라서 군 D_4의 부분군 $\{\rho_0, \mu_2\}$에 대한 우잉여류는 $\{\{\rho_0, \mu_2\}, \{\rho_1, \mu_1\}, \{\rho_2, \mu_1\}, \{\rho_3, \delta_2\}\}$이고, 위의 좌잉여류과 다름을 확인할 수 있다.

문 8. 문제7에서 좌잉여류에 나타나는 순서를 따라 표 8.12를 다시 작성하라. 위수 4인 잉여군을 갖는다고 생각하는가? 그렇다면 그것은 Z_4와 동형인가? 또는 $Klein$ 4-군 V와 동형인가?

풀 이

·	ρ_0	μ_2	ρ_1	δ_2	ρ_2	μ_1	ρ_3	δ_1
ρ_0	ρ_0	μ_2	ρ_1	δ_2	ρ_2	μ_1	ρ_3	δ_1
μ_2	μ_2	ρ_0	δ_1	ρ_3	μ_1	ρ_2	δ_2	ρ_1
ρ_1	ρ_1	δ_2	ρ_2	μ_1	ρ_3	δ_1	ρ_0	μ_2
δ_2	δ_2	ρ_1	μ_2	ρ_0	δ_1	ρ_3	μ_1	ρ_2
ρ_2	ρ_0	μ_1	ρ_3	δ_1	ρ_0	μ_2	ρ_1	δ_2
μ_1	μ_1	ρ_2	δ_2	ρ_1	μ_2	ρ_0	δ_1	ρ_3
ρ_3	ρ_3	δ_1	ρ_0	μ_2	ρ_1	δ_2	ρ_2	μ_1
δ_1	δ_1	ρ_3	μ_1	ρ_2	δ_2	ρ_1	μ_2	ρ_0

No. 잉여군이 될 수 없다.

문 9. D_4의 부분군 $\{\rho_0, \rho_2\}$에 대해 문제 6을 반복하라.

풀 이

$\{\rho_0, \rho_2\} = \rho_2\{\rho_0, \rho_2\}$

$\rho_1\{\rho_0, \rho_2\} = \{\rho_1, \rho_3\} = \rho_3\{\rho_0, \rho_2\}$

$\mu_1\{\rho_0, \rho_2\} = \{\mu_1, \mu_2\} = \mu_2\{\rho_0, \rho_2\}$

$\delta_1\{\rho_0, \rho_2\} = \{\delta_1, \delta_2\} = \delta_2\{\rho_0, \rho_2\}$

문 10. 앞의 연습 문제를 반복해서 이번에는 우잉여류를 구하라. 이들은 좌잉여류와 같은가?

풀 이

$\{\rho_0, \rho_2\} = \{\rho_0, \rho_2\}\rho_2$

$\{\rho_0, \rho_2\}\rho_1 = \{\rho_1, \rho_3\} = \{\rho_0, \rho_2\}\rho_3$

$\{\rho_0, \rho_2\}\mu_1 = \{\mu_1, \mu_2\} = \{\rho_0, \rho_2\}\mu_2$

$\{\rho_0, \rho_2\}\delta_1 = \{\delta_1, \delta_2\} = \{\rho_0, \rho_2\}\delta_2$

이고, 위의 좌잉여류롸 같음을 확인할 수 있다.

문 11. 문제 9에서의 좌잉여류에 의해서 나타나는 순서에 따라 표 8.12을 다시 작성하라. 위수 4인 잉여군이 된다고 생각하는가? 그렇다면 그것은 Z_4와 동형인가 또는 $Klein$ 4-군 V와 동형인가?

풀 이

– 생략함 –

문 12. 군 Z_{24}에서의 $\langle 3 \rangle$의 지수를 구하라.

풀 이

$$|Z_{24} : \langle 3 \rangle| = \frac{|Z_{24}|}{|\langle 3 \rangle|} = 3$$

문 13. 예제 10.7의 기호를 사용해서 군 S_3에서의 $\langle \mu_1 \rangle$의 지수를 구하라.

풀 이

$$|S_3 : \langle \mu_1 \rangle| = \frac{|S_3|}{|\langle \mu_1 \rangle|} = \frac{6}{2} = 3$$

문 14. 표 8.12에서 주어진 군 D_4에서의 $\langle \mu_3 \rangle$의 지수를 구하라.

풀 이

$$|D_4 : \langle \mu_3 \rangle| = \frac{|D_4|}{|\langle \mu_3 \rangle|} = \frac{8}{2} = 4$$

문 15. Let $\sigma = (1\ 2\ 5\ 4)(2\ 3)$ in S_5. Find the index of $\langle \sigma \rangle$ in S_5

풀 이

$\sigma = (1\ 2\ 5\ 4)(2\ 3) = (1\ 2\ 3\ 5\ 4)$이므로 $|\langle \sigma \rangle| = 5$이다.

그러므로 $|S_5 : \langle \sigma \rangle| = \frac{|S_5|}{|\langle \sigma \rangle|} = \frac{5!}{5} = 4! = 24$

문 16. Let $\mu = (1\ 2\ 4\ 5)(3\ 6)$ in S_6. Find the index of $\langle \mu \rangle$ in S_6

풀 이

$$|S_6 : \langle \mu \rangle| = \frac{|S_6|}{|\langle \mu \rangle|} = \frac{6!}{4} = 180$$

※ 문제 17과 18에서 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 17. Let G be a group and let $H \subseteq G$. The *left coset* of H containing a is $aH = \{ah | h \in H\}$.

풀 이

H가 G의 부분집합이 아니라 보다 강화된 부분군이어야 한다.

즉, G가 군이고 H가 군 G의 부분군일 때, a를 포함하는 H의 좌잉여류는 $aH = \{ah | h \in H\}$이다.

문 18. Let G be a group and $H \leq G$. The *index* of H in G is the number of right cosets of H in G.

풀 이

옳은 정의이다. 게다가 G에서 H의 지수는 좌잉여류의 개수와도 같다.

문 20. 참, 거짓을 판정하라.

(a) 모든 군의 부분군은 좌잉여류를 갖는다.

풀 이 T

(b) 유한군의 부분군의 좌잉여류의 개수는 G의 위수를 나눈다.

풀 이 T

G: 유한군, $H \leq G$라 하자.

그러면 라그랑지 정리에 의하여 $|G:H| = \frac{|G|}{|H|}$이다.

즉, $|G:H| \mid |G|$ 이다.

따라서, 좌잉여류의 개수 즉, G에 대한 H의 지수는 G의 지수를 나눈다.

(c) 위수가 소수인 모든 군은 가환이다.

풀 이 T

위수가 소수인 군은 순환군이다. 그리고 순환군은 가환군이다. 따라서 위수가 소수인 군은 가환군이다.

(d) 무한군의 유한 부분군에는 좌잉여류가 없다.

풀 이 F

(반례) Z^*는 무한군이고 $\{1\}$은 유한 부분군이다. 하지만 $a \in Z^*$에 대하여 $a\{1\} = \{a\}$인 좌잉여류를 갖는다.

(e) 군의 부분군은 그 자신의 좌잉여류이다.

풀 이 T

$\{e\}H = H$는 H의 좌잉여류이다.

(f) 유한군의 부분군 만이 좌잉여류를 가질 수 있다.

풀 이 F

(반례) Z는 무한군이고 $\langle 2 \rangle$는 무한위수를 갖는 Z의 부분군이다. 하지만 $\langle 2 \rangle, 1 + \langle 2 \rangle$인 좌잉여류를 갖는다.

(g) $n > 1$일 때, A_n은 S_n내에서 지수가 2이다.

풀 이 T

$\phi : A_n \to B_n, \phi(\sigma) = (1\ 2)\sigma$라 하자. 그러면 ϕ는 군동형사상임을 쉽게 보일 수 있다. 따라서 $|A_n| = |B_n|$이다. 여기서 $S_n = A_n \cup B_n, A_n \cap B_n \neq \varnothing$ 이므로 $|S_n : A_n| = \frac{|S_n|}{|A_n|} = 2$이다.

(h) 라그랑지의 정리는 훌륭한 결과이다.

풀 이 T

주어진 군과 부분군의 지수와의 관계를 알게 되면서 주어진 군에 대한 부분군을 찾는데 보다 유용하게 되었다. 그런 이유에서도 라그랑지 정리는 충분히 훌륭한 결과이다.

(i) 모든 유한군은 그 군의 위수의 모든 약수에 대하여 그 약수를 위수로 갖는 원소를 포함한다.

풀 이 F

라그랑지 정리의 역은 일반적으로 성립하지 않는다.

(반례) A_4에서 위수 6인 부분군을 갖지 않는다.

(j) 모든 유한순환군은 그 군의 위수의 모든 약수에 대하여 그 약수를 위수로 갖는 원소를 포함한다.

풀 이 T

G를 위수 n인 순환군이라고 하자. $\exists a \in G \; s.t. \; G = \langle a \rangle$

그러면 $d|n$에 대하여 $|\langle a^k \rangle| = \frac{n}{(k,n)} = d$ 인 k가 존재함을 보이면 충분하다.

$k = \frac{n}{d}$라 하자. 그러면 $\left|\left\langle a^{\frac{n}{d}} \right\rangle\right| = \frac{n}{(\frac{n}{d}, n)} = d$임을 알 수 있다.

여기서 $a^{\frac{n}{d}} \in G$임에는 자명하다. 따라서 위의 명제는 참인 명제이다.

※ 문제 20~24에서 가능하다면 요구하는 부분군과 군의 예를 들어라. 불가능하면 그 이유를 말하라.

문 20. 좌잉여류와 우잉여류가 서로 다른 G의 분할을 생성하는 가환군G의 부분군

풀 이 불가능하다.

G가 가환군이므로 $aH = Ha$가 성립한다. 따라서 좌잉여류와 우잉여류의 개수는 같아야 한다.

문 21. 오직 하나의 세포로서 G의 분할을 생성하는 좌잉여류를 갖는 군 G의 부분군

풀 이

(예) $H = G$라 하면 H는 오직 하나의 세포로서 G의 분할을 생성하는 좌잉여류 $aH(= G)$를 갖는다.

문 22. 6개의 세포로서 그 군을 분할하는 좌잉여류를 갖는 위수 6인 군의 부분군

풀 이

(예) 위수 6인 Z_6에서 부분군 $\{0\}$에 의하여 $\{\{0\}, 1+\{0\}, 2+\{0\}, \cdots, 5+\{0\}\}$인 6의 세포서 분할한다.

문 23. 12개의 세포로서 그 군을 분할하는 좌잉여류를 갖는 위수 6인 군의 부분군

풀 이 불가능하다.

라그랑지 정리에 의하여 $12|6$를 만족한다. 하지만 이는 모순이다.

문 24. 4개의 세포로서 그 군을 분할하는 좌잉여류를 갖는 위수 6인 군의 부분군

풀 이 불가능하다.

라그랑지 정리에 의하여 $6|4$를 만족한다. 하지만 이는 모순이다.

문 25. - 생략함 -

문 26. 정리 10.1의 관계 $\sim_R$이 동치 관계임을 증명하라.

풀 이

① (반사) $a \sim_R a$일 때, $e = a \cdot a^{-1} \in H$이므로 $a \sim_R a$ 이다.

② (대칭) $a \sim_R b$일 때, $ba^{-1} = (ab^{-1})^{-1} \in H$이므로 $b \sim_R a$ 이다.

③ (추이) $a \sim_R b$, $b \sim_R c$ 일 때, $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$이므로 $a \sim_R c$ 이다.

따라서 관계 $\sim_R$는 동치관계에 있다.

문 27. H**를 군** G**의 부분군이라 하고** $g \in G$**이라 하자.** H**로부터** Hg**위로 대응하는** $1-1$**함수를 정의하여 이 함수가** $1-1$**이고** Hg**위로의 함수을 증명하라.**

풀 이

$\phi_g : H \to Hg, \phi_g(h) = hg \ (h \in H)$라 하자.

① 임의의 $h_1, h_2 \in H$에 대하여 $\phi_g(h_1) = \phi_g(h_2) \Leftrightarrow h_1 g = h_2 g \Leftrightarrow h_1 = h_2$ ($\because H \leq G$)을 만족한다.

따라서 잘 정의되어 있으며 일대일 함수이다.

② $im\phi = \{hg | h \in H\} = Hg$

따라서 위로의 함수이다.

문 28. H**를 모든** $g \in G$**와 모든** $h \in H$**에 대해서** $g^{-1}hg \in H$**를 만족하는 군** G**의 부분군이라 하자. 모든 좌잉여류** gH**는 우잉여류** Hg**와 같음을 보여라.**

풀 이

(→) 임의의 $x \in gH$에 대하여 $\exists h_1 \in H \ s.t. \ x = g \cdot h_1$

가정에 의하여 $x \cdot g^{-1} = g \cdot h \cdot g^{-1} = (g^{-1} \cdot h_1^{-1} \cdot g)^{-1} \in H$ 이다. 그러면 $\exists h_2 \in H \ s.t. \ x \cdot g^{-1} = h_2$

따라서 $x = h_2 \cdot g \in Hg$ 이다.

(←) 임의의 $y \in Hg$에 대하여 $\exists h_3 \in H \ s.t. \ y = h_3 \cdot g$

가정에 의하여 $g^{-1} \cdot y = g^{-1} \cdot h_3 \cdot g \in H$ 이다. 그러면 $\exists h_4 \in H \ s.t. \ g^{-1} \cdot y = h_4$

따라서 $y = g \cdot h_4 \in gH$ 이다.

문 29. H**를 군** G**의 부분군이라 하자.** h**의 좌잉여류로서** G**의 분할이** H**의 우잉여류로서의 분할과 같으면 모든** $g \in G$**와 모든** $h \in H$**에 대해서** $g^{-1}hg \in H$**임을 증명하라.**

풀 이 문제 28번의 역!! ($\underline{gH = Hg \ \Rightarrow \ \forall g \in G, \forall h \in H \ s.t. \ g^{-1}hg \in H}$)

모든 $g \in G$와 모든 $h \in H$에 대해서 $gH = Hg$이므로 h^*가 존재해서 $hg = gh^*$를 만족한다.

따라서 $h^* = g^{-1} \cdot h \cdot g \in H$ 이다.

※ H**를 군** G**의 부분군이라 하고** $a, b \in G$**라 하자. 문제 30~33에서 그 명제를 증명하거나 또는 반례를 들어라.**

문 30. $aH = bH$**이면** $Ha = Hb$**이다.**

풀 이

(반례) $G = S_3, \ H = \{\rho_0, \mu_1\}, \ a = \rho_1, b = \mu_3$이라 하자.

그러면 $aH = \{\rho_1, \mu_3\} = bH$이지만 $Ha = \{\rho_1, \mu_2\}$이고 $Hb = \{\mu_3, \rho_0\}$로써 $Ha \neq Hb$이다.

문 31. $Ha = Hb$**이면** $b \in Ha$**이다.**

풀 이

$b = eb \in Hb = Ha$이므로 $b \in Ha$이다.

문 32. $aH = bH$**이면** $Ha^{-1} = Hb^{-1}$**이다.**

풀 이

$aH = bH \Rightarrow Ha^{-1} = H^{-1}a^{-1} = (aH)^{-1} = (bH)^{-1} = H^{-1}b^{-1} = Hb^{-1}$

따라서 $Ha^{-1} = Hb^{-1}$이다.

문 33. $aH=bH$**이면** $a^2H=b^2H$**이다.**

풀 이

(반례) $H=\{\rho_0,\mu_2\}\leq D_4,\ a=\rho_1, b=\delta_2$라 하자.

그러면 $aH=\{\rho_1,\delta_2\}=bH$이지만 $a^2H=\{\rho_2,\mu_1\}$이고 $b^2H=\{\rho_0,\mu_2\}$로써 $a^2H\neq b^2H$ 이다.

문 34. G**가 위수** pq**를 갖는 군이라 하자. 단,** p**와** q**는 소수이다.** G**의 모든 진부분군은 순환적임을 보여라.**

풀 이

G가 위수 pq를 갖는 군이므로 라그랑지 정리에 의하여 부분군 H가 갖을 수 있는 위수는 $1, p, q$이다.

① H의 위수가 1인 경우

H는 자명군이다. 따라서 순환적이다.

② H의 위수가 p또는 q인 경우

소수를 위수로 갖는 군은 이미 순환적임을 알고 있다.(증명은 생략!!)

따라서 G의 모든 진부분군은 순환적이다.

문 35. 군 G**의 부분군** H**의 좌잉여류의 개수는 우잉여류의 개수와 같음을 보여라. 즉, 좌잉여류의 모임에서 우잉여류의 모임 위로 대응하는 1-1함수를 구성하라.**
(이 결과는 유한군에 대해서는 헤아림으로써 당연하게 됨을 주의하자. 증명은 어떤 군에 대해서도 성립되어야 한다.)

풀 이

ϕ: 좌잉여류 $\rightarrow$ 우잉여류, $\phi(aH)=Ha^{-1}$이라 하자.

① $\phi(aH)=\phi(bH)\Leftrightarrow Ha^{-1}=Hb^{-1}\Leftrightarrow aH=bH$ ($\forall a,b\in H$)

따라서 ϕ는 잘 정의되어 있으며 일대일 함수이다.

② $\forall Hg\in$우잉여류 $\exists g^{-1}H\in$좌잉여류 $s.t.\ \phi(g^{-1}H)=H(g^{-1})^{-1}=Hg$

따라서 ϕ는 위로의 함수이다.

문 36. 4장의 문제 29에서 위수 $2n$**을 갖는 모든 유한군은 위수 2인 원소를 포함함을 보였다. 라그랑지 정리를 이용하여** n**이 홀수이면, 위수** $2n$**인 가환군은 위수 2인 원소를 단 하나 포함하고 있음을 보여라.**

풀 이

존재성은 이미 보였으므로(4장의 문제 29) 유일성에 대해서 살피면 충분하다.

$a\neq b$인 $a,b\in G$에 대하여 $|a|=2=|b|$라 하자.

이제 $\{e,a,b,ab\}$는 G의 부분군이다. (부분군인 것을 보이는 것은 유한군이므로 닫혀있음을 보이면 충분하다. 구체적으로 보이는 것은 생략함.)

그러면 라그랑지 정리에 의하여 $4|2n$이다.

따라서 n은 2의 배수이다. 하지만 이는 가정 n은 홀수임에 모순된다.

따라서 위수 2인 원소는 단 하나 포함함을 알 수 있다.

문 37. 적어도 두 원소를 가지면서 비자명 진부분 집합을 갖지 않는 군은 유한군이며 소수를 위수로 가짐을 보여라.

풀 이

$|G|\geq 2$인 군 G이라 하자. $a\in G$일 때, $\langle a\rangle$는 G의 부분군임에 자명하다.
가정에서 군 G는 비자명 진부분 집합을 갖지 않으므로 $G=\langle a\rangle$이다.
즉, G는 순환군이다.
여기서 G가 무한위수를 갖는다면 G는 Z와 동형이다. 하지만 Z는 진부분군을 무한히 많이 갖음을 이미 알고 있다. 따라서 G는 유한위수를 갖는다.

$|G|=n(\geq 2)$이라 하자. $1<d<n$이고 $d|n$인 d가 존재하면 $\left\langle a^{\frac{n}{d}}\right\rangle$는 $G=\langle a\rangle$의 비자명 진부분군이다.
하지만 이는 가정에 모순된다. 따라서 d가 존재하지 않는다. 즉, n는 소수이다.
그러므로 적어도 두 원소를 가지면서 비자명 진부분 집합을 갖지 않는 군은 유한군이며 소수를 위수로 가진다.

문 38. 정리 10.14를 증명하라.
[힌트: $\{a_iH|i=1,2,\cdots,r\}$를 G에서의 H의 서로 다른 좌잉여류의 모임이라 하고 $\{b_jK|j=1,2,\cdots,s\}$를 H에서의 K의 서로 다른 좌잉여류의 모임이라 하면 $\{(a_ib_j)K|i=1,2,\cdots,r;j=1,2,\cdots,s\}$가 G에서의 K의 서로 다른 좌잉여류의 모임임을 보여라.]

풀 이

$\{a_iH|i=1,2,\cdots,r\}$를 G에서의 H의 서로 다른 좌잉여류의 모임이라 하고 $\{b_jK|j=1,2,\cdots,s\}$를 H에서의 K의 서로 다른 좌잉여류의 모임이라 하면 $\{(a_ib_j)K|i=1,2,\cdots,r;j=1,2,\cdots,s\}$가 G에서의 K의 서로 다른 좌잉여류의 모임임을 보이면 충분하다.
$g\in G=a_1H\cup\cdots\cup a_rH$라 하자. 그러면 $\exists i\ s.t.\ g\in a_iH$ 그러므로 $\exists h\in H\ s.t.\ g=a_ih$
게다가 $H=b_1K\cup\cdots\cup b_sK$ 이므로 $\exists j\ s.t.\ h\in b_jK$이고 따라서 $\exists k\in K\ s.t.\ h=b_jK$
그러면 $g=a_ih=a_i(b_jk)=(a_ib_j)k\in a_ib_jK$ 이다. 즉, $G=\bigcup_{i,j}a_ib_jK$ 이다.
이제 서로 구별됨을 보인다. $a_ib_jK=a_pb_qK$라고 가정하자.
그러면 $a_ib_j\in a_ib_jK=a_pb_qK$ 이다. 즉, $\exists k\in K\ s.t.\ a_ib_j=a_pb_qk$
그러므로 $a_i=a_pb_qkb_j^{-1}=a_p(b_qkb_j^{-1})\in a_pH$ ($\because b_qkb_j^{-1}\in H$)
그러면 $a_iH=a_pH$이다. 즉, $i=p$를 의미한다.
또한 군의 소약법칙에 의하여 $b_jK=b_qK$이고, 따라서 $j=q$이다.

문 39. H가 유한군 G의 지수 2인 부분군이라 하면 H의 모든 좌잉여류는 H의 우잉여류임을 보여라.

풀 이

임의의 $a\in G$에 대하여
① $a\in H$이면 $aH=H=Ha$임은 자명하다.
② $a\notin H$이면 가정에 의하여 $|G:H|=2$이므로 $G=H\cup Ha=H\cup aH$ 이다.
따라서 $aH=G-H=Ha$이다.
따라서 좌잉여류와 우잉여류는 같음을 알 수 있다.

문 40. 항등원 e를 갖는 군 G가 유한 위수 n을 갖는다면 모든 $a \in G$에 대하여 $a^n = e$임을 보여라.

풀 이

① $a = e$이면 $e^n = e$이므로 자명하다.
② $a \neq e$이면 라그랑지 정리에 의하여 $|\langle a \rangle| \mid |G| = n$를 만족한다.
$|\langle a \rangle| = k$라 하면 $n = kd$이고 $a^k = e$로부터 $a^n = a^{kd} = (a^k)^d = e^d = e$임을 알 수 있다.
따라서 군 G의 위수가 n이면 모든 $a \in G$에 대하여 $a^n = e$이다.

문 41. 실수들의 덧셈에 대한 군의 부분군 Z의 모든 좌잉여류는 $0 \leq x < 1$인 R에서 꼭 하나의 대표 x를 포함함을 보여라.

풀 이

(존재성) $a + Z$를 R의 좌잉여류라 하자. $[a]$를 a를 넘지 않는 최대의 정수라 하자.
그러면 $0 \leq a - [a] < 1$이고 $a - [a] \in a + Z$ 이다.
(유일성) $s, t \in R$가 $s + Z = t + Z$를 만족하는 Z의 좌잉여류의 대표 원소라 하자.
그러면 $s - t \in Z$이다. 가정에서 $0 \leq s, t < 1$이므로 따라서 $s = t$이다.
그러므로 $a - [a]$가 $a + Z$에서 $0 \leq x < 1$를 만족하는 유일한 대표 원소 x임을 알 수 있다.

문 42. 함수 $\sin$운 실수들의 덧셈에 대한 군 R의 부분군 $\langle 2\pi \rangle$의 고정된 좌잉여류의 모든 대표에 같은 값이 대응됨을 보여라. (따라서, $\sin$은 잉여류의 집합에서 잘 정의된 함수를 유도한다: 한 잉여류에 대한 함수의 값은 잉여류의 대표 x를 택해서 $\sin x$를 계산함으로써 얻어진다.)

풀 이

- 생략함 -

문 43. H와 K가 군 G의 부분군이라 하자. G위에서 "~"을 $a \sim b$일 필요충분조건은 적당한 $h \in H$와 $k \in K$에 대하여 $a = hbk$로 정의한다.

(a) ~이 G위에서 동치관계임을 증명하라.

풀 이

① (반사) $a \sim a$일 때, $a = e \cdot a \cdot e$($\because e \in H \cap K$)이므로 $a = e^{-1} \cdot a \cdot a^{-1} = e \cdot a \cdot e$가 성립한다.
따라서 $a \sim a$이다.
② (대칭) $a \sim b$일 때,
적당한 $h \in H$와 $k \in K$에 대하여 $a = hbk$를 만족한다.
그러면 $b = h^{-1} \cdot a k^{-1}$이고 이 때, $h^{-1} \in H, k^{-1} \in K$이므로 따라서 $b \sim a$이다.
③ (추이) $a \sim b$, $b \sim c$일 때,
적당한 $h_1 \in H$와 $k_1 \in K$에 대하여 $a = h_1 \cdot b \cdot k_1$를 만족하고,
적당한 $h_2 \in H$와 $k_2 \in K$에 대하여 $b = h_2 \cdot c \cdot k_2$를 만족한다.
그러면 $a = h_1 \cdot h_2 \cdot c \cdot k_2 \cdot k_1 = (h_1 \cdot h_2) \cdot c \cdot (k_2 \cdot k_1)$이고 $h_1 \cdot h_2 \in H, k_1, k_2 \in K$이므로 따라서 $a \sim c$이다.

(b) a를 포함하는 동치류 내에 있는 원소들을 서술하라.(이 동치류는 이중 잉여류라 한다.)

풀 이

$HaK = \{hak \mid h \in H, k \in K\}$

문 44. S_A**를 집합** A**의 모든 치환의 군이라 하고,** c**를** A**의 특정한 원소라 하자.**

(a) $\{\sigma \in S_A \mid \sigma(c) = c\}$**는** S_A**의 부분군** $S_{c,c}$**임을 보여라.**

풀 이

$(1\,2)(2\,1)$에 대하여 $(1\,2)(2\,1)(c) = c$를 만족한다. 따라서 $S_{c,c}$는 공집합이 아니다.

이제 임의의 $\sigma, \tau \in S_A$에 대하여 $\sigma \cdot \tau^{-1}(c) = \sigma(c) = c$이므로 $\sigma \cdot \tau^{-1} \in S_{c,c}$ 이다.

따라서 $S_{c,c}$는 S_A의 부분군이다.

(b) $d \neq c$**를** A**의 다른 특정한 원소라 하자.** $S_{c,d} = \{\sigma \in S_A \mid \sigma(c) = d\}$**가** S_A**의 부분군이 되는가? 그 이유를 설명하라.**

풀 이

부분군이 되지 않는다. 닫혀있음을 보장해 주지 못하기 때문이다.

즉, $\sigma(c) = d, \tau(c) = d, \tau(d) = c$라 하자.

그러면 $\tau, \sigma \in S_{c,d}$이지만 $\tau \cdot \sigma(c) = \tau(d) = c$이다. 따라서 $\tau \cdot \sigma \notin S_{c,d}$ 이다.

(c) (b)의 $S_{c,d}$**를 (a)의 부분군** $S_{c,c}$**로 특정지워라.**

풀 이

- 생략함 -

문 45. 위수 n**인 유한순환군은** n**의 각 약수** d**를 위수로 갖는 부분군을 꼭 하나 가짐을 증명하고 이들이 이 군이 갖는 모든 부분군임을 보여라.**

풀 이

(존재성) G를 위수 n인 순환군이라 하자.

그러면 $\exists a \in G \; s.t. \; G = \langle a \rangle$

여기서 d를 n의 약수라 하자.

그러면 $\left|\left\langle a^{\frac{n}{d}} \right\rangle\right| = \dfrac{n}{(n, \frac{n}{d})} = d$이다.

따라서 d를 약수로 갖는 부분군 $\left\langle a^{\frac{n}{d}} \right\rangle$가 존재한다.

(유일성) K를 위수 d인 군 G의 부분군이라 하자.

G가 순환군이므로 부분군인 K 또한 순환군이다.

그러면 $\exists s \;\; s.t. \; K = \langle a^s \rangle$

가정에 의하여 $|\langle a^s \rangle| = \dfrac{n}{(n,s)} = d$를 만족한다.

$(n,s) = \dfrac{n}{d} \mid s$ 이므로 $\exists t \;\; s.t. \;\; s = \dfrac{n}{d} \times t$

그러므로 $\langle a^s \rangle$는 $\left\langle a^{\frac{n}{d}} \right\rangle$의 부분군이다.

가정에 의하여 $|\langle a^s \rangle| = d = \left|\left\langle a^{\frac{n}{d}} \right\rangle\right|$이므로 결국엔 $\langle a^s \rangle = \left\langle a^{\frac{n}{d}} \right\rangle$임을 알 수 있다.

문 46. 양의 정수 n에 대해서 오일러 ϕ-함수는 $\phi(n)=s$로 정의되어 있다. 단, s는 n보다 적으면서 n은 서로소인 양의 정수의 개수들이다. 문제 45을 이용하여 $n=\sum_{d|n}\phi(d)$임을 보여라. 여기서 합은 n을 나누는 모든 양의 정수 d에 대해 취해진다.
[힌트: Z_d의 생성원의 개수는 보조정리 6.16에 의해 $\phi(d)$임에 유의하라.]

풀 이

임의의 $d|n$에 대하여 $S_d=\{s\in Z_n \,|\, |\langle s\rangle|=|s|=d\}$라 하자.

$|s||n$이므로 임의의 $s\in Z_d$에 대하여 라그랑지 정리에 의하여 $\bigcup_{d|n} S_d = Z_n$를 만족한다.

$|S_d|=\psi(d)$라 하자. $\left|\frac{n}{d}\right|=d$, $S_d\neq\varnothing$라 하자.

문제 45에 의하여 위수 d인 부분군 $\left\langle \frac{n}{d}\right\rangle$는 유일하게 하나 존재한다.

게다가 $1\le t\le d$에 대하여 $\left\langle \frac{n}{d}\right\rangle=\left\langle \frac{n}{d}\cdot t\right\rangle$이므로 필요충분하게 $(d,t)=1$임을 알 수 있다.

그러므로 $|S_d|=\psi(d)=\phi(d)$이다. $Z_n=\bigcup_{d|n} S_d$이므로 즉, $\sum_{d|n}\psi(d)=n$이므로 $\sum_{d|n}\phi(d)=n$이다.

[다른 풀이1]
Z_n에서 n을 나누는 위수 d를 갖는 임의의 원소는 위수 d인 순환부분군을 생성한다. 그리고 생성원의 개수는 보조정리 6.16에 의하여 $\phi(d)$이다. 문제 45에 의하여 n을 나누는 위수 d를 갖는 부분군은 유일함을 안다. 그러므로 Z_n은 정확히 n을 나누는 각각의 위수 d의 원소들인 $\phi(d)$를 포함한다. Z_n의 각각의 원소들의 위수는 n을 나누므로 $n=\sum_{d|n}\phi(d)$인 결과를 얻을 수 있다.

[다른 풀이2](←정수론적인 증명방법.)
먼저 $\sum_{d|1}\phi(d)=\phi(1)=1$이다. 다음에 $n\ge 2$이라 하고 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$를 n의 표준분해라고 하자.
이 때, n의 양의 정수는 모두 $d=p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}\quad(0\le f_i\le e_i)$와 같은 꼴이고 또
$\phi(d)=\phi(p_1^{f_1})\cdot\phi(p_2^{f_2})\cdots\phi(p_r^{f_r})\quad(0\le f_i\le e_i)$이므로 다음이 성립한다.

$$\sum_{d|n}\phi(d)=\left\{\phi(1)+\phi(p_1)+\cdots+\phi(p_1^{e_1})\right\}\left\{\phi(1)+\phi(p_2)+\cdots+\phi(p_2^{e_2})\right\}\cdots\left\{\phi(1)+\phi(p_r)+\phi(p_r)+\cdots+\phi(p_r^{e_r})\right\}$$

그런데 각 $i(1\le i\le r)$에 대하여 $\phi(1)+\phi(p_i)+\cdots+\phi(p_i^{e_i})=1+(p_i-1)+\cdots+(p_i^{e_i}-p_i^{e_i-1})=p_i^{e_i}$이므로,
위의 등식에 의하여 $\sum_{d|n}\phi(d)=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}=n$이다.

문 47. G를 유한군이라 하면, 각 양의 정수 m에 대하여 방정식 $x^m = e$의 G에서의 해의 개수가 기껏해야 m이면 G는 순환적임을 보여라.
[힌트: 정리 10.12와 문제 46을 이용하여 G는 위수 $n = |G|$인 원소를 포함함을 보여라.]

풀 이

$\psi(m)$를 $m|n$에 대하여 G에서 위수 m인 원소의 개수라 하자. 이제 $\psi(m) = \phi(m)$를 보이면 충분하다. 그러면 $\psi(n) = \phi(n) > 0$, 즉, 위수 n인 $a \in G$가 존재한다. 다시 말해서 $G = \langle a \rangle$는 위수 n인 순환군이다.

($\because$ 정리 10.12에 의하여 임의의 $a \in G$에 대하여 $|a||n$이므로 a는 어떤 $m|n$에 대하여 $x^m = e$의 해이다. 만약 $m|n$에 대하여 $|a| = m$를 만족하는 $a \in G$가 존재한다면 $e, a, \cdots, a^{m-1}$는 서로 다른 $x^m = e$의 해 이다. 가정에 의하여 $x^m = e$는 많아야 $e, a, \cdots, a^{m-1}$이 $x^m = e$의 모든 서로 다른 영점이다. 그러므로 $\psi(m) = \phi(m)$이다. 즉, $\psi(m) \neq 0$이면 $\psi(m) = \phi(m)$이다. 따라서 $\psi(m) = 0$또는 $\psi(m) = \phi(m)$이다. 문제 45에 의하여 $\sum_{m|n} \psi(m) = \sum_{m|n} \phi(m) = n$이므로 $m|n$을 만족하는 모든 m에 대하여 $\psi(m) = \phi(m)$를 만족한다.)

문 1. $Z_2 \times Z_4$**의 원소를 나열하고 각 원소의 위수를 구하라. 이 군은 순환군인가?**

풀 이

$|(0,0)|=1, |(0,1)|=4, |(0,2)|=2, |(0,3)|=4, |(1,0)|=2, |(1,1)|=4, |(1,2)|=2, |(1,3)|=4$
이고 이 때 위수 8인 원소가 없으므로 $Z_2 \times Z_4$의 생성원이 존재하지 않는다. 따라서 순환군이 아니다.

문 2. 군 $Z_3 \times Z_4$**에 대해 문제 1을 반복하라.**

풀 이

$|(0,0)|=1, |(0,1)|=4, |(0,2)|=3, |(0,3)|=4, |(1,0)|=3, |(1,1)|=12, |(1,2)|=6, |(1,3)|=12,$
$|(2,0)|=3, |(2,1)|=12, |(2,2)|=6, |(2,3)|=12$ 이고 이 때 위수가 12인 원소 $(1,1),(1,3),(2,1),(2,3)$이 존재한다. 따라서 $Z_3 \times Z_4$는 순환군이다.

※ 문제 3~7에서 주어진 직적의 원소의 위수를 구하라.

문 3. $Z_4 \times Z_{12}$**에서** $(2,6)$

풀 이

$|(2,6)|=2$

문 4. $Z_6 \times Z_{15}$**에서** $(2,3)$

풀 이

$|(2,3)|=15$

문 5. $Z_{12} \times Z_{18}$**에서** $(8,10)$

풀 이

$|(8,10)|=9$

문 6. $Z_4 \times Z_{12} \times Z_{15}$**에서** $(3,10,9)$

풀 이

$|(3,10,9)|=60$

문 7. $Z_4 \times Z_{12} \times Z_{20} \times Z_{24}$**에서** $(3,6,12,16)$

풀 이

$|(3,6,12,16)|=60$

문 8. $Z_6 \times Z_8$**의 모든 순환 부분군의 위수 중에서 가장 큰 수는 얼마인가? 또,** $Z_{12} \times Z_{15}$**에서는 어떠한가?**

풀 이

$[6,8]=24, [12,15]=60$

문 9. $Z_2 \times Z_2$**의 모든 비자명 진부분군들을 구하라.**

풀 이

$\langle(0,1)\rangle, \langle(1,0)\rangle, \langle(1,1)\rangle$

문 10. $Z_2 \times Z_2 \times Z_2$**의 모든 비자명 진부분군들을 구하라.**

풀 이

위수 2인 부분군: $\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(0,0,1)\rangle, \langle(1,1,0)\rangle, \langle(1,0,1)\rangle, \langle(0,1,1)\rangle, \langle(1,1,1)\rangle$

위수 4인 부분군: $\{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}$, $\{(0,0,0),(1,0,0),(0,0,1),(1,0,1)\}$
$\{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\}$, $\{(0,0,0),(1,1,0),(0,0,1),(1,1,1)\}$
$\{(0,0,0),(1,1,0),(0,1,1),(1,0,1)\}$, $\{(0,0,0),(1,1,1),(0,1,0),(1,0,1)\}$
$\{(0,0,0),(0,1,1),(0,0,1),(0,1,0)\}$

문 11. $Z_2 \times Z_4$**의 위수가 4인 부분군을 모두 구하라.**

풀 이

– 생략함 –

문 12. $Z_2 \times Z_2 \times Z_2$**의 부분군 중에서** $klein$ **4-군과 동형인 부분군을 모두 구하라.**

풀 이

$\{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}$, $\{(0,0,0),(1,0,0),(0,0,2),(1,0,2)\}$
$\{(0,0,0),(1,0,0),(0,1,2),(1,1,2)\}$, $\{(0,0,0),(1,1,0),(0,0,2),(1,1,2)\}$
$\{(0,0,0),(1,1,0),(0,1,2),(1,0,2)\}$, $\{(0,0,0),(1,1,2),(0,1,0),(1,0,2)\}$
$\{(0,0,0),(0,1,2),(0,0,2),(0,1,0)\}$

문 13. 인수들의 인수를 무시하고 Z_{60}**과 동형이 되는 두 개 이상의** Z_n**꼴의 직적으로 표현하되 가능한 한 여러 가지 방법으로 써보아라.**

풀 이

$Z_{60} \simeq Z_4 \times Z_3 \times Z_5 \simeq Z_{12} \times Z_5 \simeq Z_{20} \times Z_3 \simeq Z_4 \times Z_{15}$

문 14. 공란을 채워라.

(a) 18에 의해서 생성되는 Z_{24}**의 순환부분군은 위수 □를 갖는다.**

풀 이 4

(b) $Z_3 \times Z_4$**의 위수는 □이다.**

풀 이 12

(c) $Z_{12} \times Z_8$**의 원소**$(4,2)$**는 위수 □이다.**

풀 이 12

(d) $klein$ **4-군은** $Z_{\square} \times Z_{\square}$**과 동형이다.**

풀 이 2, 2

(e) $Z_2 \times Z \times Z_4$는 유한위수를 갖는 원소 □개를 갖는다.

풀 이 8

문 15. Find the maximum possible order for some element of $Z_4 \times Z_6$.

풀 이

$[4,6]=12$이므로 최대 가능한 원소의 위수는 12이다.

문 16. Are the groups $Z_2 \times Z_{12}$ and $Z_4 \times Z_6$ isomorphic? why or why not?

풀 이 동형이다.

유한생성가환군의 기본정리에 의하여 $Z_2 \times Z_{12} \simeq Z_2 \times Z_4 \times Z_3$이고 $Z_4 \times Z_6 \simeq Z_4 \times Z_2 \times Z_3$이다.

또한 $Z_2 \times Z_4 \simeq Z_4 \times Z_2$이므로 $Z_2 \times Z_{12} \simeq Z_4 \times Z_6$임을 알 수 있다.

문 17. Find the maximum possible order for some element of $Z_8 \times Z_{10} \times Z_{24}$.

풀 이

$[8,10,24]=240$이므로 최대 가능한 원소의 위수는 240이다.

문 18. Are the groups $Z_8 \times Z_{10} \times Z_{24}$ and $Z_4 \times Z_{12} \times Z_{40}$ isomorphic? why or why not?

풀 이 동형이 아니다.

유한생성 가환군의 기본정리에 의하여 다음은 동형이다.

$Z_8 \times Z_{10} \times Z_{24} \simeq Z_8 \times (Z_2 \times Z_5) \times (Z_3 \times Z_8)$

$Z_4 \times Z_{12} \times Z_{40} \simeq Z_4 \times (Z_3 \times Z_4) \times (Z_5 \times Z_8)$

하지만 $Z_2 \times Z_8 \not\simeq Z_4 \times Z_4$이다.

그러므로 $Z_8 \times Z_{10} \times Z_{24}$와 $Z_4 \times Z_{12} \times Z_{40}$는 동형이 아니다.

문 19. Find the maximum possible order for some element of $Z_4 \times Z_{18} \times Z_{15}$.

풀 이

$[4,18,15]=180$이므로 최대 가능한 원소의 위수는 180이다.

문 20. Are the groups $Z_4 \times Z_{18} \times Z_{15}$ and $Z_3 \times Z_{36} \times Z_{10}$ isomorphic? why or why not?

풀 이 동형이다.

유한생성 가환군의 기본정리에 의하여 다음은 동형이다.

$Z_4 \times Z_{18} \times Z_{15} \simeq Z_4 \times (Z_2 \times Z_9) \times (Z_3 \times Z_5)$

$Z_3 \times Z_{36} \times Z_{10} \simeq Z_3 \times (Z_4 \times Z_9) \times (Z_2 \times Z_5)$

따라서 $Z_4 \times Z_{18} \times Z_{15}$와 $Z_3 \times Z_{36} \times Z_{10}$는 동형이다.

※ 문제 21~25에서 앞의 예제에서 처럼 주어진 위수를 갖는 군(동형에 관계 없이)을 모두 구하라.

문 21. 위수 8

풀 이

$Z_8,\ Z_2 \times Z_2 \times Z_2,\ Z_4 \times Z_2$

문 22. 위수 16

풀 이

$Z_2 \times Z_2 \times Z_2 \times Z_2$

$Z_2 \times Z_2 \times Z_4$

$Z_2 \times Z_8$

$Z_4 \times Z_4$

Z_{16}

문 23. 위수 32

풀 이

$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2$

$Z_4 \times Z_2 \times Z_2 \times Z_2$

$Z_4 \times Z_4 \times Z_2$

$Z_8 \times Z_2 \times Z_2$

$Z_8 \times Z_4$

$Z_{16} \times Z_2$

Z_{32}

문 24. 위수 720

풀 이

$720 = 2^4 \cdot 3^2 \cdot 5^1$ 이므로

$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5$

$Z_4 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5$

$Z_4 \times Z_4 \times Z_3 \times Z_3 \times Z_5$

$Z_8 \times Z_2 \times Z_3 \times Z_3 \times Z_5$

$Z_{16} \times Z_3 \times Z_3 \times Z_5$

$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_5$

$Z_4 \times Z_2 \times Z_2 \times Z_9 \times Z_5$

$Z_4 \times Z_4 \times Z_9 \times Z_5$

$Z_8 \times Z_2 \times Z_9 \times Z_5$

$Z_{16} \times Z_9 \times Z_5 (\simeq Z_{720})$

문 25. 위수 1089

풀 이

$1089 = 3^2 \cdot 11^2$ 이므로

$Z_3 \times Z_3 \times Z_{11} \times Z_{11}$

$Z_9 \times Z_{11} \times Z_{11}$

$Z_3 \times Z_3 \times Z_{121}$

$Z_9 \times Z_{121} (\simeq Z_{1089})$

문 26. 위수 24인 가환군(동형에 관계 없이)은 몇 개 존재하는가? 위수 25인 가환군은? 그리고 위수가 (24)(25)인 가환군은?

풀 이

① $24 = 2^3 \cdot 3$이므로 위수 24인 가환군은 3개 존재한다.
실제로 $Z_2 \times Z_2 \times Z_2 \times Z_3$, $Z_4 \times Z_2 \times Z_3$, $Z_8 \times Z_3$ 이 존재한다.

② $25 = 5^2$이므로 위수 25d니 가환군은 2개 존재한다.
실제로. $Z_5 \times Z_5$, Z_{25} 이 존재한다.

③ $(24)(25) = 2^3 \cdot 3 \cdot 5^2$이므로 위수 (24)(25)인 가환군은 6개 존재한다.
실제로 $Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_5 \times Z_5$, $Z_4 \times Z_2 \times Z_3 \times Z_5 \times Z_5$, $Z_8 \times Z_3 \times Z_5 \times Z_5$, $Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_{25}$, $Z_4 \times Z_2 \times Z_3 \times Z_{25}$, $Z_8 \times Z_3 \times Z_{25}$이 존재한다.

문 27. 문제 26에서 제안된 사고를 따라 서로소인 양의 정수 m과 n에 대하여 다음을 증명하라. 만약 위수 m인 가환군(동형에 관계 없이)이 r개, 위수 n인 가환군(동형에 관계 없이)이 s개 존재한다면, 위수 mn인 가환군(동형에 관계 없이)은 rs개 존재함을 보여라.

풀 이

문 28. 문제 27을 이용하여 위수가 $(10)^5$인 가환군(동형에 관계 없이)의 수를 결정하라.

풀 이

위수가 2^5인 경우는 총 7개 존재한다. 또한 위수가 5^5인 경우도 총 7개 존재한다. 따라서 문제 27에 의하여 $(2^5, 5^5) = 1$이므로 위수가 $(10)^5$인 가환군(동흉에 관계 없이)의 수는 49(= 7·7)개 존재한다.

문 29.

(a) Let p be prime number. Fill in the second row of the table to give the number of abelian groups of order p^n. up to isomorphism.

n	2	3	4	5	6	7	8
number of groups	①	②	③	④	⑤	⑥	⑦

풀 이

① 2 ② 3 ③ 5 ④ 7 ⑤ ⑥ ⑦

(b) Let p, q and r be distinct prime numbers. Use the table you created to find the number of abelian groups. up to isomorphism of the given order.

① $p^3 \cdot q^4 \cdot r^7$ ② $(qr)^7$ ③ $q^5 \cdot r^4 \cdot q^3$

풀 이

문 30. Indicate schematically a Cayley digraph for $Z_m \times Z_n$ for the generating set $S = \{(1,0),(0,1)\}$

풀 이

문 31. Consider Cayley digraphs with two arc types. a solid are with an arrow and a dashed one with no arrow. and consisting of two regular $n-gons$. for $n \geq 3$. with solid arc sides. one inside the other. with dashed arcs joining the vertices of the outer $n-gon$ to the inner one. Figure 7.9(b) shows such a Cayley digraph with $n=3$. and Figure 7.11(b) shows one with $n=4$. The arrows on the outer $n-gon$ may have the same (clockwise or counterclockwise) direction as those on the inner $n-gon$. or they may have the opposite direction. Let G be a group with such a Cayley digraph.

풀 이

- 생략함 -

문 32. 참, 거짓을 판정하라.

(a) G_1, G_2가 군이면 $G_1 \times G_2$는 항상 $G_2 \times G_1$과 동형이다.

풀 이 T

$\phi : G_1 \times G_2 \rightarrow G_2 \times G_1, \phi(a,b) = (b,a)\ (a \in G_1, b \in G_2)$라 하자.
그러면 ϕ는 동형사상이다. (보이는 것은 생략!)
따라서 옳은 명제이다.

(b) 각 성분군에서의 계산방법을 안다면 그 군의 외직적에서의 계산은 쉽다.

풀 이 T

외직적에서의 계산은 각 성분군끼리 연산을 근거로 정의 되어 있으므로 각 성분군에서의 계산방법을 안다면 외직적의 계산을 쉽게 할 수 있다. 따라서 옳은 명제이다.

(c) 외직적은 유한위수를 갖는 군으로서만 할 수 있다.

풀 이 F

유한생성 가환군의 기본정리에 의하여 무한 위수를 Z 또한 외직적의 형태로 나타낼 수 있음을 안다.

(d) 소수를 위수로 갖는 군은 두 개의 비자명 진부분군의 내직적이 될 수 없다.

풀 이 T

소수를 위수로 갖는 군은 부분군으로 자명군과 자기 자신만을 갖는다. 따라서 두 개의 비자명 진부분군의 내직적으로 나타낼 수 없다.

(e) $Z_2 \times Z_4$는 Z_8과 동형이다.

풀 이 F

$Z_2 \times Z_4$는 순환군이 아니지만 Z_8은 순환군이다. 따라서 동형이 아니다.

(f) $Z_2 \times Z_8$는 S_8과 동형이다.

풀 이 F

$Z_2 \times Z_8$의 위수는 16이지만 S_8의 위수는 8!이다. 따라서 위수가 다르므로 동형이 아니다.

(g) $Z_3 \times Z_8$는 S_4와 동형이다.

풀 이 F

$Z_3 \times Z_8$는 순환군이지만 S_4는 순환군이 아니다.

(h) $Z_4 \times Z_8$에 속하는 모든 원소는 위수 8을 갖는다.

풀 이 F

(반례) $(0,0)$의 위수는 1이다.

(i) $Z_{12} \times Z_{15}$의 위수는 60이다.

풀 이 F

$Z_{12} \times Z_{15}$의 위수는 $180(=12 \cdot 15)$이다.

하지만 $Z_{12} \times Z_{15}$의 원소 중에서 최대로 갖을 수 있는 위수는 60$((12,15)=60)$이다.

(j) m과 n이 서로소이든 아니든 $Z_m \times Z_n$은 mn개의 원소를 갖는다.

풀 이 T

$Z_m \times Z_n = \{(a,b) | a \in Z_m, b \in Z_n\}$이므로 $Z_m \times Z_n$의 원소의 개수는 mn개 임을 알 수 있다.

문 33. 모든 비자명 가환군이 두 개의 비자명 진부분군의 내직적이 되지 않음을 예를 들어 설명하라.

풀 이

Z_p에서 Z_p는 비자명 진부분군을 갖지 않는다. 단, p는 소수

그렇기 때문에 두 개의 비자명 진부분군의 내직적이 될 수 없다.

문 34.

(a) How many subgroups of $Z_5 \times Z_6$ are isomorphic to $Z_5 \times Z_6$.

풀 이

$Z_5 \times Z_6$는 순환군이고 순환군의 부분군이 그 자신과 동형이 되는 경우는 그 자신으로 유일하다.

(b) How many subgroups of $Z \times Z$ are isomorphic to $Z \times Z$.

풀 이

$nZ \times mZ$는 $Z \times Z$의 부분군임에 자명하다.

또한 $\phi : Z \times Z \to nZ \times mZ, \phi(a,b) = (na, mb)\ (a,b \in Z)$라 하자. 그러면 ϕ는 동형사상임을 쉽게 보일 수 있다. 따라서 $Z \times Z \simeq nZ \times mZ$이다.

그러므로 $Z \times Z$와 동형인 $Z \times Z$의 부분군 $nZ \times mZ$는 무수히 많다.

문 35. 소수의 위수를 갖지 않는 두 개의 비자명 부분군의 내직적이 아닌 비자명군의 예를 드시오.

풀 이

S_3는 위수 6를 갖는다. 또한 부분군으로 $A_3(=\langle(123)\rangle),,\langle(13)\rangle,\langle(12)\rangle,\langle(23)\rangle,\{1\}$를 갖는다. 하지만 S_3는 어떠한 두 개의 비자명 부분군의 내직적으로 표현되지 않음을 알 수 있다.

문 36. 참, 거짓을 판정하라.

(a) 소수를 위수로 갖는 모든 가환군은 순환적이다.

풀 이 T

G를 위수를 소수 p를 갖는 가환군이라 하자.
$a\neq e$인 임의의 $a\in G$에 대하여 $\langle a\rangle$는 G의 부분군임에 자명하다.
그러면 라그랑지 정리에 의하여 $|\langle a\rangle|||G|=p$이다.
따라서 $\langle a\rangle$의 위수는 1 또는 p이다.
하지만 위수가 1이면 $a\neq e$인 가정에 모순이다.
따라서 $\langle a\rangle$의 위수는 p이다. 그러므로 $G=\langle a\rangle$이다.
그러므로 G는 순환군이다.

(b) 소수의 멱을 위수로 갖는 모든 가환군은 순환적이다.

풀 이 F

V_4는 가환군이면서 위수로 4를 갖는다. 즉. 소수 2의 멱을 위수로 갖는다.
하지만 V_4는 순환적이지는 않다.

(c) Z_8은 $\{4,6\}$에 의해서 생성된다.

풀 이 F

$\langle 4,6\rangle=\{0,2,4,6\}$으로 Z_8과 다름을 알 수 있다.

(d) Z_8은 $\{4,5,6\}$에 의해서 생성된다.

풀 이 T

이미 $Z_8=\langle 5\rangle$임을 알고 있다. 따라서 5를 포함하는 $\langle 4,5,6\rangle$에 의하여 생성된 부분군은 Z_8이다.

(e) 모든 유한군은 정리 11.12(유한생성가환군의 기본정리)에 의해 동형에 관계없이 분류될 수 있다.

풀 이 F

D_3는 유한군이다.
하지만 유한생성가환군의 기본정리에 의하여 동형에 관계없이 분류될 수 없다.
이유는 가환이라는 조건이 성립하지 않기 때문이다.

(f) 같은 $Betti$수를 갖는 두 개의 유한 생성 가환군은 동형이다.

풀 이 F

(반례) $Z_2\times Z_2$와 Z_4는 같은 $Betti$수 0를 갖지만 동형은 아니다.

⑼ 5의 배수를 위수로 갖는 모든 가환군은 위수 5인 순환부분군을 포함한다.

풀 이 T

G는 유한생성가환군의 기본정리에 의하여 $G \simeq Z_{p_1^{r_1}} \times \cdots \times Z_{p_s^{r_s}}$이다.

가정에서 G는 5의 배수를 위수로 가지므로 $\exists i \ s.t. \ p_i = 5$

한편, $Z_{5^{r_i}}$에서 $\langle 5^{r_i-1} \rangle$는 위수 5인 순환부분군이다. ($\because \ |\langle 5^{r_i-1} \rangle| = \frac{|Z_{5^{r_i}}|}{(5^{r_i-1}, 5^{r_i})} = \frac{5^{r_i}}{(5^{r_i-1}, 5^{r_i})} = 5$)

$H \equiv \{0\} \times \cdots \times \langle 5^{r_i-1} \rangle \times \cdots \times \{0\}$이라 하자.

그러면 H는 G의 위수 5인 순환부분군임에 자명하다.

따라서 5의 배수를 위수로 갖는 가환군은 위수 5인 순환부분군을 포함한다.

(→ 일반적으로 소수 p의 배수를 위수로 갖는 가환군은 위수 p인 순환부분군을 포함한다.)

⑽ 4의 배수를 위수로 갖는 모든 가환군은 위수 4인 순환부분군을 포함한다.

풀 이 F

(반례) $Z_2 \times Z_2$는 4를 위수로 갖는 가환군이지만 $Z_2 \times Z_2$의 원소 중 갖을 수 있는 최대의 위수는 2이다.

따라서 위수4를 갖는 생성원이 존재하지 않는다. 그러므로 잘못된 명제이다.

⑾ 6의 배수를 위수로 갖는 모든 가환군은 위수 6인 순환부분군을 포함한다.

풀 이 T

G를 6의 배수를 위수로 갖는 임의의 가환군이라 하자.

그러면 G는 2의 배수이므로 ⑼에 의하여 위수 2인 순환부분군 H를 갖는다.

또한 G는 3의 배수이므로 ⑼에 의하여 위수 3인 순환부분군 K를 갖는다.

H, K는 순환군이므로 $\exists a, b \in G \ s.t. \ H = \langle a \rangle, K = \langle b \rangle$

이제 $\langle a+b \rangle$라 하자.

그러면 $\langle a+b \rangle$는 자명하게 위수 6인 순환부분군이 된다.

따라서 6의 배수를 위수로 갖는 모든 가환군은 위수 6인 순환부분군을 포함한다.

⑿ 모든 유한 가환군은 $Betti$수를 0으로 갖는다.

풀 이 T

어떤 유한 가환군 G를 $Betti$수가 0이 아니라고 가정하자.

그러면 유한생성가환군의 기본정리에 의하여 $G \simeq Z_{s_1} \times Z_{s_2} \times \cdots \times Z_{s_r} \times Z \times \cdots$ 이다. 단, s_i는 소수의 멱

따라서 G는 무한히 많은 원소를 갖는다. 하지만 이는 유한이라는 가정에 모순이다.

따라서 모든 유한 가환구는 $Betti$수를 0으로 갖는다.

문 37. p와 q를 서로 다른 소수라 하자. 위수 p^r을 갖는 가환군(동형에 관계 없이)의 개수와 위수 q^r을 갖는 가환군(동형에 관계 없이)의 개수를 어떻게 비교할 수 있는가?

풀 이

위수 p^r을 갖는 가환군의 개수는 r에 의하여 결정된다.

따라서 위수 p^r과 q^r을 갖는 가환군의 개수는 서로 같다는 사실을 알 수 있다.

문 38. G가 위수 72인 가환군이라 하자.

(a) G는 위수 8인 부분군을 몇 개나 가지는가? 그 이유는?

풀 이

- 생략함 -

(b) G는 위수 4인 부분군을 몇 개나 가지는가? 그 이유는?

풀 이

- 생략함 -

문 39. G가 가환군이라 하자. G에서 유한위수를 갖는 원소는 부분군을 형성함을 보여라. 이 부분군이 G의 비꼬임 부분군(torsion subgroup)이라 한다.

풀 이

$T \equiv \{g \in G \mid |g| < \infty\}$라 하자.

① $e \in G$에 대하여 $|e| = 1 < \infty$이므로 $e \in T \neq \varnothing$이다.

② $T \subseteq G$임에 자명하다.

③ 임의의 $a, b \in T$에 대하여 $\exists n, m \; s.t. \; |a| = n, |b| = m$ 이고

$(a \cdot b)^{nm} = a^{mn} \cdot b^{mn}$ ($\because G: abel$) $= e^n \cdot e^m = e$이므로 $|a \cdot b| | nm$이다. 따라서 $|a \cdot b| < \infty$이므로 $a \cdot b \in T$이다.

게다가 $|a| = |a^{-1}|$이므로 $a^{-1} \in T$ 이다.

($\because$ $|a| = n < \infty$이면 $e = (a \cdot a^{-1})^n = a^n \cdot (a^{-1})^n = e \cdot (a^{-1})^n = (a^{-1})^n$이므로 $|a^{-1}| | |a|$

역으로, $|a^{-1}| = m < \infty$이면 $e = (a \cdot a^{-1})^m = a^m \cdot (a^{-1})^m = a^m \cdot e = a^m$이므로 $|a| | |a^{-1}|$

따라서 $|a| = |a^{-1}|$ 이다.)

따라서 T는 G의 부분군이다. 이 때, T는 비꼬임 부분군이라 한다.

문 40. $Z_4 \times Z \times Z_3$의 비꼬임 부분군의 위수를 구하라. 또한 $Z_{12} \times Z \times Z_{12}$의 비꼬임 부분군의 위수를 구하라.

풀 이

$Z_4 \times Z \times Z_3$의 비꼬임 부분군은 $Z_4 \times \{0\} \times Z_3$이다. 따라서 비꼬임 부분군의 위수는 12이다.

또한 $Z_{12} \times Z \times Z_{12}$의 비꼬임 부분군은 $Z_{12} \times \{0\} \times Z_{12}$이다. 따라서 비꼬임 부분군의 위수는 144이다.

문 41. 0 이 아닌 실수의 곱셈에 대한 군 R^*의 비꼬임 부분군을 구하라.

풀 이

$T \equiv \{a \in R^* \mid \exists n \; s.t. \; a^n = 1\}$라 할 때, 다음을 만족하는 $a = \pm 1$로 유일하다.

따라서 R^*의 비꼬임 부분군은 $\{1, -1\}$이다.

문 42. 0이 아닌 복소수 곱셈에 대한 군 C^*의 비꼬임 부분군 T를 구하라.

풀 이

C^*의 비꼬임 부분군은 $|a| = 1$을 만족하는 $a \in G$로 복소평면상의 반지름이 1인 원주상의 모든 점들을 원소로 갖는다.

문 43. e**가 유일한 유한위수를 갖는 원소인 가환군을 비꼬임 없는 군(torsion free)이라 한다. 정리 11.12를 사용해서 모든 유한 생성 가환군은 비꼬임 부분과 비꼬임이 없는 부분군의 내직적임을 보여라. (**$\{e\}$**는 비꼬임 부분군이며 또한 비꼬임 없는 부분군이기도 함에 주목하라.)**

풀 이

G는 유한인 가환군이므로 유한생성가환군의 기본정리에 의하여 $G \simeq Z_{p_1^{e_1}} \times \cdots \times Z_{p_r^{e_r}} \times Z \times Z \times \cdots \times Z$이다. 이제 $H = Z_{p_1^{e_1}} \times \cdots \times Z_{p_r^{e_r}}, K = Z \times Z \times \cdots \times Z$ 라 하자.

그러면 $G = H \times K$이고 $H \cap K = \{e\}$임을 알 수 있다.

문 44. 정리 11.12에서의 G**의 분해에서 소수의 멱을 위수로 하는 부분은** $Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_r}$**의 꼴로도 쓰여질 수 있다. 여기서** $i = 1, 2, 3, \cdots, r-1$**에 대해** m_i**는** m_{i+1}**을 나눈다. 그 숫자** m_i**는 유일하게 존재함을 보일 수 있으며 이를** G**의 비꼬임 계수(torsion coefficient)라 한다.**

(a) $Z_4 \times Z_9$**의 비꼬임 계수를 구하라.**

풀 이

$Z_4 \times Z_9 \simeq Z_{36}$이므로 비꼬임 계수는 $m_1 = 36$ 이다.

(b) $Z_6 \times Z_{12} \times Z_{20}$**의 비꼬임 계수를 구하라.**

풀 이

$Z_6 \times Z_{12} \times Z_{20} \simeq Z_2 \times Z_{12} \times Z_{60}$이므로 비꼬임 계수는 $m_1 = 2, m_2 = 12, m_3 = 60$ 이다.

(c) 순환군의 직적의 비꼬임 계수를 구할 수 있는 계산 공식을 써보아라.

풀 이

$G \simeq Z_{p_1^{e_1}} \times \cdots \times Z_{p_r^{e_r}}$ 라 할 때, $p_i\,(1 \le i \le r)$인 서로 다른 소수라 하자.

그러면 $G \simeq Z_{p_1^{e_1} \cdots p_r^{e_r}}$ 이고, 이때 비꼬임 계수는 $m_1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ 이다.

문 46. 가환군의 직적은 가환군임을 보여라.

풀 이

$G_i\ (1 \le i \le n)$를 가환이라 하자.

임의의 $x, y \in \prod_{i=1}^{n} G_i$ 에 대하여

$a_i, b_i \in G_i$가 존재해서 $x = (a_1, a_2, \cdots, a_n), y = (b_1, b_2, \cdots, b_n)$를 만족한다.

그러면 $x \cdot y = (a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n)$

$= (a_1 \cdot b_1, a_2 \cdot b_2, \cdots, a_n \cdot b_n)$

$= (b_1 \cdot a_1, b_2 \cdot a_2, \cdots, b_n \cdot a_n)\,(\because G_i : abel)$

$= (b_1, b_2, \cdots, b_n) \cdot (a_1, a_2, \cdots, a_n) = y \cdot x$

따라서 $\prod_{i=1}^{n} G_i$ 는 가환이다.

문 47. G를 가환군이라 하자. H를 항등원 e와 위수 2인 G의 모든 원소들로 구성된 G의 부분집합이라 하면 H가 G의 부분군임을 보여라.

풀 이

$H \equiv \{g \in G \mid |g| = 2\} \cup \{e\}$라 하자.

① $e \in H \neq \varnothing$이고 $H \subseteq G$임은 자명하다.

② 임의의 $a \in H$에 대하여 $|a^{-1}| = |a| = 2$이므로 $a^{-1} \in H$이다.

③ 임의의 $a, b \in H$에 대하여 $(ab)^2 = a^2 \cdot b^2 = e \cdot e = e$ ($\because$ G: 가환) 이므로 $|ab| \mid 2$이다.

그러면 $|ab| = 1$또는 $|ab| = 2$이다. $|ab| = 1$이면 $ab = e \in H$ 이므로 성립한다. 또한 $|ab| = 2$이면 정의에 의하여 $ab \in H$이다.

따라서 H는 G의 부분군이다.

문 48. 문제 47의 방법에 따라 H가 항등원 e와 위수가 3인 모든 원소들로 구성된 가환군 G의 부분집합이라면 H는 부분군이 되는가를 결정하라. 또한 H가 항등원 e와 위수가 4인 모든 원소들로 구성된 가환군 G의 부분집합이라면 H는 부분군이 되는가? H가 항등원 e와 위수가 n인 원소들로 구성된 가환군 G의 부분집합이라면 어떤 양의 정수 n에 대하여 H가 G의 부분군이 되는가? 5장의 문제 48과 비교해보라.

풀 이

(a) $H_3 \equiv \{g \in G \mid |g| = 3\} \cup \{e\}$

① $e \in H_3 \neq \varnothing$이고 $H_3 \subseteq G$임은 자명하다.

② 임의의 $a \in H_3$에 대하여 $|a^{-1}| = |a| = 3$이므로 $a^{-1} \in H_3$이다.

③ 임의의 $a, b \in H_3$에 대하여 $(ab)^3 = a^3 \cdot b^3 = e \cdot e = e$ ($\because$ G: 가환) 이므로 $|ab| \mid 3$이다.

그러면 $|ab| = 1$또는 $|ab| = 3$이다. $|ab| = 1$이면 $ab = e \in H_3$ 이므로 성립한다. 또한 $|ab| = 3$이면 정의에 의하여 $ab \in H_3$이다.

따라서 H_3는 G의 부분군이다.

(b) $H_4 \equiv \{g \in G \mid |g| = 4\} \cup \{e\}$

H_4같은 경우도 위의 (a)에서의 ①, ②는 쉽게 보일 수 있다. 하지만 ④는 보일 수 없다. 즉. 닫혀 있음을 보장해 주지 못한다.

실제로 $|ab| \mid 4$이면 $|ab| = 1, 2$또는 4이다. 1과 4인 경우는 위와 동일한 방법으로 쉽게 $ab \in H_4$임을 보일 수 있지만 $|ab| = 2$인 경우는 $ab \in H_4$임을 보장해 주지 못한다.

따라서 H_4는 부분군이 된다는 보장을 할 수 없다.

(c) $H_n \equiv \{g \in G \mid |g| = n\} \cup \{e\}$

$n = p$ (단, p는 소수)인 경우에 한하여 H_n는 가환군 G의 부분군이다.

① $e \in H_p \neq \varnothing$이고 $H_p \subseteq G$임은 자명하다.

② 임의의 $a \in H_p$에 대하여 $|a^{-1}| = |a| = p$이므로 $a^{-1} \in H_p$이다.

③ 임의의 $a, b \in H_p$에 대하여 $(ab)^p = a^p \cdot b^p = e \cdot e = e$ ($\because$ G: 가환) 이므로 $|ab| \mid p$이다.

그러면 $|ab| = 1$또는 $|ab| = p$이다. $|ab| = 1$이면 $ab = e \in H_p$ 이므로 성립한다. 또한 $|ab| = p$이면 정의에 의하여 $ab \in H_p$이다.

따라서 H_p는 G의 부분군이다.

문 49. G가 가환이라는 가정이 없을 경우 문제47의 반례를 구하라.

풀 이

$G=S_3$라 하자. 그러면 $H=\{1,(1\,2),(2\,3),(1\,3)\}$이다.
하지만 H는 G의 부분군이 아니다. 왜냐하면 $(1\,2)(2\,3)=(1\,2\,3)\notin T$ 이기 때문이다.

문 50. H와 K가 군이고 $G=H\times K$라 하자. 자연스럽게 H와 K가 군 G의 부분군으로 나타날 수 있음을 상기하자. 이 부분군 H (실제로 $H\times\{e\}$)와 K (실제로 $\{e\}\times K$)가 다음 성질을 가짐을 보여라.

(a) G의 모든 원소는 적당한 $h\in H$와 $k\in K$에 대해 hk의 꼴이다.

풀 이

$(h,k)=(h,e)(e,k)$

(b) 모든 $h\in H$와 $k\in K$에 대하여 $hk=kh$이다.

풀 이

$(h,e)(e,k)=(h,k)=(e,k)(h,e)$

(c) $H\cap K=\{e\}$

풀 이

$H\cap K=(H\times\{e\})\cap(\{e\}\times K)=(H\cap\{e\})\times(\{e\}\cap K)=\{e\}\times\{e\}=\{e\}$

문 51. H와 K를 앞의 문제에서 나열된 세 성질을 만족하는 군 G의 부분군이라 하자. 각 $g\in G$에 대해 $h\in H$이고 $k\in K$에 대해 표현 $g=hk$는 유일함을 보여라. 그리고 g를 (h,k)로 다시 이름 붙이면 G는 구조적으로 $H\times K$와 일치함을 보여라.
[힌트: $H\times K$ 위에서 군 연산을 이렇게 다시 이름 붙임으로써 G위에서 연산에 대응한다. 즉, g_1이 (h_1,k_1)로 g_2가 (h_2,k_2)로 다시 이름 붙여지면 g_1g_2는 (h_1h_2,k_1k_2)로 됨을 보여라.]

풀 이

(유일성) $g=h_1\cdot k_1=h_2\cdot k_2$라 하자. 단, $h_1,h_2\in H,k_1,k_2\in K$
그러면 $h_2^{-1}\cdot h_1=k_2\cdot k_1^{-1}\in H\cap K=\{e\}$이다.
따라서 $h_1=h_2,k_1=k_2$이다.
(동형성) $g_1=h_1\cdot k_1,g_2=h_2\cdot k_2$라 하자. 단, $h_1,h_2\in H,k_1,k_2\in K$
그러면 $g_1\cdot g_2=(h_1,k_1)\cdot(h_2,k_2)=(h_1\cdot h_2,k_1\cdot k_2)$
$\phi:G\to H\times K,\phi(g)=(h,k)$라 하자. 단, $h\in H,k\in K$
그러면 $g_1\cdot g_2=(h_1,k_1)\cdot(h_2,k_2)=(h_1\cdot h_2,k_1\cdot k_2)$이므로 $\phi(g_1\cdot g_2)=\phi(g_1)\cdot\phi(g_2)$이다.
위의 유일성에 의하여 단사이고 전사임에는 ϕ의 정의에 의하여 자명하다.
따라서 ϕ는 동형사상이다. 그러므로 $G\simeq H\times K$이다.

문 52. 유한 가환군이 순환군이 아닐 필요충분조건은 그 군이 적당한 소수 p에 대하여 $Z_p \times Z_p$와 동형인 부분군을 포함하는 것임을 보여라.

풀 이

(←) G가 순환군이라 하자.
그러면 군 G의 부분군 H 또한 순환군이다.
하지만 $Z_p \times Z_p$는 순환군이 아니다. 이는 모순이다.
그러므로 G는 순환군이 아니다.
(→) G는 유한인 가환군이므로
유한생성 가환군의 기본정리에 의하여 $G \simeq Z_{p_1^{e_1}} \times Z_{p_2^{e_2}} \times \cdots \times Z_{p_r^{e_r}}$이라 하자.
이 때, $p_i (1 \le i \le n)$이 서로 다른 소수이면 G는 순환군이다.
따라서 적어도 하나는 같은 소수가 존재함을 알 수 있다.
즉, $i \neq j$에 대하여 $p_i = p_j$인 i, j가 존재한다.
일반성을 잃지 않으면서 $i = 1, j = 2$라 하자. 그러면 $G \simeq Z_{p^{e_1}} \times Z_{p^{e_2}} \times Z_{p_3^{e_3}} \times \cdots \times Z_{p_r^{e_r}}$ 이다.
이 때, $H \simeq Z_p \times Z_p \times \{0\} \times \cdots \times \{0\}$이라 하자. 그러면 H는 G의 부분군임에 자명하다.
또한 $H \simeq Z_p \times Z_p$이다.
따라서 G가 순환군이 아니면 $Z_p \times Z_p$와 동형인 부분군 H가 존재함을 알 수 있다.

문 53. 만약 유한 가환군이 위수를 소수 p의 멱으로 가지면, 그 군에 있는 모든 원소는 위수를 p의 멱으로 가짐을 증명하라. 가환성의 가정이 생략되어도 좋은가? 그 이유는?

풀 이

G의 위수가 p^r이라 하자. 그러면 $a \in G$에 대하여 라그랑지 정리에 의하여 $|a| | p^r$이다.
따라서 $|a| = 1, p, p^2, \cdots, p^r$ 중에 하나임을 알 수 있다. 즉, a의 원소의 위수는 p의 멱을 가진다.
가환성은 위의 증명과정에서 사용되지 않았으므로 가환성이란 가정은 생략되어도 좋다.

문 54. G, H와 K를 유한 생성된 가환군이라 하자. 만약 $G \times K$가 $H \times K$와 동형이면, $G \simeq H$임을 보여라.

풀 이

$G \simeq Z_{p_1^{e_1}} \times Z_{p_2^{e_2}} \times \cdots \times Z_{p_r^{e_r}}$,
$H \simeq Z_{q_1^{f_1}} \times Z_{q_2^{f_2}} \times \cdots \times Z_{q_s^{f_s}}$,
$K \simeq Z_{n_1^{g_1}} \times Z_{n_2^{g_2}} \times \cdots \times Z_{n_t^{g_1}}$ 라 하자.
단, p_i, q_i, n_i는 소수
$G \times K \simeq H \times K$이므로 인자들의 분해가 같음을 알 수 있다.
여기서 $G \times K$와 $H \times K$ 둘 다 마지막에는 K의 인자들을 가지고 있으므로 결국 G와 H의 분해에서 인자들의 표현은 같음을 알 수 있다. 따라서 $G \simeq H$이다.

문 55. S_n은 $\{(1,2),(1,2,\cdots,n)\}$에 의해서 생성됨을 보여라.

[힌트: r을 움직일 때 $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}$은 호환 $(1,2),(2,3),(3,4),\cdots,(n-1,n),(n,1)$을 만들게 됨을 보이고, 모든 호환은 이들 호환의 곱임을 보인다.]

풀 이

$r=0$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}=(1,2)$

$r=1$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}=(1,2,\cdots,n)(1,2)(1,2,\cdots,n)^{n-1}=(2,3)$

$r=2$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}=(1,2,\cdots,n)^2(1,2)(1,2,\cdots,n)^{n-2}=(3,4)$

$\vdots$

$r=n-1$일 때, $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}=(1,2,\cdots,n)^{n-1}(1,2)(1,2,\cdots,n)^1=(n,1)$

임을 알 수 있다.

또한 임의의 호환 (i,j)에 대하여

$(i,j)=(i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j)(j-2,j-1)\cdots(i+1,i+2)(i,i+1)$이 성립한다.

임의의 치환은 유한개의 순환치환의 곱으로 나타낼 수 있으며 순환치환은 유한개의 호환의 곱으로 나타낼 수 있다. 즉, 임의의 치환은 유한개의 호환의 곱으로 나타낼 수 있다.

따라서 S_n상의 임의의 치환은 각각의 r에 대하여 $(1,2,\cdots,n)^r(1,2)(1,2,\cdots,n)^{n-r}$의 유한번의 곱에 의하여 나타낼 수 있다. 따라서 $S_n=\{(1,2),(1,2,3,\cdots,n)\}$이다.

※ 문제 1~15에서 주어진 사상 ϕ가 준동형사상인지를 결정하라.

[힌트: $\phi: G \to G'$에 대하여 만약 $\phi^{-1}(\{e\})$가 좌, 우잉여류가 같게 되는 부분군이 아니며, ϕ는 준동형사상이 아니다.]

문 1. $\phi(n)=n$으로 주어진 덧셈에 대한 $\phi: Z \to R$

풀 이 Yes

임의의 $a, b \in Z$ 에 대하여 $\phi(a+b)=a+b=\phi(a)+\phi(b)$이 성립한다. 따라서 ϕ는 준동형사상이다.

문 2. $\phi(x)=[x]$, $[x]$는 x를 넘지 않는 최대의 정수로 주어진 덧셈에 대한 $\phi: R \to Z$

풀 이 No

(반례) $\phi(1.5+1.6)=\phi(3.1)=3$이지만 $\phi(1.5)+\phi(1.6)=1+1=2$이다.

문 3. $\phi(x)=|x|$로 주어진 곱셈에 대한 $\phi: R^* \to R^*$

풀 이 Yes

임의의 $a, b \in R^*$에 대하여 $\phi(a\cdot b)=|a\cdot b|=|a|\cdot|b|=\phi(a)\cdot\phi(b)$이 성립한다. 따라서 ϕ는 준동형사상이다.

문 4. 호제법에서 주어진 것 처럼 $\phi(x)=$(2로 나누었을 때 x의 나머지)로 정의된 $\phi: Z_6 \to Z_2$

풀 이 Yes

임의의 $a, b \in Z_6$에 대하여 $a=2k_1+l_1, b=2k_2+l_2$인 $l_1, l_2 \in Z_2, k_1, k_2 \in Z$ $(0 \le k_1, k_2 \le 3)$가 존재한다고 한다. 그러면 $\phi(a+b)=\phi(2k_1+l_1+2k_2+l_2)=l_1+l_2=\phi(2k_1+l_1)+\phi(2k_2+l_2)=\phi(a)+\phi(b)$가 성립한다. 따라서 ϕ는 준동형사상이다.

문 5. 호제법에서 주어진 것 처럼 $\phi(x)=$(2로 나누었을 때 x의 나머지)로 정의된 $\phi: Z_9 \to Z_2$

풀 이 No

(반례) $\phi(5+_9 7)=\phi(3)=1$이지만 $\phi(5)+_2\phi(7)=1+_2 1=0$이다.

문 6. $\phi(x)=2^x$으로 주어진 $\phi: R \to R^*$, 단 R는 덧셈, R^*는 곱셈에 대한 군.

풀 이 Yes

임의의 $a, b \in R$ 에 대하여 $\phi(a+b)=2^{a+b}=2^a\cdot 2^b=\phi(a)\cdot\phi(b)$이 성립한다. 따라서 ϕ는 준동형사상이다.

문 7. $\phi_i(g_i)=(e_1, e_2, \cdots, g_i, \cdots, e_r)$로 정의된 $\phi: G_i \to G_1 \times G_2 \times \cdots \times G_i \times \cdots \times G_r$. 단, $g_i \in G_i$이며 e_j는 G_j의 항등원이다. 이것은 단사사상이다. 예제 13.8와 비교해 보자.

풀 이 Yes

임의의 $a_i, b_i \in G_i$ 에 대하여

$\phi(a_i\cdot b_i)=(e_1, e_2, \cdots, a_i\cdot b_i, \cdots, e_r)=(e_1, e_2, \cdots, a_i, \cdots, e_r)\cdot(e_1, e_2, \cdots, b_i, \cdots, e_r)=\phi(a)\cdot\phi(b)$이 성립한다.

따라서 ϕ는 준동형사상이다.

문 8. G가 어떤 군이고 $g \in G$에 대하여 $\phi(g) = g^{-1}$로 정의된 $\phi : G \to G$.

풀 이 No

$\phi(ab) = (ab)^{-1} = b^{-1}a^{-1}$이고 $\phi(a)\phi(b) = a^{-1}b^{-1}$이다.
그러므로 $b^{-1}a^{-1} \neq a^{-1}b^{-1}$이면 ϕ는 준동형사상이 아니다.
실제로 S_3에서 $\phi(\rho_1\mu_1) = \phi(\mu_3) = \mu_3^{-1} = \mu_3$이지만 $\phi(\rho_1)\phi(\mu_1) = \rho_1^{-1}\mu_1^{-1} = \rho_2\mu_1 = \mu_2$ 이다.

문 9. F를 모든 차수의 도함수를 갖는 R에서 R로 대응하는 함수의 덧셈에 대한 군이라 하자. $\phi(f) = f''$, f의 2차 도함수로 정의된 $\phi : F \to F$.

풀 이 Yes

임의의 $f, g \in F$ 에 대하여 $\phi(f+g) = (f+g)'' = f'' + g'' = \phi(f) + \phi(g)$이 성립한다.
따라서 ϕ는 준동형사상이다.

문 10. F를 R에서 R로 대응하는 모든 연속 함수들의 덧셈에 대한 군이라 하자. R는 실수들의 덧셈에 대한 군이고 $\phi(f) = \int_0^4 f(x)dx$으로 정의된 $\phi : F \to R$

풀 이 Yes

임의의 $f, g \in F$ 에 대하여 $\phi(f+g) = \int_0^4 (f+g)(x)dx = \int_0^4 f(x)dx + \int_0^4 g(x)dx = \phi(f) + \phi(g)$이 성립한다.
따라서 ϕ는 준동형사상이다.

문 11. F를 R에서 R로 대응하는 모든 함수의 덧셈에 대한 군이고 $\phi(f) = 3f$로 정의된 $\phi : F \to F$.

풀 이 Yes

임의의 $f, g \in F$ 에 대하여 $\phi(f+g) = 3(f+g) = 3f + 3g = \phi(f) + \phi(g)$이 성립한다.
따라서 ϕ는 준동형사상이다.

문 12. M_n을 실수를 요소로 갖는 모든 $n \times n$행렬의 덧셈에 대한 군이라 하고 R를 실수의 덧셈에 대한 군이라 하자. $A \in M_n$에 대하여 $\phi(A) = \det(A)$, A의 행렬식의 값으로 정의된 $\phi : M_n \to R$.

풀 이 No

(반례) $\phi\left(\begin{bmatrix}1&0\\0&1\end{bmatrix} + \begin{bmatrix}0&0\\0&1\end{bmatrix}\right) = det\ \begin{bmatrix}1&0\\0&2\end{bmatrix} = 2$ 이지만 $\phi\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}\right) + \phi\left(\begin{bmatrix}0&0\\0&1\end{bmatrix}\right) = det\ \begin{bmatrix}1&0\\0&1\end{bmatrix} + \det\ \begin{bmatrix}0&0\\0&1\end{bmatrix} = 1 + 0 = 1$ 이다.

문 13. M_n과 R를 문제 12에서와 같이 하자. $A \in M_n$에 대하여 대각합(trace) $tr(A)$는 왼쪽 상단에서 오른쪽 하단에 이르는 A의 주 대각선 상의 요소의 합일 때, $\phi(A) = tr(A)$로 정의된 $\phi : M_n \to R$.

풀 이 Yes

임의의 $(a_{ij})_{n\times n}, (b_{ij})_{n\times n} \in M_n$ 에 대하여 $\phi((a_{ij})_{n\times n}) = tr((a_{ij})_{n\times n}) = \sum_{i=1}^{n} a_{ii}$ 이고, 이 때,

$\phi((a_{ij})_{n\times n}, + (b_{ij})_{n\times n}) = \phi((a_{ij}+b_{ij})_{n\times n}) = \sum_{i=1}^{n}(a_{ii}+b_{ii}) = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = \phi((a_{ij})_{n\times n}) + \phi((b_{ij})_{n\times n})$ 이 성립한다. 따라서 ϕ는 준동형사상이다.

문 14. J_n**을 역행렬을 갖는** $n\times n$**행렬의 곱셈에 대한 군이라 하고** R**를 실수의 덧셈에 대한 군이라 하자.** $\phi(A)=tr(A)$**로 정의된** $\phi: J_n \to R$**, 단** $tr(A)$**는 문제 13에서 정의되어 있다.**

풀 이 No

(반례) $\phi(I_n \cdot I_n)=\phi(I_n)=tr(I_n)=n$이지만 $\phi(I_n)+\phi(I_n)=tr(I_n)+tr(I_n)=n+n=2n$ 이다.

문 15. F**를 모든** $x\in R$**에서 0이 아닌** R**에서** R**로 대응하는 모든 연속 함수의 곱셈에 대한 군이라 하자.** R^***를 0이 아닌 실수들의 곱셈에 대한 군이라 하자.**

$\phi(f)=\int_0^1 f(x)dx$**로 정의된** $\phi: F \to R^*$

풀 이 No

$\phi(x\cdot x)=\int_0^1 x^2dx=\left[\frac{1}{3}x^3\right]_0^1=\frac{1}{3}$ 이지만 $\phi(x)\cdot\phi(x)=\int_0^1 xdx\cdot\int_0^1 xdx=\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$이다.

※ 문제 16~24에서 Computer the indicated quantities for the given homomorphism ϕ **(See Ex 46)**

문 16. $Ker(\phi)$ **for** $\phi: S_3 \to Z_2$ **in Example 13.3**

풀 이

$\phi(\sigma)=\begin{cases}0 & ,\sigma: \text{우치환}\\ 1 & ,\sigma: \text{기치환}\end{cases}$ 이므로 따라서 $Ker(\phi)=A_3$ 이다.

문 17. $Ker(\phi)$ **and** $\phi(25)$ **for** $\phi: Z \to Z_7$ **such that** $\phi(1)=4$

풀 이

$(4,7)=1$이므로 4는 Z_7의 생성원이다. 따라서 $\phi(7n)=0\,(n\in Z)$를 만족한다.

따라서 $Ker(\phi)=7Z$ 이다.

또한 Z_7에서 $\phi(25)=\phi(1+\cdots+1)=25\cdot\phi(1)=100=2$ 이므로 $\phi(25)=2$이다.

문 18. $Ker(\phi)$ **and** $\phi(18)$ **for** $\phi: Z \to Z_{10}$ **such that** $\phi(1)=6$

풀 이

$|\langle 6\rangle|=\frac{10}{(10,6)}=5$이므로 $\phi(5n)=0\,(n\in Z)$이다. 따라서 $Ker(\phi)=5Z$ 이다.

또한 Z_{10}에서 $\phi(18)=18\cdot\phi(1)=108=8$이므로 $\phi(18)=8$이다.

문 19. $Ker(\phi)$ **and** $\phi(20)$ **for** $\phi: Z \to S_8$ **such that** $\phi(1)=(1\,4\,2\,6)(2\,5\,7)$

풀 이

$|(1\,4\,2\,6)(2\,5\,7)|=|(1\,4\,2\,5\,7\,6)|=6$이므로 $\phi(6n)=(1)\,(n\in Z)$이다. 따라서 $Ker(\phi)=6Z$ 이다.

또한 $\phi(20)=(1\,4\,2\,5\,7\,6)^{20}=(1\,4\,2\,5\,7\,6)^2=(1\,2\,7)(4\,5\,6)$이므로 $\phi(20)=(1\,2\,7)(4\,5\,6)$ 이다.

문 20. $Ker(\phi)$ **and** $\phi(3)$ **for** $\phi: Z_{10} \to Z_{20}$ **such that** $\phi(1)=8$

풀 이

$|\langle 8\rangle|=\frac{20}{(20,8)}=5$이므로 $\phi(5n)=0$이다. 따라서 $Ker(\phi)=\{0,5\}$이다. 또한 $\phi(3)=3\cdot\phi(1)=24=4$이다.

문 21. $Ker(\phi)$ and $\phi(14)$ for $\phi : Z_{24} \to S_8$ such that $\phi(1) = (2\,5)(1\,4\,6\,7)$

풀 이

$|(2\,5)(1\,4\,6\,7)| = 4$ 이므로 $\phi(4n) = (1)$이다. 따라서 $Ker(\phi) = \{0, 4, 8, 12, 16, 20\}$이다.
또한 $\phi(14) = \{(2\,5)(1\,4\,6\,7)\}^{14} = \{(2\,5)(1\,4\,6\,7)\}^2 = (1\,6)(4\,7)$이다.

문 22. $Ker(\phi)$ and $\phi(-3, 2)$ for $\phi : Z \times Z \to Z$ such that $\phi(1, 0) = 3$ and $\phi(0, 1) = -5$

풀 이

$\phi(n, m) = n \cdot \phi(1, 0) + m \cdot \phi(0, 1) = 3n - 5m = 0$이므로 $n = 5Z, m = 3Z$ 이다.
따라서 $Ker(\phi) = 5Z \times 3Z$ 이다.
또한 $\phi(-3, 2) = -3 \cdot \phi(1, 0) + 2 \cdot \phi(0, 1) = -9 - 10 = -19$

문 23. $Ker(\phi)$ and $\phi(4, 6)$ for $\phi : Z \times Z \to Z \times Z$ such that $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$

풀 이

$\phi(n, m) = n \cdot \phi(1, 0) + m \cdot \phi(0, 1) = (2n, -3n) + (-m, 5m) = (2n - m, -3n + 5m) = (0, 0)$이므로 $n = m = 0$
이다. 따라서 $Ker(\phi) = \{(0, 0)\}$이다.
또한 $\phi(4, 6) = 4 \cdot \phi(1, 0) + 6 \cdot \phi(0, 1) = (8, -12) + (-6, 30) = (2, 18)$이다.

문 24. $Ker(\phi)$ and $\phi(3, 10)$ for $\phi : Z \times Z \to S_{10}$ such that $\phi(1, 0) = (3\,5)(2\,4)$
and $\phi(0, 1) = (1\,7)(6\,10\,8\,9)$

풀 이

$|(2\,5)(2\,4)| = 2, |(1\,7)(6\,10\,8\,9)| = 4$이므로 따라서 $Ker(\phi) = 2Z \times 4Z$ 이다.
또한 $\phi(3, 10) = \{(3\,5)(2\,4)\}^3 \{(1\,7)(6\,10\,8\,9)\}^{10} = (3\,5)(2\,4)(6\,8)(10\,9)$이다.

문 25. Z에서 Z위로 대응하는 준동형사상은 몇 개 존재하는가?

풀 이

$\phi(1) = 1$ 또는 -1이므로 Z에서 Z위로 대응하는 준동형사상은 $\phi(n) = n$ 또는 $-n$ 이다.
따라서 2개 존재한다.

문 26. Z에서 Z로 대응하는 준동형사상은 몇 개 존재하는가?

풀 이

$\phi_n : Z \to nZ \subseteq Z, \phi_n(x) = nx \ (x \in Z)$라 하자.
그러면 ϕ_n는 준동형사상임에 자명하다.
따라서 Z에서 Z로 대응하는 준동형사상은 n개 만큼 존재한다.
즉, Z만큼 존재한다.
그러므로 무수히 많다고 볼 수 있다.

문 27. Z에서 Z_2로 대응하는 준동형사상은 몇 개 존재하는가?

풀 이

$\phi(1) = 0$ 또는 1이다.
따라서 Z에서 Z_2로 대응하는 준동형사상은 $\phi(n) = 0$ 또는 $\phi(n) \equiv n (\mathrm{mod} 2)$ 이다.
따라서 2개 존재한다.

문 28. G**가 군이고** $g \in G$**라 하자.** $\phi_g : G \to G$**가** $x \in G$**에 대하여** $\phi_g(x) = gx$**로 정의되어져 있다고 하면 어떤** $g \in G$**에 대하여** ϕ_g**가 준동형사상이 되는가?**

풀 이

ϕ_g가 준동형사상이라 하자. 그러면 $\phi_g(e) = g \cdot e = e$를 만족한다. 따라서 $g = e$이다.
그러므로 $g = e$일 때 ϕ_g는 준동형사상이다.

문 29. G**가 군이고** $g \in G$**라 하자.** $\phi_g : G \to G$**가** $x \in G$**에 대하여** $\phi_g(x) = gxg^{-1}$**로 정의되어져 있다고 하면 어떤** $g \in G$**에 대하여** ϕ_g**가 준동형사상이 되는가?**

풀 이

$\phi_g(e) = g \cdot e \cdot g^{-1} = e$이므로 임의의 $g \in G$와 임의의 $x, y \in G$에 대하여
$\phi_g(x+y) = g \cdot (x+y) \cdot g^{-1} = g \cdot x \cdot g^{-1} + g \cdot y \cdot g^{-1} = \phi_g(x) + \phi_g(y)$를 만족한다.
따라서 모든 $g \in G$에 대하여 ϕ_g가 준동형사상이 된다.

※ 문제 30과 31에서 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 30. ***준동형사상(homomorphism)*** **은** $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$**을 만족하는 사상이다.**

풀 이

준동형사상은 임의의 $x, y \in G$에 대하여 $\phi(x \cdot y) = \phi(x) * \phi(y)$를 만족하는 G에서 G'로의 사상이다.
단, $\cdot$는 G에서의 연산이고, $*$는 G'에서의 연산이다.

문 31. $\phi : G \to G'$**이 군 준동형사상이라 하자.** ϕ**의** ***핵(Kernel)*** **은** $\{x \in G \mid \phi(x) = e'\}$**이다.**
단, e'**는** G'**의 항등원이다.**

풀 이

옳은 정의이다.

문 32. 참, 거짓을 판정하라.

(a) A_n**이** S_n**의 정규부분군이다.**

풀 이 T

$A_n \leq B_n$임은 자명하다. 또한 $|S_n : A_n| = 2$ 이므로 $A_n \lhd S_n$이다.

(b) 어떤 두 개의 군 G**와** G'**에 대해서도** G**에서** G'**로 대응하는 준동형사상은 존재한다.**

풀 이 T

$\phi : G \to G', \phi(x) = e'$이라 하자. 그러면 ϕ는 준동형사상임에 자명하다.
단, e'는 G'의 항등원이다.

(c) 모든 준동형사상은 1-1사상이다.

풀 이 F

$\phi : G \to G', \phi(x) = e'$는 준동형사상이지만 1-1은 아니다. 단, e'는 G'의 항등원이다.

(d) 하나의 준동형사상이 1-1일 필요충분조건은 그것의 핵은 항등원 한 원소의 군으로 구성되어 있다.

풀 이 T

$(\leftarrow)$ $\phi(a)=\phi(b) \Rightarrow \phi(a)\cdot\phi(b)^{-1}=e'$

$\Rightarrow \phi(a\cdot b^{-1})=e'$ ($\because \phi$:준동형사상)

$\Rightarrow Ker(\phi)=\{e\}$이므로 $a\cdot b^{-1}=e$

$\Rightarrow a=b$

따라서 ϕ는 1-1이다.

단, $\phi: G \rightarrow G'$인 사상이며, e는 G의 항등원이고 e'는 G'의 항등원이다.

$(\rightarrow)$ 귀류법 증명!

$a \neq e$인 $a \in Ker(\phi)$가 존재한다고 하자.

그러면 $\phi(a)=e=\phi(e)$를 만족한다. 가정에 의하여 ϕ는 1-1이므로 $a=e$이다.

하지만 이는 모순이다. 따라서 $Ker(\phi)=\{e\}$이다.

(e) 6개의 원소를 갖는 군의 적당한 준동형사상에 대한 상은 4개의 원소를 가질 수도 있다.

풀 이 F

$|\phi(G)|=4 \nmid 6=|G|$이므로 위의 명제는 틀린 명제이다.

(f) 6개의 원소를 갖는 군의 어떤 준동형사상에 대한 상은 12개의 원소를 가질 수도 있다.

풀 이 F

$|\phi(G)|=12 \nmid 6=|G|$이므로 위의 명제는 틀린 명제이다.

(g) 6개의 원소를 갖는 군에서 12개의 원소를 갖는 군으로 대응하는 준동형사상은 존재한다.

풀 이 T

$\phi: Z_6 \rightarrow Z_{12}, \phi(x)=0\ (x \in Z_6)$라 하자. 그러면 ϕ는 준동형사상임에 자명하다.

(h) 6개의 원소를 갖는 군에서 10개의 원소를 갖는 군으로 대응하는 준동형사상은 존재한다.

풀 이 T

$\phi: Z_6 \rightarrow Z_{10}, \phi(x)=0\ (x \in Z_6)$라 하자. 그러면 ϕ는 준동형사상임에 자명하다.

(i) 준동형사상이 공집합을 핵으로 가질 수도 있다.

풀 이 F

$\phi: G \rightarrow G'$에 대하여 ϕ가 준동형사상이면 $\phi(e)=e'$는 항상 만족한다.

따라서 $e \in Ker(\phi) \neq \varnothing$이다.

단, e는 G의 항등원이고 e'는 G'의 항등원이다.

(j) 무한군에서 유한군으로 대응하는 준동형사상을 가지는 것은 불가능하다.

풀 이 F

가능하다. 문제 16 참조

※ 문제 33~43에서, 주어진 군에 대한 비자명 준동형사상이 존재한다면 그 예를 들어라. 만약 그런 준동형사상이 존재하지 않으면 그 이유를 설명하라.

문 33. $\phi : Z_{12} \to Z_5$

풀 이 존재하지 않는다.

$\phi(1) = 0, 1, 2, 3, 4$ 중에 하나 값을 갖는다.

① 우선 $\phi(1) = 0$이면 ϕ는 자명준동형사상이다. 따라서 $\phi(1) \neq 0$ 이다.

② $\phi(1) = k$이면 $\phi(5) = 5 \cdot \phi(1) = 5 \cdot k = 0$이고 5는 Z_{12}에서 생성원이므로 $\phi(n) = \phi(5m) = m \cdot \phi(5) = 0$이므로 ϕ는 자명준동형사상이다. 따라서 $\phi(1) \neq k$ 단, $k = 1, 2, 3, 4$

따라서 ϕ가 준동형사상이면 ϕ는 자명준동형사상이다. 즉, 비자명 준동형사상은 존재하지 않는다.

[다른 풀이]

$12 \nmid 5$이므로 비자명 준동형사상은 존재하지 않는다.

문 34. $\phi : Z_{12} \to Z_4$

풀 이 존재한다.

(예) $\phi(n) \equiv n (\mathrm{mod} 4)$라 하자. 그러면 ϕ는 준동형사상이다. 문제 4 참조.

문 35. $\phi : Z_2 \times Z_4 \to Z_2 \times Z_5$

풀 이 존재한다.

(예) $\phi(n,m) = (n,0)$ 단, $(n,m) \in Z_2 \times Z_4$

문 36. $\phi : Z_3 \to Z$

풀 이 존재하지 않는다.

$\phi(Z_3)$는 Z의 유한인 부분군이다. Z는 무한군이므로 유한인 부분군 $\{0\}$만을 갖는다.

따라서 $\phi(Z_3) = \{e\}$이다. 하지만 이는 가정에 모순된다.

따라서 비자명 준동형사상은 존재하지 않는다.

문 37. $\phi : Z_3 \to S_3$

풀 이 존재한다.

(예) $\phi(n) = \rho_n$ 단, $n \in Z_3$ 라 하자. 그러면 ϕ는 준동형사상이다.

문 38. $\phi : Z \to S_3$

풀 이 존재하지 않는다.

문 39. $\phi : Z \times Z \to 2Z$

풀 이 존재한다.

(예) $\phi(n,m) = 2n$ 단, $(n,m) \in Z \times Z$ 라 하자. 그러면 ϕ는 준동형사상이다.

문 40. $\phi : 2Z \to Z \times Z$

풀 이 존재한다.

(예) $\phi(2n) = (2n, 0)$ 단, $n \in Z$ 라 하자.

그러면 ϕ는 준동형사상이다.

문 41. $\phi : D_4 \to S_3$

풀 이 존재한다.

(예) $\phi(\sigma) = \begin{cases} (1\ 2) & , odd\ \sigma \in D_4 \\ (1) & , even\ \sigma \in D_4 \end{cases}$ 라 하자.

그러면 ϕ는 준동형사상이다.

문 42. $\phi : S_3 \to S_4$

풀 이 존재한다.

(예) $\phi(\sigma) = \begin{cases} (1\ 2) & , odd\ \sigma \in S_4 \\ (1) & , even\ \sigma \in S_4 \end{cases}$ 라 하자.

그러면 ϕ는 준동형사상이다.

문 43. $\phi : S_4 \to S_3$

풀 이 존재한다.

(예) $\phi(\sigma) = \begin{cases} (1\ 2) & , odd\ \sigma \in S_3 \\ (1) & , even\ \sigma \in S_3 \end{cases}$ 라 하자.

그러면 ϕ는 준동형사상이다.

문 44. $\phi : G \to G'$**를 군의 준동형사상이라 하자.**
만약 $|G|$**가 유한이면** $|\phi(G)|$**도 유한이며** $|G|$**의 약수임을 보여라.**

풀 이

$|G| = n$ 이라 하자.

$\phi(G) = \{\phi(g) | g \in G\}$이므로 따라서 $|\phi(G)| \leq n$ 이다.

즉, $|\phi(G)|$ 는 유한이다.

또한 임의의 $a \in G$에 대하여 $\{\phi(a)\}^n = \phi(a^n) = \phi(e) = e'$이므로 $|\phi(G)| | |G|$이다.

문 45. $\phi : G \to G'$**를 군의 준동형사상이라 하자.**
만약 $|G'|$**가 유한이면** $|\phi(G)|$**도 유한이며** $|G'|$**의 약수임을 보여라.**

풀 이

$|G'|$가 유한이면 G'의 부분군 $\phi(G)$의 위수 또한 유한이다.

또한 라그랑지 정리에 의하여 부분군 $\phi(G)$의 위수는 $|G'|$의 약수이다.

문 46. 군 G가 $\{a_i | i \in I\}$에 의해 생성된다고 하자. 단, I는 적당한 첨수의 집합이고 $a_i \in G$이다. 임의의 $i \in I$에 대하여 $\phi(a_i) = \mu(a_i)$를 만족하는 G에서 G'으로의 두 준동형사상을 $\phi : G \to G'$와 $\mu : G \to G'$라 하자. $\phi = \mu$임을 증명하여라.
[예를 들어 순환군의 준동형사상은 완전히 군의 생성원의 값에 의하여 결정되어 진다.]
[힌트: 정리 7.6과 준동형사상의 정의 13.1을 이용.]

풀 이

임의의 $a \in G$에 대하여

$r_1, r_2, \cdots, r_n \in Z$가 존재해서 $a = a_{i_1}^{r_1} \cdot a_{i_2}^{r_2} \cdots a_{i_n}^{r_n}$ ($i_n \in I$)를 만족한다.

그러면 $\phi(a) = \phi(a_{i_1}^{r_1} \cdot a_{i_2}^{r_2} \cdots a_{i_n}^{r_n})$

$$= \phi(a_{i_1}^{r_1}) \cdot \phi(a_{i_2}^{r_2}) \cdots \phi(a_{i_n}^{r_n})$$

$$= \phi(a_{i_1})^{r_1} \cdot \phi(a_{i_2})^{r_2} \cdots \phi(a_{i_n})^{r_n}$$

$$= \mu(a_{i_1})^{r_1} \cdot \mu(a_{i_2})^{r_2} \cdots \mu(a_{i_n})^{r_n}$$

$$= \mu a_{i_1}^{r_1}) \cdot \mu(a_{i_2}^{r_2}) \cdots \mu(a_{i_n}^{r_n})$$

$$= \mu(a_{i_1}^{r_1} \cdot a_{i_2}^{r_2} \cdots a_{i_n}^{r_n})$$

$$= \mu(a)$$

($\because$ ϕ, μ는 준동형사상이고 $\phi(a_i) = \mu(a_i)\ (i \in I)$)

따라서 $\phi = \mu$ 이다.

문 47. $|G|$가 소수일 때, 어떤 군의 준동형사상 $\phi : G \to G'$도 자명 준동형 사상이거나 1-1사상 중의 하나이어야 함을 보여라.

풀 이

$|G|$가 소수이면

$Ker(\phi)$의 위수는 G의 위수의 약수이므로($\because$문제44) $|Ker(\phi)| = 1$ 또는 p이다.

① $|Ker(\phi)| = 1$인 경우

$Ker(\phi) = \{e\}$이므로 필요충분하게 1-1 사상임을 알 수 있다.

② $|Ker(\phi)| = p$인 경우

$Ker(\phi) \leq G$이고 $|Ker(\phi)| = p = |G|$이므로 $Ker(\phi) = G$이다.

따라서 $\phi(G) = e'$를 만족한다.

그러므로 ϕ는 자명 준동형사상이다. 단, e'는 G'의 항등원이다.

문 48. 우치환의 부호는 $+1$이고 기치환의 부호는 -1이다.

$sgn_n(\sigma) = \sigma$**의 부호**

로 정의된 사상 $sgn_n : S_n \to \{1, -1\}$은 S_n에서 곱셈에 대한 군 $\{1, -1\}$ 위로 대응하는 준동형사상임에 주목하라. 핵은 무엇인가? 예저 13.3과 비교하라.

풀 이

$Ker(sgn_n) = A_n$이고, 곱셈군 $\{1, -1\}$은 Z_2와 동형이다.

문 49. G, G'와 G''가 군이고 $\phi: G \to G'$와 $\gamma: G' \to G''$가 준동형사상이면 합성 사상 $\gamma\phi: G \to G''$도 준동형사상임을 보여라.

풀 이

임의의 $a, b \in G$에 대하여

$$\begin{aligned}\gamma\phi(ab) &= \gamma\{\phi(a\cdot b)\}\\ &= \gamma\{\phi(a)\cdot\phi(b)\}\\ &= \gamma\{\phi(b)\}\cdot\gamma\{\phi(b)\}\\ &= \gamma\phi(a)\cdot\gamma\phi(b)\end{aligned}$$

를 만족한다.

따라서 합성사상 $\gamma\phi: G \to G''$ 또한 준동형사상이 된다.

문 50. $\phi: G \to H$를 군 준동형사상이라 하자. $\phi[G]$가 아벨군일 필요충분조건은 모든 $x, y \in G$에 대하여 $xyx^{-1}y^{-1} \in \ker\phi$를 만족하는 것임을 보여라.

풀 이

(→) 임의의 $a, b \in G$에 대하여

$$\begin{aligned}\phi(a\cdot b\cdot a^{-1}\cdot b^{-1}) &= \phi(a)\cdot\phi(b)\cdot\phi(a^{-1})\cdot\phi(b^{-1}) \quad (\because\ \phi\text{: 준동형사상 })\\ &= \phi(a)\cdot\phi(b)\cdot\phi(a)^{-1}\cdot\phi(b)^{-1} \quad (\because\ \phi\text{: 준동형사상 })\\ &= \phi(a)\cdot\phi(a)^{-1}\cdot\phi(b)\cdot\phi(b)^{-1} \quad (\because \phi[G]\text{: 아벨군 })\\ &= e\cdot e = e\end{aligned}$$

따라서 $a\cdot b\cdot a^{-1}\cdot b^{-1} \in \ker\phi$ 이다.

(←) 임의의 $x, y \in \phi[G]$에 대하여

$a, b \in G$가 존재해서 $x = \phi(a), y = \phi(b)$를 만족한다.

그러면

$$\begin{aligned}e &= \phi(a\cdot b\cdot a^{-1}\cdot b^{-1})\\ &= \phi(a)\cdot\phi(b)\cdot\phi(a^{-1})\cdot\phi(b^{-1}) \quad (\because\ \phi\text{: 준동형사상 })\\ &= \phi(a)\cdot\phi(b)\cdot\phi(a)^{-1}\cdot\phi(b)^{-1} \quad (\because\ \phi\text{: 준동형사상 })\\ &= x\cdot y\cdot x^{-1}\cdot y^{-1}\end{aligned}$$

이다.

따라서 $xy = yx$이다.

그러므로 $\phi[G]$는 아벨군이다. 단, e는 H의 항등원이다.

문 51. G가 어떤 군이고 a가 G의 원소라 하자. $\phi: Z \to G$를 $\phi(n) = a^n$으로 정의되어 있다고 하면, ϕ가 준동형사상임을 보여라. ϕ의 상과 ϕ의 핵의 가능성을 기술하라.

풀 이

$\phi(0) = a^0 = 1$이고 ϕ가 준동형사상이므로 1은 G의 항등원이다.

이제 임의의 $n, m \in Z$에 대하여 $\phi(n+m) = a^{n+m} = a^n\cdot a^m = \phi(n)\cdot\phi(m)$ 이다.

따라서 ϕ는 준동형사상이고 이 때, G의 연산은 곱셈연산이다.

ϕ의 상은 $\langle a\rangle$이며, ϕ의 핵은 Z의 부분군이기 때문에 Z의 부분군 중에 하나이다.

문 52. $\phi: G \to G'$**가 핵** H**를 갖는 준동형사상이고** $a \in G$**라 하자.** $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$**임을 보여라.**

풀 이

$K \equiv \{x \in G \mid \phi(x) = \phi(a)\}$라 하자.

이제 $K = Ha$임을 보인다.

(→) 임의의 $x \in K$에 대하여

$$\begin{aligned}\phi(x) = \phi(a) &\Rightarrow \phi(x)\cdot\phi(a)^{-1} = e' \\ &\Rightarrow \phi(x)\cdot\phi(a^{-1}) = e' \\ &\Rightarrow \phi(x\cdot a^{-1}) = e' \\ &\Rightarrow x\cdot a^{-1} \in H \ (\because \ Ker(\phi) = H) \\ &\Rightarrow \exists\, h \in H \ s.t. \ x\cdot a^{-1} = h \\ &\Rightarrow x = ha \ (a \in G)\end{aligned}$$

따라서 $x \in Ha$ 이다.

(←) 임의의 $y \in Ha$에 대하여

$$\begin{aligned}\exists\, h \in H \ s.t. \ y = ha &\Rightarrow y\cdot a^{-1} = h \\ &\Rightarrow \phi(y\cdot a^{-1}) = e' \\ &\Rightarrow \phi(y)\cdot\phi(a^{-1}) = e' \\ &\Rightarrow \phi(y)\cdot\phi(a)^{-1} = e' \\ &\Rightarrow \phi(y) = \phi(a) \ (a \in G)\end{aligned}$$

따라서 $y \in K$이다. 단, e'는 G'의 항등원이다.

문 53. G**가 군이라 하자.** $h, k \in G$**이고,** $\phi: Z \times Z \to G$**가** $\phi(m,n) = h^m k^n$**으로 정의되어 있다고 하면,** ϕ**가 준동형사상이 될** h**과** k**에 관련된 필요충분조건을 구하고 그것을 증명하라.**

풀 이

(→) $\phi(1,0) = h^1 k^0 = h, \phi(0,1) = h^0 k^1 = k$이므로

$\phi(1,1) = \phi((1,0)+(0,1)) = \phi(1,0)\cdot\phi(0,1) = hk$이고

$\phi(1,1) = \phi((0,1)+(1,0)) = \phi(0,1)\cdot\phi(1,0) = kh$이 성립한다.

따라서 $kh = hk$이다.

(←) 임의의 $(n_1, m_1), (n_2, m_2) \in Z \times Z$ 에 대하여

$$\phi((n_1,m_1)+(n_2,m_2)) = \phi(n_1+n_2, m_1+m_2) = h^{n_1+n_2}k^{m_1+m_2} = (h^{n_1}k^{m_1})(h^{n_2}k^{m_2}) = \phi(n_1,m_1)\cdot\phi(n_2,m_2)$$

이 성립한다. ($\because \ hk = kh$)

따라서 ϕ는 준동형사상이다.

문 54. 앞의 연습문제에서 설명된 사상 ϕ**가 모든** $h, k \in G$**의 선택에 대해 준동형사상이 될** G**에 대한 필요충분조건을 구하라.**

풀 이

G가 군이라 하자.

$h, k \in G$이고, $\phi: Z \times Z \to G$가 $\phi(m,n) = h^m k^n$으로 정의되어 있다고 하면,

ϕ가 준동형사상이 될 필요충분조건은 임의의 $h, k \in G$에 대하여 $hk = kh$를 만족하는 것이다.

즉, G가 아벨군이다.

문 55. G**를 군이라 하고** h**를** G**의 원소** n**은 양의 정수라 하자.** $\phi : Z_n \to G$, $\phi(i) = h^i \ (0 \le i \le n)$**으로 정의 할 때,** ϕ**가 준동형사상이 될** G**에 대한 필요충분조건을 구하라.**

풀 이

ϕ가 준동형사상이 될 필요충분조건은 $|\phi(Z_n)| = |h| | n = |Z_n|$를 만족하는 것이다.

※ 문제 1~8에서 주어진 잉여군의 위수를 구하라.

문 1. $Z_6/\langle 3\rangle$

풀 이

$Z_6/\langle 3\rangle=\{\langle 3\rangle, 1+\langle 3\rangle, 2+\langle 3\rangle\}$이므로 $|Z_6/\langle 3\rangle|=3$ 이다.

문 2. $(Z_4\times Z_{12})/(\langle 2\rangle\times\langle 2\rangle)$

풀 이

$(Z_4\times Z_{12})/(\langle 2\rangle\times\langle 2\rangle)=\{\langle 2\rangle\times\langle 2\rangle, (1,0)+\langle 2\rangle\times\langle 2\rangle, (0,1)+\langle 2\rangle\times\langle 2\rangle, (1,1)+\langle 2\rangle\times\langle 2\rangle\}$이 므 로 주어진 잉여군의 위수는 4이다.

문 3. $(Z_4\times Z_2)/\langle (2,1)\rangle$

풀 이

$|(Z_4\times Z_2)/\langle (2,1)\rangle|=\frac{8}{2}=4.$

문 4. $(Z_3\times Z_4)/(\{0\}\times Z_5)$

풀 이

$(Z_3\times Z_5)/(\{0\}\times Z_5)\simeq Z_3$ 이므로 주어진 잉여군의 위수는 3 이다.

문 5. $(Z_2\times Z_4)/\langle (1,1)\rangle$

풀 이

$|(Z_2\times Z_4)/\langle (1,1)\rangle|=\frac{8}{4}=2$

문 6. $(Z_{12}\times Z_{18})/\langle (4,3)\rangle$

풀 이

$|(Z_{12}\times Z_{18})/\langle (4,3)\rangle|=\frac{12\cdot 18}{[3,6]}=\frac{12\cdot 18}{6}=36$

문 7. $(Z_2\times S_3)/\langle (1,\rho_1)\rangle$

풀 이

$|(Z_2\times S_3)/\langle (1,\rho_1)\rangle|=\frac{(2)\cdot(3!)}{[2,3]}=2$

문 8. $(Z_{11}\times Z_{15})/\langle (1,1)\rangle$

풀 이

$\langle (1,1)\rangle\simeq Z_{11}\times Z_{15}$ 이므로 $(Z_{11}\times Z_{15})/\langle (1,1)\rangle\simeq\{e\}$ 이다. 따라서 주어진 잉여군의 위수는 1이다.

※ 문제 9~15에서 주어진 잉여군에 속하는 원소의 위수를 구하라.

문 9. $Z_{12}/\langle 4\rangle$**에 속하는** $5+\langle 4\rangle$**.**

풀 이

$5+\langle 4\rangle = 1+\langle 4\rangle$이다. 따라서 주어진 원소의 위수는 4 이다.

문 10. $Z_{60}/\langle 12\rangle$**에 속하는** $26+\langle 12\rangle$**.**

풀 이

$26+\langle 12\rangle = 2+\langle 12\rangle$이다. 따라서 주어진 원소의 위수는 6 이다.

문 11. $(Z_3\times Z_6)/\langle (1,1)\rangle$**에 속하는** $(2,1)+\langle (1,1)\rangle$**.**

풀 이

$(2,1)+\langle (1,1)\rangle = (1,0)+\langle (1,1)\rangle$이다 따라서 주어진 원소의 위수는 3 이다.

문 12. $(Z_4\times Z_4)/\langle (1,1)\rangle$**에 속하는** $(3,1)+\langle (1,1)\rangle$**.**

풀 이

$(3,1)+\langle (1,1)\rangle = (2,0)+\langle (1,1)\rangle$ 이다
그러면 $(2,0)+\langle (1,1)\rangle+(2,0)+\langle (1,1)\rangle = (0,0)+\langle (1,1)\rangle$ 이다.
따라서 주어진 원소의 위수는 2이다.

문 13. $(Z_4\times Z_8)/\langle (0,2)\rangle$**에 속하는** $(3,1)+\langle (0,2)\rangle$**.**

풀 이

$2\{(3,1)+\langle (0,2)\rangle\} = (2,0)+\langle (0,2)\rangle$
$3\{(3,1)+\langle (0,2)\rangle\} = (1,1)+\langle (0,2)\rangle$
$4\{(3,1)+\langle (0,2)\rangle\} = (0,0)+\langle (0,2)\rangle$
이다. 따라서 주어진 원소의 위수는 4 이다.

문 14. $(Z_4\times Z_8)/\langle (1,2)\rangle$**에 속하는** $(3,3)+\langle (1,2)\rangle$**.**

풀 이

$\{(3,3)+\langle (1,2)\rangle\} = (2,1)+\langle (1,2)\rangle$
$2\{(3,3)+\langle (1,2)\rangle\} = (0,2)+\langle (1,2)\rangle$
$3\{(3,3)+\langle (1,2)\rangle\} = (1,1)+\langle (1,2)\rangle$
$4\{(3,3)+\langle (1,2)\rangle\} = (0,4)+\langle (1,2)\rangle$
$5\{(3,3)+\langle (1,2)\rangle\} = (0,1)+\langle (1,2)\rangle$
$6\{(3,3)+\langle (1,2)\rangle\} = (1,0)+\langle (1,2)\rangle$
$7\{(3,3)+\langle (1,2)\rangle\} = (0,3)+\langle (1,2)\rangle$
$8\{(3,3)+\langle (1,2)\rangle\} = \langle (1,2)\rangle$
이다. 따라서 주어진 원소의 위수는 8 이다.

문 15. $(Z_6 \times Z_8)/\langle(4,4)\rangle$**에 속하는** $(2,0)+\langle(4,4)\rangle$**.**

풀 이

$\{(2,0)+\langle(4,4)\rangle\}=(2,0)+\langle(4,4)\rangle$
$2\{(2,0)+\langle(4,4)\rangle\}=(4,0)+\langle(4,4)\rangle$
$3\{(2,0)+\langle(4,4)\rangle\}=\langle(4,4)\rangle$
이다. 따라서 주어진 원소의 위수는 3 이다.

문 16. 예제 8.7에서의 군 S_3**의 부분군** $H=\{\rho_0,\mu_1\}$**에 대하여** $i_{\rho_1}(H)$**를 계산하라.**

풀 이

$i_{\rho_1}(H)=\{\rho_1\rho_0\rho_1^{-1},\rho_1\mu_1\rho_1^{-1}\}=\{\rho_0,\mu_2\}$

※ 문제 17~19에서 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 17. A *normal subgroup* H **of** G **is one satisfying** $hG=Gh$ **for all** $h\in H$

풀 이

G의 *정규부분군* H는 G의 부분군이며 임의의 $g\in G$에 대하여 $gH=Hg$를 만족하는 것이다.

문 18. A *normal subgroup* H **of** G **is one satisfying** $g^{-1}hg\in H$ **for all** $h\in H$ **and all** $g\in G$

풀 이

옳은 정의이다.

문 19. An *automorphism* of a group G **is a homomorphism mapping** G **into** G**.**

풀 이

군 G의 *자기동형사상은* G에서 G로의 동형사상이다. 즉, 위의 조건에 일대일 대응이란 조건이 첨가되어야 한다.

문 20. 군 G**의 정규부분군에서 중요한 것은 무엇인가?**

풀 이

임의의 $g\in G$에 대하여 $gH=Hg$이 만족한다는 사실이 중요하다.
그 근거로는 잉여군 G/H가 이 조건이 성립하기 때문에 군을 이룬다.
따라서 잉여군 G/H를 배우기 위해서는 정규성이 중요한 부분을 차지한다.

문 21. 어떤 학생에게 H**가 가환군** G**의 정규부분군이면** G/H**도 가환임을 증명하도록 요청했다. 그 학생의 증명은 다음과 같이 시작되었다.**

G/H**가 가환임을 보여야 한다.** a**와** b**를** G/H**의 두 원소라 하자.**

(a) 이 증명을 읽은 교수님은 왜 이 학생의 답안지에서 터무니없는 말을 찾게 되는가?

풀 이

a와 b가 G/H의 두 원소가 될 수 없다.

(b) 이 학생은 어떻게 썼어야 되는가?

풀 이

aH와 bH가 G/H의 두 원소라 하자.

(c) 증명을 완성하라.

풀 이

임의의 $aH, bH \in G/H$에 대하여 $(aH)(bH) = (abH) = (baH) = (bH)(aH)$이 성립한다.
($\because$ G가 아벨군이므로 $ab = ba$)
따라서 G/H는 가환군이다.

문 22. 비꼬임군(torsion group)은 모든 원소가 유한 위수를 갖는 군이다. 어떤 학생에게 G가 비꼬임군이면 G의 모든 정규부분군 H에 대하여 G/H도 역시 비꼬임군임을 증명하도록 요청했다. 그 학생은 다음과 같이 썼다.

G/H의 각 원소가 유한 위수임을 보여야 한다. $x \in G/H$라 하자.

(a) 이 증명을 읽은 교수님은 왜 이 학생의 답안지에서 터무니없는 말을 찾게 되는가?

풀 이

x는 G의 원소이지 G/H의 원소가 아니다.

(b) 이 학생은 어떻게 썼어야 되는가?

풀 이

$xH \in G/H$라 하자.

(c) 증명을 완성하라.

풀 이

임의의 $xH \in G/H$에 대하여 G가 비꼬임군이므로 $\exists k \; s.t. \; |x| = k$
그러면 $(xH)^k = x^k H = eH = H$ 이다. 따라서 $|xH| | k$이다. 즉, $|xH| < \infty$ 이다.
그러므로 G/H의 각 원소는 유한 위수를 갖는다.

문 23. 참, 거짓을 판정하라.

(a) 잉여군 G/H에 대하여 이야기하는 것이 의미를 갖기 위한 필요충분조건은 N이 군 G의 정규부분군이다.

풀 이 T

N이 군 G의 정규부분군일 필요충분조건은 G/N이 군이다.

(b) 가환군 G의 모든 부분군은 G의 정규부분군이다.

풀 이 T

H를 군 G의 부분군이라 하자.
그러면 G가 가환이기 때문에 모든 $g \in G$에 대하여 $gH = Hg$를 만족한다.
따라서 H는 정규부분군이다.

(c) 가환군의 내적 자기동형사상은 항등함수 뿐이다.

풀 이 T

$I_g[H]=gHg^{-1}=H$ ($\because$ G : 가환)

(d) 유한군의 모든 잉여군은 다시 유한위수를 갖는다.

풀 이 T

$\phi: G \to G/H,\ \phi(x)=xH$ ($x \in G$) 인 표준 준동형사상이라 하자.
그러면 $|G/H|=|\phi(G)||\,|G|$ 을 만족한다.
따라서 G의 위수가 유한이면 잉여군 G/H 또한 위수가 유한이다.

(e) 비꼬임군의 모든 잉여군은 비꼬임군이다.

풀 이 T

임의의 $xH \in G/H$에 대하여 G가 비꼬임군이므로 $\exists k\ s.t.\ |x|=k$
그러면 $(xH)^k=x^kH=eH=H$ 이다. 따라서 $|xH||k$이다. 즉, $|xH|<\infty$ 이다.
그러므로 G/H의 각 원소는 유한 위수를 갖는다.

(f) 비꼬임이 없는 군의 모든 잉여군은 비꼬임이 없다.

풀 이 F

(반례)
Z는 비꼬임이 없는 군이다. 하지만 $Z/nZ \simeq Z_2$는 비꼬임이 있다.

(g) 가환군의 모든 잉여군은 가환이다.

풀 이 T

임의의 $aH, bH \in G/H$에 대하여 $(aH)(bH)=(abH)=(baH)=(bH)(aH)$이 성립한다.
($\because$ G가 아벨군이므로 $ab=ba$)
따라서 G/H는 가환군이다.

(h) 비가환군의 모든 잉여군은 비가환이다.

풀 이 F

(반례) S_3는 비가환군이다.
하지만 $S_3/A_3 \simeq Z_2$는 가환군이다.

(i) Z/nZ는 위수 n을 갖는 순환군이다.

풀 이 T

제1 동형정리에 의하여 $Z/nZ \simeq Z_n$ 이 성립한다.

(j) R/nR는 위수 n을 갖는 순환군이다. 여기서 $nR=\{nr|r \in R\}$이며 R는 덧셈에 대한 군이다.

풀 이 F

임의의 $a+nR=n\cdot\frac{a}{n}+nR$이고 $\frac{a}{n} \in R$이므로 $a \in nR$이다. 즉, $R/nR \simeq \{e\}$이다.
따라서 $n>1$에 대하여 위의 명제는 성립하지 않는다.

문 24. A_n은 S_n의 정규부분군임을 보이고 S_n/A_n을 계산하라. 즉, S_n/A_n과 동형인 이미 알려진 군을 구하라.

풀 이

① 항등치환은 우치환이므로 $A_n \neq \varnothing$ 이고, A_n이 S_n의 부분집합임에는 자명하다.

② 임의의 $\sigma, \tau \in A_n$에 대하여 $\sigma\tau^{-1} = (\text{우치환})(\text{우치환})^{-1} = (\text{우치환}) \in A_n$ 이 성립한다.

따라서 A_n은 S_n의 부분군이다.

③ 임의의 $\delta \in S_n$와 임의의 $\rho \in A_n$에 대하여

$\delta\rho\delta^{-1} = \begin{cases} (\text{우치환})(\text{우치환})(\text{우치환})^{-1} = (\text{우치환}) \in A_n & , \delta : (\text{우치환}) \\ (\text{기치환})(\text{우치환})(\text{기치환})^{-1} = (\text{우치환}) \in A_n & , \delta : (\text{기치환}) \end{cases}$ 이 성립한다.

따라서 A_n은 S_n의 정규부분군이다.

④ $\phi : S_n \to Z_2,\ \phi(\sigma) = \begin{cases} 0 & , \sigma : (\text{우치환}) \\ 1 & , \sigma : (\text{기치환}) \end{cases}$ 라 하자. 그러면 ϕ는 전사인 준동형사상이다.

ϕ의 핵은 A_n이므로 제1동형정리에 의하여 $S_n/A_n \simeq Z_2$ 이다. 실제로 $S_n/A_n = \{A_n, (1\ 2)A_n\}$ 이다.

문 25. Complete the proof of theorem 14.4 by showing that if H is a subgroup of a group G and if left coset multiplication $(aH)(bH) = (ab)H$ is well defined. then $Ha \subseteq aH$.

풀 이

- 생략함 -

문 26. 가환군 G의 비꼬임 부분군 T는 G의 정규부분군이며 G/T는 비꼬임이 없는 군임을 보여라. (문제 22 참조)

풀 이

$T = \{a \in G \mid |a| < \infty\}$라 하자.

① $|e| = 1$이므로 $e \in T \neq \varnothing$ 이다. 또한 $T \subseteq G$이다.

② 임의의 $a, b \in T$에 대하여 $\exists\, n, m \in Z^+\ s.t.\ a^n = e, b^m = e$

$(ab)^{nm} = (a^n)^m (b^m)^n = e^m e^n = e$이므로 $|ab| \mid nm$ 이다. 따라서 $|ab| < \infty$ 이다. 그러므로 $ab \in T$이다.

③ $|a| = s, |a^{-1}| = t$ 라 하자. 단, $s, t \in Z^+$

그러면 $(a^{-1})^s = (a^s)^{-1} = e^{-1} = e$ 이므로 $t \mid s$이다. 역으로 $(a)^t = ((a^{-1})^t)^{-1} = e^{-1} = e$ 이므로 $s \mid t$ 이다.

따라서 $|a| = |a^{-1}|$이므로 $a^{-1} \in T$ 이다.

③ ②, ③으로부터 T는 G의 부분군이다.

④ G가 가환군이므로 임의의 $g \in G$에 대하여 $Hg = gH$가 성립한다. 따라서 T는 G의 정규부분군이다.

⑤ T가 정규부분군이므로 G/T는 군임에 자명하다.

⑥ G가 비꼬임군이면 문제 22 에 의항 G/T 또한 비꼬임 군이 되어 모순된다.

따라서 G는 비꼬임이 없는 군이다. 즉, $\exists\, a \in G\ s.t.\ |a| = \infty$

이제 G/T를 비꼬임군이라 가정하자.

그러면 $\exists\, m \in N\ s.t.\ (aH)^m = a^m H = eH (= H)$ 이므로 $a^m \in H$이다. 가정에 의하여 H는 비꼬임 군이므로 $\exists\, k_0 \in N\ s.t.\ |a^m| = k_0$. 따라서 $|a| < \infty$임을 알 수 있다. 이는 a가 유한위수를 갖지 않는다는 가정에 모순된다. 그러므로 G/T는 비꼬임이 없는 군이다.

문 27. 만약 G의 내적 자기동형사상 i_g가 존재하여 $i_g(H)=K$이면 부분군 H는 부분군 K에 공액이라고 한다. 공액관계는 G의 부분군의 모임에서 동치 관계임을 증명하라.

풀 이

① (반사) $i_e[H]=eHe^{-1}=H$이므로 $H\sim H$ 이다.

② (대칭) $H\sim K$이면 즉, $i_g(H)=K$이면

$gHg^{-1}=K \Rightarrow H=g^{-1}Kg \Rightarrow (g^{-1})K(g^{-1})^{-1}=H$ 이고

이 때, $g^{-1}\in G$이 존재하므로 $i_{g^{-1}}(K)=H$ 이다. 따라서 $K\sim H$ 이다.

③ (추이) $K\sim H, K\sim S$이면 즉, $i_a(H)=K, i_b(K)=S$이면

$baHa^{-1}b^{-1}=(ba)H(ba)^{-1}=S$이므로 $i_{ba}(H)=S$ 이다. 따라서 $H\sim S$ 이다.

문 28. 앞의 문제에서 공액관계에 의해서 주어진 분할의 세포속의 포함관계를 이용해서 군 G의 정규부분군을 특정 지워라. 즉, 동치조건을 찾아라.

풀 이

정규부분군은 공액조건을 만족하는 군이 유일하게 자기 자신만을 갖는다. 즉, $\widetilde{H}$ 를 H와 서로 공액인 부분군들의 모임이라 할 때, $\widetilde{H}=\{H\}$을 만족하는 것이다.

문 29. 문제 27를 참고로 하여 $\{\rho_0,\mu_2\}$와 공액인 S_3 (예제 8.7)의 모든 부분군을 구하라.

풀 이

$\widetilde{\{\rho_0,\mu_2\}}=\{\{\rho_0,\mu_1\},\{\rho_0,\mu_2\},\{\rho_0,\mu_3\}\}$

문 30. H를 군 G의 정규부분군이라 하고 $m=(G:H)$라 하자. 모든 $a\in G$에 대하여 $a^m\in H$임을 보여라.

풀 이

$|G/H|=|G:H|=m$이므로

임의의 $a\in G$에 대하여 $(aH)^m=H \Rightarrow a^mH=H$ 를 만족한다. 따라서 $a^m\in H$ 이다.

문 31. 군 G의 정규부분군의 공통집합은 다시 G의 정규부분군임을 보여라.

풀 이

H, K를 각각 G의 정규부분군이라 하자.

e를 G의 항등원이라 할 때, $e\in H$이고 $e\in K$이므로 $H\cap K$는 공집합이 아니며 G의 부분집합임에는 자명하다. 또한 임의의 $a,b\in H\cap K$에 대하여

$a,b\in H$ 이고 $a,b\in K \Rightarrow ab^{-1}\in H$ 이고 $ab^{-1}\in K$ ($\because H\le G, K\le G$)를 만족한다.

따라서 $ab^{-1}\in H\cap K$이다. 그러므로 $H\cap K$는 G의 부분군이다.

이제 정규성을 보이면 충분하다.

임의의 $g\in G$에 대하여 $g(H\cap K)g^{-1}=gHg^{-1}\cap gKg^{-1}=H\cap K$ ($\because H\lhd G, K\lhd G$)를 만족한다.

따라서 $H\cap K$는 G의 정규부분군이다.

문 32. G의 고정된 부분집합 S를 포함하는 가장 적은 정규부분군에 대하여 언급하는 것은 의미있는 것임을 보여라. [힌트: 문제 31을 이용하라.]

풀 이

$K=\bigcap_{S\subseteq H} H$라 하자. 단, H는 S를 포함하는 G의 정규부분군이다.

그러면 K는 문제 31에 의하여 G의 정규부분군이다. 또한 S를 포함하는 최소의 정규부분군이다.

문 33. let G be a group. An element of G that can be expressed in the form $aba^{-1}b^{-1}$ for some $a,b\in G$ is a *commntator(교환자)* in G. The preceding exercise shows that there is a smallest normal subgroup C of a group G containing all commutators in G ; the subgroup C is the *commutator subgroup(교환자 부분군)* of G. Show that G/C is am abelian group.

풀 이

임의의 $aC,bC\in G/C$에 대하여 $(aC)(bC)(aC)^{-1}(bC)^{-1}=aba^{-1}b^{-1}C$ 이다.

가정에 의하여 C는 G에서 모든 가환자를 포함한다. 따라서 $(aC)(bC)(aC)^{-1}(bC)^{-1}=C$ 이다.

즉, $(aC)(bC)=C(bC)(aC)\Leftrightarrow abC=baC$ 이 성립한다. 따라서 G/C는 가환이다.

문 34. 유한군 G가 주어진 위수를 갖는 꼭 하나의 부분군 H만 갖는다면 H는 G의 정규부분군임을 보여라.

풀 이

H를 군 G의 부분군이라 하자. 임의의 $g\in G$에 대하여 $|gHg^{-1}|=|H|$임은 자명하다. 그러면 가정에 의하여 $gHg^{-1}=H$임을 알 수 있다. 따라서 H는 G의 정규부분군이다.

문 35. H와 N은 G의 부분군이며 N이 G에서 정규적이면, $H\cap N$은 H에서 정규적임을 보여라. $H\cap N$은 G에서는 정규적일 필요가 없음을 예로 들어 보여라.

풀 이 제 2 동형정리의 증명!!

① $H\cap N$가 H의 부분군임에는 자명하다.

② 임의의 $h\in H$에 대하여 $h(H\cap N)h^{-1}=hHh^{-1}\cap hNh^{-1}=H\cap N$ 이다.

($\because$ $h\in H$ 이므로 $hHh^{-1}=H$이고, $H\lhd G$이므로 $h\in H\subseteq G$에 대하여 $hNh^{-1}=N$ 이다.)

따라서 $H\cap N$는 G의 정규부분군이다. 즉, $H\cap N\lhd G$ 이다.

③ $G=N=S_3, H=\{\rho_0,\mu_1\}$이라 하자.

그러면 $N\lhd G$이지만 $N\cap H=H$는 G의 정규부분군이 아니다.

문 36. G가 고정된 유한위수 s를 갖는 부분군을 적어도 하나 포함하는 군이라 하자. 위수 s인 G의 모든 부분군의 공통집합은 G의 정규부분군임을 보여라.

[힌트: H가 위수 s를 갖는다면 모든 $x\in G$에 대하여 $x^{-1}Hx$로 위수 s를 갖음을 이용하라.]

풀 이

$K\equiv\cap\{H_i\leq G\,||H_i|=s\ (i\in I)\}$라 하자.

① H_i가 G의 부분군이므로 부분군의 교집합인 K 또한 G의 부분군이다.

② K가 위수 s를 갖는 최소의 부분군이다.

임의의 $g\in G$에 대하여 $|K|=s=|gKg^{-1}|$이므로 $gKg^{-1}\subseteq K$ 가 성립한다.

따라서 $Kg=gK$이므로 $K\lhd G$이다.

문 37.

(a) 군 G의 내적 자기동형사상은 함수합성에 대하여 군을 이루고 있음을 보여라.

풀 이

임의의 두 내적 자기동형사상의 합성은 준동형사상의 합성이 준동형사상이 된다는 사실로부터 준동형사상임을 알 수 있다. 또한 1-1대응의 합성은 1-1대응이므로 결국에는 자기동형사상의 합성이 자기동형사상이 됨을 안다. 또한 항등사상이 항등원의 역할을 하며, 역사상 또한 자기동형사상으로 역원의 역할을 한다는 사실을 안다. 그러므로 자기동형사상은 함수합성에 대하여 군을 이룸을 알 수 있다.

(b) 군 G의 내적 자기동형사상은 함수의 합성에 대한 모든 자기동형사상의 군의 정규부분군임을 보여라. [주의: 내적 자기동형사상들이 부분군을 이루고 있음을 반드시 보여라.]

풀 이

$H \equiv \{ i_a \mid i_a : G \to G, i_a(x) = axa^{-1} (a, x \in G) \}$**라 하자.**

① 임의의 $i_a, i_b \in H$ 에 대하여 ($\forall x \in G$)

$i_a(i_b(x)) = i_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = i_{ab}(x)$를 만족한다.

따라서 연산에 관해 닫혀있다.

i_e는 항등원의 역할을 함에 자명하다.

그러면 위의 $i_a(i_b(x)) = i_{ab}(x)$로부터 $i_a(i_{a^{-1}}(x)) = i_e$임을 알 수 있다. 즉, $i_{a^{-1}}$가 역원의 역할을 한다.

따라서 $H \leq G^*$ 이다.

② 임의의 $i_a \in H$와 임의의 $\phi \in G^*$에 대하여

$(\phi \cdot i_a \cdot \phi^{-1})(x) = (\phi \cdot i_a)(\phi^{-1}(x)) = \phi(a \cdot \phi^{-1}(x) \cdot a^{-1}) = \phi(a) \cdot \phi(\phi^{-1}(x) \cdot \phi(a^{-1}) = \phi(a) \cdot x \cdot \phi(a)^{-1} = i_{\phi(a)}(x)$

를 만족한다. 따라서 $\phi \cdot i_a \cdot \phi^{-1} = i_{\phi(a)} \in H$ 이다.

그러므로 $H \lhd G^*$이다. 단, G^*는 자기동형사상들의 모임이다.

문 38. $i_g : G \to G$가 항등 내적 자기동형사상 i_g가 되는 모든 $g \in G$들의 집합은 군 G의 정규부분군임을 보여라.

풀 이

$H = \{ g \in G \mid i_g = i_e \}$라 하자. $e \in H$ 이므로 $H \neq \varnothing$이다. 또한 정의에 의하여 $H \subseteq G$임에 자명하다.

임의의 $a, b \in H$ 에 대하여 ($\forall x \in G$)

$i_{ab}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = axa^{-1}$ ($\because i_b = i_e$)

$= x$ ($\because i_a = i_e$) $= exe^{-1} = i_e(x)$

를 만족한다. 또한 $i_a(x) = i_e(x) \Leftrightarrow axa^{-1} = exe^{-1} = x \Leftrightarrow x = a^{-1}x(a^{-1})^{-1} \Leftrightarrow i_{a^{-1}}(x) = i_e(x)$

따라서 $ab \in H$ 이고 $a^{-1} \in H$ 이다. 그러므로 H는 G의 부분군이다.

임의의 $a \in H$와 임의의 $g \in G$에 대하여 ($\forall x \in G$)

$i_{gag^{-1}}(x) = (gag^{-1})x(gag^{-1})^{-1} = g\{a(g^{-1}xg)a^{-1}\}g^{-1}$

$= g(g^{-1}xg)g^{-1}$ ($\because i_a = i_e$) $= exe = exe^{-1} = i_e(x)$

를 만족한다. 따라서 $gag^{-1} \in H$이다.

그러므로 H는 G의 정규부분군이다.

문 39. G와 G'가 군이며 H와 H'는 각각 G와 G'의 정규부분군이라 하고, ϕ가 G에서 G'로 대응하는 준동형사상이라 하자. 만약 $\phi(H)\subseteq H'$이면 ϕ가 자연스러운 준동형사상 $\phi_* : (G/H) \to (G'/H')$를 유도함을 보여라. (이 사실은 대수적 위상에 끊임없이 사용되어 진다.)

풀 이

임의의 $gH \in G/H$에 대하여 $\phi_*(gH) = \phi(g)H'$라 하자.

$g, g' \in G$에 대하여 $gH = g'H$라 하자.

그러면 $g^{-1}g' \in H$이고 따라서 $\phi(g^{-1}g') \in \phi[H] \subseteq H'$ 이다.

즉, $\phi(g^{-1})\cdot\phi(g') \in H'$이므로 $\phi(g)H' = \phi(g')H' \Leftrightarrow \phi_*(gH) = \phi_*(g'H)$이다.

따라서 ϕ_*는 잘 정의된 사상이다.

이제 임의의 $aH, bH \in G/H$에 대하여 ϕ는 준동형사상이므로

$\phi_*((aH)(bH)) = \phi_*(abH) = \phi(ab)H' = \phi(a)\cdot\phi(b)H' = \{\phi(a)H'\}\cdot\{\phi(b)H'\} = \phi_*(aH)\cdot\phi_*(bH)$

따라서 ϕ_*는 준동형사상이다.

문 40. Use the properties $\det(AB) = \det(A)\cdot\det(B)$ and $\det(I_n) = 1$ for $n \times n$ matrices to show the following;

(a) The $n \times n$ matrices with determinant 1 form a normal subgroup of $GL(n, R)$.

풀 이

$H \equiv \{A \in GL(n, R) \mid \det(A) = 1\}$라 하자.

① $\det(I_n) = 1$이므로 $H \neq \varnothing$이다. 또한 정의로부터 $H \subseteq GL(n, R)$임에는 자명하다.

임의의 $A, B \in H$에 대하여 $\det(AB^{-1}) = \det(A)\cdot\det(B^{-1}) = 1\cdot 1 = 1$이므로 따라서 $AB^{-1} \in H$ 이다.

그러므로 H는 $GL(n, R)$의 부분군이다.

② 임의의 $A \in H$와 임의의 $B \in GL(n, R)$에 대하여

$\det(B^{-1}AB) = \det(B^{-1})\cdot\det(A)\cdot\det(B) = \det(A) = 1$ 이므로 따라서 $BAB^{-1} \in H$이다.

따라서 H는 $GL(n, R)$의 정규부분군이다.

(b) The $n \times n$ matrices with determinant ± 1 form a normal subgroup of $GL(n, R)$.

풀 이

$H \equiv \{A \in GL(n, R) \mid \det(A) = \pm 1\}$라 하자.

① $\det(I_n) = 1$이므로 $H \neq \varnothing$이다. 또한 정의로부터 $H \subseteq GL(n, R)$임에는 자명하다.

임의의 $A, B \in H$에 대하여 $\det(AB^{-1}) = \det(A)\cdot\det(B^{-1}) = \pm 1$이므로 따라서 $AB^{-1} \in H$ 이다.

그러므로 H는 $GL(n, R)$의 부분군이다.

② 임의의 $A \in H$와 임의의 $B \in GL(n, R)$에 대하여

$\det(B^{-1}AB) = \det(B^{-1})\cdot\det(A)\cdot\det(B) = \det(A) = \pm 1$ 이므로 따라서 $BAB^{-1} \in H$이다.

따라서 H는 $GL(n, R)$의 정규부분군이다.

문 41. Let G be a group, and let $P(G)$ be the set of all subsets of G. For any $A, B \in P(G)$, let us define the product subset $AB = \{ab | a \in A, b \in B\}$.

(a) Show that multiplication of subsets is associative and has an identity element, but that $P(G)$ is not a group under this operation.

풀 이

① 결합법칙이 성립함을 보인다.

- 생략함 -

② 항등원을 갖는다.

e를 G의 항등원이라 하자. 그러면 $\{e\} \in P(G)$이고 곱셈의 정의에 의하여 $A\{e\} = \{e\}A = A$이 성립한다. 따라서 $\{e\}$는 $P(G)$의 항등원이다.

③ 위의 연산에 대하여 군을 이루지 않음을 보인다.

G가 자명군이면 군을 이룬다. 따라서 G가 자명군이 아니라고 가정하자.

임의의 $A \in P(G)$에 대하여 $B \in P(G)$가 존재해서 $AB = BA = \{e\}$라 하자.

그러면 임의의 $a_i \in A, b_j \in B$에 대하여 $a_i b_j = e$를 만족한다. 즉, a_i와 b_j는 역원의 관계에 있다.

하지만 G에서 역원은 유일하게 하나 존재한다. 그러므로 A와 B는 원소를 하나만 갖는다.

여기서 A, B는 임의의 원소이므로 $a_i = b_j = e$이다. 따라서 G는 자명군이다.

이는 가정에 모순된다. 따라서 $P(G)$는 이 연산에 관하여 군을 이루지 않는다.

(b) Show that if N is a normal subgroup of G, then the set of cosets of N is closed under the above operation on $P(G)$, and that this operation agrees with the multiplication given by the formula in Corollary 14.5.

풀 이

- 생략함 -

(c) Show (without using Corollary 14.5) that the cosets of N in G form a group under the above operation. Is its identity element the same as the identity element of $P(G)$?

풀 이

- 생략함 -

※ 문제 1~12에서 유한생성 가환군에 대한 기본정리에 따라 주어진 군을 분류하라.

문 1. $(Z_2 \times Z_4)/\langle(0,1)\rangle$

풀 이

$(Z_2 \times Z_4)/\langle(0,1)\rangle \simeq Z_2$

문 2. $(Z_2 \times Z_4)/\langle(0,2)\rangle$

풀 이

$(Z_2 \times Z_4)/\langle(0,2)\rangle \simeq Z_2 \times Z_2$

문 3. $(Z_2 \times Z_4)/\langle(1,2)\rangle$

풀 이

$(Z_2 \times Z_4)/\langle(1,2)\rangle \simeq Z_4$

문 4. $(Z_4 \times Z_8)/\langle(1,2)\rangle$

풀 이

$(Z_4 \times Z_8)/\langle(1,2)\rangle \simeq Z_8$

문 5. $(Z_4 \times Z_4 \times Z_8)/\langle(1,2,4)\rangle$

풀 이

$(Z_4 \times Z_4 \times Z_8)/\langle(1,2,4)\rangle \simeq Z_4 \times Z_8$

문 6. $(Z \times Z)/\langle(0,1)\rangle$

풀 이

$(Z \times Z)/\langle(0,1)\rangle \simeq Z$

문 7. $(Z \times Z)/\langle(1,2)\rangle$

풀 이

$(Z \times Z)/\langle(1,2)\rangle \simeq Z$

문 8. $(Z \times Z \times Z)/\langle(1,1,1)\rangle$

풀 이

$(Z \times Z \times Z)/\langle(1,1,1)\rangle \simeq Z \times Z$

문 9. $(Z \times Z \times Z_4)/\langle(3,0,0)\rangle$

풀 이

$(Z \times Z \times Z_4)/\langle(3,0,0)\rangle \simeq Z_3 \times Z \times Z_4$

문 10. $(Z\times Z\times Z_8)/\langle(0,4,0)\rangle$

풀 이

$(Z\times Z\times Z_8)/\langle(0,4,0)\rangle \simeq Z\times Z_4\times Z_8$

문 11. $(Z\times Z)/\langle(2,2)\rangle$

풀 이

$(Z\times Z)/\langle(2,2)\rangle \simeq Z_2\times Z$

문 12. $(Z\times Z\times Z)/\langle(3,3,3)\rangle$

풀 이

$(Z\times Z\times Z)/\langle(3,3,3)\rangle \simeq Z_3\times Z\times Z$

문 13. Find both the center $Z(D_4)$ and the commutator subgroup C of the group D_4 of symmetries of the square in Table 8. 12

풀 이

$D_4=\{\rho_0,\rho_1,\rho_2,\rho_3,\mu_1,\mu_2,\delta_1,\delta_2\}$이고 이 때, $Z(D_4)=\{\rho_0,\rho_2\}$이다.
또한 D_4는 비가환군이므로 $C\neq\{e\}$이다. 따라서 $C=Z(D_4)=\{\rho_0,\rho_2\}$ 이다.

문 14. $Z_3\times S_3$**의 중심과 교환자 부분군을 찾아라.**

풀 이

- 생략함 -

문 15. $S_3\times D_4$**의 중심과 교환자 부분군을 찾아라.**

풀 이

- 생략함 -

문 16. $Z_4\times Z_4$**의 위수가 4보다 적거나 같은 모든 부분군을 설명하고, 각각의 경우에 정리 11.12에서 처럼 이 부분군을 법으로 하는** $Z_4\times Z_4$**의 잉여군을 분류하라. 즉, 부분군을 구하고 이 부분군을 법으로 하는** $Z_4\times Z_4$**의 잉여군은** $Z_2\times Z_4$**와 동형인가를 조사하여라.**
[힌트: $Z_4\times Z_4$**는 6개의 위수가 4인 서로 다른 순환 부분군을 갖는다. 부분군** $\langle(1,0)\rangle$**와 같이 생성원을 구함으로써 그들을 설명하라.** $klein$ **4-군과 동형인 위수 4인 부분군은 하나 존재하며 위수 2인 부분군은 3개 존재한다.]**

풀 이

부분군	잉여군	부분군	잉여군
$\langle(1,0)\rangle$	Z_4	$\langle 2\rangle\times\langle 2\rangle$	$Z_2\times Z_2$
$\langle(0,1)\rangle$	Z_4	$\langle(2,0)\rangle$	$Z_2\times Z_4$
$\langle(1,1)\rangle$	Z_4	$\langle(0,2)\rangle$	$Z_4\times Z_2$
$\langle(1,2)\rangle$	Z_4	$\langle(2,2)\rangle$	$Z_2\times Z_4$
$\langle(1,3)\rangle$	Z_4	$\langle(0,0)\rangle$	$Z_4\times Z_2$

※ 문제 17과 18에서

문 17. The *center* of a group G contains all elements of G that commute with every element of G.

풀 이

군 G의 중심은 $\{x \in G \mid ax = xa (a \in G)\}$이다.

문 18. The *commutator subgroup* of a group G is $\{a^{-1}b^{-1}ab \mid a, b \in G\}$.

풀 이

교환자 부분군에 대한 옳은 정의이다.

문 19. 참, 거짓을 판정하라.

(a) 순환군의 모든 잉여군은 순환적이다.

풀 이 T

임의의 순환군을 G라 하자. 그러면 $\exists a \in G \; s.t. \; G = \langle a \rangle$

임의의 부분군 H라 하면 순환군의 부분군이므로 H 또한 순환군이고 $\exists i \in I \; s.t. \; H = \langle a^i \rangle$

$G/H = \langle a \rangle / \langle a^i \rangle = \{\langle a^i \rangle, a + \langle a^i \rangle, a^2 + \langle a^i \rangle, \cdots, a^{i-1} + \langle a^i \rangle\}$이다.

따라서 Z_i와 동형이다. 즉, 순환군의 잉여군은 다시 순환적이 된다.

(b) 비순환군의 잉여군은 다시 비순환군이다.

풀 이 F

S_3는 비순환군이지만 $S_3/A_3 \simeq Z_2$는 순환군이다.

(c) 덧셈에 대한 R/Z는 위수 2인 원소를 갖지 않는다.

풀 이 F

$0.5 + Z$는 위수 2인 R/Z의 원소이다.

(d) 덧셈에 대한 R/Z는 모든 $n \in Z^+$에 대하여 위수 n인 원소를 갖는다.

풀 이 T

모든 $n \in Z^+$에 대하여 $\frac{1}{n} + Z$는 위수 n인 R/Z의 원소이다.

(e) 덧셈에 대한 R/Z는 위수 4인 원소를 무한개 갖는다.

풀 이 F

$R/Z = \{r + Z \mid 0 \le r < 1\}$이고 이 때, $r + Z$가 위수 4 이기 위해서는 $4r \in Z$ 이다.

따라서 $r = \frac{1}{4}$로 유일하다.

(f) 군 G의 교환자 부분군이 $\{e\}$이면 G는 가환이다.

풀 이 T

임의의 $a, b \in G$에 대하여 $aba^{-1}b^{-1} = e$이므로 $ab = ba$가 성립한다. 따라서 G는 가환이다.

(g) G/H가 가환이면 G의 교환자 부분군 C는 H를 포함한다.

풀 이 F

정리 15.20에 의하여 C는 H의 부분군이다.

(h) 단순군 G의 교환자 부분군은 G자신이어야만 한다.

풀 이 F

G 또는 $\{e\}$이어야 한다. 따라서 G자신만이어야 한다는 것은 잘못된 명제이다.

(i) 비가환 단순군 G의 교환자 부분군은 G자신이어야 한다.

풀 이 T

교환자 부분군이 $\{e\}$이면 G는 가환이므로 모순된다.

(j) 모든 비자명 유한 단순군은 소수를 위수로 갖는다.

풀 이 F

(반례) A_5는 단순군이지만 위수는 $\frac{5!}{2}$는 소수가 아니다.

※ 문제 20~23에서 F를 R에서 R로 대응하는 모든 함수의 덧셈에 대한 군이라 하고 F^*를 R의 어떤 점에서도 함수값 0을 취하지 않는 F의 모든 원소의 곱셈에 대한 군이라 하자.

문 20. K를 상수함수로 이루어진 F의 부분군이라 하자. F/K와 동형이 되는 F의 부분군을 찾아라.

풀 이

$\{f\in F|f(0)=0\}$ 또는 임의의 $a\in R$에 대하여 $\{f\in F|f(a)=0\}$

문 21. K^*를 상수함수로 구성된 F^*의 부분군이라 하자. F^*/K^*와 동형이 되는 F^*의 부분군을 찾아라.

풀 이

$\{f\in F^*|f(0)=1\}$ 또는 임의의 $a\in R$에 대하여 $\{f\in F^*|f(a)=1\}$

문 22. K를 F의 연속함수의 부분군이라 하자. 위수를 2로 갖는 F/K의 원소를 찾을 수 있는가? 그 이유는?

풀 이 No

위수를 2로 갖는 F/K의 원소가 존재하고 이는 $f+K$라 하자. 단, $f\notin K$

만약 $g=f+f\in K$이면 $f=\frac{1}{2}g$이므로 f는 연속함수이다. 따라서 $f\in K$이다.

이는 가정에 모순된다. 따라서 위수를 2로 갖는 F/K의 원소는 존재하지 않는다.

문 23. K^*를 F^*의 연속함수의 부분군이라 하자. 위수를 2로 갖는 F^*/K^*의 원소를 찾을 수 있겠는가? 그 이유는?

풀 이

위수를 2로 갖는 F^*/K^*의 원소가 존재하고 이는 $f+K^*$라 하자. 단, $f\notin K^*$

만약 $g=f\cdot f\in K^*$이면 $f^2=g$이므로 f는 연속함수이다. 따라서 $f\in K^*$이다.

이는 가정에 모순된다. 따라서 위수를 2로 갖는 F^*/K^*의 원소는 존재하지 않는다.

※ 문제 24~26에서 U를 곱셈에 대한 군 $\{z\in C||z|=1\}$이라 하자.

문 24. $z_0\in U$라 하면 $z_0U=\{z_0z|z\in U\}$가 U의 부분군임을 증명하고, U/z_0U를 계산하라.

풀 이

① $z=1$에 대하여 $z_01=z_0$이므로 $z_0U\neq\varnothing$이고 $z_0U\subseteq U$임에 자명하다.

임의의 $z_0z_1, z_0z_2\in z_0U$에 대하여 $z_0z_1(z_0z_2)^{-1}=z_0(z_1z_2^{-1}z_0^{-1})\in z_0U$를 만족한다.

($\because z_1, z_2, z_0\in U$이므로 $|z_1z_2^{-1}z_0^{-1}|=|z_1||z_2^{-1}||z_0^{-1}|=1\cdot1\cdot1=1$이므로 $(z_1z_2^{-1}z_0^{-1})\in U$)

따라서 z_0U는 U의 부분군이다.

② $\phi: U\to z_0U, \phi(z)=z_0z$라 하자.

그러면 $\phi(z_1+z_2)=z_0(z_1+z_2)=z_0z_1+z_0z_2=\phi(z_1)+\phi(z_2)\ (z_1, z_2\in U)$이므로 ϕ는 준동형사상이다.

$\phi(z_1)=\phi(z_2)\ \Leftrightarrow\ z_0z_1=z_0z_2\ \Leftrightarrow\ z_1=z_2$

($\because U$ 가 군이므로 소약법칙에 의하여)이므로 따라서 ϕ는 1-1사상이고 잘 정의되어 있는 사상이다.

또한 임의의 $z\in U$에 대하여 $z_0^{-1}z\in U$가 존재해서 $\phi(z_0^{-1}z)=z_0(z_0^{-1}z)=(z_0z_0^{-1})z=z$ 이므로 따라서 ϕ는 전사사상이다. 그러므로 U와 z_0U는 동형이다. 따라서 $U/z_0U\simeq U/U\simeq\{e\}$이다.

문 25. $U/\langle-1\rangle$은 이 책에서 언급된 어떤 군과 동형인가?

풀 이

$\phi: U\to U, \phi(z)=z^2$라 하자. 그러면 ϕ는 전사인 준동형사상이고 $Ker(\phi)=\langle-1\rangle$임을 알 수 있다.
따라서 제 1동형정리에 의하여 $U/\langle-1\rangle\simeq U$ 이다.

문 26. $n\in Z^+$에 대하여 $z_n=\cos\left(\frac{2\pi}{n}\right)+i\sin\left(\frac{2\pi}{n}\right)$이라 하자. $U/\langle z_n\rangle$은 우리가 알고 있는 어떤 군과 동형인가?

풀 이

$\phi: U\to U, \phi(z)=z^n$라 하자. 그러면 ϕ는 전사인 준동형사상이고 $Ker(\phi)=\langle z_n\rangle$임을 알 수 있다.
따라서 제 1동형정리에 의하여 $U/\langle z_n\rangle\simeq U$ 이다.

문 27. 덧셈에 대한 군 R/Z는 이 책에서 언급된 어떤 군과 동형인가?

풀 이

$\phi: R\to U, \phi(r)=\cos(2n\pi)+i\sin(2n\pi)$라 하자.
그러면 ϕ는 전사인 준동형사상이고 $Ker(\phi)=Z$임을 알 수 있다.
따라서 제 1동형정리에 의하여 $R/Z\simeq U$ 이다.

문 28. G의 모든 원소는 1보다 큰 유한위수를 갖지 않지만 잉여군 G/H의 모든 원소는 유한 위수를 갖는 군 G의 예를 들어라.

풀 이

Q는 1보다 큰 유한 위수를 갖지 않지만

$Q/Z=\left\{\frac{n}{m}+Z\,|\,0\le n<m(n, m\in Z)\right\}$는 임의의 원소 $\frac{n}{m}+Z$에 대하여 $\left|\frac{n}{m}+Z\right|\le m$를 만족한다.

따라서 모든 원소는 유한위수를 갖는다.

문 29. H와 K를 군 G의 부분군이라 하자. G/H와 G/K는 동형이 아니지만 $H \simeq K$일수 있음을 예로 들어 보아라.

풀 이

$G = Z_2 \times Z_4$, $H = \langle (1,0) \rangle, K = \langle (0,2) \rangle$라 하자.

그러면 $G/H \simeq Z_4$이지만 $G/K \simeq Z_2$이다. 하지만 $H \simeq K$ 이다.

실제로 $\phi : H \to K, \phi(a,0) = (0,2a)$는 동형사상이다.

문 30. 모든 단순군의 중심에 대해 설명하라.

(a) 아벨군

풀 이

임의의 아벨군은 정규부분군이다. 따라서 중심은 전체 군이다.

(b) 비아벨군

풀 이

중심은 정규부분군이므로 $\{e\}$이다.

문 31. 모든 단순군의 교환자에 대해 설명하라.

(a) 아벨군

풀 이

아벨군의 교환자 부분군은 $\{e\}$이다.

(b) 비아벨군

풀 이

교환자부분군은 정규부분군이므로 $\{e\}$이다.

문 32. 문 33. - 생략함 -

문 34. 유한군 G가 G에 속하는 지수 2인 진 부분군을 포함한다면 G는 단순군이 아님을 보여라.

풀 이

$\varnothing \neq H \subsetneq G$인 유한군 G의 부분군 H에 대하여 $|G:H| = 2$라 하자.

임의의 $g \in G$에 대하여

$g \in H$이면 $gHg^{-1} = H$임이 자명하다.

$g \notin H$이면 $gH \cup H = Hg \cup H$이므로 $Hg = gH$이다.

따라서 H는 비자명 진부분군이 아닌 정규부분군이다. 따라서 G는 단순군이 아니다.

문 35. $\phi : G \to G'$를 군의 준동형사상이라 하고 N을 G의 정규부분군이라 하자. $\phi(N)$이 $\phi(G)$의 정규부분군임을 보여라.

풀 이

① $\phi(N)$이 $\phi(G)$의 부분군임에는 자명하다.

② 임의의 $\phi(g) \in \phi(G)$에 대하여

$\phi(g)\phi(N)\phi(g)^{-1} = \phi(g)\phi(N)\phi(g^{-1}) = \phi(gNg)^{-1} = \phi(N)$ 를 만족한다.($\because \phi$는 준동형사상이고 $N \lhd G$)

따라서 $\phi(N) \lhd \phi(G)$이다.

문 36. $\phi: G \to G'$**를 군의 준동형사상이라 하고** N'**를** G'**의 정규부분군이라 하자.**
$\phi^{-1}(N')$**는** G**의 정규부분군이다.**

풀 이

① $N' \neq \varnothing$ 이므로 $\phi^{-1}(N') \neq \varnothing$ 이고 $\phi^{-1}(N') \subseteq G$임에는 자명하다.
이제 임의의 $a, b \in \phi^{-1}(N')$에 대하여 $a', b' \in N'$ 이 존재해서 $\phi(a) = a', \phi(b) = b'$를 만족한다.
또한 $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = a'(b')^{-1} \in N'$를 만족한다.($\because$ ϕ는 준동형사상이고 $N' \lhd G'$)
따라서 $ab^{-1} \in \phi^{-1}(N')$이다. 그러므로 $\phi^{-1}(N')$이 G의 부분군이다.
② 임의의 $g \in G$와 임의의 $n \in \phi^{-1}(N')$에 대하여 $g' \in G'$이 존재해서 $\phi(g) = g', \phi(n) \in N'$를 만족한다.
또한 $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} \in N'$ 를 만족한다.($\because$ ϕ는 준동형사상이고 $N' \lhd G'$)
따라서 $gng^{-1} \in \phi^{-1}(N')$이다. 그러므로 $\phi^{-1}(N')$이 G의 정규부분군이다.

문 37. G**가 비가환군이면, 잉여군** $G/Z(G)$**는 순환군이 아님을 보여라.**

풀 이 대우증명한다!!
잉여군 $G/Z(G)$가 순환군이라 하자. $\exists a \in G \; s.t. \; G/Z(G) = \langle aZ(G) \rangle = \{a^i Z(G) | i \in I\}$
그러면 $G = \bigcup_{i \in I} a^i Z(G)$ 이다.
이제 임의의 $x, y \in G$에 대하여 $\exists i, j \in I \; s.t. \; x = a^i G(Z), y = a^j G(Z)$
또한 $xy = (a^i G(Z))(a^j G(Z)) = a^{i+j} G(Z) = a^{j+i} G(Z) = (a^j G(Z))(a^i G(Z)) = yx$ 를 만족한다.
따라서 G는 가환군이다.

문 38. 위수가 pq**인 비가환군** G**가 자명중심을 가짐을 보여라. 단,** p, q**는 소수**

풀 이

$|Z(G)| \neq 1$이라 하자. 그러면 라그랑지 정리에 의하여 $|Z(G)| \,|\, |G| = pq$이고 $|Z(G)| \neq pq$이므로
$|Z(G)| = 1, p$ 또는 q이다. 단, p, q는 소수
$Z(G)$의 위수가 소수이면 $Z(G)$는 순환군이다. 이는 문제 39에 의하여 G가 비가환군임에 모순된다.
따라서 $|Z(G)| = 1$ 이다. 즉, $Z(G) = \{e\}$이다.

문 39. 주어진 단계와 힌트를 이용하여 A_n**은** $n \geq 5$**에 단순군임을 보여라.**
(a) $n \geq 3$**이면** A_n**은 모든 3-순환치환을 포함한다.**
(b) $n \geq 3$**에 대하여** A_n**은 3-순환치환에 의하여 생성됨을 보여라.**
[힌트: $(a,b)(c,d) = (a,c,b)(a,c,b)$**이고** $(a,c)(a,b) = (a,b,c)$**이다.]**
(c) $n \geq 3$**일 때** r**과** s**를** $\{1, 2, \cdots, n\}$**의 고정된 원소라 하자.** $1 \leq i \leq n$**에 대하여** A_n**은** n**개의 "특별한"** (r, s, i)**의 꼴을 갖는 3-순환치환에 의해서 생성됨을 보여라.**
[힌트: $(r,s,i)^2, (r,s,j)(r,s,i)^2, (r,s,j)^2(r,s,i)$**와** $(r,s,i)^2(r,s,k)(r,s,j)^2(r,s,i)$**를 계산하여 모든 3-순환치환을 "특별한" 순환치환의 곱임을 보여라.]**
(d) $n \geq 3$**에 대하여** N**을** A_n**의 정규부분군이라 하자.** N**이 하나의 3-순환치환을 포함한다면** $N = A_n$**이다.**
[힌트: $(r,s,i) \in N$**이면** $i = 1, 2, \cdots, n$**에 대하여** $(r,s)(i,j)(r,s,i)^2((r,s)(i,j))^{-1}$**을 계산하여** $(r,s,j) \in N$**임을 보여라.]**
(e) $n \geq 5$**에 대하여** N**을** A_n**의 비자명 정규부분군이라 하자. 다음 경우 중 한가지가 성립하여야 하며 각 경우에** $N = A_n$**임을 보여라.**

경우1 N은 3-순환치환을 포함한다.

경우2 N은 적어도 하나는 길이가 3보다 큰 서로소인 순환치환의 곱이다.

[힌트: N의 서로소인 곱 $\sigma=\mu(a_1,a_2,\cdots,a_r)$을 포함한다고 가정하자. $\sigma^{-1}(a_1,a_2,a_3)\sigma(a_1,a_2,a_3)^{-1}$은 N에 속함을 보이고 그것을 계산하라.]

경우3 N은 $\sigma=\mu(a_4,a_5,a_6)(a_1,a_2,a_3)$꼴의 서로서인 곱을 포함한다.

[힌트: $\sigma^{-1}(a_1,a_2,a_4)\sigma(a_1,a_2,a_4)^{-1}$가 N에 속함을 보이고 이것을 증명하라.]

경우4 N은 $\sigma=\mu(a_1,a_2,a_3)$의 꼴의 서로소인 곱을 포함한다. 단, μ는 서로소인 호환의 곱이다.

[힌트: $\sigma^2\in N$임을 보이고 이것을 계산하라.]

경우5 N은 $\sigma=\mu(a_3,a_4)(a_1,a_2)$꼴의 서로소인 곱을 포함한다. 단, μ는 짝수개의 서로소인 호환의 곱이다.

[힌트: $\sigma^{-1}(a_1,a_2,a_3)\sigma(a_1,a_2,a_3)^{-1}$가 N에 속함을 보이고 그것을 계산하여 $\sigma=(a_2,a_4)(a_1,a_3)$가 속함을 보여라. 처음에는 $n\geq 5$를 이용하여 $i\in\{1,2,3,\cdots,n\}$를 구한다. 단, $i\neq a_1,a_2,a_3,a_4$이다. $\beta=(a_1,a_3,i)$라 하자. $\beta^{-1}\alpha\beta\alpha\in N$임을 보이고 그것을 계산하라.]

풀 이

- 순서대로 하면 되지만 복잡하며 구지 할 필요성을 느끼지 못해 생략함 -

실제로 $n\geq 5$일 때, S_n은 $\{1\}\triangleleft A_n\triangleleft S_n$인 조성열을 갖는다. 따라서 A_n은 단순군이다.
뿐만 아니라. $n=3$일 때, A_3 또한 단순군이다.

문 40. N**을** G**의 정규부분군이라 하고** H**를** G**의 임의의 부분군이라 하자.** $HN=\{hn|h\in H, n\in N\}$**으로 하면** HN**이** G**의 부분군임을 보이고,** N**과** H**를 포함하는 가장 작은 부분군임을 보여라.**

풀 이

① $N\lhd G, H\leq G$라 하자.

임의의 $h_1n_1, h_2n_2\in HN$ 에 대하여

$$\begin{aligned}(h_1n_1)(h_2n_2)^{-1} &= h_1n_1n_2^{-1}h_2^{-1}\\ &= h_1(n_1n_2^{-1})h_2^{-1}\\ &= h_1h_2^{-1}(n_1n_2^{-1}) \quad (\because N\lhd G \text{ 이므로 } (n_1n_2^{-1})h_2^{-1}=h_2^{-1}(n_1n_2^{-1}))\end{aligned}$$

이 성립한다. $H\leq G, N\leq G$이므로 $h_1h_2^{-1}\in H, n_1n_2^{-1}\in N$이다.

따라서 $(h_1n_1)(h_2n_2)^{-1}\in HN$ 이다. 그러므로 $HN\leq G$이다.

② K를 N과 H를 포함하는 가장 작은 부분군이라 하자.

이제 $K=HN$임을 보이자.

(→) $H=H\{e\}\subseteq HN, N=\{e\}N\subseteq HN$ 이므로 N과 H를 포함하는 부분군이다.

따라서 K의 정의에 의하여 $K\subseteq HN$이다.

(←) 임의의 $x\in HN$에 대하여 $h\in H, n\in N$이 존재해서 $x=hn$을 만족한다.

또한 $xn^{-1}=h\in H\subseteq K$ 이고 $h^{-1}x=n\in N\subseteq K$ 이다.

그러면 $x=(xn^{-1})\cdot n\in K$이고 $x=h\cdot(h^{-1}x)\in K$ 이다. ($\because h\in H\subseteq K, n\in N\subseteq K$ 이고 $K\leq G$)

따라서 $x\in K$이다. 그러므로 $HN\subseteq K$이다.

문 41. 앞의 연습문제를 참조로 하여 M**도 또한** G**의 정규 부분군이라 하자.** NM**이 다시** G**의 정규부분군임을 보여라.**

풀 이

문제 40 에 의하여 $NM\leq G$임에는 자명하다.

임의의 $g\in G$에 대하여 $gNMg^{-1}=(gNg^{-1})(gMg^{-1})=NM$ ($\because N\lhd G,\ M\lhd G$)이 성립한다.

따라서 $NM\lhd G$ 이다.

문 42 H**와** K**가** $H\cap K=\{e\}$**인** G**의 정규 부분군이라면 모든** $h\in H$**와** $k\in K$**에 대하여** $hk=kh$**이다.**

[힌트: 교환자 $hkh^{-1}k^{-1}=(hkh^{-1})k^{-1}=h(hk^{-1}k^{-1})$**를 생각해 보자.]**

풀 이

임의의 $h\in H$와 $k\in K$에 대하여

$hkh^{-1}k^{-1}=(hkh^{-1})k^{-1}\in K\cdot K=K$ 이고 $hkh^{-1}k^{-1}=h(hk^{-1}k^{-1})\in H\cdot H=H$ 이 성립한다.

그러면 $hkh^{-1}k^{-1}=(hkh^{-1})k^{-1}=h(hk^{-1}k^{-1})\in H\cap K=\{e\}$ 이다.

따라서 $hkh^{-1}k^{-1}=e$ 이다. 즉, $hk=kh$ 이다.

※ 문제 1~6에서 주어진 환에서의 곱을 계산하라.

문 1. Z_{24}**에서 (12)(16)**

풀 이

$(12)(16) \equiv (12)(-8) \equiv (12)(2)(-4) \equiv (24)(-4) \equiv 0(-4) \equiv 0(\mathrm{mod}24)$ 따라서 Z_{24}에서 (12)(16)=0 이다.

문 2. Z_{32}**에서 (16)(3)**

풀 이

$(16)(3) \equiv 48 \equiv 16(\mathrm{mod}32)$ 따라서 Z_{32}에서 (16)(3)=16 이다.

문 3. Z_{15}**에서 (11)(-4)**

풀 이

$(11)(-4) \equiv (-4)(-4) \equiv 16 \equiv 1(\mathrm{mod}15)$ 따라서 Z_{15}에서 (11)(-4)=1 이다.

문 4. Z_{26}**에서 (20)(-8)**

풀 이

$(20)(-8) \equiv (-6)(-8) \equiv 48 \equiv 22(\mathrm{mod}26)$ 따라서 Z_{26}에서 (20)(-8)=22 이다.

문 5. $Z_5 \times Z_9$**에서** $(2,3) \bullet (3,5)$

풀 이

$(2,3) \bullet (3,5) \equiv (6,15) \equiv (1,6)(\mathrm{mod}(5,9))$ 따라서 $Z_5 \times Z_9$에서 $(2,3) \bullet (3,5) = (1,6)$ 이다.

문 6. $Z_4 \times Z_{11}$**에서** $(-3,5) \bullet (2,-4)$

풀 이

$(-3,5) \bullet (2,-4) \equiv (-6,-20) \equiv (2,2)(\mathrm{mod}(4,11))$ 따라서 $Z_4 \times Z_{11}$에서 $(-3,5) \bullet (2,-4) = (2,2)$ 이다.

※ 문제7~13에서 주어진 덧셈과 곱셈 연산이 그 집합 위에서 정의되어(닫혀있어) 환 구조를 만드는지를 결정하라. 환이 되지 않으면 그 이유를 말하고 만약, 환이 되면 그 환이 가환환인지, 단위원을 갖는지, 체가 되는지를 설명하라.

문 7. 일반적 덧셈과 곱셈을 갖는 nZ

풀 이

$n=0$이면 $nZ=\{0\}$으로 자명환이 된다.

$n \neq 0$일때 nZ는 덧셈과 곱셈에 관하여 닫혀 있고 덧셈에 대하여 가환환을 만족한다.

이때 $n=\pm 1$이면 Z이므로 단위원을 갖는 가환환이지만 그 이외에는 단위원을 갖지 않는 가환환이다.

또한 nZ는 역원을 갖지 않기 때문에 체가 될 수 없다.

문 8. 일반적 덧셈과 곱셈을 갖는 Z^+

풀 이

덧셈과 곱셈에 관하여 닫혀있지만 덧셈에 대하여 역원이 존재하지 않는다 따라서 환이 될 수 없다.

문 9. 성분에 의한 덧셈과 곱셈을 갖는 $Z\times Z$

풀 이

Z가 가환환이므로 $Z\times Z$ 또한 가환환을 이룬다. 그리고 $Z\times Z$는 (1,1)을 단위원으로 갖는 가환환이다. 하지만 역원이 존재하지 않는다. 따라서 체는 아니다.

문 10. 성분에 의한 덧셈과 곱셈을 갖는 $2Z\times Z$

풀 이

Z,2Z가 가환환이므로 직적 $2Z\times Z$ 또한 가환환을 이룬다. 하지만 $(1,1)\notin 2Z\times Z$이므로 단위원을 갖지 않는 가환환이다. 따라서 체도 될수 없다.

문 11. 일반적 덧셈과 곱셈을 갖는 $\{a+b\sqrt{2}\,|\,a,b\in Z\}$

풀 이

단위원을 갖는 가환환이다. 하지만 역원이 존재하지 않으므로 체는 아니다.

문 12. 일반적 덧셈과 곱셈을 갖는 $\{a+b\sqrt{2}\,|\,a,b\in Q\}$

풀 이

단위원을 갖는 가환환이다. 또한 곱셈에 대한 역원이 존재한다. 따라서 체이기도 하다.

문 13. 일반적 덧셈과 곱셈을 갖는 $r\in R$에 대한 모든 순허수 ri들의 집합.

풀 이

덧셈에 관하여 닫혀 있지만 곱셈에 대하여 $i\times i=-1$이 되어 닫혀 있지 않다. 따라서 환이 아니다.

※ 문제 14~19에서 주어진 환의 가역원들을 구하라.

문 14. Z

풀 이 -1, +1

문 15. $Z\times Z$

풀 이 (-1, -1), (-1, +1), (+1, -1),(+1, +1)

문 16. Z_5

풀 이 1, 2, 3, 4

문 17. Q

풀 이 Q^*

문 18. $Z\times Q\times Z$

풀 이 $(-1,\ Q^*,\ -1),\ (-1,\ Q^*,\ +1),\ (+1,\ Q^*,\ -1),\ (+1,\ Q^*,\ +1)$

문 19. Z_4

풀 이 1,3

문 20. 행렬의 환 $M_2(Z_2)$를 생각하면,

(a) 이 환의 위수, 즉 이 환에 속하는 원소의 수를 구하여라.

풀 이

$M_2(Z_2)=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix},\begin{pmatrix}0&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix}\right\}$
이므로 $|M_2(Z_2)|=16$이다. 따라서 위수는 16이다.

(b) 이 환에서 모든 가역원을 나열하라.

풀 이

$\det(A)\neq 0$인 $A\in M_2(Z_2)$를 찾는다. 따라서 이 환의 모든 가역원은 다음과 같다.
$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}$

문 21. R, R'**은 각각** $1\neq 0$**과** $1'\neq 0'$**인 단위원을 갖는 환이라 하자.** $\Phi(1)\neq 0'$**이고** $\Phi(1)\neq 1'$**인** $\Phi: R\to R'$**으로의 준동형사상이 만약 가능하다면 예를 들어라.**

풀 이

$\Phi: Z\to Z\times Z, \Phi(n)=(n,0)$라 하자.
그러면 Φ는 $\Phi(1)=(1,0)\neq(0,0)$이고 $\Phi(1)=(1,0)\neq(1,1)$ 준동형사상이다.

문 22. (선형대수학) $\det: M_n(R)\to R$, $\det(A)=|A|$, $A\in M_n(R)$
det 는 환 준동형사상이 되겠는가? 왜 그렇고 왜 그렇지 않은가?

풀 이

$n=1$일때 $A=(-1), B=(2)$라 하면 $\det(A+B)=1$이지만 $\det(-1)+\det(2)=3$이다.
따라서 환 준동형사상이 아니다.
$n\neq 1$일때 $\det(AB)=\det(A)\det(B), A,B\in M_2(R)$은 성립한다.
하지만 $\det(A+B)=\det(A)+\det(B), A,B\in M_2(R)$은 성립하지 않는다.
일례로 $A=\begin{pmatrix}2&1\\0&1\end{pmatrix}, B=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$일때,
$\det(A+B)=\begin{vmatrix}1&1\\0&0\end{vmatrix}=0$이지만 $\det A+\det B=\begin{vmatrix}2&1\\0&1\end{vmatrix}+\begin{vmatrix}-1&0\\0&-1\end{vmatrix}=3$으로서 같지 않기 때문이다.
따라서 환 준동형사상이 아니다. 그러므로 det는 모든 경우에서 환 준동형 사상이 될수 없다.

문 23. Z에서 Z로의 임의의 환 준동형사상을 나타내라.

풀 이

$\Phi : Z \to Z$ 를 임의의 환 준동형사상이라 하자.

그러면 $\Phi(1) = 0$또는 1이다.

(a) $\Phi(1) = 0$이면

$\Phi(n) = \Phi(n \cdot 1) = \Phi(n) \cdot \Phi(1) = \Phi(n) \cdot 0 = 0$

$\forall a,b \in Z \; s.t. \; \Phi(a+b) = 0 = 0+0 = \Phi(a)+\Phi(b), \; \Phi(ab) = 0 = 0 \cdot 0 = \Phi(a) \cdot \Phi(b)$

(b) $\Phi(1) = 1$이면

$\Phi(n) = \Phi(n \cdot 1) = \Phi(1+\cdots+1) = n \cdot \Phi(1) = n$

$\forall a,b \in Z \; s.t. \; \Phi(a+b) = a+b = \Phi(a)+\Phi(b), \; \Phi(ab) = ab = \Phi(a) \cdot \Phi(b)$

따라서 Φ는 $\Phi(n) = 0$ 또는 $\Phi(n) = n$인 환 준동형사상을 나타낼 수 있다..

문 24. Z에서 $Z \times Z$로의 임의의 환 준동형사상을 나타내라.

풀 이

$\Phi : Z \to Z \times Z$ 를 임의의 환 준동형사상이라 하자.

그러면 $\Phi(1) = (0,0),(1,0),(0,1)$또는 $(1,1)$이다.

(a) $\Phi(1) = (0,0)$이면 $\Phi(n) = \Phi(n \cdot 1) = \Phi(n) \cdot \Phi(1) = \Phi(n) \cdot (0,0) = (0,0)$

$\forall a,b \in Z \; s.t.$

$\Phi(a+b) = (0,0) = (0,0)+(0,0) = \Phi(a+b)$

$\Phi(ab) = (0,0) = (0,0) \cdot (0,0) = \Phi(a) \cdot \Phi(b)$

(b) $\Phi(1) = (1,0)$이면 $\Phi(n) = \Phi(n \cdot 1) = \Phi(1+1+\cdots+1) = n \cdot \Phi(1) = n \cdot (1,0) = (n,0)$

$\forall a,b \in Z \; s.t.$

$\Phi(a+b) = (a+b,0) = (a,0)+(b,0) = \Phi(a)+\Phi(b)$

$\Phi(ab) = (ab,0) = (a,0) \cdot (b,0) = \Phi(a) \cdot \Phi(b)$

(c) $\Phi(1) = (0,1)$이면 $\Phi(n) = \Phi(n \cdot 1) = \Phi(1+1+\cdots+1) = n \cdot \Phi(1) = n \cdot (0,1) = (0,n)$

$\forall a,b \in Z \; s.t.$

$\Phi(a+b) = (0,a+b) = (0,a)+(0,b) = \Phi(a)+\Phi(b)$

$\Phi(ab) = (0,ab) = (0,a) \cdot (0,b) = \Phi(a) \cdot \Phi(b)$

(c) $\Phi(1) = (1,1)$이면 $\Phi(n) = \Phi(n \cdot 1) = \Phi(1+1+\cdots+1) = n \cdot \Phi(1) = n \cdot (1,1) = (n,n)$

$\forall a,b \in Z \; s.t.$

$\Phi(a+b) = (a+b,a+b) = (a,a)+(b,b) = \Phi(a)+\Phi(b)$

$\Phi(ab) = (ab,ab) = (a,a) \cdot (b,b) = \Phi(a) \cdot \Phi(b)$

따라서 Φ는 $\Phi(n) = (0,0)$ 또는 $\Phi(n) = (n,0)$또는$\Phi(n) = (0,n)$또는$\Phi(n) = (n,n)$인 환 준동형사상을 나타낼 수 있다.

문 25. $Z \times Z$에서 Z로의 임의의 환 준동형사상을 나타내라.

풀 이

$\Phi : Z \times Z \to Z$를 임의의 환 준동형사상이라 하자.

그러면 $\Phi((1,0)) = 0$또는 1, $\Phi((0,1)) = 0$또는 1 또는 이다.

(a) $\Phi((1,0)) = 0$이고$\Phi((0,1)) = 0$이면

$\Phi(n,m) = \Phi((n,0)+(0,m)) = \Phi(n,0)+\Phi(0,m) = n\Phi(1,0)+m\Phi(0,1) = 0$

$\forall a,b,c,d \in Z \; s.t.$

$\Phi((a,b)+(c,d)) = 0 = 0+0 = \Phi((a,b))+\Phi((c,d))$

$\Phi((a,b) \cdot (c,d)) = 0 = 0 \cdot 0 = \Phi((a,b)) \cdot \Phi((c,d))$

(b) $\Phi((1,0)) = 0$이고$\Phi((0,1)) = 1$이면

$\Phi(n,m) = \Phi((n,0)+(0,m)) = \Phi(n,0)+\Phi(0,m) = n\Phi(1,0)+m\Phi(0,1) = m$

$\forall a,b,c,d \in Z\ s.t.$
$\Phi((a,b)+(c,d)) = b+d = \Phi((a,b))+\Phi((c,d))$
$\Phi((a,b)\bullet(c,d)) = bd = \Phi((a,b))\bullet\Phi((c,d))$

(c) $\Phi((1,0))=1$이고$\Phi((0,1))=0$이면

$\Phi(n,m) = \Phi((n,0)+(0,m)) = \Phi(n,0)+\Phi(0,m) = n\Phi(1,0)+m\Phi(0,1) = n$

$\forall a,b,c,d \in Z\ s.t.$
$\Phi((a,b)+(c,d)) = a+c = \Phi((a,b))+\Phi((c,d))$
$\Phi((a,b)\bullet(c,d)) = ac = \Phi((a,b))\bullet\Phi((c,d))$

(d) $\Phi((1,0))=1$이고$\Phi((0,1))=1$이면

$\Phi(n,m) = \Phi((n,0)+(0,m)) = \Phi(n,0)+\Phi(0,m) = n\Phi(1,0)+m\Phi(0,1) = n+m$

$\forall a,b,c,d \in Z\ s.t.$
$\Phi((a,b)+(c,d)) = a+b+c+d = \Phi((a,b))+\Phi((c,d))$
$\Phi((a,b)\bullet(c,d)) = ac+bd \neq (a+b)\bullet(c+d) = \Phi((a,b))\bullet\Phi((c,d))$

(a)~(c)는 환 준동형사상이지만 (d)는 환 준동형사상이 아니다.

따라서 Φ는 $\Phi(n,m)=0$, $\Phi(n,m)=n$, $\Phi(n,m)=m$이 환 준동형사상이다.

문 26. $Z\times Z\times Z$에서 Z로의 환 준동형사상은 몇 개나 있는가?

풀 이

$\Phi : Z\times Z\times Z \to Z$를 임의의 환 준동형사상이라 하자.

그러면 $\Phi((1,0,0))=0$또는 1, $\Phi((0,1,0))=0$또는 1 ,$\Phi((0,0,1))=0$또는 1또는 이다.

(a) $\Phi((1,0,0))=0, \Phi((0,1,0))=0, \Phi((0,0,1))=0$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = 0$

(b) $\Phi((1,0,0))=0, \Phi((0,1,0))=0, \Phi((0,0,1))=1$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = m$

(c) $\Phi((1,0,0))=0, \Phi((0,1,0))=1, \Phi((0,0,1))=0$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = n$

(d) $\Phi((1,0,0))=1, \Phi((0,1,0))=0, \Phi((0,0,1))=0$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = l$

(e) $\Phi((1,0,0))=1, \Phi((0,1,0))=1, \Phi((0,0,1))=0$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = l+n$

(f) $\Phi((1,0,0))=1, \Phi((0,1,0))=0, \Phi((0,0,1))=1$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = l+m$

(g) $\Phi((1,0,0))=0, \Phi((0,1,0))=1, \Phi((0,0,1))=1$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = n+m$

(h) $\Phi((1,0,0))=1, \Phi((0,1,0))=1, \Phi((0,0,1))=1$인 경우

$\Phi(l,n,m) = \Phi((l,0,0)+(0,n,0)+(0,0,m)) = \Phi(l,0,0)+\Phi(0,n,0)+\Phi(0,0,m)$
$= l\Phi(1,0,0)+n\Phi(0,1,0)+m\Phi(0,0,1) = l+m+n$

(a)~(d)는 환 준동형사상이지만 (e)~(h)는 환 준동형사상이 아니다.

따라서 $\Phi : Z\times Z\times Z \to Z$로의 환 준동형사상은 4개 존재한다.

문 27. 환 $M_3(R)$에서 방정식 $X^2 = I_3$의 해를 구하고자 한다.

$X^2 = I_3 \Leftrightarrow X^2 - I_3 = 0$

$X^2 - I_3 = (X - I_3)(X + I_3) = 0$
$\Rightarrow X = I_3$ 또는 $X = -I_3$

풀이가 맞나? 만약 아니면 가능하다면 반례를 들어 잘못된 곳을 지적하시오.

풀 이

환 $M_3(R)$은 정역이 아니다.

따라서 $(X - I_3)(X + I_3) = 0 \Rightarrow X = I_3$ 또는 $X = -I_3$ 라고 볼수 없다.

(반례)

$X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$일때 $X^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$이지만

$X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \neq I_3$ 또는 $X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \neq -I_3$ 이다.

문 28. 환 Z_{11}에서 방정식 $x^2 + x - 6 = 0$의 해를 이차방정식의 인수분해를 통하여 모두 찾아라.

풀 이

$x^2 + x - 6 = (x - 2)(x + 3) = 0$ 이다.

이때 환 Z_{11}은 정역이므로 $(x - 2)(x + 3) = 0 \Rightarrow x - 2 = 0$ 또는 $x + 3 = 0 \Rightarrow x = 2$ 또는 $x = -3 = 8$이 성립한다. 따라서 구하고자 하는 해는 2, 8 이다.

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 29. 0이 아닌 단위원을 갖은 환이 다음을 만족할 때 *체 F*라 한다.
F의 0이 아닌 원소에 대하여 곱셈에 관한 연산이 군을 이룬다.

풀 이

곱셈에 관한 군이 아니라 곱셈에 관한 가환군을 이룰 때 F를 체라 한다. 그러므로 다음과 같이 수정해야 한다. 0이 아닌 단위원을 갖은 환이 다음을 만족할 때 체 F라 한다. F의 0이 아닌 원소에 대하여 곱셈에 관한 연산이 가환군을 이룬다.

문 30. A *unit* in a ring is an element of magnitude 1.

풀 이

$a \neq 0$인 임의의 $a \in R$에 대하여 $b \neq 0$인 $b \in R$가 존재해서 $ab = 1$ 또는 $ba = 1$을 만족하는 원소 $a \in R$를 가역원(단원)이라고 한다.

문 31. ab=0 이지만 a와 b 둘다 0 이 아닌 두 원소 a와 b를 갖는 환의 예를 찾아라.

풀 이

환 Z_6에서 2와 3은 둘 다 영이 아니지만 $2 \cdot 3 = 0$이다.

문 32. 부분환이 단위원 $1' \neq 1$과 단위원 0을 갖는다는 환의 예를 들어라.
[힌트: 직적을 생각하거나 Z_6의 부분환을 생각해 보라.]

풀 이

$Z \times Z$의 단위원은 $(1,1)$이지만 부분환인 $Z \times \{0\}$의 단위원은 $(1,0)$으로써 $(1,1) \neq (1,0)$임을 알수 있다.

문 33. 참과 거짓을 판단하시오.

(a) 모든 체는 환이다.

풀 이 (True)

단위원을 가진 가환인 나눗셈환이 체이다. 따라서 체는 환이다.

(b) 모든 환은 곱에 대한 항등원을 갖는다.

풀 이 (False)

2Z는 환이지만 곱에 대한 항등원을 갖지 않는다.

(c) 단위원을 갖는 모든 환은 적어도 두 개의 가역원을 갖는다.

풀 이 (False)

Z_2인 경우는 단위원을 갖는 환이다. 하지만 가역원은 1 하나 뿐이다.

(d) 단위원을 갖는 모든 환은 기껏해야 두 개의 가역원을 갖는다.

풀 이 (False)

Z_5의 경우는 단위원을 갖는 환이다 하지만 가역원은 1,2,3,4로서 4개 존재한다.

(e) 체의 부분집합이 유도된 연산에 대하여 환은 되지만 부분체는 안될 수도 있다.

풀 이 (True)

R의 부분집합 Z를 생각해 보자. Z는 환은 되지만 부분체는 안된다.

(f) 환에 대한 분배법칙은 별로 중요하지 않다.

풀 이 (False)

환이 되기 위한 조건에 좌 분배법칙과 우 분배법칙이 있다. 따라서 중요하다.

(g) 체에서의 곱은 가환이다.

풀 이 (True)

체는 단위원을 가진 가환인 나눗셈환이다. 따라서 곱에 대해 가환이다.

(h) 체의 0이 아닌 원소는 그 체에서의 곱셈에 대한 군이 된다.

풀 이 (True)

체는 0이 아닌 원소에 대하여 닫혀 있고 단위원 1을 포함하며 임의의 원소에 대한 역원이 존재한다. 따라서 0이 아닌 원소는 그 체에서의 곱셈에 대한 군이 된다. 즉 F가 체가 되기 위한 필요충분조건은 $< F,+ >, < F^*, \bullet >$이 둘 다 가환군을 만족할 때 이다

(i) 모든 환에서의 덧셈은 가환이다.

풀 이 (True)

환의 정의에서 덧셈에 대한 아벨군이다. 따라서 덧셈에 대하여 가환이다.

(j) 환의 모든 원소는 덧셈에 대한 역원을 갖는다.

풀 이 (True)

환은 덧셈에 대한 가환군 이다. 따라서 환의 모든 원소는 덧셈에 대한 역원을 갖는다.

문 34. (예제18.4)에서 주어진 함수의 집합 F 위에서 정의된 곱셈은 환에 대한 공리 R_2와 R_3를 만족함을 보여라.

풀 이

합과 곱에 대한 연산은 $(f+g)(x)=f(x)+g(x)$,$(fg)(x)=f(x)g(x)$로 정의한다.

임의의 $f,g,h\in F$와 임의의 x에 대하여

$[(fg)h(x)]=(fg)(x)h(x)=f(x)g(x)h(x)=f(x)(gh)(x)=[f(gh)](x)$

이므로 곱셈에 관한 결합법칙이 성립한다. 따라서 공리 R_2가 성립한다.

또한 $[(f+g)h](x)=(f+g)(x)h(x)=[f(x)+g(x)]h(x)$
$=f(x)h(x)+g(x)h(x)=(fh)(x)+(gh)(x)=(fh+gh)(x)$
$[h(f+g)](x)=h(x)(f+g)(x)=h(x)[f(x)+g(x)]=$
$h(x)f(x)+h(x)g(x)=(hf)(x)+(hg)(x)=(hf+hg)(x)$

이므로 우 분배법칙과 좌 분배법칙이 성립한다. 따라서 공리R_3가 성립한다.

문 35. (예제18.10)의 평가함수 Φ_a는 준동형사상이 되기 위한 곱셈에 대한 조건을 만족함을 보여라.

풀 이

임의의 $f,g\in F$와 임의의 $a\in R$에 대하여 $\Phi_a(fg)=(fg)(a)=f(a)g(a)=\Phi_a(f)\Phi_a(g)$가 성립한다.

따라서 환 준동형 사상이 되기 위한 곱셈에 대한 조건을 만족한다.

문 36. 동형사상은 환들의 모임 위에서 동치관계를 만든다는 사실을 증명하기 위하여 (정의18.12) 다음에 객관적 논법을 완성하라.

풀 이

환 R,R',R''에 대하여

(i) $\Phi:R\to R,\Phi(a)=a(a\in R)$이면 Φ는 동형사상이다.

(ii) $\Phi:R\to R'$인 사상 Φ가 동형사상이면 역 사상 $\Phi^{-1}:R'\to R$ 또한 동형사상이다.

(iii) $\Phi:R\to R'$와 $\Phi':R'\to R''$인 사상 Φ,Φ'이 동형사상이면 $(\Phi'\bullet\Phi):R\to R''$ 또한 동형사상이다.

문 37. 만약 U가 단위원을 갖는 환 $<R,+,\bullet>$에서 모든 가역원의 모임이면 $<U,\bullet>$군임을 보여라. [주의: U는 곱셈에 대하여 닫혀 있음을 보이면 된다.]

풀 이

항등원 $1\in U\neq\varnothing$ 이고 결합법칙은 자명하게 성립한다.

$\forall a,b\in U\ \exists c,d\in U\ s.t.\ ac=ca=1,bd=db=1$

이때 $(ab)(dc)=a(bd)c=ac=1=d(ca)b=(dc)(ab)$이므로 $ab\in U$이다. 또한 가역원의 정의에 의하여 임의의 원소에 대해 역원이 존재한다. 따라서 $<U,\bullet>$은 군이 됨을 알 수 있다.

문 38. 환 R에 속하는 모든 a와 b에 대하여 $a^2-b^2=(a+b)(a-b)$일 필요충분조건은 R가 가환임을 보여라.

풀 이

(⇨) 임의의 a와 b에 대하여 $a^2-b^2=(a+b)(a-b)$이면 다음이 성립한다.

$a^2-b^2=(a+b)(a-b)=a^2-ab+ba-b^2$
$\Leftrightarrow ab=ba$

따라서 환 R은 가환이다.

(⇦)환 R이 가환이므로 임의의 a와 b에 대하여 ab=ba이다.

따라서 $(a+b)(a-b)=a^2-ab+ba-b^2=a^2-b^2$ 이 성립한다.

문 39. <R,+>를 가환군이라 하고, 모든 $a,b\in R$에 대하여 ab=0 로 정의한다면 $<R,+,\bullet>$은 환임을 보여라.

풀 이

<R,+>를 가환군이므로 0을 원소로 포함한다. 그리고 조건에 의하여 모든 $a,b\in R$에 대하여 ab=0 로 정의한다면 $ab=0\in R$이므로 곱셈에 대하여 닫혀 있음을 알 수 있다.

임의의 $a,b,c\in R$에 대하여 $(ab)c=(0)c=0=a(0)=a(bc)$이므로 결합법칙이 성립한다. 또한 $a(b+c)=0=0+0=ab+ac,\ (b+c)a=0=0+0=ba+ca$ 이므로 좌 분배법칙과 우 분배법칙이 성립한다. 따라서 환의 모든 조건을 만족한다. 그러므로 $<R,+,\bullet>$ 은 환이다.

문 40. 환 2Z와 3Z는 동형이 아님을 보여라. 체 R와 C도 동형이 아님을 보여라.

풀 이

(a) 환 2Z와 3Z는 동형이라고 가정하자. 그러면 Z/2Z≈Z/3Z이 되어 $Z_2\approx Z_3$을 만족한다. 이는 모순이다. 따라서 환 2Z와 3Z는 동형이 아니다.

(b) x^2+1은 체 R에서는 기약이지만 C에서는 가약이다. 따라서 체 R와 C도 동형이 아니다.

문 41.(신입생 지수법칙) p를 소수라 하자. 환 Z_p에서 모든 $a,b\in Z_p$에 대하여 $(a+b)^p=a^p+b^p$임을 보여라. [힌트: $(a+b)^n$에 대한 이항전재가 가환환에서는 유효함을 보여라.]

풀 이

환 Z_p는 가환환이므로 다음이 성립한다.

$(a+b)^p=\sum_{i=0}^{p}\binom{p}{i}a^{p-i}b^i$ 여기서 $i\neq 0,p$일때 $p|\binom{p}{i}$ 이다.

이때 $(a+b)^p=\sum_{i=0}^{p}\binom{p}{i}a^{p-i}b^i=\binom{p}{0}a^p+\binom{p}{1}a^{p-1}b+\cdots+\binom{p}{p-1}ab^{p-1}+\binom{p}{p}b^p$

$=\binom{p}{0}a^p+(0)a^{p-1}b+\cdots+(0)ab^{p-1}+\binom{p}{p}b^p=a^p+b^p$

이다. 따라서 환 Z_p에서 모든 $a,b\in Z_p$에 대하여 $(a+b)^p=a^p+b^p$이 성립한다.

문 42. 환에 대한 (문제32)과는 대조적으로 체의 부분체의 단위원은 전체 체의 단위원과 같음을 보여라.

풀 이

체 F의 부분체를 S라 하고 각각의 단위원을 $1,1'$이라 하자. 임의의 $a\in S$와 그 역 $a^{-1}\in S$에 대하여 $a,a^{-1}\in F$이므로 다음이 성립한다.

$$1=a\cdot a^{-1}=a^{-1}\cdot a=1'$$

따라서 체의 부분체의 단위원은 전체 체의 단위원과 같음을 알 수 있다.

문 43. 단위원을 갖는 환에서 가역원의 곱셈에 대한 역은 유일함을 보여라.

풀 이

가역원의 a의 곱셈에 대한 역을 b,c라 하자.(b≠c) 그러면 ab=ba=1이고 ac=ca=1을 만족한다. 여기서, 환 R은 결합법칙이 성립하므로 다음이 성립한다.

b=b1=b(ac)=(ba)c=1c=c

이는 모순이다. 따라서 가역원의 곱셈에 대한 역은 유일하다.

문 44. 환R의 원소가 $a^2=a$을 만족하면 멱등원(idempotent)이라 한다.
(a) 가환환의 모든 멱등원의 집합(부울환)은 곱셈에 대하여 닫혀 있다.

풀 이

가환환R의 모든 멱등원의 집합을 S라 하자.

임의의 $a,b\in S$ 에 대하여 $(ab)^2=(ab)(ab)=a(ba)b=a(ab)b=(a)^2(b)^2=ab$를 만족한다.

따라서 $ab\in S$이므로 가환환의 모든 멱등원의 집합은 곱셈에 대하여 닫혀 있다.

(b) 환$Z_6\times Z_{12}$에서의 모든 멱등원을 찾아라.

풀 이

환 R에서 모든 멱등원의 집합을 B(R)이라 하자. 그러면 $B(Z_6)=\{0,1,2,4\}, B(Z_{12})=\{0,1,4,9\}$이다.

따라서 환$Z_6\times Z_{12}$의 모든 멱등원의 집합은 다음과 같이 찾을수 있다.

$$B(Z_6\times Z_{12})=\begin{Bmatrix}(0,0),(0,1),(0,4),(0,9),(1,0),(1,1),(1,4),(1,9),\\(3,0),(3,1),(3,4),(3,9),(4,0),(4,1),(4,4),(4,9)\end{Bmatrix}$$

문 45. (선형대수학) Recall that for an $m\times n$ matrix A, the transpose A^T of A is the matrix whose $j-th$ column is the $j-th$ row of A. Show that if A is an $m\times n$ matrix such that A^TA is invertible then the projection matrix $P=A(A^TA)^{-1}A^T$ is an idempotent in the ring of the matrices.

풀 이

$$\begin{aligned}P^2&=\{A(A^TA)^{-1}A^T\}\{A(A^TA)^{-1}A^T\}\\&=A(A^TA)^{-1}(A^TA)(A^TA)^{-1}A^T\\&=A(A^TA)^{-1}A^T=P\end{aligned}$$

이므로 P는 n차 행렬환에서 멱등원이다.

문 46. 환 R의 원소 a가 $n\in Z^+$에 대하여 $a^n=0$이면, a를 멱영원(nilpotent)이라 한다. 만약 a와 b가 가환환에서 멱영원을 가지면 a+b도 멱영원임을 보여라.

풀 이

가환환R의 모든 멱영원의 집합을 N라 하자.

임의의 $a,b\in N$ 에 대하여 $n,m\in Z^+$ 가 존재해서 다음을 만족한다.

$a^n=0, b^m=0$

그러면 $(a+b)^{n+m}=\sum_{i=0}^{n+m}\binom{n+m}{i}a^{n+m-i}b^i$ 이고

이때 $a^n=0$또는 $b^m=0$ 이므로 임의의i에 대하여 $a^{n+m-i}b^i=0$이다.

따라서 $(a+b)^{n+m}=\sum_{i=0}^{n+m}\binom{n+m}{i}a^{n+m-i}b^i=0$인 $n+m\in Z^+$ 이 존재함을 알 수 있다.

그러므로 a,b가 멱영원이면 a+b도 멱영원이다.

문 47. 환 R가 0이 아닌 멱영원을 갖지 않을 필요충분조건은 0는 R에서 $x^2=0$에 대한 유일한 해임을 보여라.

풀 이

(⇨) 환 R가 0이 아닌 멱영원을 갖지 않는다고 하자. 그리고 0이 아닌 R에서 $x^2=0$에 대한 근 a가 존재한다고 가정하자. 그러면 $a^2=0$이 되게 하는 $2\in Z^+$가 존재하고 따라서 a는 멱영원이 된다. 하지만 이는 모순이다. 따라서 0는 R에서 $x^2=0$에 대한 유일한 해이다.

(⇦) 환 R가 0이 아닌 멱영원을 갖는다고 가정하자.

그러면 0이 아닌 임의의 a에 대하여 $n\in Z^+$ 가 존재해서 다음을 만족한다.

$a^n=0$

여기서 $E=\{n\in Z^+|a^n=0\}$라고 정의하면

정수의 정렬성의 원리에 의하여 E는 최소 원소 n_0를 갖는다.

(i) n_0가 짝수인 경우.

$n_0=2k(k\in Z^+)$이고 따라서$a^n=(a^k)^2=0$ 이 되어 n_0의 최소성에 따라 방정식 $x^2=0$을 만족하는 0이 아닌 해 a^k가 존재하게 되어 모순이다.

(ii) n_0가 홀수인 경우 .

$n_0=2k+1(k\in Z^+)$이고 따라서 $a^n=(a^k)^2a=0$이고

a는 0이 아니므로 $(a^{k+1})^2=((a^k)^2a)a=0$이 되어 n_0의 최소성에 따라 방정식 $x^2=0$을 만족하는 0이 아닌 해 a^{k+1}가 존재하게 되어 모순이다.

따라서 환 R가 0이 아닌 멱영원을 갖지 않는다.

문 48. 환 R의 부분집합 S가 R의 부분환이 될 필요충분조건은 다음 사실이 성립하는 것임을 보여라.

$0 \in S$
$\forall a,b \in S \Rightarrow (a-b) \in S$
$\forall a,b \in S \Rightarrow ab \in S$

풀 이

(⇨) 환 R의 부분집합 S가 R의 부분환이면 덧셈에 대하야 가환환이므로 첫 번째와 두 번째 조건이 성립하며 또한 곱셈에 대하여 닫혀 있으므로 세 번째 조건도 자명하게 성립한다.
(⇦) $0 \in S$이므로 S는 공집합이 아닌 환 R의 부분 집합이다. 또한 환 R 의 부분집합 S는 자명하게 결합법칙과 분배법칙이 성립한다.
또한 조건에 의하여 $\forall a,b \in S \Rightarrow (a-b) \in S,\ ab \in S$ 이 성립하므로 S는 덧셈에 대한 가환군이며 곱셈에 대한 반군임을 알 수 있다. 따라서 S는 환이다. 그러므로 환 R의 부분집합 S가 R의 부분환이 된다.

문 49.

(a) 환 R의 부분환들의 공통집합은 다시 R의 부분환임을 보여라.

풀 이

S, T를 환 R의 부분환이라 하자. 이때 $0 \in S$이고$0 \in T$이므로$0 \in S \cap T \neq \varnothing$ 이다
그러면 임의의 $a,b \in S \cap T$에 대하여 $a,b \in S$이고$a,b \in T$이므로 $a-b, ab \in S$이고$a-b, ab \in T$이다
따라서 $a-b, ab \in S \cap T$이므로 $S \cap T$ 또한 환 R의 부분환이 된다.

(b) 체 F의 부분체들의 공통집합은 다시 F의 부분체임을 보여라.

풀 이

S, T를 체 F의 부분체이라 하자. 이때 $0 \in S$이고$0 \in T$이므로$0 \in S \cap T \neq \varnothing$ 이다
그러면 임의의 $a,b \in S \cap T$에 대하여 $a,b \in S$이고$a,b \in T$이므로 $a-b, ab^{-1} \in S$이고$a-b, ab^{-1} \in T$이다
따라서 $a-b, ab^{-1} \in S \cap T$이므로 $S \cap T$ 또한 체 F의 부분체이 된다.

문 50. R은 환이고 a는 R의 고정된 원소라 하자. $I_a = \{x \in R | ax = 0\}$이라 하면 I_a는 R의 부분환임을 보여라.

풀 이

R을 환이라 하고 a는 R의 고정된 원소라 하자. 이때 $a \cdot 0 = 0$이므로 $0 \in I_a$이다.
따라서 $I_a \neq 0$이다. 그러면 임의의 $x,y \in I_a$에 대하여
$a(x-y) = ax - ay = 0 - 0 = 0,\ a(xy) = (ax)y = (0)y = 0$ 이다. 따라서 $x-y, xy \in I_a$이다.
그러므로 I_a는 R의 부분환이다.

문 51. R은 환이며 a는 R의 고정된 원소라 하자. R_a가 a를 포함하는 R의 모든 부분환들의 공통집합인 R의 부분환이라 하면(문제49 참조) 환 R_a는 a에 의하여 생성된 R의 부분환이라 한다. 가환군 <R_a,+> 는 $\{a^n | n \in Z^+\}$에 의해 생성(제7장과 같은 의미에서) 됨을 보여라.

풀 이

$R_a \equiv \cap \{H | a \in H$인 R의 부분환 $\}$, $< a > = \{a^n | n \in Z^+\}$라 할 때 $< R_a, + > = < a >$임을 보인다.
(⇨) $< a >$는 a를 포함하는 부분군이다. 따라서 $< R_a, + > \subset < a >$ 가 성립한다.
(⇦) $\forall b \in < a > \ \exists m \in Z^+ \ s.t.\ b = a^m$ 이 때 $< R_a, + >$ 는 a를 포함하는 가환군이므로
$b = a^m \in < R_a, + >$이 성립한다. 따라서 $< a > \subset < R_a, + >$ 이다. 그러므로 $< R_a, + > = < a >$을 알 수 있다.

문 52. (중국인의 나머지 정리에 관한 2가지 결론) Let r and s be positive integers such that $\gcd(r,s)=1$. Use the isomorphism in Example 18.15 to show that for $n,m\in Z$. there exist an integer x such that $x\equiv m(\mathrm{mod}r)$ and $x\equiv n(\mathrm{mod}s)$

풀 이

(예제 18.15)에서 $\Phi: Z_{rs}\to Z_r\times Z_s, \Phi(a)=a(1,1)$은 동형사상이다.

$x=\Phi^{-1}(m,n)$이라 하자. 그러면 $\Phi(x)=x(1,1)$는 x번의 합 $1+1+\cdots+1$은 Z_r에서는 m에 그리고 Z_s에서는 n에 대응됨을 알 수 있다. 따라서 $x\equiv m(\mathrm{mod}r)$, $x\equiv n(\mathrm{mod}s)$ 라 볼 수 있다.

문 53.

(a) State and prove the generalization of Example 18.15 for a direct product with n factors.

풀 이

(진술) $i\neq j$이면 $\gcd(b_i,b_j)=1$인 정수 $b_1,\cdots,b_n$라 하자.

그러면 $Z_{b_1\cdots b_n}\approx Z_{b_1}\times\cdots\times Z_{b_n}$이 되게 하는 $\Phi: Z_{b_1\cdots b_n}\to Z_{b_1}\times\cdots\times Z_{b_n}, \Phi(a)=a(1,1,\cdots,1)$가 존재한다.

(증명) -생 략-

(b) 중국인의 나머지 정리를 증명하시오:

Let $a_i,b_i\in Z^+$ for $i=0,1,2,\cdots,n$ and let $\gcd(b_i,b_j)=1$ for $i\neq j$. then there exist $x\in Z^+$ such that $x\equiv a_i(\mathrm{mod}b_i)$ for$i=0,1,2,\cdots,n$.

풀 이

$\Phi: Z_{b_1\cdots b_n}\to Z_{b_1}\times\cdots\times Z_{b_n}, \Phi(a)=a(1,1,\cdots,1)$은 동형사상이다.

$x=\Phi^{-1}(a_1,\cdots a_n)$이라 하자. 그러면 $\Phi(x)=x(1,\cdots,1)$는 x번의 합 $1+1+\cdots+1$은 Z_{b_i}에서 a_i $(1\leq i\leq n)$에 대응됨을 알 수 있다. 따라서 $x\equiv a_i(\mathrm{mod}b_i)(1\leq i\leq n)$라 볼 수 있다.

문 54. S는 집합이며, +와 ·는 S 위에서 이항연산일 때 다음 조건을 만족하는 $<S,+,\cdot>$을 생각해 보자.

<S,+>는 군이다.

S^*는 덧셈에 대한 항등원을 제외한 S의 모든 원소라 하면 <S^*,·>는 군이다.

모든 $a,b,c\in S$에 대하여 $a(b+c)=ab+ac$이고, $(a+b)c=ac+bc$이다.

그러면 $<S,+,\cdot>$이 나눗셈환임을 보여라.

[힌트: 덧셈에 대한 가환성을 증명하기 위하여 (1+1)(a+b)에 배분법칙을 적용하라.]

풀 이

나눗셈환임을 보이기 위하여 <S,+> 가환군임을 보이면 충분하다.

임의의 a, b∈S에 대하여 분배법칙이 성립하므로 다음이 성립한다.

(1) (1+1)(a+b)=1·(a+b) + 1·(a+b)=1·a+1·b+1·a+1·b=a+b+a+b

(2) (1+1)(a+b)=(1+1)·a+(1+1)·b=1·a+1·a+1·b+1·b=a+a+b+b

(1)=(2) 이고 <S,+>는 군이므로 덧셈에 관한 소약 법칙이 성립한다.

따라서 a+b=b+a 가 성립한다. 그러므로 <S,+>는 가환군이다.

<S,·>는 0을 제외한 모든 원소에 대하여 군을 이루므로 결합법칙과 이항연산에 대하여 닫혀 있음을 알 수 있다.

그리고 세 번째 조건에 의하여 좌 분배법칙과 우 분배법칙이 성립하므로 <S,+,·>는 환이다.

또한 <S,·> 0을 제외한 모든 원소에 대하여 군을 이루기 때문에 단위원 1을 포함하고 가역원을 갖는다.

그러므로 <S,+,·>는 나눗셈환이다.

문 55. 모든 $a\in R$에 대하여 $a^2=a$이면 환 R를 부울환이라 한다. 모든 부울환은 가환임을 보여라.

풀 이

R을 부울환이라 하자. 그러면 임의의 $a,b\in R$에 대하여 다음이 성립한다.

$(a+a)^2=(a+a)=a+a$
$(a+a)^2=a^2+a^2+a^2+a^2=a+a+a+a$
$\Rightarrow a+a=0$
$\Rightarrow a=-a$

이고

$(a+b)=(a+b)^2=(a+b)(a+b)=a^2+ab+ba+b^2=a+ab+ba+b$
$\Rightarrow ab+ba=0$
$\Rightarrow ab=-ba=ba$

따라서 모든 부울환은 가환이다.

문 56. (집합론의 법칙을 알고 있는 학생들을 위하여)집합 S에 대하여 $P(S)$를 S의 모든 부분집합들의 모임이라 하자. $P(S)$ 위에서 이항연산 +와 ·을 다음과 같이 정의하기로 한다.

$A,B\in P(S)$에 대하여

$A+B=(A\cup B)-(A\cap B)=\{x|x\in A$ 또는 $x\in B$이지만 $x\notin A\cap B\}$이고

$A\cdot B=A\cap B$로 정의한다.

(a) $P(S)$에 대한 이항연산 +와 ·의 연산표를 만들어라. 단 $S=\{a,b\}$

[힌트: $P(S)$는 4개의 원소를 갖는다.]

풀 이

+	∅	{a}	{b}	S
∅	∅	{a}	{b}	S
{a}	{a}	∅	S	{b}
{b}	{b}	S	∅	{a}
S	S	{a}	{b}	∅

·	∅	{a}	{b}	S
∅	∅	∅	∅	∅
{a}	∅	{a}	∅	{a}
{b}	∅	∅	{b}	{b}
S	∅	{a}	{b}	S

(b) 임의의 집합 S에 대하여 <P(S),+,·>는 부울환임을 보여라.(문제55번 참조)

풀 이

{∅}∈P(S)이므로 P(S)≠∅이다.

임의의 A, B∈P(S)에 대하여 A+B, A·B∈P(S) 임은 P(S)의 정의에 의하여 자명하다.

임의의 A, B, C∈P(S)에 대하여

(A+B)+C={(A∪B)−(A∩B)}+C=[{(A∪B)−(A∩B)}∪C]−[{(A∪B)−(A∩B)}∩C]
=(A∪B∪C)−(A∩B)−(A∩C)−(B∩C)

A+(B+C)=A+{(B∪C)−(B∩C)}=[A∪{(B∪C)−(B∩C)}]−[A∩{(B∪C)−(B∩C)}]
=(A∪B∪C)−(A∩B)−(A∩C)−(B∩C)

(A·B)·C=(A∩B)·C=(A∩B)∩C=A∩B∩C=A∩(B∩C)=A·(B∩C)=A·(B·C)

이 성립하여 (A+B)+C=A+(B+C), (A·B)·C=A·(B·C)임을 알 수 있다.

따라서 덧셈과 곱셈에 관하여 결합법칙이 성립한다.

여기서 <P(S),·>는 반군임을 알 수 있다.

{∅}∈P(S)가 존재해서 모든 A∈P(S)에 대하여 다음을 만족한다.

A+{∅}=(A∪{∅})−(A∩{∅})=A−{∅}=A

{∅}+A=({∅}∪A)−({∅}∩A)=A−{∅}=A

따라서 {∅}는 P(S)에서 덧셈에 관하여 항등원임을 알 수 있다.

또한 모든 A∈P(S)에 대하여 A+A=(A∪A)−(A∩A)={∅}

이 되게 하는 A∈P(S)이 존재하므로 A∈P(S)는 자기 자신을 역원으로 가진다.
그리고 임의의 A, B∈P(S)에 대하여
A+B=(A∪B)-(A∩B)=(B∪A)-(B∩A)=B+A
이 성립한다. 따라서 <P(S),+>는 가환군이다.
임의의 A, B, C∈P(S)에 대하여
A·B=A∩B=B∩A=B·A (곱셈에 관한 교환법칙)이고
A·(B+C)=A·{(B∪C)-(B∩C)}=A∩{(B∪C)-(B∩C)}=[{(A∩B)∪(A∩C)}-{(A∩B)∩(A∩C)}]
=[{(A∩B)∪(A∩C)}-{(A∩B)∩(A∩C)}]=[{(A·B)∪(AC)}-{(A·B)∩(A·C)}]=A·B+A·C (좌 분배법칙)
이 성립한다. 따라서 (A+B)·C=C·(A+B)=C·A+C·B=A·C+B·C(우 분배법칙)은 자명하게 성립한다.
그러므로 <P(S),+,·>는 환이다.
또한 모든 A∈P(S)에 대하여 $A^2 = A \bullet A = A \cap A = A$이 성립한다. 그러므로 <P(S),+,·>는 부울환이다.

문 1. Z_{12}**에서 방정식** $x^3-2x^2-3x=0$**의 모든 해를 구하라.**

풀 이

$x^3-2x^2-3x=x(x^2-2x-3)=x(x-3)(x+1)=x(x-3)(x-11)=0$

이므로 자명하게 0, 3, 11일 때 주어진 방정식은 영이 된다.

하지만 Z_{12}는 영인자를 가지므로 영인자를 갖는 경우에 대하여 추가적으로 생각해 보아야한다.

2·6=3·4=0 이므로 다음의 경우가 나타나는 x의 값을 찾아보면 5, 8, 9에서도 해가 됨을 알 수 있다.

따라서 구하고자 하는 모든 해는 0, 3, 5, 8, 9, 11이다.

문 2. 체 Z_7 **과** Z_{23}**에서 방정식** $3x=2$**를 각각 풀어라.**

풀 이

(a) $3x\equiv 2(\mathrm{mod}7)\Rightarrow 15x\equiv 10(\mathrm{mod}7)\Rightarrow x\equiv 3(\mathrm{mod}7)$

따라서 구하고자 하는 해는 3이다.

(b) $3x\equiv 2(\mathrm{mod}23)\Rightarrow 24x\equiv 16(\mathrm{mod}23)\Rightarrow x\equiv 16(\mathrm{mod}23)$

따라서 구하고자 하는 해는 17이다.

문 3. Z_6**에서 방정식** $x^2+2x+2=0$**의 모든 해를 구하라.**

풀 이

$$x^2+2x+2\equiv 0(\mathrm{mod}6)\Leftrightarrow\begin{cases}x^2+2x+2\equiv 0(\mathrm{mod}2)\\ x^2+2x+2\equiv 0(\mathrm{mod}3)\end{cases}$$

(a) $x^2+2x+2\equiv 0(\mathrm{mod}2)$ 인 경우

$x^2+2x+2\equiv 0(\mathrm{mod}2)\Rightarrow x^2\equiv 0(\mathrm{mod}2)\Rightarrow x\equiv 0(\mathrm{mod}2)$

(b) $x^2+2x+2\equiv 0(\mathrm{mod}3)$ 인 경우

$x^2+2x+2\equiv 0(\mathrm{mod}3)\Rightarrow x^2+2x+1\equiv -1(\mathrm{mod}3)\Rightarrow x^2+2x+1\equiv 2(\mathrm{mod}3)$
$\Rightarrow x^2+2x+1\equiv -1(\mathrm{mod}3)\Rightarrow (x+1)^2\equiv -1(\mathrm{mod}3)$

이때 드장드르 기호에 의하여 해의 존재성을 살펴보면 $(\frac{-1}{3})=-1$이므로 (b)의 경우의 이차방정식의 해는 존재하지 않는다. 따라서 (a)와(b)에서 모두 해가 존재해야 하는데 그렇지 않기 때문에 주어진 방정식은 $x^2+2x+2=0$의 해는 Z_6에서 존재하지 않는다.

문 4. Z_6**에서 방정식** $x^2+2x+4=0$**의 모든 해를 구하라.**

풀 이

$$x^2+2x+4\equiv 0(\mathrm{mod}6)\Leftrightarrow\begin{cases}x^2+2x+4\equiv 0(\mathrm{mod}2)\\ x^2+2x+4\equiv 0(\mathrm{mod}3)\end{cases}$$

(a) $x^2+2x+4\equiv 0(\mathrm{mod}2)$ 인 경우: $x^2+2x+4\equiv 0(\mathrm{mod}2)\Rightarrow x^2\equiv 0(\mathrm{mod}2)\Rightarrow x\equiv 0(\mathrm{mod}2)$

(b) $x^2+2x+4\equiv 0(\mathrm{mod}3)$ 인 경우

$x^2+2x+4\equiv 0(\mathrm{mod}3)\Rightarrow x^2+2x+1\equiv 0(\mathrm{mod}3)\Rightarrow (x+1)^2\equiv 0(\mathrm{mod}3)$
$\Rightarrow x+1\equiv 0(\mathrm{mod}3)\Rightarrow x\equiv 2(\mathrm{mod}3)$

따라서 중국인의 나머지 정리에 의하여 $x\equiv 0(\mathrm{mod}2), x\equiv 2(\mathrm{mod}3)\Leftrightarrow x\equiv 2(\mathrm{mod}6)$

그러므로 $x^2+2x+4\equiv 0(\mathrm{mod}6)$ 에서의 해는 2 뿐이다.

※ 문제 5~10에서 주어진 환의 표수를 구하라.

문 5. $2Z$

풀 이

1∉2Z이므로 표수는 0이다.

문 6. $Z\times Z$

풀 이

(1,1)∈$Z\times Z$이지만 n·(1,1)=(0,0) 이 되게 하는 양의 정수 ∄n이다.
따라서 $Z\times Z$의 표수는 0이다.

문 7. $Z_3\times 3Z$

풀 이

(1,1)∉$Z_3\times 3Z$이므로 $Z_3\times 3Z$의 표수는 0이다.

문 8. $Z_3\times Z_3$

풀 이

(1,1)∈$Z_3\times Z_3$이고 3·(1,1)=(0,0) 이 되게 하는 양의 정수 3이 존재한다.
따라서 $Z_3\times Z_3$의 표수는 3이다.

문 9. $Z_3\times Z_4$

풀 이

(1,1)∈$Z_3\times Z_4$이고 12·(1,1)=(0,0) 이 되게 하는 양의 정수 12가 존재한다.
따라서 $Z_3\times Z_4$의 표수는 12이다.

문 10. $Z_6\times Z_{15}$

풀 이

(1,1)∈$Z_6\times Z_{15}$이고 Z_6의 표수는 6이고 Z_{15}의 표수는 15이다.
따라서 $Z_6\times Z_{15}$의 표수는 lcm(6, 15)=30이다.
즉 30(1,1)=(0,0) 이 되게 하는 양의 정수 30이 존재한다.

문 11. 표수가 4인 단위원을 갖는 가환환을 R이라 하자. a, b∈R에 대하여 $(a+b)^4$을 계산하여 간단히 하라.

풀 이

표수가 4이므로 4·1=0을 만족한다. 따라서 a, b∈R에 대하여

$$\begin{aligned}(a+b)^4 &= \binom{4}{0}a^4+\binom{4}{1}a^3b+\binom{4}{2}a^2b^2+\binom{4}{3}a^1b^3+\binom{4}{4}b^4\\ &= 1a^4+4a^3b+6a^2b^2+4a^1b^3+b^4\\ &= 1a^4+(0)a^3b+(2+(0))a^2b^2+(0)a^1b^3+b^4\\ &= a^4+2a^2b^2+b^4\end{aligned}$$

이 성립하여 $(a+b)^4=a^4+2a^2b^2+b^4$임을 알 수 있다.

문 12. 표수가 3인 단위원을 갖는 가환환을 R이라 하자. a, b∈R에 대하여 $(a+b)^9$을 계산하여 간단히 하라.

풀 이

표수가 3이므로 3·1=0을 만족한다. 따라서 a, b∈R에 대하여

$$(a+b)^9 = \binom{9}{0}a^9 + \binom{9}{1}a^8b + \cdots + \binom{9}{8}ab^8 + \binom{9}{9}b^9$$

이 성립한다. 이때 $3|\binom{9}{1}, \cdots, 3|\binom{9}{8}$이므로 $(a+b)^9 = a^9 + b^9$임을 알 수 있다.

문 13. 표수가 3인 단위원을 갖는 가환환을 R이라 하자. a, b∈R에 대하여 $(a+b)^6$을 계산하여 간단히 하라.

풀 이

표수가 3이므로 3·1=0을 만족한다. 따라서 a, b∈R에 대하여

$$\begin{aligned}(a+b)^6 &= a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6 \\ &= a^6 + 2a^3b^3 + b^6\end{aligned}$$

이 성립한다. 따라서 $(a+b)^6 = a^6 + 2a^3b^3 + b^6$ 임을 알 수 있다.

문 14. $M_2(Z)$에서 행렬 $\begin{pmatrix}1&2\\2&4\end{pmatrix}$은 영인자임을 보여라.

풀 이

$\begin{pmatrix}1&2\\2&4\end{pmatrix}\begin{pmatrix}1&-2\\1&-2\end{pmatrix} = 0$이지만 $\begin{pmatrix}1&2\\2&4\end{pmatrix}, \begin{pmatrix}1&-2\\1&-2\end{pmatrix} \neq 0$이므로 $\begin{pmatrix}1&2\\2&4\end{pmatrix}$은 $M_2(Z)$에서 영인자이다.

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 15. 만약 ab=0 이면 a와 b는 영인자이다.

풀 이

[a≠0,b≠0일 때]라는 조건이 첨가되어야 한다. 즉, a≠0,b≠0일 때 ab=0 이면 a와 b는 영인자이다.

문 16. 환 R의 임의의 원소 a에 대하여 n·a=0이면 n은 R의 표수이다.

풀 이

[을 만족하는 가장 작은 양의 정수]라는 조건이 첨가되어야 한다. 즉, 환 R의 임의의 원소 a에 대하여 n·a=0을 만족하는 가장 작은 양의 정수 n을 R의 표수라 한다.

문 17. 참과 거짓을 판단하시오.

(a) n이 소수가 아니면 nZ는 0인자를 갖는다.

풀 이 (False)

n=1일 때 Z는 0인자를 갖지 않는다.

(b) 모든 체는 정역이다.

풀 이 (True)

임의의 체 F에 대하여 임의의 원소 a, b∈ F에 대하여 a≠0이고 ab=0이면 a는 곱셈에 대한 역원을 갖기 때문에 b=0임을 알 수 있다. 따라서 체 F는 정역이다.

(c) nZ의 표수는 n이다.

풀 이 (False)

n=1일 때 Z의 표수는 0이다.

(d) 모든 n≧1에 대하여 환으로서 Z와 nZ는 동형이다.

풀 이 (False)

n>1인 경우 Z는 곱셈에 대한 단위원 1을 갖는다. 하지만 nZ는 곱셈에 대한 단위원 1을 갖지 않는다. 따라서 동형이 아니다.

(e) 정역과 동형인 환에서는 약분법칙이 성립한다.

풀 이 (True)

D를 정역, R을 정역 D와 동형인 환이라 하자. 그러면 임의의 a, b, c∈ R 에 대하여 a≠0이고 a(b-c)=0이면 R은 정역이므로 b-c=0이 성립한다. 따라서 ab=ac 이면 b=c 이므로 약분법칙이 성립한다.

(f) 표수가 0인 모든 정역은 무한이다.

풀 이 (True)

표수가 0인 임의의 정역 D가 유한이라 가정하자. 즉 D의 위수를 0이 아닌 n이라 하면 덧셈군 (D,+)에서 1의 위수는 n이다. 이는 표수가 0임에 모순된다. 따라서 표수가 0인 모든 정역은 무한이다.

(g) 두 정역의 직적은 다시 정역이다.

풀 이 (False)

Z는 정역이지만 ZxZ는 정역이 아니다. 즉, (1,0),(0,1)∈ZxZ이지만 (0,0)=(1,0)·(0,1)이다.

(h) 단위원을 갖는 가환환에서 0인자는 곱에 대한 역원을 갖지 않는다.

풀 이 (True)

갖는다고 가정하자. 단위원을 갖는 가환환에서 a를 0인자라고 하자. 그러면 곱에 대한 역원 b가 존재해서 다음이 성립한다.

1=ab=ba=0

이는 1=0이므로 모순이다. 따라서 단위원을 갖는 가환환에서 0인자는 곱에 대한 역원을 갖지 않는다.

(i) nZ는 Z의 부분정역이다.

풀 이 (False)

n=2인 경우, 2Z는 단위원을 갖지 않는다. 따라서 정역이 아니다.

(j) Z는 Q의 부분체이다.

풀 이 (False)

Z는 체가 아니다.

문 18. Each of the six numbered region in Fig 19.10 corresponds to a certain type of a ring. Give an example of a ring in each of the six cells. For example. a ring in the region numbered 3 must be commutative (it is inside the commutative circle) have unity. but not be an integral domain

풀 이 -생 략-

문 19. (선형대수학의 한 학기를 이수한 학생들을 위한 문제) F를 체라 하자. 0인자가 되는 $M_n(F)$의 원소 A의 서로 다른 다섯 가지 형태를 구하라.

풀 이 - 생 략-

문 20. Redraw Fig19.10 to include a subset corresponding to strictly skew fields.

풀 이 - 생 략-

문 21. -생 략-

문 22. -생 략-

문 23. $a^2=a$를 만족하는 환 R의 원소를 멱등원이라 한다. 나눗셈환은 꼭 두 개의 멱등원을 포함함을 보여라.

풀 이

$0^2=0, 1^2=1$이다. 이제 $a\neq 0,1$인 $a\in R$인 멱등원이라 하자. 그러면 $a^2=a$이 성립한다.
이때 R 은 나눗셈 환이므로 $b\neq o$가 존재해서 다음을 만족한다.

$$a=a\cdot 1=a(ab)=a^2b=ab=1$$

이는 a≠1임에 모순이다. 따라서 나눗셈환은 꼭 두 개의 멱등원을 포함한다.

문 24. 정역 D의 부분정역의 공통집합도 역시 D의 부분정역이 됨을 보여라.

풀 이

H, k 를 정역 D의 부분 정역이라 하자. 그러면 1∈H 이고 1∈K 이므로 1∈H∩K이다. 따라서 H∩K≠∅인 단위원을 갖는 가환환이다. a≠0인 임의의 원소 a, b∈H∩K에 대하여 ab=0이면
a, b∈H 이므로 a≠0, ab=0일때 b=0 이고 a, b∈K 이므로 a≠0, ab=0일때 b=0 이다.
따라서 b=0 인 b∈H∩K이다. 그러므로 정역 D의 부분정역의 공통집합도 역시 D의 부분정역이다.

문 25. 단위원을 갖고 0인자를 갖지 않는 유환환 R는 나눗셈환임을 보여라.(가환성을 증명하기는 어렵지만 이것은 실제로 체이다. 정리24.10)
[참고: a≠0가 가역원임을 보이기 위해 R에서 a≠0의 "곱에 대한 좌측 역원" 또는 "곱에 대한 우측역원"임을 보여야 한다.]

풀 이

단위원을 갖고 0인자를 갖지 않는 유환환 R은 필요충분하게 R은 유한 정역이다. 여기서 유한 정역 R이 나눗셈환임을 보이면 충분하다. R이 유한개의 원소로 이루어져 있으므로 $R=\{1,a_1,a_2,\cdots,a_n\}$이라 하자. 0이 아닌 임의의 원소 a∈R에 대하여 $aR=\{a,aa_1,aa_2,\cdots,aa_n\}$는 aR⊆R이다.
여기서 임의의 $i\neq j$에 대하여 $aa_i=aa_j$이면 R이 정역이므로(0인자를 갖지 않으므로) $a_i=a_j$이 되어 모순이다. 따라서 aR의 위수는 n+1이다. 따라서 aR=R이다.
그러므로 ab=1이 되게 하는 원소 b∈R 가 존재한다. 따라서 R은 나눗셈환이다.

문 26. R는 적어도 두 개의 원소를 포함하는 환이라 하자. 0이 아닌 각 a∈R에 대하여 aba=a를 만족하는 유일한 b가 존재한다고 가정하자.

(a) R는 0인자를 갖지 않음을 보여라.

풀 이

0이 아닌 원소 a를 환 R의 0인자라 하자. 그러면 0이 아닌 원소 c가 존재해서 ac=0 또는 ca=0 을 만족한다. 또한 조건에 의하여 aba=a를 만족하게 하는 유일한 b가 존재한다.
이때 a(b+c)a=aba+aca=aba=a를 만족한다. 그러면 b의 유일성에 의하여 b+c=b이고 따라서 c=0이 된다. 이는 모순이다. 따라서 R은 0인자를 갖지 않는다.

(b) bab=b임을 보여라.

풀 이

0이 아닌 원소 a에 대하여 aba=a 를 만족하게 하는 유일한 원소 b가 존재한다고 하자. 그러면 (bab-b)a=baba-ba=b(aba)-ba=ba-ba=0이 성립한다. 여기서 R은 0인자를 갖지 않고 a≠0이므로 bab-b=0이 된다. 따라서 bab=b이다.

(c) R는 단위원을 가짐을 보여라.

풀 이

0이 아닌 원소 a에 대하여 aba=a 를 만족하게 하는 유일한 원소 b가 존재한다고 하자. 0이 아닌 원소 c에 대하여 caba=ca가 성립한다. 여기서 0인자를 갖지 않으므로 a 를 오른쪽 소약법칙에 의하여 소거하면 babc=bc를 만족한다.
또한 (b)에 의하여 babc=bc가 성립한다. 여기서 0인자를 갖지 않으므로 b 를 왼쪽 소약법칙에 의하여 소거하면 (ab)c=c. 그러면 c(ab)=c=(ab)c 이 성립하는 ab가 존재함을 알 수 있다. 여기서 ab는 단위원의 역할을 한다.

(d) R가 나눗셈환임을 보여라.

풀 이

(c)에 의하여 ab=1이라 하면 단위원을 갖는다. 그리고 0이 아닌 원소 a에 대하여 aba=a 를 만족하게 하는 유일한 원소 b가 존재한다고 하자. 그러면 (ab-1)a=aba-a=a-a=0 이고 a≠0이므로 ab=1 임을 알 수 있다. 또한 a(ba-1)=aba-a=0 이고 a≠0이므로 ba=1 임을 알 수 있다. 따라서 ab=ba=1이 되게 하는 b가 존재하므로 R은 나눗셈환이다.

문 27. 정역 D의 부분정역의 표수는 D의 표수와 같음을 보여라.

풀 이

정역 D의 부분정역을 D'이라 하고 각각의 표수를 n,m이라 하자. 그러면 0이 아닌 임의의 a∈D'에 대하여 a∈D이기도 하므로 다음이 성립한다.

$a \cdot m = 0 = a \cdot n$

따라서 소약 법칙에 의하여 n=m이 된다. 그러므로 정역 D의 부분정역의 표수는 D의 표수와 같다.

문 28. D가 정역이면 {n·1 | n∈Z}는 D의 모든 부분정역에 포함되는 D의 부분정역임을 보여라.

풀 이

<1>={n・1 | n∈Z}라 하자. 임의의 n,m∈Z에 대하여

n・1-m・1=(n-m)・1이고 n-m∈Z, (n・1)(m・1)=(nm・1)이고 nm∈Z

이므로 <1>는 부분환이다. 그리고 1∈<1>이고 (n・1)(m・1)=(nm・1)=(mn・1)=(m・1)(n・1)이므로 단위원을 갖는 가환환이다. 임의의 n・1, m・1∈<1>에 대하여

(n・1)(m・1)=0 이면 n・1, m・1∈D이기도 하므로 n・1≠0, m・1≠0임을 알 수 있다.

따라서 <1>은 0인자를 갖지 않는다. 그러므로 <1>는 D의 부분 정역이다.

문 29. 정역 D의 표수는 0이거나 소수 p임을 보여라.

[힌트: D의 표수가 mn이면 D에서 (m·1)(n·1)을 생각해 보라.

풀 이

정역 D의 표수가 0이 아니라고 하자. 그러면 표수는 임의의 n이다. 여기서 n이 소수가 아니라면 n은 합성수이고 n=st(1<s<n,1<t<n)와 같이 정수들의 곱으로 표현된다. 여기서 표수의 정의에 의하여 1・n=(1・s)(1・t)=0이고 D가 정역이므로 1・s=0 또는 1・t=0이 된다. 이는 n이 1・n=0을 만족한다는 가장 작은 양의정수라는 표수의 정의에 모순된다. 따라서 표수는 0이거나 소수p이다.

문 30. 이 연습문제에서 모든 환 R는 R과 같은 표수를 갖는 환 S로 확장될 수 있음을 보이고 있다. 만약, R의 표수 0을 갖는다면 $S=R\times Z$라 하고, 만약 R가 표수 n을 가지면 $S=R\times Z_n$으로 하자. S에서 덧셈은 일상의 성분에 의한 덧셈이고 곱셈은

$$(r_1,n_1)(r_2,n_2)=(r_1r_2+n_1r_2+n_2r_1,n_1n_2)$$

로 정의한다. 단 n·r은 (18장)에서 설명한 의미를 갖는다.

(a) S가 환임을 보여라.

풀 이

$<S,+,\bullet>$이 환이 되기 위하여 곱셈에 대하여 결합법칙이 성립함을 보이면 나머지는 자명하므로 충분하다. 임의의 $(r_1,n_1),(r_2,n_2),(r_3,n_3)\in S$에 대하여

$$[(r_1,n_1)(r_2,n_2)](r_3,n_3)=(r_1r_2+n_1r_2+n_2r_1,n_1n_2)(r_3,n_3)$$
$$=(r_1r_2r_3+n_1r_2r_3+n_2r_1r_3+n_3r_1r_2++n_1n_2r_3+n_3n_1r_2+n_2n_3r_1,n_1n_2n_3)$$
$$(r_1,n_1)[(r_2,n_2)(r_3,n_3)]=(r_1,n_1)(r_2r_3+n_2r_3+n_3r_2,n_2n_3)$$
$$=(r_1r_2r_3+n_1r_2r_3+n_2r_1r_3+n_3r_1r_2++n_1n_2r_3+n_3n_1r_2+n_2n_3r_1,n_1n_2n_3)$$

따라서 $[(r_1,n_1)(r_2,n_2)](r_3,n_3)=(r_1,n_1)[(r_2,n_2)(r_3,n_3)]$이 성립하고 따라서 $<S,+,\bullet>$는 환이다.

(b) S가 단위원을 가짐을 보여라.

풀 이

$(0,1)\in S,(r_1,n_1)(0,1)=(r_1,n_1)=(0,1)(r_1,n_1)$이므로 S는 단위원(0,1)을 갖는다.

(c) S와 R이 같은 표수를 가짐을 보여라.

풀 이

R의 표수가 0이면 $S=R\times Z$에 대하여 (1,1)∈S 이고 임의의 정수 n에 대하여 n(1,1)≠0 이다. 따라서 S의 표수도 0이다. R의 표수가 n이면 $S=R\times Z_n$에 대하여 (1,1)∈S 이고 정수 n에 대하여 n(1,1)=0 이다. 만약 n보다 작은 정수m 에 대하여 m(1,1)=0이면 m·1=0 이 되어 Z_n의 표수가 n임에 모순이다. 따라서 S의 표수는 n이다. 따라서 S와 R은 같은 표수를 갖는다.

(d) r∈R에 대하여 $\Phi(r)=(r,0)$으로 정의된 사상 $\Phi: R\to S$는 S의 부분환 위로 동형적으로 대응한다.

풀 이

임의의 a,b∈R 에 대하여

$\Phi(a+b)=(a+b,0)=(a,0)+(b,0)=\Phi(a)+\Phi(b),\ \Phi(ab)=(ab,0)=(a,0)(b,0)=\Phi(a)\Phi(b)$

이므로 환 준동형 사상이다. 그리고 $\Phi(a)=\Phi(b)\Rightarrow(a,0)=(b,0)\Rightarrow a=b$ 이므로 단사이다.

그러므로 $im\Phi=\{\Phi(x)|x\in R\}=\Phi(R)$에 대하여 Φ는 환 동형사상이 됨을 알 수 있다. 여기서 $\Phi(R)$은 S의 부분환임은 자명하다.

Fraleigh 대수 20장 페르마 정리와 오일러 정리

※ 유한체의 0이 아닌 원소의 곱셈에 대한 군이 순환적임은 뒤에 알게 되겠지만, 다음에 주어진 유한체에 대한 생성원을 구하여 이 사실을 설명하여라.

문 1. Z_7

풀 이

<1>={1}, <2>=<4>={1,2,4}, <6>={1,6}, Z_7=<3>=<5>이므로 생성원은 3,5 이고 이로부터 순환적임을 알 수 있다.

문 2. Z_{11}

풀 이

Z_{11}=<2>=<6>=<7>=<8>이므로 생성원은 2,6,7,8 이고 이로부터 순환적임을 알 수 있다.

문 3. Z_{17}

풀 이

Z_{17}=<3>=<5>=<6>=<7>=<10>=<11>=<12>=<14>이므로
생성원은 3,5,6,7,10,11,12,14이고 이로부터 순환적임을 알 수 있다.

문 4. 페르마의 정리를 이용하여 3^{47}를 23으로 나누었을 때의 나머지를 구하라.

풀 이

페르마 정리에 의하여 $3^{23-1} \equiv 1(\mathrm{mod}23)$임을 알 수 있다.
그러면 $3^{47} \equiv 3^{2(23-1)}3^3 \equiv 27 \equiv 4(\mathrm{mod}23)$이다.
그러므로 3^{47}를 23으로 나누었을 때의 나머지는 4이다.

문 5. 페르마의 정리를 이용하여 37^{49}를 7으로 나누었을 때의 나머지를 구하라.

풀 이

페르마 정리에 의하여 $37^{7-1} \equiv 1(\mathrm{mod}7)$임을 알 수 있다.
그러면 $37^{49} \equiv 2^{49} \equiv 2^{8(7-1)}2^1 \equiv 2(\mathrm{mod}7)$이다.
그러므로 3^{49}를 7로 나누었을 때의 나머지는 2이다.

문 6. $2^{(2^{17})}+1$**을 19로 나누었을 때의 나머지를 계산하라.**
[힌트: 2^{17}**의 18을 법으로 하는 나머지를 계산할 필요가 있을 것이다.]**

풀 이

페르마 정리에 의하여 $2^{17} \equiv (2^4)^4 2 \equiv (-2)^4 2 \equiv 32 \equiv 14(\mathrm{mod}18)$이므로
$2^{(2^{17})}+1 \equiv 2^{14}+1 \equiv 6+1 \equiv 7(\mathrm{mod}19)$이 성립한다. 따라서 구하는 나머지는 7이다.

문 7. $n \le 30$에 대하여 $\Phi(n)$의 값을 표로 만들어라.

풀 이

$\Phi(1)$	$\Phi(2)$	$\Phi(3)$	$\Phi(4)$	$\Phi(5)$	$\Phi(6)$	$\Phi(7)$
1	1	2	2	4	2	6
$\Phi(8)$	$\Phi(9)$	$\Phi(10)$	$\Phi(11)$	$\Phi(12)$	$\Phi(13)$	$\Phi(14)$
4	6	4	10	4	12	6
$\Phi(15)$	$\Phi(16)$	$\Phi(17)$	$\Phi(18)$	$\Phi(19)$	$\Phi(20)$	$\Phi(21)$
8	8	16	6	18	8	12
$\Phi(22)$	$\Phi(23)$	$\Phi(24)$	$\Phi(25)$	$\Phi(26)$	$\Phi(27)$	$\Phi(28)$
10	22	8	20	12	18	12
$\Phi(29)$	$\Phi(30)$					
28	8					

문 8. p가 소수일 때, $\Phi(p^2)$를 계산하라.

풀 이

p가 소수일 때 $\Phi(p^2) = \Phi(p)\Phi(p) = (p-1)(p-1) = (p-1)^2$이 성립한다.

문 9. p와 q가 서로 다른 소수일 때 $\Phi(pq)$를 계산하라.

풀 이

p와 q가 서로 다른 소수일 때 $\Phi(pq) = \Phi(p)\Phi(q) = (p-1)(q-1)$이 성립한다.

문 10. 페르마의 정리에 대한 오일러의 일반적인 정리를 이용하여 7^{1000}을 24로 나누었을 때의 나머지를 구하라.

풀 이

gcd(7,24)=1이므로 오일러의 일반적인 정리에 의하여
$7^{24} \equiv 7(\mathrm{mod}24)$이고 $1000 \equiv 16(\mathrm{mod}24)$이므로 $7^{1000} \equiv 7^{16} \equiv (7^2)^8 \equiv (49)^8 \equiv (2 \cdot 24+1)^8 \equiv 1(\mathrm{mod}24)$
이 성립한다. 따라서 구하는 나머지는 1이다.

※ 문제 11~18에서 (예제20.14)와 (예제20.15)에서 했듯이 주어진 합동방정식의 모든 해를 구하라.

문 11. $2x \equiv 6(\mathrm{mod}4)$

풀 이

gcd(2,4)=2이므로 $2x \equiv 6(\mathrm{mod}4) \Leftrightarrow x \equiv 3 \equiv 1(\mathrm{mod}2)$이 성립한다.
따라서 구하고자 하는 해는 $x \equiv 1(\mathrm{mod}4)$ 또는 $x \equiv 3(\mathrm{mod}4)$이다.

문 12. $22x \equiv 5(\mathrm{mod}15)$

풀 이

$22x \equiv 5(\mathrm{mod}15) \Leftrightarrow 7x \equiv 5(\mathrm{mod}15) \Leftrightarrow 14x \equiv 10(\mathrm{mod}15) \Leftrightarrow x \equiv 5(\mathrm{mod}15)$
따라서 구하고자 하는 해는 $x \equiv 5(\mathrm{mod}15)$이다.

문 13. $36x \equiv 15(\mathrm{mod}24)$

풀 이

gcd(36,24)=6이지만 $6 \nmid 15$이므로 해는 존재하지 않는다.

문 14. $45x \equiv 15(\mathrm{mod}24)$

풀 이

gcd(45,24)=3이므로

$45x \equiv 15(\mathrm{mod}24) \Leftrightarrow 15x \equiv 5(\mathrm{mod}8) \Leftrightarrow (-1)x \equiv 5(\mathrm{mod}8) \Leftrightarrow x \equiv -5(\mathrm{mod}8) \Leftrightarrow x \equiv 3(\mathrm{mod}8)$

이 성립한다. 따라서 구하고자 하는 해는 $x \equiv 3(\mathrm{mod}8)$ 이다.

또는 $x \equiv 3(\mathrm{mod}8), x \equiv 11(\mathrm{mod}8), x \equiv 19(\mathrm{mod}8)$ 이다.

문 15. $39x \equiv 125(\mathrm{mod}9)$

풀 이

$39x \equiv 125(\mathrm{mod}9) \Leftrightarrow 3x \equiv 8(\mathrm{mod}9)$ 이고 gcd(3,9)=3이지만 $3 \nmid 8$이므로 해는 존재하지 않는다.

문 16. $41x \equiv 125(\mathrm{mod}9)$

풀 이

$41x \equiv 125(\mathrm{mod}9) \Leftrightarrow 5x \equiv 8(\mathrm{mod}9) \Leftrightarrow 10x \equiv 16(\mathrm{mod}9) \Leftrightarrow x \equiv 7(\mathrm{mod}9)$

따라서 구하고자 하는 해는 $x \equiv 7(\mathrm{mod}9)$ 이다.

문 17. $155x \equiv 75(\mathrm{mod}65)$

풀 이

gcd(155,65)=5이므로

$155x \equiv 75(\mathrm{mod}65) \Leftrightarrow 31x \equiv 15(\mathrm{mod}13) \Leftrightarrow 5x \equiv 2(\mathrm{mod}13) \Leftrightarrow 40x \equiv 16(\mathrm{mod}13) \Leftrightarrow x \equiv 3(\mathrm{mod}13)$

이 성립한다. 따라서 구하고 자 하는 해는

$x \equiv 3(\mathrm{mod}13), x \equiv 16(\mathrm{mod}13), x \equiv 29(\mathrm{mod}13), x \equiv 42(\mathrm{mod}13), x \equiv 55(\mathrm{mod}13)$이다.

문 18. $39x \equiv 52(\mathrm{mod}130)$

풀 이

gcd(39,130)=13이므로

$39x \equiv 52(\mathrm{mod}130) \Leftrightarrow 3x \equiv 4(\mathrm{mod}10) \Leftrightarrow -9x \equiv -12(\mathrm{mod}10) \Leftrightarrow x \equiv 8(\mathrm{mod}10)$

이 성립한다. 따라서 구하고자 하는 해는

$x \equiv 8(\mathrm{mod}10), x \equiv 18(\mathrm{mod}10), x \equiv 28(\mathrm{mod}10), x \equiv 38(\mathrm{mod}10), x \equiv 48(\mathrm{mod}10), x \equiv 58(\mathrm{mod}10)$
$, x \equiv 68(\mathrm{mod}10), x \equiv 78(\mathrm{mod}10), x \equiv 88(\mathrm{mod}10), x \equiv 98(\mathrm{mod}10), x \equiv 108(\mathrm{mod}10), x \equiv 118(\mathrm{mod}10)$
$, x \equiv 128(\mathrm{mod}10)$

문 19. p를 3보다 크거나 같은 소수라 하자. 아래의 (문제28)을 이용하여 $(p-2)!$의 p를 법으로하는 나머지를 구하라.

풀 이

(문제28)에 의하여 $(p-1)! \equiv -1(\mathrm{mod}p)$이므로

$(p-1)(p-2)! \equiv -1(\mathrm{mod}p) \Leftrightarrow -1(p-2)! \equiv -1(\mathrm{mod}p) \Leftrightarrow (p-2)! \equiv 1(\mathrm{mod}p)$

따라서 구하고자 하는 나머지는 1이다.

문 20. 아래의 (문제28)를 이용하려 34!의 37을 법으로 하는 나머지를 구하라.

풀 이

(문제28)에 의하여 $35! = (37-2)! \equiv 1(\mathrm{mod}37)$이므로

$35 \cdot 34! \equiv 1(\mathrm{mod}37) \Leftrightarrow (-2)34! \equiv 1(\mathrm{mod}37) \Leftrightarrow (-36)34! \equiv 18(\mathrm{mod}37) \Leftrightarrow 34! \equiv 18(\mathrm{mod}37)$

따라서 구하고자 하는 나머지는 18이다.

문 21. 아래의 (문제28)를 이용하려 49!의 53을 법으로 하는 나머지를 구하라.

풀 이

(문제28)에 의하여 $51! = (53-2)! \equiv 1(\mathrm{mod}53)$이므로

$51 \cdot 50 \cdot 49! \equiv 1(\mathrm{mod}53) \Leftrightarrow (-2)(-3)49! \equiv 1(\mathrm{mod}53)$
$\Leftrightarrow (6)49! \equiv 1(\mathrm{mod}53) \Leftrightarrow (54)49! \equiv 9(\mathrm{mod}53) \Leftrightarrow 49! \equiv 9(\mathrm{mod}53)$

따라서 구하고자 하는 나머지는 9이다.

문 22. 아래의 (문제28)를 이용하려 24!의 29을 법으로 하는 나머지를 구하라.

풀 이

(문제28)에 의하여 $27! = (29-2)! \equiv 1(\mathrm{mod}29)$이므로

$27 \cdot 26 \cdot 25 \cdot 24! \equiv 1(\mathrm{mod}29) \Leftrightarrow (-2)(-3)(-4)24! \equiv 1(\mathrm{mod}29) \Leftrightarrow (-24)24! \equiv 1(\mathrm{mod}29)$
$\Leftrightarrow (5)24! \equiv 1(\mathrm{mod}29) \Leftrightarrow (30)24! \equiv 6(\mathrm{mod}29) \Leftrightarrow 24! \equiv 6(\mathrm{mod}29)$

따라서 구하고자 하는 나머지는 6이다.

문 23. 참과 거짓을 판정하라.

(a) 모든 정수 a와 소수 p에 대하여 $a^{p-1} \equiv 1(\mathrm{mod}p)$이다.

풀 이 (False)

a=3, p=3일 때 $3^{3-1} \equiv 0(\mathrm{mod}3)$이다.

(b) 소수 p에 대한 a≠0(mod p)을 만족하는 모든 정수 a에 대하여 $a^{p-1} \equiv 1(\mathrm{mod}p)$이다.

풀 이 (True)

페르마의 정리에 의하여 성립한다.

(c) 모든 $n \in Z^+$에 대하여 $\Phi(n) \leq n$이다.

풀 이 (True)

n=1일 때 $\Phi(1) = 1$이고

n≥2일 때 $n = p_1^{r_1} \cdots p_s^{r_s}$의 꼴이며 다음이 성립한다.

$$\Phi(n) = \Phi(p_1^{r_1} \cdots p_s^{r_s}) = \Phi(p_1^{r_1}) \cdots \Phi(p_s^{r_s}) = n(1-\frac{1}{p_1}) \cdots (1-\frac{1}{p_s}) \leq n$$

따라서 모든 $n \in Z^+$에 대하여 $\Phi(n) \leq n$이 성립한다.

(d) 모든 $n \in Z^+$에 대하여 $\Phi(n) \leq n-1$이다.

풀 이 (False)

n=1일 때 $\Phi(1) = 1$이다.

(e) Z_n에서 가역원은 n보다 적으면서 n과 서로소인 양의 정수이다.

풀 이 (True)

a를 Z_n에서 가역원이라 하자. 이 때 gcd(a,n)=d>1이라 가정하면 a·(n/d)=(a'·d)n'=a'(dn')=a'n=0이 된다. 따라서 a는 0인자가 된다. 이는 모순이다. 그러므로 a는 n과 서로소인 정수이다. 그리고 Z_n에서 n보다 큰 정수는 존재하지 않으므로 자명하게 a는 보다 적어야 한다.

(f) Z_n에서 두 가역원의 곱은 역시 가역원이다.

풀 이 (True)

U(Z_n)은 곱셈에 대하여 군을 이룬다. 그러므로 닫혀있음은 자명하다.

(g) Z_n에서 두 비가역원의 곱은 가역원이 될 수도 있다.

풀 이 (False)

a와 b를 비가역원이라 하자. 여기서 두 비가역원의 곱이 가역원이 될 수도 있다고 가정하자. 그러면 임의의 0이 아닌 원소 e가 존재해서 e(ab)=(ab)e=1을 만족한다. a와 b는 0인자 이므로 0이 아닌 원소 c,d 가 존재해서 다음을 만족한다.

d=e(ab)d=ea(bd)=ea·0=0

c=c(ab)e=(ca)be=0·be=0

이는 모순이다. 따라서 Z_n에서 두 비가역원의 곱은 가역원이 될 수도 없다.

(h) Z_n에서 가역원과 비가역원의 곱은 절대 가역원이 될 수 없다.

풀 이 (True)

a를 가역원, b를 비가역원이라 하자. 여기서 가역원과 비가역원의 곱이 가역원이 될 수도 있다고 가정하자. 그러면 임의의 0이 아닌 원소 e가 존재해서 e(ab)=(ab)e=1을 만족한다. b는 0인자 이므로 0이 아닌 원소 d 가 존재해서 다음을 만족한다.

d=e(ab)d=ea(bd)=ea·0=0

이는 모순이다. 따라서 Z_n에서 가역원과 비가역원의 곱은 가역원이 될 수 없다.

(i) p가 소수일 때 모든 합동방정식 $ax \equiv b(\mathrm{mod}p)$는 해를 갖는다.

풀 이 (False)

$3x \equiv 2(\mathrm{mod}3)$은 해를 갖지 않는다.

(j) d를 양의 정수 a와 m의 최대 공약수라 하자. d가 b를 나누면 합동방정식 $ax \equiv b(\mathrm{mod}m)$는 정확히 d개의 합동이 아닌 해를 갖는다.

풀 이 (True)

d가 b를 나누므로 해는 존재한다. a=a'd, b=b'd, m=m'd라 하면 $ax \equiv b(\mathrm{mod}m) \Leftrightarrow a'x \equiv b'(\mathrm{mod}m')$

이고 $a'x \equiv b'(\mathrm{mod}m')$는 해를 하나 갖는다. 이때 $x \equiv c(\mathrm{mod}m')$라 하면

$x \equiv c(\mathrm{mod}m') \Leftrightarrow x \equiv c+m'(\mathrm{mod}m), x \equiv c+2m'(\mathrm{mod}m), \cdots x \equiv c+(d-1)m'(\mathrm{mod}m)$

로서 정확히 d개의 합동이 아닌 해를 갖는다.

문 24. Z_{12}에서 가역원의 곱셈에 대한 군의 연산표를 만들어라. 그것은 위수가 4인 어떤 군과 동형인가?

풀 이

U(Z_{12})={1,5,7,11}이므로 다음과 같이 군의 연산표를 만들 수 있다.

◦	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\approx < Z_2 \times Z_2, + >$

문 25. -생 략-

문 26. -생 략-

문 27. 1과 p-1은 자기 자신이 곱에 대한 역원이 되는 체 Z_p의 유일한 원소임을 보여라.

[힌트: 방정식 $x^2-1=0$을 생각하라.]

풀 이

체 Z_p에서 방정식 $x^2-1=0$의 해는 많아야 두 개 존재한다. 만약 두 개 이상이면 정역에 모순이다.
그러므로 $x^2-1 \equiv 0(\mathrm{mod}p)$의 해는 Z_p가 체이므로 많아야 두 개 존재한다.

$x^2-1 \equiv 0(\mathrm{mod}p) \Leftrightarrow x^2 \equiv 1(\mathrm{mod}p) \Leftrightarrow x \equiv 1(\mathrm{mod}p)$또는$x \equiv -1 \equiv p-1(\mathrm{mod}p)$

따라서 1과 p-1은 자기 자신이 곱에 대한 역원이 되는 체 Z_p의 유일한 원소이다.

문 28. (문제27)를 이용하여 p가 소수이면 (p-1)!≡-1(mod p)라는 윌슨의 정리를 유도하라.
[n이 (n-1)!≡ -1(mod p)을 만족하는 1보다 큰 정수이면, n은 소수이다. n이 소수가 아니면 (n-1)!의 법으로 하는 나머지는 무엇인가를 생각해 보라.]

풀 이

(문제27)로부터 체 Z_p에서 1과 p-1만이 자기 자신이 곱에 대한 역원임을 알았다. 즉 1과 p-1이외의 수들은 서로 다른 수들이 곱이 역원이 된다. 즉 체 Z_p에서 짝수개의 (p-2)(p-3)…(2)의 곱은 1이 된다.
따라서 p≥3인 경우 (p-1)!≡(p-1)(p-2)…(2)(1)≡(p-1)(1)(1)≡p-1≡-1(mod p)이다. 또한 p=2인 경우 (2-1)!≡-1≡1(mod 2)이므로 따라서 p가 소수이면 (p-1)!≡-1(mod p)라는 윌슨의 정리를 유도할 수 있다.

문 29. 페르마의 정리를 이용하려 임의의 양의 정수 n에 대하여 $n^{37}-n$은 383838로 나누어짐을 보여라.
[힌트:383838=(37)(19)(13)(7)(3)(2)이다.]

풀 이

페르마 소정리 $a^p \equiv a(\mathrm{mod}p)$임을 이용하면 다음과 같은 결과를 얻을 수 있다.

$n^{37}-n \equiv 0(\mathrm{mod}2),\ n^{37}-n \equiv 0(\mathrm{mod}3),\ n^{37}-n \equiv 0(\mathrm{mod}7),$
$n^{37}-n \equiv 0(\mathrm{mod}13),\ n^{37}-n \equiv 0(\mathrm{mod}19),\ n^{37}-n \equiv 0(\mathrm{mod}37)$

따라서 필요충분하게 $n^{37}-n \equiv 0(\mathrm{mod}383838)$이 성립한다.
그러므로 임의의 양의 정수 n에 대하여 $n^{37}-n$은 383838로 나누어진다.

문 30. (문제29)을 참고로 하여 모든 양의 정수 n에 대하여 $n^{37}-n$을 나누는 383838보다 큰 수를 찾아라.

풀 이

$n^{37}-n \equiv 0(\mathrm{mod}5)$도 성립하므로 5(383838)=1919190으로도 나누어진다.

문 1. C의 부분정역 $D=\{n+mi|n,m\in Z\}$의 분수체 F를 구하라. 여기서 "구하라"는 것은 C에서 D의 분수체를 형성하는 C의 원소를 구하라는 의미이다.

풀 이

$$F=\left\{\frac{x}{y}|x,y\in D,y\neq 0\right\}=\left\{\frac{a+bi}{c+di}|a,b,c,d\in Z,\ c\neq 0\text{ 또는 }d\neq 0,\right\}$$
$$=\left\{\frac{(ac+bd)+i(bc-ad)}{c^2+d^2}|a,b,c,d\in Z,\ c^2+d^2\neq 0\right\}$$
$$=\{m+ni|m,n\in Q\}$$

문 2. R의 부분정역 $D=\{n+m\sqrt{2}|n,m\in Z\}$의 분수체 F를 구하라. (문제1과 같은 의미에서)

풀 이

$$F=\left\{\frac{x}{y}|x,y\in D,y\neq 0\right\}=\left\{\frac{a+b\sqrt{2}}{c+d\sqrt{2}}|a,b,c,d\in Z,\ c\neq 0\text{ 또는 }d\neq 0,\right\}$$
$$=\left\{\frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}|a,b,c,d\in Z,\ c^2-2d^2\neq 0\right\}$$
$$=\{m+n\sqrt{2}|m,n\in Q\}$$

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 3. A *field of quotients* of integral domain D is a field F which D can be embedded so that every nonzero element of D is a unit in F.

풀 이

해석) 정역 D의 분수체 F는 임의의 0이 아닌 D의 원소는 F에서 가역원으로 포함될 수 있는 체이다.
▷ 맞는 정의인 듯!!

문 4. 참과 거짓을 판정하라.

(a) Q는 Z의 분수체이다.

풀 이 (True)

$Q=\left\{\frac{a}{b}|a,b\in Z,b\neq o\right\}$이므로 Q는 Z의 분수체이다.

(b) R는 Z의 분수체이다.

풀 이 (False)

$\sqrt{2}\neq\frac{a}{b}$인 $a,b\in Z,b\neq o$가 존재하지 않는다.

(c) R는 R의 분수체이다.

풀 이) (True)

R은 체이므로 $R=\left\{\frac{a}{b}|a,b\in R,b\neq o\right\}=\{x|x\in R\}=R$이 성립한다. 따라서 R는 R의 분수체이다.

(d) C는 R의 분수체이다.

풀 이 (False)

i는 R의 원소가 아니다.

(e) D가 체이면 D의 임의의 분수체는 D와 동형이다.

풀 이 (True)

D가 체이므로 임의의 $a,b\in D,b\neq 0$에 대하여 $\frac{a}{b}\in D$이 성립한다. 따라서 D의 분수체를 F라 할때 다음이 성립한다.

$$F=\left\{\frac{a}{b}|a,b\in D,b\neq 0\right\}\approx\{a|a\in D\}=D$$

그러므로 D가 체이면 D의 임의의 분수체는 D와 동형이다.

(f) D가 0인자를 갖지 않는다는 사실은 정역 D의 분수체 F의 구성 도중에 여러 번 사용되었다.

풀 이 (True)

$F=\left\{\frac{a}{b}|a,b\in D,b\neq o\right\}$라고 할 때, $\forall q_1,q_2\,\exists m_1,m_2,n_1,n_2\in D,\ m_1\neq 0,m_2\neq 0\ s.t.\ q_1=\frac{n_1}{m_1},q_2=\frac{n_2}{m_2}$

이고 이때 D가 0인자를 갖는다면 $q_1q_2=\frac{n_1n_2}{m_1m_2}$ 에서 $m_1m_2=0$이 되어 정의되지 않는다. 이 처럼 분수체의 F의 구성 중에서 두 원소의 곱이 정의되기 위해서는 0인자를 갖지 않는다는 사실을 사용해야 한다. 따라서 D가 0인자를 갖지 않는다는 사실은 정역 D의 분수체 F의 구성 도중에 여러 번 사용되었다.

(g) 정역 D의 모든 원소는 D의 분수체 F에서 가역원이다.

풀 이 (False)

$0\in D$이지만 0은 분수체 F에서 가역원이 아니다

(h) 정역 D의 0이 아닌 모든 원소는 D의 분수체 F에서 가역원이다.

풀 이 (True)

$a\in D,a\neq 0$이면 $\frac{1}{a}\in F=\left\{\frac{a}{b}|a,b\in D,b\neq o\right\}$이 존재해서 다음을 만족한다.

$$a\cdot\frac{1}{a}=1$$

따라서 정역 D의 0이 아닌 모든 원소는 D의 분수체 F에서 가역원이다.

(i) 정역 D의 부분정역 D'의 분수체 F'는 D의 분수체의 부분체로 간주할 수 있다.

풀 이 (True)

$D'\subseteq D\Rightarrow F'\subseteq F$임은 자명하고 F'은 체이므로 부분체로 간주할 수 있다.

(j) Z의 모든 분수체는 Q와 동형이다.

풀 이 (True)

Z의 임의의 분수체는 $Q=\left\{\frac{a}{b}|a,b\in Z,b\neq o\right\}$이고 Q는 자기 자신과 동형이다.

문 5. 정역 D의 진부분 정역 D'의 분수체 F'가 D에 대한 분수체가 될 수 있음을 예를 들어 보여라.

풀 이

$2Z \subset Z$이고 $Q = \left\{ \frac{y}{x} | x,y \in 2Z, x \neq o \right\} = \left\{ \frac{a}{b} | a,b \in Z, b \neq o \right\}$

문 6. 단계3의 앞부분이 모두 성립할 때 단계 3의 2(덧셈은 결합적임)를 증명하라.
(참고: 덧셈에 관한 연산은 다음과 같이 정의되어 있다. $[(a,b)]+[(c,d)]=[(ad+bc,bd)]$**)**

풀 이

$\forall [(a,b)],[(c,d)],[(e,f)] \in F$
$\{[(a,b)]+[(c,d)]\}+[(e,f)] = [(ad+bc,bd)]+[(e,f)] = [(adf+bcf+bde,bdf)]$
$[(a,b)]+\{[(c,d)]+[(e,f)]\} = [(a,b)]+[(cf+de,df)] = [(adf+bcf+bde,bdf)]$
따라서 $\{[(a,b)]+[(c,d)]\}+[(e,f)] = [(a,b)]+\{[(c,d)]+[(e,f)]\}$가 성립함을 알 수 있다.
그러므로 덧셈에 관하여 결합적이다.

문 7. 단계3의 앞부분이 모두 성립할 때 단계 3의 3를 증명하라.
($[(0,1)]$**은 F에서 덧셈에 관한 항등원이다.)**

풀 이

$\exists [(0,1)] \in F \ \forall [(a,b)] \in F \ s.t. \ [(a,b)]+[(0,1)] = [(a,b)] = [(0,1)]+[(a,b)]$

문 8. 단계3의 앞부분이 모두 성립할 때 단계 3의 4를 증명하라.
($[(-a,b)]$**은 F에서** $[(a,b)]$**의 덧셈에 관한 역원이다.)**

풀 이

$\forall [(a,b)] \in F \ \exists [(-a,b)] \in F \ s.t.$
$[(a,b)]+[(-a,b)] = [(0,b^2)] = [(0,1)] = [(0,b^2)] = [(-a,b)]+[(a,b)]$

문 9. 단계3의 앞부분이 모두 성립할 때 단계 3의 5(곱셈에 관하여 결합적)를 증명하라.
(참고: 곱셈에 관한 연산은 다음과 같이 정의되어 있다. $[(a,b)] \cdot [(c,d)] = [(ac,bd)]$**)**

풀 이

$\forall [(a,b)],[(c,d)],[(e,f)] \in F \ s.t.$
$\{[(a,b)] \cdot [(c,d)]\} \cdot [(e,f)] = [(ac,bd)] \cdot [(e,f)] = [(ace,bdf)]$
$[(a,b)] \cdot \{[(c,d)] \cdot [(e,f)]\} = [(a,b)] \cdot [(ce,df)] = [(ace,bdf)]$
따라서 $\{[(a,b)] \cdot [(c,d)]\} \cdot [(e,f)] = [(a,b)] \cdot \{[(c,d)] \cdot [(e,f)]\}$가 성립함을 알 수 있다.
그러므로 곱셈에 관하여 결합적이다.

문 10. 단계3의 앞부분이 모두 성립할 때 단계 3의 6를 증명하라.
(F는 곱셈에 관하여 가환적이다.)

풀 이

$\forall [(a,b)],[(c,d)] \in F \ s.t. [(a,b)] \cdot [(c,d)] = [(ac,bd)] = [(ca,db)] = [(c,d)] \cdot [(a,b)]$

문 11. 단계3의 앞부분이 모두 성립할 때 단계 3의 7를 증명하라.
(F는 분배법칙이 성립한다.)

풀 이

$\forall [(a,b)],[(c,d)],[(e,f)] \in F s.t.$
$[(a,b)] \bullet \{[(c,d)]+[(e,f)]\} = [(a,b)] \bullet [(cf+de,df)] = [(acf+ade,bdf)]$
$[(a,b)] \bullet [(c,d)]+[(a,b)] \bullet [(e,f)] = [(ac,bd)]+[(ae,bf)] = \left[(abcf+abed,b^2df)\right] = [(acf+ade,bdf)]$
따라서 좌 분배법칙이 성립한다. (문제10번)에 의하여 곱셈에 관하여 가환적이므로 우 분배법칙도 자명하게 성립한다. 그러므로 F는 분배법칙에 관하여 닫혀 있다.

문 12. R이 가환환이고, T≠{∅}은 곱에 대하여 닫혀있는 공집합이 아닌 R의 부분집합이라 하고, T가 0인자를 포함하지 않는다고 하자. $R \times T$로 시작하여 이 절의 구성을 똑같이 따르면 R가 부분 분수환 $Q(R,T)$에 포함됨을 알 수 있다. 이런 과정이 가능한 이유를 생각하여 다음 사실들을 증명하라.
(a) R이 단위원을 갖지 않더라도 $Q(R,T)$는 단위원을 갖는다.

풀 이

1∉R인 환 R이라 하자. 임의의 $0 \neq a \in T \subseteq R$에 대하여 $[(a,a)] \in Q(R,T)$이 존재하고 이때 임의의 원소 $[(b,c)] \in Q(R,T)$에 대하여

$$[(b,c)] \bullet [(a,a)] = [(ba,ca)] = [(b,c)]$$
$$[(a,a)] \bullet [(b,c)] = [(ab,ac)] = [(b,c)]$$

이 성립한다. 따라서 $Q(R,T)$는 단위원 $[(a,a)](a \neq 0$인 $a \in T)$을 갖는다.

(b) $Q(R,T)$에서 T의 0이 아닌 모든 원소들은 가역원이다.

풀 이

임의의 $0 \neq a \in T \subseteq R$에 대하여 $a \equiv [(aa,a)]$라 정의하자.
T는 0인자를 갖지 않으므로 $[(aa,a)] \in Q(R,T)$이고 $[(a,aa)] \in Q(R,T)$이 존재해서 다음을 만족한다.

$$[(aa,a)] \bullet [(a,aa)] = [(aaa,aaa)] = [(a,a)]$$
$$[(a,aa)] \bullet [(aa,a)] = [(aaa,aaa)] = [(a,a)]$$

여기서 $[(a,a)](a \neq 0$인 $a \in T)$은 $Q(R,T)$의 항등원이므로 따라서 $Q(R,T)$에서 T의 0이 아닌 모든 원소들은 가역원임을 알 수 있다.

문 13. (문제12)로부터 0인자가 아닌 원소 a를 포함하는 모든 가환환은 단위원을 갖는 환으로 확장될 수 있음을 보여라. 19장의 문제30번과 비교해 보라.

풀 이

$T=\{a\}$인 경우를 생각해 보면 (19장의 문제30번)과 전혀 다른 점을 발견할 수 있다.

문 14. (문제12)을 참고로 하여 환 $Q(Z,\{2^n | n \in Z^+\})$와 동형이 되는 R의 부분환을 구하라.

풀 이

$Q(Z,\{2^n | n \in Z^+\}) \subseteq \left\{\frac{a}{2^n} | a \in Z, n \in Z^+\right\} = \left\{\frac{n}{m} | n,m \in Z, m \neq 0\right\} = Q$임은 자명하고

$Q(Z,\{2^n | n \in Z^+\})$는 체이고 표수가 0이므로 $Q(Z,\{2^n | n \in Z^+\})$는 Q와 동형인 소체를 갖는다.

따라서 $Q(Z,\{2^n | n \in Z^+\}) \supseteq \left\{\frac{a}{2^n} | a \in Z, n \in Z^+\right\} = \left\{\frac{n}{m} | n,m \in Z, m \neq 0\right\} = Q$이 성립한다.

그러므로 $Q(Z,\{2^n | n \in Z^+\}) = \left\{\frac{a}{2^n} | a \in Z, n \in Z^+\right\} = \left\{\frac{n}{m} | n,m \in Z, m \neq 0\right\} = Q$이다.

[문제4번이 (j)에 의해서도 $Q(Z,\{2^n | n \in Z^+\})$는 Q와 동형임을 알 수 있다.)

문 15. (문제12)을 참고로 하여 환 $Q(3Z,\{6^n|n\in Z^+\})$와 동형이 되는 R의 부분환을 구하라.

풀 이

$Q(3Z,\{6^n|n\in Z^+\}) \subseteq \left\{\frac{3a}{6^n}|a\in Z,n\in Z^+\right\}=\left\{\frac{n}{m}|n,m\in Z,m\neq 0\right\}=Q$임은 자명하고

$Q(3Z,\{6^n|n\in Z^+\})$는 체이고 표수가 0이므로 $Q(3Z,\{6^n|n\in Z^+\})$는 Q와 동형인 소체를 갖는다.

따라서 $Q(3Z,\{6^n|n\in Z^+\}) \supseteq \left\{\frac{3a}{6^n}|a\in Z,n\in Z^+\right\}=\left\{\frac{n}{m}|n,m\in Z,m\neq 0\right\}=Q$이 성립한다.

그러므로 $Q(3Z,\{6^n|n\in Z^+\})=\left\{\frac{3a}{6^n}|a\in Z,n\in Z^+\right\}=\left\{\frac{n}{m}|n,m\in Z,m\neq 0\right\}=Q$이다.

문 16. (문제12)을 참고로 하여 T가 0인자를 갖지 않는다는 조건을 제외하고, 공집합이 아닌 T≠{∅}가 곱셈에 대해 닫혀 있다고 가정하자. R를 T의 모든 0이 아닌 원소가 가역원이 되는 단위원을 갖는 가환환으로 확장되도록 하기 위해서는, 0인자는 가역원이 될 수 없으므로 T가 0인자를 포함하지 않아야 한다. 본문에서와 같이 우선 $R\times T$로 시작하는 환을 구성할 때, 처음으로 문제가 생기는 곳을 찾아보아라. 특히, $R=Z_6$와 T={1,2,4}에 대하여, 처음으로 문제가 발생하는 곳을 설명해 보아라.

[힌트: 단계 3을 참조할 것.]

풀 이

$R=Z_6, T=\{1,2,4\}$라 하자. 그러면

$1\cdot 4\equiv 2\cdot 2\equiv 4(\mathrm{mod}6)$이므로 $[(1,2)]\sim[(2,4)]$

$2\cdot 1\equiv 4\cdot 2\equiv 2(\mathrm{mod}6)$이므로 $[(2,4)]\sim[(2,1)]$

이 성립한다. 하지만 $1\cdot 1\not\equiv 2\cdot 2(\mathrm{mod}6)$이므로 $[(2,1)]\not\sim[(1,2)]$이다. 즉. 추이적 성질을 만족하지 않는다. 따라서 곱셈에 대한 소약 법칙이 닫혀 있지 않음을 알 수 있다.

※ 문제1~4에서 주어진 다항식 환에 속하는 다항식의 합과 곱을 구하라.

문 1. $Z_8[x]$**에서** $f(x)=4x-5, g(x)=2x^2-4x+2$

풀 이

$f(x)+g(x)=(4x-5)+(2x^2-4x+2)=2x^2-3$

$f(x)g(x)=(4x-5)(2x^2-4x+2)=4x(2x^2-4x+2)-5(2x^2-4x+2)$

$=-5(2x^2-4x+2)=-2x^2+4x+6$

문 2. $Z_2[x]$**에서** $f(x)=x+1,\ g(x)=x+1$

풀 이

$f(x)+g(x)=(x+1)+(x+1)=2(x+1)=0,$

$f(x)g(x)=(x+1)(x+1)=x^2+2x+1=x^2+1$

문 3. $Z_6[x]$**에서** $f(x)=2x^2+3x+4, g(x)=3x^2+2x+3$

풀 이

$f(x)+g(x)=(2x^2+3x+4)+(3x^2+2x+3)=5x^2+5x+1$

$f(x)g(x)=(2x^2+3x+4)(3x^2+2x+3)=x^3+5x$

문 4. $Z_5[x]$**에서** $f(x)=2x^3+4x^2+3x+2, g(x)=3x^4+2x+4$

풀 이

$f(x)+g(x)=(2x^3+4x^2+3x+2)+(3x^4+2x+4)=3x^4+2x^3+4x^2+1$

$f(x)g(x)=(2x^3+4x^2+3x+2)(3x^4+2x+4)=x^7+2x^6+4x^5+x^3+2x^2+x+3$

문 5. $Z_2[x]$**에서 3차 이하의 다항식의 개수는 몇 개 인가?(0 포함)**

풀 이

3차 이하의 다항식의 모양의 다음과 같다.

$a_3x^3+a_2x^2+a_1x+a_0\ (a_i=0,1)$

따라서 다항식의 개수는 16(=$_2\Pi_4=2^4$)개 이다.

문 6. $Z_5[x]$**에서 2차 이하의 다항식의 개수는 몇 개 인가?(0 포함)**

풀 이

(문제5)를 참고하면 다항식의 개수는 125개 이다.

※문제7~8을 (정리22.4)에서 $F=E=C$**이라 두고 주어진 평가 준동형사상에 대하여 계산하라.**

문 7. $\Phi_2(x^2+3)$

풀 이

C상에서 $\Phi_2(x^2+3)=2^2+3=7$

문 8. $\Phi_i(2x^3-x^2+3x+2)$

풀 이

C상에서 $\Phi_i(2x^3-x^2+3x+2)=2i^3-i^2+3i+2=-2i+1+3i+2=i+3$

※ 문제 9~11을 (정리22.4)에서 $F=E=Z_7$이라 두고 주어진 평가 준동형사상에 대하여 계산하라.

문 9. $\Phi_3((x^4+2x)(x^3-3x^2+3))$

풀 이

Z_7상에서 $\Phi_3((x^4+2x)(x^3-3x^2+3))=(3^4+2\cdot 3)(3^3-3\cdot 3^2+3)=3\cdot 3=9=2$

문 10. $\Phi_5((x^3+2)(4x^2+3)(x^7+3x^2+1))$

풀 이

Z_7상에서 $\Phi_5((x^3+2)(4x^2+3)(x^7+3x^2+1))=(5^3+2)(4\cdot 5^2+3)(5^7+3\cdot 5^2+1)=6$

문 11. $\Phi_4(3x^{106}+5x^{99}+2x^{53})$

풀 이

Z_7상에서 $\Phi_4(3x^{106}+5x^{99}+2x^{53})=3\cdot 4^{106}+5\cdot 4^{99}+2\cdot 4^{53}=12+40+4=0$

※문제12~15에서 계수를 주어진 유한체에서 갖는 다항식들의 모든 근을 구하라.
[힌트: 한 가지 방법은 하나하나 대입해 보는 방법이다.]

문 12. Z_2**에서** x^2+1

풀 이

$x^2+1\equiv 0(\mathrm{mod}2)\Leftrightarrow x^2\equiv -1(\mathrm{mod}2)\Leftrightarrow x^2\equiv 1(\mathrm{mod}2)\Leftrightarrow x\equiv 1(\mathrm{mod}2)$ 따라서 구하는 해는 1이다.

문 13. Z_7**에서** x^3+2x+2

풀 이

Z_7는 체이므로 0인자가 존재하지 않는다.

$x^3+2x+2=x^3-5x+2=(x-2)^2(x+3)=0$ 으로부터 해를 찾으면 2와 4(=-3)이다.

문 14. Z_5**에서** $x^5+3x^3+x^2+2x$

풀 이

하나하나 대입해 보면

$\Phi_0(x^5+3x^3+x^2+2x)=0$

$\Phi_1(x^5+3x^3+x^2+2x)=2\neq 0$

$\Phi_2(x^5+3x^3+x^2+2x)=4\neq 0$

$\Phi_3(x^5+3x^3+x^2+2x)=4\neq 0$

$\Phi_4(x^5+3x^3+x^2+2x)=0$

따라서 구하고자 하는 해는 0, 4이다.

문 15. Z_7**에서** $f(x)g(x)$ **단,** $f(x)=x^3+2x^2+5$**이고** $g(x)=3x^2+2x$**이다.**

풀 이

Z_7는 체이므로 0인자가 존재하지 않는다.

$f(x)g(x)=(x^3+2x^2+5)(3x^2+2x)=-2x^2(x-2)(x^2+4x+1)(2x-1)$

따라서 구하고자하는 해는 0, 2, 4이다.

문 16. $\Phi_a : Z[x]\to Z_5$**를 정리 22.4에서 처럼 평가 준동형사상이라 하자. 페르마의 정리를 사용하여** $\Phi_3(x^{231}+3x^{117}-2x^{53}+1)$**을 계산하라.**

풀 이

$\Phi_3(x^{231}+3x^{117}-2x^{53}+1)=3^{231}+3\bullet 3^{117}-2\bullet 3^{53}+1$ 이고 gcd(3,5)=1이므로 페르마의 정리를 이용하면 $3^4\equiv 1(\mathrm{mod}5)$ 가 성립한다. 그러면

$\Phi_3(x^{231}+3x^{117}-2x^{53}+1)=3^{231}+3\bullet 3^{117}-2\bullet 3^{53}+1\equiv 2+4-1+1\equiv 1(\mathrm{mod}5)$

임을 알 수 있다.

문 17. 페르마의 정리를 사용하여 $2x^{219}+3x^{74}+2x^{57}+3x^{44}$**의** Z_5**에서의 모든 근을 구하라.**

풀 이

0은 주어진 방정식의 근이다. 이제 x≠0인 근이라 하면 페르마의 정리에 의하여 $x^5\equiv x(\mathrm{mod}5)$가 성립하여 주어진 방정식은 다음과 합동이 된다.

$2x^{219}+3x^{74}+2x^{57}+3x^{44}\equiv x^4+2x^3+3x^2+2x(\mathrm{mod}5)$

여기서 $\Phi_1(x^4+2x^3+3x^2+2x)=3\neq 0,$

$\Phi_2(x^4+2x^3+3x^2+2x)=3\neq 0$

$\Phi_3(x^4+2x^3+3x^2+2x)=3\neq 0,$

$\Phi_4(x^4+2x^3+3x^2+2x)=1\neq 0$

이므로 $x^4+2x^3+3x^2+2x\equiv 0(\mathrm{mod}5)$은 해를 갖지 않는다. 따라서 Z_5에서 0이 유일한 근이다.

문 18. ***A polynomial with coefficients*** **in a ring R is an infinite formal sum**

$$\sum_{i=1}^{\infty}a_ix^i=a_0+a_1x+\cdots+a_nx^n+\cdots$$

where $a_i\in R$ **for** $i=0,1,2,\cdots$

풀 이

환 R에서 계수를 가진 다항식은 유한항을 제외한 무한항의 계수가 0인 다음과 같은 형식적인 무한합이다.

$\sum_{i=1}^{\infty}a_ix^i=a_0+a_1x+\cdots+a_nx^n+\cdots$ **where** $a_i\in R$ **for** $i=0,1,2,\cdots$

문 19. Let F be a field and let $f(x)\in F[x]$**. A** ***zero of*** $f(x)$ **is an** $\alpha\in F$ **such that** $\Phi_\alpha(f(x))=0$**. where** $\Phi_\alpha : F[x]\to F$ **is the evaluation homomorphism mapping x into** α**.**

풀 이

옳은 정의이다.

문 20. $(Q[x])[y]$**의 원소** $f(x,y)=(3x^2+2x)y^3+(x^2-6x+1)y^2+(x^4-2x)y+(x^4-3x+2)$**에 대하여 생각해 보자.** $(Q[y])[x]$ **의 원소로 간주되도록** $f(x,y)$**를 다시 써보라.**

풀 이

$$\begin{aligned}f(x,y)&=(3x^2+2x)y^3+(x^2-6x+1)y^2+(x^4-2x)y+(x^4-3x+2)\\&=3y^3x^2+2y^3x+y^2x^2-6y^2x+y^2+yx^4-2yx+x^4-3x+2\\&=yx^4+x^4+3y^3x^2+y^2x^2+2y^3x-6y^2x-2yx-3x+y^2+2\\&=(y+1)x^4+(3y^3+y^2)x^2+(2y^3-6y^2-2y)x-3x+(y^2+2)\end{aligned}$$

문 21. 평가 준동형사상 $\Phi_5 : Q[x]\to R$**를 생각해 보자.** Φ_5**의 핵에 속하는 여섯 개의 원소들을 구하라.**

풀 이

$(x-5),(x-5)^2,(x-5)^3,(x-5)^4,(x-5)^5,(x-5)^6$

문 22. $Z_4[x]$**에서 가역원이 되는 차수가 0보다 큰 다항식을 구하라.**

풀 이

$f(x)=2x+1$이라 하면 $f(x)f(x)=(2x+1)(2x+1)=1$ 이므로 $f(x)=2x+1\in U(Z_4[x])$이다.

문 23. 참, 거짓을 말하라.

(a) 다항식 $(a_nx^n+\cdots+a_1x+a_0)\in R[x]$**가 0일 필요충분조건은** $i=0,1,\cdots,n$**에 대하여** $a_i=0$**이다.**

풀 이 (True)

$i=0,1,\cdots,n$에 대하여 $a_i=0$ 이면 자명하게 다항식 $(a_nx^n+\cdots+a_1x+a_0)\in R[x]$가 0이다.

역으로 $a_nx^n+\cdots+a_1x+a_0=0$이면 $\{x^n,\cdots x,1\}$은 기저이므로 $i=0,1,\cdots,n$에 대하여 $a_i=0$이다.

(b) R이 가환환이면 R[x]도 가환이다.

풀 이 (True)

임의의 $f(x)=a_nx^n+\cdots a_1x+a_0, g(x)=b_nx^n+\cdots b_1x+b_0\in R[x]$에 대하여

$$\begin{aligned}f(x)g(x)&=(a_nx^n+\cdots a_1x+a_0)(b_nx^n+\cdots b_1x+b_0)\\&=(a_nb_n)x^{2n}+(a_{n-1}b_n+a_nb_{n-1})x^{2n-1}+\cdots(a_1b_0+a_0b_1)x+a_0b_0\\&=(b_na_n)x^{2n}+(b_na_{n-1}+b_{n-1}a_n)x^{2n-1}+\cdots(b_0a_1+b_1a_0)x+b_0a_0\\&=g(x)f(x)\end{aligned}$$

따라서 R이 가환이면 R[x]도 가환이다.

(c) D가 정역이면 D[x]도 정역이다.

풀 이 (True)

임의의 $f(x),g(x)\in D[x]$에 대하여 모두가 영 다항식이 아니면 $\deg f(x)g(x)=\deg f(x)+\deg g(x)$이 D가 정역이므로 성립하여 $f(x)g(x)$는 영 다항식이 아님을 알 수 있다. 그러므로 D[x]는 정역이다.

(d) R가 0인자를 포함하는 환이면 R[x]도 0인자를 포함한다.

풀 이 (True)

a∈R가 R에서 0인자 이면 R⊆R[x]이므로 R[x]도 0인자를 포함한다.

(e) R가 환이고 R[x]에 속하는 f(x)와 g(x)이 차수가 각각 3과 4이면, f(x)g(x)는 차수가 8이 될 수도 있다.

풀 이 (False)

일반적으로 임의의 $f(x),g(x)\in R[x]$에 대하여 $\deg f(x)\deg g(x)\geq \deg f(x)g(x)$이 성립한다. 따라서 f(x)와 g(x)이 차수가 각각 3과 4이면, f(x)g(x)는 차수가 7이하로만 될 수도 있다. 그러므로 차수가 8일수는 없다.

(f) R가 환이고 R[x]에 속하는 f(x)와 g(x)이 차수가 각각 3과 4이면, f(x)g(x)는 차수가 7이 다.

풀 이 (False)

$Z_6[x]$에 대하여 $f(x)=2x^3+x, g(x)=3x^4+5$이라 하면 $\deg f(x)=3, \deg g(x)=4$이지만
$\deg f(x)g(x)=\deg(2x^3+x)(3x^4+5)=\deg(4x^3+3x^5+5x)=5$이다.

(g) F가 체 E의 부분체이고 $\alpha\in E$가 $f(x)\in F[x]$의 근이면 α는 모든 $g(x)\in F[x]$에 대하여 $h(x)=f(x)g(x)$의 근이다.

풀 이 (True)

$\alpha\in E$가 $f(x)\in F[x]$의 근이므로 $f(\alpha)=0$이고 모든 $g(x)\in F[x]$에 대하여
$h(\alpha)=f(\alpha)g(\alpha)=0\bullet g(\alpha)=0$이므로$h(x)=f(x)g(x)$의 근이다.

(h) F가 체이면 F[x]의 가역원은 F에 속하는 가역뿐이다.

풀 이 (True)

0이 아닌 임의의 $f(x)\in U(F[x])$에 대하여 0이 아닌 $g(x)\in F[x]$가 존재해서 다음을 만족한다.

$$f(x)g(x)=g(x)f(x)=1$$

그러면 $\deg f(x)g(x)=0$이 성립하고 F가 체이므로 따라서 $\deg f(x)=0, \deg g(x)=0$임을 알 수 있다.
그러므로 $f(x)\in U(F[x])=U(F)$이다.

(i) R가 환이면 x는 R[x]에서 결코 0인자가 아니다.

풀 이 (True)

부정원 x는 벡터차원에서의 기저의 역할을 할 뿐 R[x]에서의 덧셈과 곱셈의 연산에 있어서 영향을 주지는 않는다. 따라서 0인자가 아니다.

(j) R가 환이면 R[x]에 속하는 0인자는 R에 속하는 0인자 뿐이다.

풀 이 (False)

$2x, 3x\in Z_6[x]$이고 $2x\bullet 3x=6x^2=0$이지만 $2x,3x\notin Z_6$이다.

문 24. D가 정역이면 D[x]가 정역임을 보여라.

풀 이

임의의 $f(x),g(x)\in D[x]$에 대하여 모두가 영 다항식이 아니면 $\deg f(x)g(x)=\deg f(x)+\deg g(x)$이 D가 정역이므로 성립하여 $f(x)g(x)$는 영 다항식이 아님을 알 수 있다. 그러므로 D[x]는 정역이다.

문 25. D가 정역이고 x가 부정원이라 하자.

(a) D[x]에 속하는 가역원을 구하라.

풀 이

$U(D[x]) = U(D) = D^*$

(b) Z[x]에 속하는 가역원을 구하라.

풀 이

$U(Z[x]) = U(Z) = \{-1, 1\}$

(c) $Z_7[x]$에 속하는 가역원을 구하라.

풀 이

$U(Z_7[x]) = U(Z_7) = \{1,2,3,4,5,6\}$

문 26. R이 환이고 x는 부정원일 때 R[x]에 대한 좌측배분법칙을 증명하라.

풀 이

$\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{n} b_i x^i, \sum_{i=0}^{n} c_i x^i \in R[x]$ 에 대하여

$(\sum_{i=0}^{n} a_i x^i)((\sum_{i=0}^{n} b_i x^i) + (\sum_{i=0}^{n} c_i x^i)) = (\sum_{i=0}^{n} a_i x^i) \cdot \sum_{i=0}^{n} (b_i + c_i) x^i = \sum_{i=0}^{n} d_i x^i$

단, $d_i = \sum_{k=0}^{i} [a_k \cdot (b_{k-i} + c_{k-i})]$

$(\sum_{i=0}^{n} a_i x^i)(\sum_{i=0}^{n} b_i x^i) + (\sum_{i=0}^{n} a_i x^i)(\sum_{i=0}^{n} c_i x^i) = (\sum_{i=0}^{n} e_i x^i) + (\sum_{i=0}^{n} f_i x^i)$

단, $e_i = \sum_{k=0}^{i} [a_k \cdot b_{k-i}]$, $f_i = \sum_{k=0}^{i} [a_k \cdot c_{k-i}]$

여기서 $d_i = e_i + f_i$가 성립하므로 따라서

$(\sum_{i=0}^{n} a_i x^i)((\sum_{i=0}^{n} b_i x^i) + (\sum_{i=0}^{n} c_i x^i)) = (\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) + (\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{n} c_i x^i)$

가 성립하여 좌 분배법칙이 성립함을 알 수 있다.

문 27. F를 표수가 0인 체, 그리고 D를 형식적 다항식 도함수 사상, 즉

$D(a_0 + a_1 x + \cdots + a_n x^n) = a_1 + \cdots\ n a_n x^{n-1}$

(a) $D : F[x] \to F[x]$는 $< F[x], + >$에서 그 자신으로 대응하는 준동형사상임을 보여라. 이때 D가 환 준동형사상이 되는가?

풀 이

임의의 $f(x), g(x) \in F[x]$에 대하여

$D(f(x) + g(x)) = (f(x) + g(x))' = f(x)' + g(x)' = D(f(x)) + D(g(x))$

이므로 군 준동형사상이다.

하지만

$D(f(x)g(x)) = (f(x)g(x))' = f(x)'g(x) + f(x)g(x)'$
$D(f(x))D(g(x)) = f(x)'g(x)'$

으로서 $D(f(x)g(x)) \neq D(f(x))D(g(x))$임을 알 수 있다.

그러므로 D는 환 준동형사상은 아니다.

(b) D의 핵을 구하라.

풀 이

$D(a_0+a_1x+\cdots+a_nx^n)=a_1+\cdots na_nx^{n-1}=0\Leftrightarrow a_i=0\ (1\le i\le n)$

따라서 $\ker D=\{a_0|a_0\in F\}=F$

(c) F[x]의 D에 대한 상을 구하라.

풀 이

$\forall\, a_0+a_1x+\cdots+a_nx^n\in F[x],\ \exists\, a_0x+\frac{a_1}{2}x^2+\cdots+\frac{a_n}{n+1}x^{n+1}\in F[x]\ s.t.$

$D(a_0x+\frac{a_1}{2}x^2+\cdots+\frac{a_n}{n+1}x^{n+1})=a_0+a_1x+\cdots+a_nx^n$

그러므로 $imD=F[x]$이다.

문 28. F를 체 E의 부분체라 하자.

(a) $\alpha_i\in E$**에 대하여 정리22.4에서와 비슷한 평가 준동형사상**

$\Phi_{\alpha_1,\cdots,\alpha_n}:F[x_1,\cdots,x_n]\to E$

를 정의하라.

풀 이

$\Phi_{\alpha_1,\cdots,\alpha_n}(f(x_1,\cdots,x_n))=f(\alpha_1,\cdots,\alpha_n)\ \ (f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n])$

(b) $E=F=Q$**일 때** $\Phi_{-3,2}(x_1^2x_2^3+3x_1^4x_2)$**를 계산하라.**

풀 이

$\Phi_{-3,2}(x_1^2x_2^3+3x_1^4x_2)=(-3)^2(2)^3+3(-3)^4(2)=9\cdot 8+3\cdot 81\cdot 2=72+486=558$

(c) f(x)의 근에 대한 이 책에서 정의와 비슷하게 다항식 $f(x_1,\cdots x_m)\in F[x_1,\cdots x_m]$**의 근의 개념을 정의하라.**

풀 이

임의의 $f(x_1,\cdots x_m)\in F[x_1,\cdots x_m]$에 대하여

$\Phi_{\alpha_1,\cdots,\alpha_n}(f(x_1,\cdots,x_n))=0$ 이 되게 하는 $(\alpha_1,\cdots,\alpha_n)$을 $f(x_1,\cdots,x_n)$의 근이라 한다.

문 29. R를 환이라 하고 R^R를 R에서 R로 대응하는 모든 함수의 집합이라 하자. $\Phi,\Psi\in R^R$에 대하여 $\Phi+\Psi$를

$$(\Phi+\Psi)(r)=(\Phi)(r)+(\Psi)(r)$$

로 곱 $\Phi\bullet\Psi$를

$$(\Phi\bullet\Psi)(r)=(\Phi)(r)\bullet(\Psi)(r)$$

로 정의하면 $<R^R,+,\bullet>$가 환 임을 보여라. 단 $r\in R$이고 $\bullet$은 함수의 합성이 아니다.

풀 이

곱셈과 덧셈에 관하여 닫혀 있음은 자명하고

$\forall\Phi,\Psi,\Omega\in R^R\ s.t.$
$[(\Phi+\Psi)+\Omega](r)=(\Phi+\Psi)(r)+\Omega(r)=[(\Phi)(r)+(\Psi)(r)]+\Omega(r)$
$=(\Phi)(r)+(\Psi)(r)+\Omega(r)=(\Phi)(r)+[(\Psi)(r)+\Omega(r)]$
$=(\Phi)(r)+(\Psi+\Omega)(r)=[(\Phi(\Psi+\Omega)](r)$

따라서 덧셈에 관하여 결합적이다.

$\exists 0\in R^R\ \forall\Phi\in R^R\ s.t.\ (\Phi+0)(r)=(\Phi)(r)+(0)(r)=(\Phi)(r)=(0)(r)+(\Phi)(r)=(0+\Phi)(r)$

따라서 덧셈에 관한 항등원 $0\in R^R$이 존재한다.

여기서 $0:R\rightarrow R, 0(r)=0$으로 정의된 사상이다.

$\forall\Phi\in R^R\ \exists -\Phi\ s.t.$
$(\Phi+(-\Phi))(r)=(\Phi)(r)-(\Phi)(r)=(0)(r)=-(\Phi)(r)+(\Phi)(r)=((-\Phi)+\Phi)(r)$

따라서 덧셈에 관한 역원이 존재한다.

여기서 $-\Phi$는 Φ의 역사상이다.

$\forall\Phi,\Psi\in R^R\ s.t.$
$(\Phi+\Psi)(r)=(\Phi)(r)+(\Psi)(r)=(\Psi)(r)+(\Phi)(r)=(\Psi+\Phi)(r)$

따라서 덧셈에 관하여 가환적이다.

그러므로 $<R^R,+>$는 가환군이다.

$\forall\Phi,\Psi,\Omega\in R^R\ s.t.$
$[(\Phi\bullet\Psi)\bullet\Omega](r)=(\Phi\bullet\Psi)(r)\bullet\Omega(r)=[(\Phi)(r)\bullet(\Psi)(r)]\bullet\Omega(r)$
$=(\Phi)(r)\bullet(\Psi)(r)\bullet\Omega(r)=(\Phi)(r)\bullet[(\Psi)(r)\bullet\Omega(r)]$
$=(\Phi)(r)\bullet(\Psi\bullet\Omega)(r)=[(\Phi\bullet(\Psi\bullet\Omega)](r)$

따라서 곱셈에 관하여 결합적이다.

$\forall\Phi,\Psi\in R^R\ s.t.$
$(\Phi\bullet\Psi)(r)=(\Phi)(r)\bullet(\Psi)(r)=(\Psi)(r)\bullet(\Phi)(r)=(\Psi\bullet\Phi)(r)$

따라서 곱셈에 관하여 가환적이다.

그러므로 좌 분배법칙이 성립함을 보이면 우 분배법칙은 자명하게 성립한다.

$\forall\Phi,\Psi,\Omega\in R^R\ s.t.$
$[\Phi\bullet(\Psi+\Omega)](r)=(\Phi)(r)\bullet(\Psi+\Omega)(r)=(\Phi)(r)\bullet[(\Psi)(r)+(\Omega)(r)]$
$=(\Phi)(r)\bullet(\Psi)(r)+(\Phi)(r)\bullet(\Omega)(r)=(\Phi\bullet\Psi)(r)+(\Phi\bullet\Omega)(r)$
$=[\Phi\bullet\Psi+\Phi\bullet\Omega](r)$

따라서 분배법칙이 성립한다.

그러므로 $<R^R,+,\bullet>$는 환이다.

문 30. (문제29)을 참고하여 F를 체라 하자. F^F의 원소 Φ를 모든 $a \in F$에 대하여 $\Phi(a) = f(a)$를 만족하는 $f(x) \in F[x]$에 존재하면, Φ를 F위에서 다항식함수라 한다.

(a) F위에서 모든 다항식함수의 집합 P_F는 F^F의 부분환임을 보여라.

풀 이

$0 \in P^F$이므로 $P^F \neq \varnothing$ 이고 $P^F \subset F^F$임은 자명하다.

임의의 $f(x), g(x) \in P^F$에 대하여 $f(x) - g(x), f(x)g(x) \in P^F$임은 자명하다.

따라서 F위에서 모든 다항식함수의 집합 P_F는 F^F의 부분환이다.

(b) 환 P_F는 F[x]와 반드시 동형일 필요가 없음을 보여라.

[힌트: F가 유한체이면 P_F와 F[x]는 같은 원소의 수를 갖지 않음을 보여라.]

풀 이

Z_3인 경우를 생각보자. $Z_3^{Z_3}$의 원소의 개수는 27(=3^3)개 이지만 $Z_3[x]$의 원소의 개수는 무한이다. 따라서 반드시 동형일 필요는 없다.

31. (문제29)와 (문제30)을 참조하여 다음 물음에 답하라.

(a) $Z_2^{Z_2}$에 속하는 원소의 개수를 구하라. 또한 $Z_3^{Z_3}$에 속하는 원소의 개수는?

풀 이

$Z_2^{Z_2}$의 원소의 개수는 4개이고, $Z_3^{Z_3}$의 원소의 개수는 27개이다.

(b) 유한생성가환군에 대한 기본정리인 정리11.12에 의하여 <$Z_2^{Z_2}$,+>와 <$Z_3^{Z_3}$,+>를 분류하라.

풀 이

$Z_2^{Z_2}$의 표수는 2이고 $Z_3^{Z_3}$의 표수는 3이므로 유한 생성 가환군에 대한 기본정리에 의하여

$Z_2^{Z_2} \approx Z_2 \times Z_2 \times Z_2$이고 $Z_3^{Z_3} \approx Z_3 \times Z_3 \times Z_3$임을 알수 있다.

(c) F가 유한체이면 F^F= P_F임을 증명하라.

[힌트: 물론 $F^F \supseteq P_F$이다. F가 원소 $a_1, \cdots a_n$를 갖는다고 하자.

만약

$$f_i(x) = c(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)$$

이면 $i \neq j$에 대하여 $f_i(a_j) = 0$이며 값 $f_i(a_i)$는 $c \in F$의 선택에 의해 조절될 수 있다. 이 사실을 이용하여 F 위의 모든 함수는 다항식함수임을 보여라.]

풀 이

다항식 $f_i(x)$를 다음과 같이 정의하자.

$$f_i(x) = c(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)$$

즉. $i \neq j$에 대하여 $f_i(a_j) = 0$이고 그 외는 $f_i(a_i) = c$라고 한다.

$\Phi \in F^F$이고 $\Phi(a_i) = c_i$라고 하자. 또한 $f(x) = \sum_{i=1}^{n} c_i f_i(x)$로 정의한 임의의 $f(x) \in F[x]$라 하자.

그러면 $f(a_k) = f_1(a_k) + f_2(a_k) + f_3(a_k) + \cdots f_n(a_k) = 0 + 0 + 0 + \cdots + c_k + \cdots + 0 = c_k$이 성립한다. 그러므로 $k = 1, 2, 3, \cdots, n$에 대하여 $f(a_k) = \Phi(a_k)$이고 따라서 F^F에서 모든 사상Φ는 다항식함수이다.

따라서 $F^F = P_F$이다.

Fraleigh 대수 23장 체에서 다항식의 인수분해

※ 문제1~4는 호제법에서 설명했던 r(x)의 차수가 g(x) 보다 낮은 다항식으로써 f(x)=g(x)q(x)+r(x)가 되도록 q(x)와 r(x)를 구하라.

문 1. $Z_7[x]$**에서** $f(x)=x^6+3x^5+4x^2-3x+2$ 와 $g(x)=x^2+2x-3$

풀 이

$Z_7[x]$에서 $q(x)=x^4+x^3+x^2+x-2=x^4+x^3+x^2+x+5, r(x)=4x-4=4x+3$

문 2. $Z_7[x]$**에서** $f(x)=x^6+3x^5+4x^2-3x+2$ 와 $g(x)=3x^2+2x-3$

풀 이

$Z_7[x]$에서 $q(x)=5x^4-2x^2+6x, r(x)=-6x+2=x+2$

문 3. $Z_{11}[x]$**에서** $f(x)=x^5-2x^4+3x-5$ 와 $g(x)=2x+1$

풀 이

$Z_{11}[x]$에서 $q(x)=6x^4+7x^3+2x^2-x+2, r(x)=4$

문 4. $Z_{11}[x]$**에서** $f(x)=x^4+5x^3+3x^2$ 와 $g(x)=5x^2-x+2$

풀 이

$Z_{11}[x]$에서 $q(x)=5x^2-x+2, r(x)=x$

※ 문제5~8는 주어진 유한체의 곱셈에 관한 단원군의 모든 생성원을 구하라.

문 5. Z_5

풀 이

$U(Z_5)=\{1,2,3,4\}$이고 $<1>=1, <4>=\{1,4\}, <2>=<3>=U(Z_5)$

따라서 주어진 체의 곱셈에 관한 단원군의 모든 생성원은 2,3 이다.

문 6. Z_7

풀 이

$U(Z_7)=\{1,2,3,4,5,6\}$이고 $<1>=1, <2>=<3>=<4>=<5>=<6>=U(Z_7)$

따라서 주어진 체의 곱셈에 관한 단원군의 모든 생성원은 2,3,4,5,6 이다.

문 7. Z_{17}

풀 이

$U(Z_{17})=\{1,2,3,4,\cdots,16\}$이고 $<1>=1, <2>=<3>=<4>=\cdots=<16>=U<Z_{17}>$

따라서 주어진 체의 곱셈에 관한 단원군의 모든 생성원은 2,3,4,…,15,16 이다.

문 8. Z_{23}

풀 이

$U(Z_{23})=\{1,2,3,4,\cdots,22\}$이고 $<1>=1,<2>=<3>=<4>=\cdots=<22>=U<Z_{23}>$
따라서 주어진 체의 곱셈에 관한 단원군의 모든 생성원은 2,3,4,…,22 이다.

문 9. 다항식 x^4+4는 $Z_5[x]$에서 일차 인수로 인수분해 될 수 있다. 그 인수분해를 구하라.

풀 이

$Z_5[x]$에서 다음과 같이 일차인수로 인수분해 된다.

$x^4+4=x^4-1=(x^2+1)(x^2-1)=(x^2-4)(x^2-1)=(x+2)(x-2)(x+1)(x-1)$

문 10. 다항식 x^3+2x^2+2x+1는 $Z_7[x]$에서 일차 인수로 인수분해 될 수 있다. 그 인수분해를 구하라.

풀 이

$Z_7[x]$에서 다음과 같이 일차인수로 인수분해 된다.

$x^3+2x^2+2x+14=(x+1)(x^2+x+1)=(x+1)(x^2+x-6)=(x+1)(x+3)(x-2)$

문 11. 다항식 $2x^3+3x^2-7x-5$는 $Z_{11}[x]$에서 일차 인수로 인수분해 될 수 있다. 그 인수분해를 구하라.

풀 이

$Z_{11}[x]$에서 다음과 같이 일차인수로 인수분해 된다.

$2x^3+3x^2-7x-5=2x^3+3x^2+4x+6=(2x+3)(x^2+2)=(2x+3)(x^2-9)\ =(2x+3)(x+3)(x-3)$

문 12. x^3+2x+3는 $Z_5[x]$의 기약다항식인가? 그 이유를 설명하고 이 다항식을 $Z_5[x]$의 기약다항식의 곱으로 표현하라.

풀 이

$\Phi_\alpha : Z_5[x]\to Z_5, \Phi_\alpha(f(x))=f(\alpha)$인 평가 준동형사상이라 하자.

$$\Phi_0(x^3+2x+3)=3,\Phi_1(x^3+2x+3)=1,\Phi_2(x^3+2x+3)=0$$
$$\Phi_3(x^3+2x+3)=1,\Phi_4(x^3+2x+3)=0$$

이므로 x^3+2x+3는 $x-2,x-4$를 인수로 갖는다. 따라서 기약다항식이 아닌 가약다항식이고 $Z_5[x]$에서 $(x-4)(x-4)(x-2)$와 같은 기약다항식의 곱으로 표현할 수 있다.

문 13. $2x^3+x^2+2x+2$는 $Z_5[x]$에서 기약다항식인가? 그 이유를 설명하고 이 다항식을 $Z_5[x]$의 기약다항식의 곱으로 표현하라.

풀 이

$\Phi_\alpha : Z_5[x]\to Z_5, \Phi_\alpha(f(x))=f(\alpha)$인 평가 준동형사상이라 하자.

$$\Phi_0(2x^3+x^2+2x+2)=2,\Phi_1(2x^3+x^2+2x+2)=2,\Phi_2(2x^3+x^2+2x+2)=1$$
$$\Phi_3(2x^3+x^2+2x+2)=1,\Phi_4(2x^3+x^2+2x+2)=4$$

이므로 $2x^3+x^2+2x+2$는 $Z_5[x]$에서 기약다항식이다. 따라서 $Z_5[x]$에서 $(2x^3+x^2+2x+2)$와 같은 기약다항식의 곱으로 표현할 수 있다.

문 14. $f(x)=x^2+8x-2$**는 Q 위에서 기약임을 보여라.** $f(x)$**가 R 위에서 기약인가? C 위에서서 기약인가?**

풀 이

Q 위에서 $f(x)=x^2+8x-2$은 2∤1, 2∣8, 2∣-2, 4∤-2 이므로 Eisenstein 판정법에 의하여 기약이다. 하지만 R과 C 위에선 기약이 아니고 다음과 같이 인수분해 된다.

$f(x)=x^2+8x-2=(x+4+3\sqrt{2})(x+4-3\sqrt{2})$

문 15. $f(x)$**를** $g(x)=x^2+6x+12$**로 바꾸어 (문제14)을 반복하라.**

풀 이

Q 위에서 $g(x)=x^2+6x+12$은 3∤1, 3∣6, 3∣12, 9∤12 이므로 Eisenstein 판정법에 의하여 기약이다. 또한 R 위에서도 판별식 D/4 < 0 이므로 기약이다. 하지만 C 위에선 기약이 아니고 다음과 같이 인수분해 된다. $g(x)=x^2+6x+12=(x+3-\sqrt{3}\,i)(x+3+\sqrt{3}\,i)$

문 16. x^3+3x^2-8**은 Q 위에서 기약임을 설명하라.**

풀 이

$f(x)=x^3+3x^2-8$일 때 $g(x)=f(x+2)$라 하자. 그러면 $g(x)=x^3+9x^2+24x+12$이다. 여기서 3∤1, 3∣9, 3∣24, 9∤12 이므로 Eisenstein 판정법에 의하여 $g(x)$는 기약이다. 따라서 $f(x)$도 기약이다. 그러므로 x^3+3x^2-8는 Q 위에서 기약이다.

문 17. x^4-22x^2+1**은 Q 위에서 기약임을 설명하라.**

풀 이

(1) 일차식으로 인수분해되는 경우

$f(x)=x^4-22x^2+1$ 이 Q에서 가약이면 $\frac{(\text{상수항의 계수})}{(\text{최고차항의 계수})}$의 약수 1,-1을 근으로 갖는다.

하지만 $f(1)=-20, f(-1)=-20$으로 0이 아니다. 그러므로 x^4-22x^2+1은 Q 위에서 기약이다.

(2) 이차식으로 인수분해되는 경우

즉, $f(x)=x^4-22x^2+1=(x^2-\alpha)(x^2-\beta)$이면 근과 계수와의 관계에 의하여 $\alpha+\beta=22, \alpha\beta=1$이다. 하지만 이를 만족하는 Q 상의 해는 존재하지 않는다. 그러므로 x^4-22x^2+1은 Q 위에서 기약이다.

(1)과 (2)에 의하여 x^4-22x^2+1은 Q 위에서 기약이다.

※ 문제18~21에서 Z[x]에 속하는 다음 다항식은 Q 위에서 기약성에 대한 Eisenstein의 공식을 만족하는지 결정하라.

문 18. x^2-12

풀 이

여기서 3∤1, 3∣-12, 9∤-12 이므로 Eisenstein 판정법을 만족한다.

문 19. $8x^3+6x^2-9x+24$

풀 이

여기서 3∤8, 3∣6, 3∣-9, 3∣24, 9∤-24 이므로 Eisenstein 판정법을 만족한다.

문 20. $4x^{10}-9x^3+24x-18$

풀 이

여기서 3∤4, 3∣-9, 3∣24, 3∣-18이지만 9∣-18 이므로 Eisenstein 판정법을 만족하지 않는다.

문 21. $2x^{10}-25x^3+10x^2-30$

풀 이

여기서 5∤2, 5∣-25, 5∣10, 5∣-30, 25∤-30 이므로 Eisenstein 판정법을 만족한다.

문 22. $6x^4+17x^3+7x^2+x-10$**의 Q에서의 모든 근을 구하라.**

풀 이

$6x^4+17x^3+7x^2+x-10=(6x^4+17x^3+5x^2)+(2x^2+x-10)=x^2(6x^2+17x+5)+(2x^2+x-10)$
$=x^2(3x+1)(2x+5)+(2x+5)(x-2)=(2x+5)(3x^3+x^2+x-2)$

여기서 $3x^3+x^2+x-2$는 기약이므로 근은 $-\frac{5}{2}$로 유일하다.

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 23. A polynomial f(x)∈F[x] is *irreducible over the field F* iff f(x)≠g(x)h(x) for any polynomial g(x), h(x)∈F[x]

풀 이

$\deg g(x)\geq 1, \deg h(x)\geq 1$ 인 임의의 다항식 $g(x), h(x)\in F[x]$에 대하여 f(x)≠g(x)h(x) 일 필요충분조건은 다항식 f(x)∈F[x]가 F 위에서 기약이다.

문 24. A nonconstant polynomial f(x)∈F[x] is *irreducible over the field F* iff in any factorization of it in F[x] one of the factors is in F.

풀 이

상수가 아닌 f(x)∈F[x]이 체*F 위에서 기약* 일 필요충분조건은 f(x)=g(x)h(x)로 인수분해 될 때 g(x) 또는 h(x)가 F의 가역원임을 뜻한다.

문 25. 참, 거짓을 구하라.

(a) x-2는 Q위에서 기약이다.

풀 이 (True)

2∤1, 2∣-2, 4∤-2 이므로 Eisenstein 판정법에 의하여 Q 위에서 기약이다.

(b) 3x-6은 Q위에서 기약이다.

풀 이 (True)

2∤3, 2∣-6, 4∤-6 이므로 Eisenstein 판정법에 의하여 Q 위에서 기약이다.

(c) x^2-3**은 Q위에서 기약이다.**

풀 이 (True)

3∤1, 3∣-3, 9∤-3 이므로 Eisenstein 판정법에 의하여 Q 위에서 기약이다.

(d) x^2+3은 Z_7에서 기약이다.

풀 이 (False)

Z_7에서 $x^2+3=x^2-4=(x-2)(x+2)$이므로 가약이다.

(e) F가 체이면 F[x]의 가역원은 F의 0이 아닌 원소와 일치한다.

풀 이 (True)

0이 아닌 임의의 $f(x)\in U(F[x])$에 대하여 0이 아닌 $g(x)\in F[x]$가 존재해서
다음을 만족한다.

$f(x)g(x)=g(x)f(x)=1$

그러면 $\deg f(x)g(x)=0$이 성립하고 F가 체이므로 따라서 $\deg f(x)=0, \deg g(x)=0$임을 알 수 있다.
그러므로 $f(x)\in U(F[x])=U(F)$이다. 따라서 다항식환 F[x]의 가역원은 F의 가역원과 같다.

(f) F가 체이면 F(x)의 가역원은 F의 0이 아닌 원소와 일치한다.

풀 이 (False)

유리식체 F(x)의 가역원은 0 아닌 모든 원소가 될 수 있다.

즉 $x\in f(x)$이면 $\frac{1}{x}\in F(x)$가 존재해서 $x \cdot \frac{1}{x}=1$을 만족한다.

(g) 체 F에서 계수를 갖는 차수가 n인 다항식 f(x)는 기껏해야 n개의 근을 갖는다.

풀 이 (True)

n+1개의 근을 갖는다고 가정하자. 나눗셈 정리에 의하여 각각의 근을 인수로 갖는 일차다항식이 존재한다. f(x)는 일차다항식들의 곱이고 따라서 n+1개의 일차다항식의 곱으로 나타낼 수 있다. 하지만 이는 f(x)의 차수가 n이라는데 모순이다. 따라서 차수가 n인 다항식 f(x)는 기껏해야 n개의 해는 갖는다.

(h) 체 F에서 계수를 갖는 차수가 n인 다항식 f(x)를 F≤E인 임의의 체 E에서 기껏해야 n개의 근을 갖는다.

풀 이 (True)

(g)에 의하여 확대체E에서도 기껏해야 n개의 해를 갖는다.
F에서 근이 존재하지 않는 경우에도 확대체 E에서는 근이 존재할 수 있다.
하지만 어떠한 확대체이든 차수가 n인 다항식에서 근은 많아야 n개 존재한다.

[참고. 복소 계수 다항식에서 n차 다항식은 정확히 n개의 근을 갖는다. 이를 대수학의 기본정리라 한다.]

(i) F[x]에 속하는 차수가 1인 모든 다항식은 체 F에서 적어도 하나의 근을 갖는다.

풀 이 (True)

F가 체이므로 차수가 1인 일차 다항식 ax+b=0 (a≠0)은 다음을 만족한다.

$$ax+b=0(a\neq 0)$$
$$\Rightarrow (ax+b)-b=0-b\ (\because -b:\ b\text{의 덧셈에 대한 역원})$$
$$\Rightarrow ax+(b-b)=-b\ (\because \text{덧셈에 관한 결합법칙과 역원의 정의})$$
$$\Rightarrow ax=-b$$
$$\Rightarrow \frac{1}{a}(ax)=\frac{1}{a}(-b)\ (\because \frac{1}{a}:\ a(a\neq 0)\text{의 곱셈에 대한 역원})$$
$$\Rightarrow (\frac{1}{a}a)x=-\frac{b}{a}\ (\because \text{곱셈에 관한 결합법칙과 역원의 정의})$$
$$\Rightarrow x=-\frac{b}{a}$$

따라서 $x=-\frac{b}{a}\ (a\neq 0)$을 근으로 갖는다.

그러므로 적어도 하나의 근을 갖는다고 할 수 있다.

(j) F[x]에 속하는 각 다항식은 체 F에서 기껏해야 유한개의 근을 갖는다.

풀 이 (True)

다항식은 정의에 의하여 유한 차수를 갖는다.

따라서 (g)에 의하여 기껏해야 다항식의 유한차수만큼의 유한개의 근을 갖는다는 것을 알 수 있다.

문 26. $x+2$가 $Z_p[x]$에서 $x^4+x^3+x^2-x+1$의 인수가 되는 모든 홀수인 소수 p를 구하라.

풀 이

$f(x)=x^4+x^3+x^2-x+1$라 할 때 $x+2$이 인수가 되기 위해서는 $Z_p[x]$에서

$f(-2)=2^4-2^3+2^2+2+1=0$이 되게 하는 소수 p를 찾아야 한다.

그러면 $f(-2)=2^4-2^3+2^2+2+1=15$이고 따라서 $15\equiv 0(\mathrm{mod}p)$인 소수 p를 찾으면 된다.

그러므로 찾고자 하는 소수 p 는 3, 5 이다.

※ 문제27~30에서 주어진 환에 속하는 정해진 차수를 갖는 기약 다항식을 모두 구하라.

문 27. $Z_2[x]$에서 차수가 2

풀 이

$$x^2+0x+0=x^2$$
$$x^2+0x+1=x^2-1=(x-1)(x+1)$$
$$x^2+1x+0=x^2+x=x(x+1)$$
$$x^2+1x+1=x^2+x+1$$

이고 여기서 x^2+x+1는 0 또는 1을 근으로 갖지 않는다.

따라서 기약 다항식은 x^2+x+1 하나 뿐이다.

문 28. $Z_2[x]$**에서 차수가 3**

풀 이

$x^3+0x^2+0x+0=x^3$
$x^3+0x^2+0x+1=x^3+1=x^3-1=(x-1)(x^2+x+1)$
$x^3+0x^2+1x+0=x^3+x=x(x^2+1)$
$x^3+1x^2+0x+0=x^3+x^2=x^2(x+1)$
$x^3+1x^2+1x+0=x^3+x^2+x=x(x^2+x+1)$
$x^3+1x^2+0x+1=x^3+x^2+1$
$x^3+0x^2+1x+1=x^3+x+1$
$x^3+1x^2+1x+1=x^3+x^2+x+1=x^3+3x^2+3x+1=(x+1)^3$

이고 여기서 x^3+x^2+1, x^3+x+1는 0 또는 1을 근으로 갖지 않는다.

따라서 기약다항식은 x^3+x^2+1, x^3+x+1 이다.

문 29. $Z_3[x]$**에서 차수가 2**

풀 이

$x^2+0x+0=x^2$
$x^2+0x+1=x^2+1$
$x^2+0x+2=x^2+2=x^2-1=(x+1)(x-1)$
$x^2+1x+0=x^2+x=x(x+1)$
$x^2+1x+1=x^2+x+1=x^2-2x+1=(x-1)^2$
$x^2+1x+2=x^2+x+2$
$x^2+2x+0=x^2+2x=x(x+2)$
$x^2+2x+1=x^2+2x+1=(x+1)^2$
x^2+2x+2
$2x^2+0x+0=2x^2$
$2x^2+0x+1=2x^2+1=2x^2-2=2(x+1)(x-1)$
$2x^2+0x+2=2x^2+2$
$2x^2+1x+0=2x^2+x=x(2x+1)$
$2x^2+1x+1=2x^2+x+1$
$2x^2+1x+2=2x^2+x+2=-x^2-2x-1=-(x+1)^2$
$2x^2+2x+0=2x^2+2x=2x(x+1)$
$2x^2+2x+1$
$2x^2+2x+2=-x^2+2x-1=-(x-1)^2$

이고 여기서 $x^2+1, x^2+x+2, x^2+2x+2, 2x^2+2, 2x^2+x+1, 2x^2+2x+1$는 0, 1, 2를 근으로 갖지 않는다. 따라서 기약인 다항식은 $x^2+1, x^2+x+2, x^2+2x+2, 2x^2+2, 2x^2+x+1, 2x^2+2x+1$ 이다.

문 30. $Z_3[x]$**에서 차수가 3**

풀 이

기약 다항식은 다음과 같다.

$x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+2x^2+1,$
$x^3+2x^2+2, x^3+x^2+x+2, x^3+x^2+2x+1$
$x^3+2x^2+x+1, x^3+2x^2+2x+2$
$2x^3+x+2, 2x^3+x+1, 2x^3+2x^2+1, 2x^3+x^2+2,$
$2x^3+x^2+1, 2x^3+2x^2+2x+1, 2x^3+2x^2+x+2$
$2x^3+x^2+2x+2, 2x^3+x^2+x+1$

문 31. $Z_p[x]$**에 속하는 기약인 2차 다항식의 개수를 구하라. 단, p는 소수이다.**

[힌트: x^2+ax+b **형태의 기약이 아닌 다항식의 개수를 구하고, 기약이 아닌 2차 다항식의 개수를 구하여 전체 2차식의 개수에서 이것을 뺀다.]**

풀 이

총 경우의 수: (p-1)p·p

중근을 갖는 경우: (p-1)p , 서로 다른 근을 갖는 경우: (p-1)p(p-1)/2

그러면

(기약다항식)의 개수=(총 다항식)의 개수-(가약 다항식)의 개수

=(p-1)p·p-[(p-1)p + (p-1)p(p-1)/2]

$=\frac{(p-1)^2p}{2}$

따라서 $Z_p[x]$에 속하는 기약인 2차 다항식의 개수는 $\frac{(p-1)^2p}{2}$개 이다.

문 32. -생 략-

문 33. -생 략-

문 34. $Z_p[x]$**에서 다항식** x^p+a**는 임의의** $a\in Z_p$**에 대하여 기약이 아님을 증명하라.**

풀 이

(1) $p=2$일 때 x^2, x^2+1는 가약이다.

(2) $p\geq 3$인 소수일 때

$(-a)^p+a\equiv -a^p+a\equiv -a+a\equiv 0(\mathrm{mod}p)$ ($\because$페르마의 소정리)

그러므로 다항식 x^p+a는 $x+a$를 인수로 갖는다.

(1),(2)에 의하여 모든 소수에 대하여 가약임을 알 수 있다.

따라서 임의의$a\in Z_p$에 대하여 $Z_p[x]$에서 다항식 x^p+a는 기약이 아니다.

문 35. F가 체이고 a≠0가 F[x]에 속하는 $f(x)=a_0+a_1x+\cdots+a_nx^n$**의 근이면** $\frac{1}{a}$**은**

$g(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ **의 근임을 보여라.**

풀 이

$\frac{1}{a}$이 $f(x)=a_0+a_1x+\cdots+a_nx^n$의 근이면 다음이 성립한다.

$$f(\frac{1}{a})=a_0+a_1(\frac{1}{a})+\cdots+a_n(\frac{1}{a})^n=0$$
$$\Rightarrow a^n\left[a_0+a_1(\frac{1}{a})+\cdots+a_n(\frac{1}{a})^n\right]=a^n\cdot 0=0\ (a\neq 0)$$
$$\Rightarrow a_0a^n+a_1(a^{n-1})+\cdots+a_n=0$$
$$\Rightarrow g(a)=0$$

따라서 $g(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$의 근임을 알 수 있다.

문 36. (나머지 정리) F가 체일 때, f(x)∈F[x]이고 $\alpha \in F$라 하자. f(x)를 $x-\alpha$로 나누었을때, 나머지 r(x)는 호제법과 일치하여 $f(\alpha)$임을 보여라.

풀 이

유클리드 호제법에 의하여 다음이 성립한다.

$f(x)=(x-\alpha)g(x)+r(x), \deg r(x)=0$

이때 $f(\alpha)=(\alpha-\alpha)g(\alpha)+r(\alpha)=r(\alpha)$이고 $\deg r(x)=0$ 이므로 따라서 $r(x)=f(\alpha)$인 상수임을 알 수 있다.

문 37. $\sigma_m : Z \to Z_m$을 $a \in Z$에 대하여 $\sigma_m(a)=$(a를 m으로 나눈 나머지)로 정의된 준동형사상이라 하자.

(a) $\overline{\sigma_m}: Z[x] \to Z_m[x]$를

$\overline{\sigma_m}(a_0+a_1x+\cdots+a_nx^n)=\sigma_m(a_0)+\sigma_m(a_1)x+\cdots+\sigma_m(a_n)x^n$

로 정의할 때, $\overline{\sigma_m}$는 Z[x]에서 $Z_m[x]$ 위로 대응하는 준동형사상임을 보여라.

풀 이

임의의 $\sum_{i=0}^{n} a_ix^i, \sum_{i=0}^{n} b_ix^i \in Z[x]$에 대하여 σ_m이 준동형사상이므로 다음이 성립한다.

$$\overline{\sigma}\left(\sum_{i=0}^{n} a_ix^i+\sum_{i=0}^{n} b_ix^i\right)=\overline{\sigma}\left(\sum_{i=0}^{n}(a_i+b_i)x^i\right)=\sum_{i=0}^{n}\sigma_m(a_i+b_i)x^i$$
$$=\sum_{i=0}^{n}\sigma_m(a_i)x^i+\sum_{i=0}^{n}\sigma_m(b_i)x^i=\overline{\sigma}\left(\sum_{i=0}^{n} a_ix^i\right)+\overline{\sigma}\left(\sum_{i=0}^{n} b_ix^i\right)$$

$$\overline{\sigma}\left(\sum_{i=0}^{n} a_ix^i \cdot \sum_{i=0}^{n} b_ix^i\right)=\overline{\sigma}\left(\sum_{m=0}^{2n}\left(\sum_{i=0}^{m} a_{m-i}b_i\right)x^i\right)=\sum_{m=0}^{2n}\sigma_m\left(\sum_{i=0}^{m} a_{m-i}b_i\right)x^i$$
$$=\sum_{i=0}^{n}\sigma_m(a_i)x^i \cdot \sum_{i=0}^{n}\sigma_m(b_i)x^i=\overline{\sigma}\left(\sum_{i=0}^{n} a_ix^i\right)\cdot\overline{\sigma}\left(\sum_{i=0}^{n} b_ix^i\right)$$

따라서 $\overline{\sigma_m}$은 환 준동형사상이다.

(b) f(x)∈Z[x]와 $\overline{\sigma_m}(f(x))$ 둘 다 차수 n을 갖고 $\overline{\sigma_m}(f(x))$가 $Z_m[x]$에서 차수 n보다 낮은 두 다항식으로 인수분해 되지 않는다면 f(x)는 Q[x]에서 기약임을 보여라.

풀 이 대우 증명한다!!

$f(x)$가 $Z[x]$에서 차수 n보다 낮은 두 다항식으로 인수분해 된다고 하자.

즉 $g(x), h(x) \in Z[x], 1 \le \deg g(x), \deg h(x) < n$ 이 존재해서 $f(x)=g(x)h(x)$을 만족한다고 하자.

그러면 $\overline{\sigma_m}(f(x))=\overline{\sigma_m}(g(x)h(x))=\overline{\sigma_m}(g(x))\overline{\sigma_m}(h(x))$이 성립한다.

이때 $\deg(\overline{\sigma_m}(g(x))), \deg(\overline{\sigma_m}(h(x))) < n$이다. 따라서 $\overline{\sigma_m}(f(x))$가 $Z_m[x]$에서 차수 n보다 낮은 두 다항식으로 인수분해 된다.

(c) (b)를 이용하여 $x^3+17x+36$은 Q[x]에서 기약임을 보여라.
[힌트: 계수를 간단히 만들 수 있도록 소수 m을 정하여 보라.]

풀 이

$\overline{\sigma_5}(x^3+17x+36)=x^3+2x+1$이고 이때

$\Phi_0(x^3+2x+1)=1, \Phi_1(x^3+2x+1)=4, \Phi_2(x^3+2x+1)=3$
$\Phi_3(x^3+2x+1)=2, \Phi_4(x^3+2x+1)=3$

으로서 근을 갖지 않는다 따라서 기약이다. 그러므로 (b)에 의하여 $x^3+17x+36$은 Q[x]에서 기약이다.

문 1. $Z\times Z$에서 $Z\times Z$로 대응하는 모든 환 준동형사상을 적어라.

풀 이

$(1,0),(0,1)$이 $Z\times Z$의 기저이므로 $f(1,0)=(0,0),(1,0),(0,1),(1,1), f(0,1)=(0,0),(1,0),(0,1),(1,1)$에 대응될 수 있다.

(1) $f(1,0)=(0,0), f(0,1)=(0,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(0,0)$

(2) $f(1,0)=(0,0), f(0,1)=(1,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(n,0)$

(3) $f(1,0)=(0,0), f(0,1)=(0,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(0,n)$

(4) $f(1,0)=(0,0), f(0,1)=(1,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(n,n)$

(5) $f(1,0)=(0,1), f(0,1)=(0,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(0,m)$

(6) $f(1,0)=(0,1), f(0,1)=(1,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(n,m)$

(7) $f(1,0)=(0,1), f(0,1)=(0,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(0,m+n)$

(8) $f(1,0)=(0,1), f(0,1)=(1,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(n,m+n)$

(9) $f(1,0)=(1,0), f(0,1)=(0,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m,0)$

(10) $f(1,0)=(1,0), f(0,1)=(1,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m+n,0)$

(11) $f(1,0)=(1,0), f(0,1)=(0,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m,n)$

(12) $f(1,0)=(1,0), f(0,1)=(1,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m+n,n)$

(13) $f(1,0)=(1,1), f(0,1)=(0,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m,m)$

(14) $f(1,0)=(1,1), f(0,1)=(1,0)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m+n,m)$

(15) $f(1,0)=(1,1), f(0,1)=(0,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m,m+n)$

(16) $f(1,0)=(1,1), f(0,1)=(1,1)$인 경우 $f(m,n)=m\cdot f(1,0)+n\cdot f(0,1)=(m+n,m+n)$

여기서 $f(m,n)=(0,0), f(m,n)=(n,0), f(m,n)=(0,n), f(m,n)=(n,n), f(m,n)=(0,m)$
$f(m,n)=(n,m), f(m,n)=(m,0), f(m,n)=(m,n), f(m,n)=(m,m)$

인 환 준동형사상을 찾을 수 있다.

문 2. Z_2와 동형이 되는 부분환을 포함하는 Z_n을 만족하는 양의 정수 n을 모두 찾아라.

풀 이

f를 환 준동형사상이라 사상이라 하자.

그러면 Z_n는 {f(0), f(1)}를 부분군으로 갖는다.

이때 f(0)=0임은 자명하고 f(1)=m(m≠0)일 때 f(1)+f(1)=0이므로 2m=n을 만족하고

또한 f(1)f(1)=f(1)이므로 m·m=m을 만족한다.

여기서 m·1=m, m·2=0, m·3=m·2+m·1=m, m·4=m·2+m·2=0 이므로

m·m=m이기 위해서는 m의 형태는 홀수 이어야 한다.

따라서 찾고 있는 양의정수 n=2m=2(2k+1)=4k+2 (k≧0인 정수)=2,6,8,… 이다.

문 3. Z_{12}의 모든 아이디얼 N을 구하고 각 경우에 Z_{12}/N을 계산하라. 즉 잉여환과 동형이 되는 환을 구하라.

풀 이

우선 Z_{12}의 부분군을 찾는다.

{0}, <1>={0,1,2,3,4,5,6,7,8,9,10,11}=Z_{12},

<2>={0,2,4,6,8,10}, <3>={0,3,6,9}, <4>={0,4,8},<6>={0,6}

여기서 {0}와 <1>은 자명하게 아이디얼임을 알 수 있고 나머지에 대하여 임의의 a∈Z_{12}에 곱에 관하여 닫혀 있는지 알아보자. p=2,3,4,6에 대하여 <p>는 Z_{12}에서 p의 배수들의 모임이다. 따라서 ap=pa∈<p>임을 쉽게 알 수 있다. 따라서 주어진 6개의 부분군이 모두 Z_{12}의 아이디얼이 됨을 알 수 있다.

이때 $Z_{12}/\{0\}\approx Z_{12}, Z_{12}/Z_{12}\approx\{0\}$, $Z_{12}/<2>\approx Z_2$, $Z_{12}/<3>\approx Z_3$, $Z_{12}/<4>\approx Z_4$, $Z_{12}/<6>\approx Z_6$와 동형임을 알 수 있다.

문 4. $2Z/8Z$에 대한 덧셈과 곱셈 연산표를 구하라. $2Z/8Z$와 Z_4는 동형환인가?

풀 이

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

·	0	2	4	6
0	0	0	0	0
2	0	4	0	4
4	0	0	0	0
6	0	4	0	4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

덧셈에 관한 연산에서는 동형이지만 곱셈에 관한 연산에서는 동형이 아님을 알 수 있다.

따라서 동형환이 아니다.

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 5. An *isomorphism of a ring* R with a ring R' is a homomorphism $\Phi: R\to R'$ such that $\ker\Phi=\{0\}$

풀 이

동형이 되기 위해서는 환 준동형사상인 조건과 전단사의 조건이 있어야 한다. 그런 점에서 위의 정의에는 전사인 조건이 추가 되어야 한다.

문 6. An *ideal* N of a ring R is an additive subgroup of <R,+> such that for all r∈R and all n∈N. we have rn∈N and nr∈N.

풀 이

아이디얼(이데알)에 관한 옳은 정의이다.

문 7. *The kernel of a homomorphism* Φ mapping a ring R into a ring R' is $\{\Phi(r)=0'|r\in R\}$.

풀 이

$\{\Phi(r)=0'|r\in R\}\Rightarrow\{r\in R|\Phi(r)=0'\}$ 와 같이 바뀌어야 옳은 정의가 된다.

문 8. f를 R에서 R로 대응하며, 모든 차수의 도함수를 갖는 모든 함수의 환이라 하자. 도함수는 사상 $\delta: F \to F$를 만든다. 단 $\delta(f(x)) = f'(x)$이다. δ는 준동형사상인가? 그 이유는? 이 문제와 예제 26.12사이의 관계를 구하라.

풀 이

$f(x), g(x) \in F[x]$에 대하여 $\delta(f(x)g(x)) = f'(x)g(x) + f(x)g'(x) \neq \delta(f(x))\delta(g(x))$이므로 환 준동형사상이 아니다.

문 9. R는 단위원 1_R을 가지며, $\Phi(1_R) \neq 0$이지만 $\Phi(1_R)$는 S에 대한 단위원이 아닌 환 준동형사상 $\Phi: R \to S$의 예를 들어라.

풀 이

$\Phi: Z \to Z \times Z, \Phi(a) = (a,0)$이라 하면 이는 환 준동형사상이고
또한 Z 단위원을 갖고 $\Phi(1) = (1,0) \neq (0,0)$이지만 (1,0)은 $Z \times Z$의 단위원은 아니다.

문 10. 참, 거짓을 판정하라.

(a) 환 준동형사상의 개념은 잉여환의 개념과 밀접한 관계가 있다.

풀 이 (True)

환 동형정리에 의하여 잉여환과 동형인 환을 찾을 수 있는데 그 과정에서 환 준동형사상이 중요한 역할을 한다.

(b) 환에서 준동형사상은 군에서 동형사상과 같은 것이다.

풀 이 (False)

환에서 준동형사상은 군에서 준동형사상과 같은 역할을 한다. 동형사상과 같은 역할을 하는 것이 아니다.

(c) 환 준동형사상이 1-1이 될 필요충분조건은 그 핵이 {0}일 때이다.

풀 이 (True)

($\Rightarrow$) $f(a) = 0 \Rightarrow f(a) = 0 = f(0)$이고 1-1 이므로 다음이 성립한다.

$a = 0 \Rightarrow \ker f = \{0\}$

($\Leftarrow$) $f(a) = f(b) \Rightarrow f(a) - f(b) = 0 \Rightarrow f(a-b) = 0$이고 $\ker f = \{0\}$으므로 다음이 성립한다.

$a - b = 0 \Rightarrow a = b$

(d) Q는 R에서 아이디얼이다.

풀 이 (False)

$\sqrt{2} \in R$이지만 $\sqrt{2} \notin Q$이므로 Q는 R의 이데알이 아니다.

(e) 환에서 모든 아이디얼은 그 환의 부분환이다.

풀 이 (True)

환 R의 임의의 아이디얼을 I라고 하면 다음이 성립한다.

(1) 임의의 a,b∈I에 대하여 a-b∈I 가 성립한다.

(2) 임의의 r∈R과 임의의 a∈I에 대하여 ra∈I, ar∈I가 성립한다.

이제 아이디얼 I가 환 R의 부분환이기 위하여 다음이 성립함을 보이면 된다.

(3) 임의의 a,b∈I에 대하여 a-b∈I 가 성립한다.

(4) 임의의 a,b∈I에 대하여 ab∈I 가 성립한다.
여기서 (3)임은 (1)에 의하여 자명하고
(4)임은 임의의 b∈I⊆R이므로 임의의 a∈I에 대하여 ab∈I 임을 알 수 있다.
그러므로 임의의 아이디얼 I는 환 R의 부분환이다.

(f) 모든 환에서 모든 부분환은 그 환의 아이디얼이다.

풀 이 (False)
R에서 Q는 부분환이지만 아이디얼은 아니다.

(g) 모든 가환환의 모든 잉여환은 다시 가환환이다.

풀 이 (True)
환 R이 가환환이고 M을 환 R의 아이디얼이라 하자. 임의의 a,b∈R/M에 대하여 c.d∈R가 존재하여 다음이 성립한다.
a=c+M, b=d+M
ab=(c+M)(d+M)=cd+M=dc+M=(d+M)(c+M)=ba (여기서 cd+M=dc+M은 환 R이 가환환이기 때문에 성립한다.) 따라서 임의의 가환환이 모든 잉여환은 다시 가환환이다.

(h) 환 $Z/4Z$와 Z_4는 동형이다.

풀 이 True
$\phi: Z \to Z_4, \phi(a) = (a$를 4로 나눈 나머지$)$라 하면 ϕ는 전사인 환 준동형사상이고
이때 $\ker\phi = 4Z$이므로 환 제 1동형정리에 의하여 둘은 동형이다.

(i) 단위원을 갖는 환 R에서 아이디얼 N가 R전체가 될 필요충분조건은 1∈N이다.

풀 이 (True)
(⇨) 1∉N이라 가정하자. 그러면 N+<1>은 다음을 만족한다.
N⊊N+<1>⊆R
하지만 이는 N=R 임에 모순이다. 그러므로 1∈N이다.
(⇦) 1∈N이면 아이디얼의 정의에 의하여 임의의 a∈R에 대해 a・1∈N이 성립한다. 그러므로 R=N 이다.

(j) 환에서 아이디얼의 개념은 군에서 정규부분군의 개념과 같다.

풀 이 (True)
잉여환에서의 동형정리와 잉여군에서의 동형정리를 보면 알 수 있다.

문 11. R를 환이라 하자. {0}와 R는 둘 다 R의 아이디얼임을 관찰하자. 잉여환 R/R과 R/{0}는 실제로 연관이 있는가? 그 이유는?

풀 이

{0}과 R이 덧셈에 대한 가환군이 됨은 자명하므로 다음을 보인다.
임의의 a∈R, 0∈{0}에 대해 0·a=0∈{0}, a·0=0∈{0}이므로 {0}은 R의 아이디얼이다. 또한 임의의 a∈R, b∈R에 대해 R이 환이므로 ab∈R, ba∈R이다 따라서 R은 R의 아이디얼이다. 그리고 R/R≈{0}, R/{0}≈R이 됨을 알 수 있다.

문 12. 정역의 잉여환이 체가 될 수 있음을 보여라.

풀 이

$Z/3Z \simeq Z_3$이고 여기서 Z_3가 체이므로 $Z/3Z$ 또한 체이다.

문 13. 정역의 잉여환이 0인자를 가질 수 있음을 보여라.

풀 이

$Z/4Z \simeq Z_4$이고 여기서 Z_4가 0인자를 가진다. 그러므로 $Z/4Z$는 0인자를 갖는다.
실제로 (2+4Z)(2+4Z)=0+4Z이다.

문 14. 0인자를 갖는 환의 잉여환은 정역일수도 있음을 보여라.

풀 이

$Z \times Z/Z \times \{0\} \simeq Z$

문 15. 환$Z \times Z$에서 아이디얼이 아닌 부분환을 구하여라.

풀 이

$2Z \times 4Z$

문 16. 어느 학생에서 환 R에서 아이디얼 N을 법으로 하는 잉여환이 가환이 될 필요충분조건은 모든 r,s∈R에 대하여 <rs-sr>∈N임을 증명하도록 하였다. 그 학생은 다음과 같이 시작하였다. R/N이 가환이라 가정하면 모든 r,s∈R에 대하여 rs=sr 이다.
(a) 이것을 읽은 교수님이 의미가 없다고 하는 이유는 무엇인가?

풀 이

R/N에서 가환의 정의를 잘 이해하지 못하고 잘못 쓰고 있기 때문에...

(b) 이 학생이 무엇이라고 썼어야 옳은가?

풀 이

R/N이 가환이면 임의의 (a+N),(b+N)∈R/N에 대해 (a+N)(b+N)=(b+N)(a+N)이 성립한다.

(c) 이것을 증명하라.("필요충분 조건"임에 주의할것)

풀 이

R/N이 가환이면 임의의 a+N, b+N∈R/N에 대해 다음이 성립한다.
(a+N)(b+N)=ab+N=ba+N=(b+N)(a+N)
여기서 ab+N=ba+N이면 (ab+N)-(ba+N)∈N이고 그러므로 ab-ba∈N이 성립한다.
역으로 ab-ba∈N이면 ab+N=ba+N이 성립한다.
따라서 (a+N)(b+N)=(b+N)(a+N)이 성립한다.

문 17. Let $R=\{a+b\sqrt{2}\,|\,a,b\in Z\}$ and R' consist of all 2×2 matrices of the form $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ for a,b∈Z. Show that R is a subring of *R(실수체)* and that R' is a subring of $M_2(Z)$. Then show that $\Phi: R\to R'$. where $\Phi(a+b\sqrt{2})=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ is an isomorphism.

풀 이

(1) R이 *R(실수체)*의 부분환임을 보이자.

우선 $R\subseteq R$ 임은 자명하다.

임의의 $x,y\in R$에 대하여 $a,b,c,d\in Z$이 존재하여 다음을 만족한다.

$x=a+\sqrt{2}\,b, y=c+\sqrt{2}\,d$

이때 $x-y=(a+\sqrt{2}\,b)-(c+\sqrt{2}\,d)=(a-c)+\sqrt{2}\,(b-d)\in R\,(\because a-c,b-d\in Z)$ 이고

$xy=(a+\sqrt{2}\,b)(c+\sqrt{2}\,d)=(ac+2bd)+\sqrt{2}\,(ad+bc)\in R\,(\because ac+2bd,ad+bc\in Z)$

이 성립한다. 그러므로 R이 *R(실수체)*의부분환이다.

(2) $R'=\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}|a,b\in Z\right\}$가 $M_2(Z)$의 부분환임을 보이자.

우선 $R'=\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}|a,b\in Z\right\}\subseteq M_2(Z)$임은 자명하다.

임의의 $x,y\in R$에 대하여 $a,b,c,d\in Z$이 존재하여 다음을 만족한다.

$x=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}, y=\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}$

이때 $x-y=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}-\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}=\begin{pmatrix} a-c & 2(b-d) \\ (b-d) & a-c \end{pmatrix}\in R'\,(\because a-c,b-d\in Z)$

$xy=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}=\begin{pmatrix} ac+2bd & 2(ad+bc) \\ (ad+bc) & ac+2bd \end{pmatrix}\in R'\,(\because ac+2bd,\ ad+bc\in Z)$

이 성립한다. 그러므로 $R'=\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}|a,b\in Z\right\}$은 $M_2(Z)$의 부분환이다.

(3) $\Phi: R\to R'$, $\Phi(a+b\sqrt{2})=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$가 동형사상임을 보이자.

$\forall x,y\in R\ \exists a,b,c,d\in Z\ s.t.\ x=a+b\sqrt{2}, y=c+b\sqrt{2}$

이때

$$\Phi(x)+\Phi(y)=\Phi(a+b\sqrt{2})+\Phi(c+b\sqrt{2})=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}+\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}=\begin{pmatrix} a+c & 2(b+d) \\ (b+d) & a+c \end{pmatrix}=\Phi(x+y)$$

$$\Phi(x)\Phi(y)=\Phi(a+b\sqrt{2})\Phi(c+b\sqrt{2})=\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}=\begin{pmatrix} ac+2bd & 2(ad+bc) \\ (ad+bc) & ac+2bd \end{pmatrix}=\Phi(xy)$$

이 성립하므로 Φ는 환 준동형사상이다.

또한 $\Phi(x)=\Phi(y)\Rightarrow\Phi(a+b\sqrt{2})=\Phi(c+b\sqrt{2})\Rightarrow\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}=\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}\Rightarrow a=c, b=d$

$$im\Phi=\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}|a,b\in Z\right\}=R'$$

이 성립하므로 Φ는 전단사인 사상이다.

위의 결과들에 의하여 따라서 Φ는 동형사상이다.

문 18. 체의 각 준동형사상은 1-1이거나 모든 것이 0에 대응하는 사상임을 보여라.

풀 이

F를 체라 하고 임의의 준동형사상을 $f : F \to F$라 하자.
ker f=0이면 자명하게 준동형사상은 1-1이다. 따라서 ker f≠0 이라 가정하자.
그러면 v≠0인 v가 존재해서 f(v)=0을 만족한다.
이때 F는 체이므로 v의 역원 v' 이 존재하고 f가 준동형사상이므로

f(1)=f(v)·f(v')=0·f(v')=0

을 만족한다. 따라서 F의 모든 것이 0에 대응하는 사상임을 알 수 있다.
그러므로 체의 각 준동형사상은 1-1이거나 모든 것이 0에 대응하는 사상임을 알 수 있다.

문 19. R, R' 와 R"가 환이고 $\Phi : R \to R'$와 $\Psi : R' \to R''$가 준동형사상이면 합성함수 $\Psi\Phi : R \to R''$도 준동형사상임을 보여라.

풀 이

임의의 $a,b \in R$에 대하여

$$\Psi\Phi(a+b) = \Psi(\Phi(a+b)) = \Psi(\Phi(a)+\Phi(b)) = \Psi(\Phi(a)) + \Psi(\Phi(b)) = \Psi\Phi(a) + \Psi\Phi(b)$$
$$\Psi\Phi(a \cdot b) = \Psi(\Phi(a \cdot b)) = \Psi(\Phi(a) \cdot \Phi(b)) = \Psi(\Phi(a)) \cdot \Psi(\Phi(b)) = \Psi\Phi(a) \cdot \Psi\Phi(b)$$

이 성립한다. 따라서 합성함수 $\Psi\Phi : R \to R''$도 준동형사상이다.

문 20. R은 단위원을 갖고 소수인 표수 p를 갖는 가환환이라 하자. $\Phi(a) = a^p$으로 정의된 사상 $\Phi_p : R \to R$가 준동형사상임을 보여라. (이 준동형사상을 Frobenius 준동형사상이라 한다.)

풀 이

임의의 $a,b \in R$에 대하여

$$\Phi(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i,\ \Phi(a)+\Phi(b) = a^p + b^p, \Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b)$$

가 성립한다. 여기서 가환환 R의 표수가 p 이므로 p·1=0이다
그러면 0<i<p 에 대하여 $\binom{p}{i} = 0$ 이 성립한다.

따라서 $\Phi(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p = \Phi(a) + \Phi(b)$임을 알 수 있다.

그러므로 Φ는 환 준동형사상이다.

문 21. R과 R'가 환이며 $\Phi : R \to R'$는 $\Phi(R) \neq \{0\}$를 만족하는 환 준동형사상이라 하면 R는 단위원 1를 가지고 R'가 0인자를 갖지 않으면 $\Phi(1)$는 S에 대한 단위원임을 보여라.

풀 이

임의의 $x \in \Phi(R)$에 대해 $a \in R$이 존재해서 $x = \Phi(a)$를 만족한다.
그러면 $\Phi(1)x = \Phi(1)\Phi(a) = \Phi(1 \cdot a) = \Phi(a) = x$이 성립한다.
또한 $x\Phi(1) = \Phi(a)\Phi(1) = \Phi(a \cdot 1) = \Phi(a) = x$이 성립한다.
이제 $\Phi(1)$이 $\Phi(R)$의 단위원임을 보이자.
$\Phi(1) = 0$이면 $\Phi(a) = \Phi(a \cdot 1) = \Phi(a)\Phi(1) = 0$이 되어 $\Phi(R) \neq \{0\}$임에 모순이다.
이제 $\Phi(1) \neq 0$이고 $1' \in R'$을 R'의 단위원이라 하면 $\Phi(1)\Phi(1) = \Phi(1 \cdot 1) = \Phi(1) = \Phi(1) \cdot 1'$
이고 R'이 0인자를 갖지 않으므로 $\Phi(1) = 1'$임을 알 수 있다.
따라서 $\Phi(1)$은 $\Phi(R)$의 단위원임을 알 수 있다.

문 22. $\Phi : R \to R'$**는 환 준동형사상이고 N은 R의 아이디얼이라 하자.**

(a) $\Phi[N]$**은** $\Phi[R]$**의 아이디얼임을 보여라.**

풀 이

$N \subseteq R \Rightarrow \Phi[N] \subseteq \Phi[R]$임은 자명하고 $\forall x,y \in \Phi[N]\ \exists a,b \in N\ s.t.\ x = \Phi[a],\ y = \Phi[b]$이고 다음이 성립한다.

$x - y = \Phi[a] - \Phi[b] = \Phi[a-b] \in \Phi[N]$ ($\because \Phi$가 환준동형사상, N는 R의 아이디얼)

또한 $\forall r' \in \Phi[R] \forall x \in \Phi[N]\ \exists r \in R, a \in N\ s.t.\ r' = \Phi[r],\ x = \Phi[a]$이고 다음이 성립한다.

$r'x = \Phi[r]\Phi[a] = \Phi[ra] \in \Phi[N],\ xr' = \Phi[a]\Phi[r] = \Phi[ar] \in \Phi[N]$
($\because \Phi$가 환준동형사상, N는 R의 아이디얼)

따라서 $\Phi[N]$은 $\Phi[R]$의 아이디얼이다.

(b) $\Phi[N]$**이 R'의 아이디얼일 필요는 없음을 예를 들어 보여라.**

풀 이

$\Phi[R] = Z, \Phi[N] = 2Z, R' = R$(실수체)라 하자. 그러면 위의 관계를 만족한다.
하지만 2Z는 R(실수체)의 아이디얼은 아니다.

(c) N' 은 $\Phi[R]$**와 R'의 아이디얼이라 하자.** $\Phi^{-1}[N']$**은 R의 아이디얼임을 보여라.**

풀 이

임의의 $a,b \in \Phi^{-1}[N']$에 대하여 $a',b' \in N'$이 존재해서 $\Phi[a] = a', \Phi[b] = b'$을 만족한다.
이때 $\Phi[a-b] = \Phi[a] - \Phi[b] = a' - b' \in N'$이므로 $a - b \in \Phi^{-1}[N']$이 성립한다.
따라서 $\Phi^{-1}[N']$는 덧셈에 대한 가환군을 이룬다. 임의의 $r \in R$와 임의의 $a \in \Phi^{-1}[N']$에 대하여 $a' \in N'$이 존재해서 $\Phi[a] = a'$을 만족한다. 이때 $\Phi[ra] = \Phi[r]\Phi[a] = \Phi[r]a' \in N'$($\because N'$는 $\Phi[R]$의 아이디얼)이므로 $ra \in \Phi^{-1}[N']$이 성립한다. 마찬가지로 $\Phi[ar] = \Phi[a]\Phi[r] = a'\Phi[r] \in N'$($\because N'$는 $\Phi[R]$의 아이디얼)이므로 $ar \in \Phi^{-1}[N']$이 성립한다. 그러므로 $\Phi^{-1}[N']$은 R의 아이디얼이다.

문 23. F가 체이고 S가 n개의 직적 $F \times F \times \cdots \times F$**의 임의의 부분집합이라 하자. S의 각 원소** $(a_1, \cdots, a_n)$**을 근으로 갖는 모든** $f(x_1, \cdots x_n) \in F[x_1, \cdots x_n]$**의 집합** N_S**는** $F[x_1, \cdots x_n]$**에서 아이디얼임을 보여라. 이 사실은 대수기하에서 아주 중요하다.**

풀 이

$\Phi_a : F \times F \times \cdots \times F \to F$, $\Phi[f(x_1, \cdots, x_n)] = f(a_1, \cdots, a_n)$인 전사인 평가 준동형 사상이라 하자.
이때 $\ker\Phi_a = \{\Phi_a(f(x_1, \cdots, x_n)) = 0 | f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]\}$임을 알 수 있다.
위에서 $N_s = \{\Phi_a(f(x_1, \cdots, x_n)) = 0 | f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]\}$는 다음과 같이 정의되고 있으므로 $N_s = \ker\Phi_a$임을 알 수 있고 여기서 $\ker\Phi_a$는 $F[x_1, \cdots x_n]$의 아이디얼이므로
따라서 N_S은 $F[x_1, \cdots x_n]$의 아이디얼임을 알 수 있다.

문 24. 체의 잉여환은 한 원소를 갖는 자명환이거나 그 체와 동형임을 보여라.

풀 이

임의의 체를 F라 하면 체F의 아이디얼은 {0}과 자기 자신 F 뿐이다.
따라서 F/{0}≈F, F/F={0}이 성립함을 알 수 있다.

문 25. R가 단위원을 갖는 환이고 N이 N≠R인 R의 아이디얼이면 R/N은 0이 아닌 단위원을 갖는 환임을 보여라.

풀 이

N≠R이므로 1∉N이다. 그러면 1+N≠0+N이고 임의의 a+N∈R/N에 대하여

(a+N)(1+N)=a+N=(1+N)(a+N)

이 성립한다. 그러므로 R/N은 0이 아닌 단위원을 갖는 환임을 알 수 있다.

문 26. R가 가환환이고 a∈R라 하면 $I_a=\{x\in R|ax=0\}$는 R의 아이디얼임을 보여라.

풀 이

임의의 $x,y\in I_a$에 대해 $a(x-y)=ax=ay=0-0=0$이므로 $x-y\in I_a$이 성립한다.

임의의 $r\in R$과 임의의 $x\in I_a$에 대해 $a(rx)=(ar)x=(ra)x=r(ax)=r0=0$이므로 $rx=xr\in I_a$가 성립한다. 따라서 $I_a=\{x\in R|ax=0\}$는 R의 아이디얼이다.

문 27. 환R에서의 아이디얼의 공통집합은 다시 아이디얼임을 보여라.

풀 이

I_a,I_b를 환 R의 아이디얼이라 하자. 임의의 x,y∈$I_a\cap I_b$에 대하여 x,y∈I_a이고 x,y∈I_b이므로 다음이 성립한다.

x-y∈I_a 이고 x-y∈I_b

그러므로 x-y∈$I_a\cap I_b$이 성립하여 덧셈에 대한 가환군임을 알 수 있다. 또한 임의의 r∈R과 임의의 x∈$I_a\cap I_b$에 대하여 x∈I_a이고 x∈I_b이므로 ra, ar∈I_a 이고 ra, ar∈I_b 이 성립한다. 따라서 ra, ar∈$I_a\cap I_b$이고 그러므로 $I_a\cap I_b$는 R의 아이디얼이다.

문 28. R와 R'를 환이라 하고 N과 N'를 각각 R와 R'의 아이디얼이라 하자. Φ가 R에서 R'로 대응하는 준동형사상이라 할 때 $\Phi[N]\subseteq N'$이면 Φ는 표준 준동형사상 $\Phi_*:R/N\to R'/N'$를 유도할 수 있음을 보여라.

풀 이

$\phi:R\to R'$인 준 동형 사상이라 하자. 이때 $\Phi_*(a+N)=\Phi(a)+N'$으로 정의하자.

$$a+N=b+N\Rightarrow a-b\in N\Rightarrow\Phi(a)-\Phi(b)=\Phi(a-b)\in\Phi(N)\subseteq N'$$
$$\Rightarrow\Phi(a)+N'=\Phi(b)+N'\Rightarrow\Phi_*(a+N)=\Phi_*(b+N)$$

이 성립하므로 Φ_*는 잘 정의된 사상이다.

이제 임의의 $x,y\in R/N$에 대하여 $a,b\in R$이 존재해서 다음을 만족한다.

$x=a+N, y=b+N$

그러면
$$\Phi_*(x+y)=\Phi_*((a+N)+(b+N))=\Phi_*((a+b)+N)$$
$$=\Phi(a+b)+N'=\Phi(a)+\Phi(b)+N'=(\Phi(a)+N')+(\Phi(b)+N')$$
$$=\Phi_*(a+N)+\Phi_*(b+N)=\Phi_*(x)+\Phi_*(y)$$
$$\Phi_*(xy)=\Phi_*((a+N)(b+N))=\Phi_*((ab)+N)=\Phi(ab)+N'$$
$$=\Phi(a)\Phi(b)+N'=(\Phi(a)+N')(\Phi(b)+N')$$
$$=\Phi_*(a+N)\Phi_*(b+N)=\Phi_*(x)\Phi_*(y)$$

이 성립한다. 따라서 Φ는 표준 준동형사상 Φ_*을 유도할 수 있다.

문 29. Φ가 단위원을 갖는 환 R에서 환 R' 위에 대응하는 준동형사상이라 하고 u는 R에서 가역원이라 하자. $\Phi(u)$가 R'에서 가역원이 될 필요충분 조건은 R의 임의의 가역원이 Φ의 핵에 속하지 않을 때 임을 보여라.

풀 이

(⇦)임의의 $u\in U(R)$에 대하여 $\Phi(u)\neq 0$이라 하자. 그러면 $u'\in U(R)$이 존재해서 다음을 만족한다.

$\Phi(u)\Phi(u')=\Phi(uu')=\Phi(1)$

이제 $\Phi(1)$이 R'에서의 항등원임을 보이자. 임의의 $\Phi(a)\in\Phi(R)$에 대하여 $\Phi(a)\Phi(1)=\Phi(a)=\Phi(1)\Phi(a)$ 이므로 $\Phi(1)$은 $\Phi(R)$에서의 항등원이고 이때 $\Phi(R)$는 R'의 부분환이므로 항등원의 유일성에 의하여 $\Phi(1)$은 R'의 항등원임을 알 수 있다. 따라서 $\Phi(u)\in U(R')$임을 알 수 있다.

(⇨) $\Phi(u_0)=0$인 $u_0\in U(R)$이 존재한다고 가정하여 모순됨을 보인다.

$u_0\in U(R)$이므로 $u_0'\in U(R)$이 존재하여 $u_0u_0'=1$ 이 성립한다.

이때 Φ는 환 준동형사상이므로 다음이 성립한다.

$0=\Phi(u_0)\Phi(u_0')=\Phi(u_0u_0')=\Phi(1)$

이는 $\Phi(1)$이 R'의 곱셈에 관한 항등원임에 모순된다. 그러므로 임의의 $u\in U(R)$에 대하여 $\Phi(u)\neq 0$임을 알 수 있다.

문 30. 환 R의 원소 a가 만약 적당한 $n\in Z^+$에 대하여 $a^n=0$를 만족하면 a를 멱영원이라 한다. 가환환 R에서 모든 멱영원의 모임은 아이디얼임을 보여라. 이 아이디얼을 R의 근기(radical)라 한다.

풀 이

S를 R의 근기들의 모임이라 하자. $0^1=0$이므로 $0\in S\neq\varnothing$이다. 이제 S가 R의 아이디얼임을 보인다.

임의의 $a,b\in S$에 대하여 $n,m\in Z^+$가 존재해서 $a^n=0, b^m=0$을 만족한다.

그러면 $(a-b)^{n+m}=\sum_{i=0}^{n+m}\binom{n+m}{i}a^{n+m-i}(-b)^i$ 이고

여기서 $a^n=0, b^m=0$이므로 임의의 $i(0\le i\le n+m)$에 대하여 $\binom{n+m}{i}=0$을 만족한다.

따라서 $(a-b)^{n+m}=0$을 만족하는 $n+m\in Z^+$가 존재한다. 그러므로 $a-b\in S$이다.

임의의 $r\in R$과 임의의 $a\in S$에 대하여 $n\in Z^+$가 존재해서 $a^n=0$을 만족한다.

그러면 $(ar)^n=(ra)^n=r^na^n=0$이 성립하는 $n\in Z^+$이 존재함을 알 수 있다. 따라서 $ra=ar\in S$이다.

그러므로 S는 R의 아이디얼이다.

문 31. (문제30)에서 주어진 정의를 참고로 하여 환 Z_{12}의 근기를 구하고 이것이 (문제3)에서 찾은 Z_{12}의 아이디얼 중의 하나임을 관찰해 보라. Z의 근기는 무엇이며 Z_{32}의 근기는 무엇인가?

풀 이

$U(Z_{12})=\{1,5,7,11\}$은 곱셈에 관하여 닫혀 있으므로 Z의 근기가 될 수 없다. 이제 남은 원소는 0,2,3,4,6,8,9,10이 있다. 여기서 2,3,4,8,9,10 은 2와 3을 동시에 갖지 않았으므로 $a^n\equiv 0(\mathrm{mod}12)$인 $n\in Z^+$가 존재하지 않는다. 따라서 $(Z_{12}\text{의 근기})=\{0,6\}$이다. 이제 Z의 근기는 자명환 {0}이며 $(Z_{32}\text{의 근기})=\{0,2,4,6,8,\cdots,30\}$임을 알 수 있다.

문 32. (문제30)을 참고로 하여 N이 가환환 R의 근기이면 R/N은 자명 아이디얼 {0+N}을 근기로 가짐을 보여라.

풀 이

0+N 이외의 원소가 존재한다고 가정하여 모순됨을 보이자. a∉N인 a+N이 R/N에서 멱영원이라고 가정하자. 즉. $(a+N)^k = a^k + N = 0 + N$이 되게 하는 양의정수 k가 존재한다고 하자. 그러면 $a^k \in N$이고 이는 $a^{ks} = (a^k)^s = 0$이 되게 하는 양의정수 s가 존재해서 결국은 $a \in N$임을 알 수 있다. 이는 모순이다. 따라서 R/N의 근기는 {0+N}이다.

문 33. R를 가환환 그리고 N을 R의 아이디얼이라 하자. (문제30)을 참고로 하여 N의 모든 원소가 멱영원이고 R/N의 근기가 R/N이면 R의 근기는 R임을 보여라.

풀 이

임의의 a∈R에 대하여

(1) a∈N이면 가정에 의하여 멱영원이다.

(2) a∉N이면 a+N≠0+N이고 R/N의 근기가 R/N이므로

$(a+N)^k = a^k + N = 0 + N$이 되게 하는 양의정수 k가 존재한다. 그러면 $a^k \in N$이고 이는 $a^{ks} = (a^k)^s = 0$이 되게 하는 양의정수 s가 존재해서 결국은 a가 멱영원임을 알 수 있다. 따라서 R의 모든 원소가 멱영원이므로 R의 근기는 R이다.

문 34. R를 가환환 그리고 N을 R의 아이디얼이라 하자. 적당한 $n \in Z^+$에 대하여 $a^n \in N$을 만족하는 모든 $a \in R$의 집합 $\sqrt{N}$을 N의 근기라 한다. 이 용어가 (문제30)에서 주어진 것과 일치하는가?

풀 이

일치하지 않는다!!다만 R의 아이디얼 N의 멱영원들의 집합인 경우는 일치한다.

(1) (R의 근기(radical))=$\{a \in R \mid \exists\, n \in Z^+ \ s.t. \ a^n = 0\}$

(2) $\sqrt{N} = \{a \in R \mid \exists\, n \in Z^+ \ s.t. \ a^n \in N\}$. 여기서 N은 R의 아이디얼이다.

[(1) ⊆ (2)] 임의의 $b \in (R\text{의 근기})$에 대하여 $\exists\, n_1 \in Z^+ \ s.t. \ b^{n_1} = 0$이 성립한다. 여기서 0은 N의 덧셈에 관한 항등원이므로 다음이 성립한다.

$b^{n_1} = 0 \in N$

따라서 $b^{n_1} \in \sqrt{N}$이 성립한다.

[(1) ⊉ (2)]

(반례) $R = Z, N = 4Z \Rightarrow \sqrt{N} = 2Z \neq 4Z$

(단, N이 멱영원의 집합일 경우)[(1) ⊇ (2)] 임의의 $c \in \sqrt{N}$에 대하여 $\exists\, n_2 \in Z^+ \ s.t. \ c^{n_2} \in N$이 성립한다. 그러면 $\exists\, n_3 \in Z^+ \ s.t. \ c^{n_2 n_3} = (c^{n_2})^{n_3} = 0 \Rightarrow \exists\, n_2 n_3 \in Z^+ \ s.t. \ c^{n_2 n_3} = 0$

따라서 $c \in (R\text{의 근기})$이다. 그러므로 $(R\text{의 근기}) = \sqrt{N}$이라고 볼 수 있다.

문 35. (문제34)를 참고로 하여 가환환 R의 진부분 아이디얼 N의 예를 들어 다음을 보여라.

(a) $\sqrt{N}$은 N과 같을 필요가 없다.

풀 이

$R = Z, N = 4Z \Rightarrow \sqrt{N} = 2Z \neq 4Z$

(b) $\sqrt{N}$은 N과 같을 수도 있다.

풀 이

$R=Z, N=2Z \Rightarrow \sqrt{N}=2Z$

문 36. (문제34)의 아이디얼 $\sqrt{N}$과 R/N의 근기와의 관계는 어떠한가? (문제30 참조) 대답을 조심스럽게 해라.

풀 이

$N=\sqrt{N}$이면 (문제32)에 의하여 $R/N=\{0+N\}$임을 $N\neq\sqrt{N}$이면 $R/N\supsetneq\{0+N\}$임을 알 수 있다.

문 37. $a,b\in R$에 대하여 $\Phi(a+bi)=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}$로 정의된 $\Phi: C\to M_2(R)$는 C와 $M_2(R)$의 부분환 $\Phi[C]$의 동형사상임을 보여라.

풀 이

임의의 $a+bi, c+di\in C$에 대하여

$$\Phi(a+bi)+\Phi(c+di)=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}+\begin{pmatrix} c & d \\ -d & c\end{pmatrix}=\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c\end{pmatrix}$$
$$=\Phi((a+c)+(b+d)i)=\Phi((a+bi)+(c+di))$$
$$\Phi(a+bi)\Phi(c+di)=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}\begin{pmatrix} c & d \\ -d & c\end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd\end{pmatrix}$$
$$=\Phi((ac-bd)+(ad+bc)i)=\Phi((a+bi)(c+di))$$

이 성립하므로 Φ는 환 준동형사상이다.

$\begin{pmatrix} a & b \\ -b & a\end{pmatrix}=\begin{pmatrix} c & d \\ -d & c\end{pmatrix}\Rightarrow a=c$이고 $b=d \Rightarrow a+bi=c+di$

이므로 Φ는 단사이다. 여기서 $im\Phi=\Phi[C]$이므로 따라서 $C\simeq\Phi[C]$임을 알 수 있다.

문 38. R를 단위원을 갖는 환, 그리고 Hom(<R,+>)를 24장에서 설명한 <R,+>의 자기 준동형사상의 환이라 하자. x∈R일 때 a∈R 그리고 $\lambda_a: R\to R$를 $\lambda_a(x)=ax$로 정의하자.

(a) λ_a는 <R, +>의 자기 준동형사상임을 보여라.

풀 이

$\lambda_a(x+y)=a(x+y)=ax+ay=\lambda_a(x)+\lambda_a(y)\ (\forall x,y\in R)$

이 성립하므로 λ_a는 준동형사상이다. 따라서 자기 자신에서 자기 자신으로의 준동형사상이므로 자기 준동형사상임을 알 수 있다.

(b) $R'=\{\lambda_a | a\in R\}$는 Hom(<R,+>)의 부분환임을 보여라.

풀 이

임의의 $a,b\in R$에 대하여 $(\lambda_a\lambda_b)(x)=(\lambda_a)(\lambda_b(x))=(\lambda_a)(bx)=a(bx)=(ab)x=\lambda_{ab}(x)(\forall x\in R)$이 성립하므로 R'은 곱셈에 관하여 닫혀 있다. 또한
$(\lambda_a-\lambda_b)(x)=(\lambda_a)(x)-\lambda_b(x)=ax-bx=(a-b)x=\lambda_{a-b}(x)(\forall x\in R)$이 성립하므로 R'은 덧셈에 관하여 가환군이다. 따라서 R'은 $Hom(<R,+>)$의 부분환이다.

(c) (b)의 R'는 R와 동형임을 보임으로써 R에 대한 Cayley의 정리와 유사한 정리임을 증명하라.

풀 이

$\phi : R \to R', \phi(a) = \lambda_a$로 정의된 사상이라 하자.

(b)에 의하여 $\phi(a+b) = \lambda_{a+b} = \lambda_a + \lambda_b = \phi(a) + \phi(b)$
$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a)\phi(b) \ (\forall\, a, b \in R)$

이 성립하여 환 준동형사상임을 알 수 있다. 전사임은 (b)에 의하여 자명하므로 단사임을 보이자.

$\phi(a) = \phi(b) \Rightarrow \lambda_a = \lambda_b \Rightarrow ax = bx \ (\forall\, x \in R) \quad \Rightarrow 1 \in R$이므로 $1a = 1b \Rightarrow a = b$

따라서 ϕ는 전단사이고 그러므로 ϕ는 환 동형사상이다.

Fraleigh 대수 27장 소아이디얼과 극대아이디얼

※ 다음 주어진 환에서의 모든 소 아이디얼과 모든 극대 아이디얼을 구하라.

문 1. Z_6

풀 이

단위원을 가진 가환환이 유환환일때 극대 아이디얼과 소 아이디얼은 동일한 개념이므로 그 점에 유념하여 소 아이디얼과 극대 아이디얼을 찾는다.
M:극대 아이디얼 ⇔ R/M: 체 이므로
R/M이 되가 되기 위한 극대 아이디얼 M을 찾는다.
여기서 잉여환은 Z_2, Z_3와 동형이 될수 있으므로 다음과 같은 소 아이디얼과 극대 아이디얼을 찾을수 있다.
소 아이디얼: {0,2,4},{0,3}
극대 아이디얼: {0,2,4},{0,3}

문 2. Z_{12}

풀 이

극대 아이디얼에 의한 잉여환이 Z_2, Z_3와 동형이 될 수 있으므로 다음과 같은 소 아이디얼과 극대 아이디얼을 찾을수 있다.
소 아이디얼: {0,2,4,6,8,10},{0,3,6,9}
극대 아이디얼: {0,2,4,6,8,10},{0,3,6,9}

문 3. $Z_2 \times Z_2$

풀 이

극대 아이디얼에 의한 잉여환이 Z_2와 동형이 될 수 있으므로 다음과 같은 소 아이디얼과 극대 아이디얼을 찾을수 있다.
소 아이디얼: {(0,0),(0,1)},{(0,0),(1,0)}
극대 아이디얼: $\{0\}\times\{0\}, \{0\}\times Z_2, Z\times\{0\}$

문 4. $Z_2 \times Z_4$

풀 이

소 아이디얼:
극대 아이디얼:

※ 다음 주어진 잉여환R/M 의 형태가 체가 되게 하는 모든 $c \in R$을 구하여라.

문 5. $Z_3[x]/<x^2+c>$

풀 이

$Z_3[x]/<x^2+c>$: 체 $\Leftrightarrow$ x^2+c: 기약다항식 이므로

x^2+c이 기약다항식이 되게 하는 모든 $c \in Z_3[x]$을 구하면 된다.

그러면

$c=0$일때 x^2: $Z_3[x]$에서 가약

$c=1$일때 x^2+1: $Z_3[x]$에서 기약

$c=2$일때 $x^2+2=x^2-1=(x+1)(x-1)$: $Z_3[x]$에서 기약

따라서 구하고자 하는 c=2 뿐이다.

문 6. $Z_3[x]/<x^2+x+c>$

풀 이

$c=0$일때 $x^2+x=x(x+1)$: $Z_3[x]$에서 가약

$c=1$일때 $x^2+x+1=x^2-2x+1=(x-1)^2$: $Z_3[x]$에서 가약

$c=2$일때 x^2+x+2: $Z_3[x]$에서 기약

따라서 구하고자 하는 c=2 뿐이다.

문 7. $Z_3[x]/<x^3+cx^2+1>$

풀 이

$c=0$일때 $x^3+1=(x+1)(x^2-x+1)=(x-2)(x^2-x+1)$: $Z_3[x]$에서 가약

$c=1$일때 $x^3+x^2+1=(x-1)(x^2+2x+2)$: $Z_3[x]$에서 가약

$c=2$일때 x^3+2x^2+1: $Z_3[x]$에서 기약

따라서 구하고자 하는 c=2 뿐이다.

문 8 $Z_5[x]/<x^2+x+c>$

풀 이

$c=0$일때 $x^2+x=x(x+1)$: $Z_5[x]$에서 가약

$c=1$일때 x^2+x+1: $Z_5[x]$에서 기약

$c=2$일때 x^2+x+2: $Z_5[x]$에서 기약

$c=3$일때 $x^2+x+3=x^2+x-2=(x-2)(x+1)$: $Z_5[x]$에서 가약

$c=4$일때 $x^2+x+4=x^2-4x+4=(x-2)^2$: $Z_3[x]$에서 가약

따라서 구하고자 하는 c=1,2 뿐이다.

문 9. $Z_5[x]/ < x^2+cx+1 >$

풀 이

$c=0$일때 $x^2+1=x^2-4=(x+2)(x-2)$: $Z_5[x]$에서 가약

$c=1$일때 x^2+x+1: $Z_5[x]$에서 기약

$c=2$일때 $x^2+2x+1=(x+1)^2$: $Z_5[x]$에서 가약

$c=3$일때 $x^2+3x+1=x^2-2x+1=(x-1)^2$: $Z_5[x]$에서 가약

$c=4$일때 x^2+4x+1: $Z_5[x]$에서 기약

따라서 구하고자 하는 c=1,4 뿐이다.

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 10. 환R의 *극대 아이디얼*은 R의 다른 임의의 아이디얼을 안에 포함하지 않는 아이디얼이다.

풀 이

극대 아이디얼은 환R과 극대 아이디얼 사이에 임의의 다른 아이디얼을 포함하지 않는 아이디얼이다.

문 11. 가환환 R의 *소 아이디얼*은 임의의 소수p에 대하여 $pR=\{pr|r\in R\}$의 형태의 아이디얼이다.

풀 이

$pR\subsetneq R$인 조건이 추가 되어야 한다.

문 12. *소체*는 진부분 부분체를 갖지 않는 체이다.

풀 이

소체는 가장 작은 부분체이다. 즉 체의 모든 부분체들의 교집합이다.

문 13. 단위원을 가진 가환환의 *주이데알N*은 다음과 같은 성질을 갖는 아이디얼이다.

$a\in N$가 존재할 때 N은 a를 포함하는 가장 작은 아이디얼이다.

풀 이

옳은 정의이다.

문 14. 참과 거짓을 판단하시오.

(a) 단위원을 갖는 모든 가환환에서 모든 소 아이디얼은 극대 아이디얼이다.

풀 이

(False)

Z는 단위원을 갖는 가환환이다.

여기서 (0)은 소 아이디얼이지만 $(0)\subsetneq 2Z\subsetneq Z$이므로 극대 아이디얼은 아니다.

(b) 단위원을 갖는 모든 가환환에서 모든 극대 아이디얼은 소 아이디얼이다.

풀 이

(True)

단위원을 갖는 임의의 가환환을 R 이라고 하고 M을 극대 아이디얼 P를 소이데알이라고 하자.

R이 단위원을 갖는 가환환이므로 다음이 성립한다.

M이 극대 아이디얼 ⇔ R/M: 체

R/M: 체 이면 R/M: 정역

R/P: 정역 ⇔ P:소 아이디얼

따라서 극대 아이디얼이면 소 아이디얼임을 알수 있다.

(c) Q는 그 자신이 소부분체이다.

풀 이 (True)

Q는 체이고 표수는 0 이므로 Q와 동형인 부분체를 갖는다. 따라서 그 자신이 소부분체이다.

(d) C의 소부분체는 R이다.

풀 이 (False)

C의 표수는 0 이므로 소부분체는 Q이다.

(e) 모든 체는 소체와 동형이 되는 부분체를 포함한다.

풀 이 (True)

임의의 체F는 정역이다. 따라서 표수는 0또는 소수p 이다. F의 표수가 소수p이면 Z_p와 동형이 되는 부분체를 포함하고 F의 표수가 0이면 Q와 동형이 되는 부분체를 포함한다. 여기서 Z_p, Q는 임의의 체F에서 가장 작은 체이므로 소체이고 따라서 모든 체는 소체와 동형이 되는 부분체를 포함한다.

(f) 0인자를 갖는 환은 부분환으로서 소체 중의 하나를 포함할 수 있다.

풀 이 (True)

Z_6은 0인자를 갖는 환으로써 부분환으로 Z_2를 갖는다 이때 Z_2는 소체이므로 0인자를 갖는 환은 부분환으로서 소체 중의 하나를 포함할 수 있다.

(g) 표수 0을 갖는 모든 체는 Q와 동형인 부분체를 포함한다.

풀 이 (True)

정수환 Z에 대하여 사상 $\Phi : Z \to F, \Phi(k) = k \cdot 1$ (1은 F의 단위원)으로 정의할 때

모든 $k, l \in Z$에 대하여

$$\Phi(k+l) = (k+l) \cdot 1 = k \cdot 1 + l \cdot 1 = \Phi(k) + \Phi(l)$$
$$\Phi(kl) = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1) = \Phi(k)\Phi(l)$$

이므로 $\Phi : Z \to F$ 는 환준동형사상이다. 따라서 환 제1동형정리에 의하여 다음이 성립한다.

$$Z/\ker\Phi \approx im\Phi = \{k \cdot 1 | k \in Z\} \subset F$$

한편, $\ker\Phi = \{k \in Z | k \cdot 1 = 0\} = nZ, n \geq 0$인 정수 n 이 존재한다.

그런데 표수가 0이므로 핵$\ker\Phi = 0$이다.

따라서

$$Z/\ker\Phi \approx Z/(0) \approx Z$$
$$Z \approx im\Phi = \{k \cdot 1 | k \in Z\} \subseteq F$$

여기서 $D = \{k \cdot 1 | k \in Z\}$라고 하면 D는 F의 부분환으로서 Z의 동형이므로 D는 정역이다. 이제 Q(D)를

F에 포함되는 분수체라고 하면

$$Q(D)=\left\{\frac{a\bullet 1}{b\bullet 1}|a,b\in Z,b\neq 0\right\}$$

이고 Q(D)는 F의 부분체이다. 한편 유리수체 Q와 부분체 Q(D) 사이의 다음과 같은 동형사상임을 보일 수 있다.

$$\Theta : Q\rightarrow Q(D),\Theta(\frac{a}{b})=\frac{a\bullet 1}{b\bullet 1}(a,b\in Z,b\neq 0)$$

그러므로 F는 유리수체 Q와 동형인 부분체를 포함한다.

(h) F를 체라 하자. F[x]는 0인자를 갖지 않기 때문에 F[x]의 모든 아이디얼은 소 아이디얼이다.

풀 이 (False)

소 아이디얼I의 성질에 의하여 $I\neq F[x]$이므로 $\deg f(x)=0,f(x)\neq 0$인 경우 $<f(x)>=(1)=F[x]$이 성립하므로 소 아이디얼이 아니다.

(i) F를 체라 하자. F[x]의 모든 아이디얼은 주 아이디얼이다.

풀 이 (True)

I를 $F[x]$의 임의의 아이디얼이라 하자. 이때 $I=<f(x)>,f(x)\in F[x]$임을 보이자.

$I=(0)$이면 $I=(0),0\in F[x]$이고 $I=F[x]$이면 $I=(1),1\in F[x]$이므로 주 아이디얼이다.

$I\neq(0)$이고 $I\neq F[x]$인 경우 즉, $(0)\subsetneq I\subsetneq F[x]$라 가정하자.

I에 속하는 원소 중에서 상수다항식이 아닌 다항식 중에서 차수가 가장 작은 다항식을$f(x)$라 하자. 그러면 $<f(x)>\subset I$ 가 성립한다.또 임의의 $g(x)\in I$에 대하여 $g(x)\in<f(x)>$임을 보인다.

$g(x)\in I$이므로 나눗셈 정리에 의하여 다음이 성립한다.

$g(x)=q(x)f(x)+r(x),\ q(x)\in I,r(x)\in I,\ 0\leq\deg r(x)<\deg f(x)$

여기서 $r(x)=g(x)-q(x)f(x)\in<f(x)>$이므로

$f(x)$의 최소성에 의하여 $r(x)=0$이다. 그러므로 $I=<f(x)>$이다.

(j) F를 체라 하자. F[x]의 모든 아이디얼은 극대 아이디얼이다.

풀 이 (False)

$\deg f(x)=0,f(x)\in F[x]$ 인 경우

즉 $f(x)=a,a\in F$인 상수 다항식인 경우 $<f(x)>=<a>=F[x]$를 만족한다.

이때 $<f(x)>$는 극대 아이디얼이 아니다.

참고) $\deg f(x)\geq 1$ 인 경우 대해서는 극대 아이디얼이 된다.

문 15. $Z\times Z$ 의 극대 아이디얼을 찾아라.

풀 이

$(Z\times Z)/(Z\times pZ)\approx Z_p,p$는 소수 이고

여기서 Z_p는 체이므로 $Z\times Z$의 극대아이디얼은 $Z\times pZ$ 또는 $pZ\times Z$ 의 형태이다.

따라서 $Z\times 2Z$도 극대 아이디얼이 되는 한 예이다.

문 16. $Z\times Z$에서 극대가 아닌 소 아이디얼을 찾아라.

풀 이

$(Z\times Z)/(Z\times(0))\approx Z$이고 여기서 Z는 체가 아닌 정역이므로 $Z\times(0)$은 소 아이디얼이지만 극대 아이디얼이 아닌 예가 될수 있다.

문 17. $Z\times Z$**에서 소 아이디얼이 아닌 진부분 비자명 아이디얼을 찾아라.**

풀 이

$(Z\times Z)/(Z\times 4Z)\approx Z_4$이므로 $Z\times 4Z$는 소 아이디얼이 아닌 진부분 비자명 아이디얼이다.
$(1,4)=(1,2)(1,2)\in Z\times 4Z$이지만 $(1,2)\notin Z\times 4Z$ 이다.

문 18. $Q[x]/<x^2-5x+6>$**은 체인가? 그 이유는?**

풀 이

체가 아니다. $x^2-5x+6=(x-2)(x-3)$과 같이 가약이기 때문에 $<x^2-5x+6>$은 극대 아이디얼이 아니고 따라서 $Q[x]/<x^2-5x+6>$은 체가 아니다.

문 19. $Q[x]/<x^2-6x+6>$**은 체인가? 그 이유는?**

풀 이

체이다. $Q[x]$상에서 x^2-6x+6은 Eisenstein 판정법에 의하여 기약이므로 $<x^2-6x+6>$은 극대 아이디얼이고 따라서 잉여환 $Q[x]/<x^2-6x+6>$은 체이다.

문 20 - 23 -생략-

문 24. R가 단위원을 갖는 유한 가환환이라 하자. R의 모든 소 아이디얼은 극대 아이디얼임을 보여라.

풀 이

R이 단위원을 갖는 가환환이고 P를 R의 임의의 소 아이디얼 이라고 하자 그러면 필요충분하게 R/P는 정역이 된다. 이때 조건에 의하여 R이 유환환 이므로 R/P은 유환인 정역이다 따라서 R/P는 체이고 그러므로 필요충분하게 P는 극대이데알 임을 알 수 있다.

문 25. ***[따름정리][R이 단위원을 갖는 환이고 표수가*** $n\geq 1$***이라 하면 R는*** Z_n***과 동형인 부분환을 포함한다. 또, R의 표수 0을 가지면 R는 Z와 동형이 부분환을 포함한다]*** **에서 단위원을 갖는 모든 환은 Z 또는** Z_n**과 동형이 되는 부분환을 포함함을 알았다. 단위원을 갖은 환이** $n\neq m$**에 대하여** Z_n**과 동형인 부분환과** Z_m**과 동형인 부분환을 동시에 포함할수 있는가? 가능하다면 예를 들고, 불가능하다면 증명해 보아라.**

풀 이 가능하다.
$Z_2\times Z_3$ 같은 경우 $(Z_2\times Z_3)/(Z_2\times(0))\approx Z_3$,$(Z_2\times Z_3)/((0)\times Z_3)\approx Z_2$ 만족한다.

문 26. (문제25)를 계속하여 단위원을 갖는 환이 서로 다른 두 소수 p,q **에 대하여 체** Z_p**와 동형인 부분환과 체** Z_q **와 동형인 부분환을 동시에 포함할 수 있는가? 가능하다면 예를 들고, 불가능하다면 증명하라.**

풀 이

가능하다.
$Z_2\times Z_3$ 같은 경우, $(Z_2\times Z_3)/(Z_2\times(0))\approx Z_3$, $(Z_2\times Z_3)/((0)\times Z_3)\approx Z_2$ 을 만족한다.

문 27. (문제26)의 개념에 따라 $p \neq q$이고 p와 q가 소수일 때 Z_p, Z_q와 동형인 부분환을 포함하는 정역이 존재할 수 있는가? 이유를 들거나 예를 들어 보아라.

풀 이

존재할 수 없다.
존재한다고 가정하자. 이때 정역을 D라 하고 동형인 부분환을 H라 하자. 그러면 D의 표수는 H와 같다. 그리고 H의 표수는 Z_p와 동형이므로 p이다. 또한 H의 표수는 Z_q와 동형이므로 q이다. 그러면 p=q이고 이는 $p \neq q$임에 모순된다.

문 28. 단위원을 갖는 가환환 R의 모든 극대 아이디얼은 소 아이디얼임을 극대 아이디얼과 소 아이디얼의 정의를 이용하여 직접 보여라.
[힌트: M은 R의 극대 아이디얼이고 $ab \in M$이면 $a \notin M$이라 가정하라. a와 M에 의하여 생성되는 R의 아이디얼을 생각해 보아라.]

풀 이

M을 R의 극대 아이디얼이라고 가정하자. $a \notin M$일때 $ab \in M$이면 $b \in M$임을 보이면 된다. $a \notin M$이므로 a와 M에 의하여 생성되는 R의 이데알<M,a>는 다음을 만족한다.

$$M \subsetneq < M,a > \subseteq R$$

가정에 의하여 M이 극대 아이디얼이므로 $< M,a > = R$ 이다. 즉 $1 \in < M,a >$이고 따라서 $1 = Ms + at$가 되게 하는 $s,t \in R$ 가 존재한다. 조건에 의하여 $ab \in M$이고 M은 아이디얼이므로 $b = Mbs + abt \in M$이다. 그러므로 극대 아이디얼은 소아이디얼이다.

문 29. N이 환R의 극대 아이디얼이 될 필요충분조건은 R/M인 단순환일 경우이다. 즉, 이것은 진부분 비자명 아이디얼을 포함하지 않는다 (*[정리]M이 극대 정규 부분군이 될 필요충분조건은 G/M이 단순군이다* 와 비교해 보라)

풀 이

(a) N이 환R의 극대 아이디얼이면 R/M은 체이다. 따라서 R/M의 아이디얼I는 I≠(0)일떄 항상 가역원을 원소로 포함하므로 I=R/M 이다 따라서 R/M은 단순환이다.
(b) 군에서의 정규부분군과 환에서의 아이디얼은 유사한 역할을 한다. 그런 점에서 극대 아이디얼과 극대 정규 부분군도 환과 군에서의 역할이 유사함을 알수 있다.

문 30. F가 체이면 F[x]에 모든 진부분 비자명 소 아이디얼은 극대 아이디얼임을 증명하라.

풀 이

(1) F가 체이면 F[x]는 주아이디얼 정역이다. 따라서 임의의 진부분 비자명 소 아이디얼을 P라 할때 $P = < f(x) >, f(x) \in F[x]$가 존재함을 할수 있다. 여기서 $f(x) = 0$이면 P는 자명 아이디얼이고 $\deg f(x) = 0, f(x) \neq 0$이면 P는 가역원을 포함하므로 F[x]가 된다. 따라서 이는 가정에 모순이므로 P는 $\deg f(x) \geq 1$을 만족하는 주 아이디얼이다.
(2) $\deg f(x) \geq 1$인 $P = < f(x) >, f(x) \in F[x]$는 극대 아이디얼임을 보이자.
$< f(x) > \subsetneq I \subseteq F[x]$인 F[x]의 아이디얼I에 대하여 $I = F[x]$임을 보인다.
$F[x]$가 PID이므로 $\exists g(x) \in F[x]\ s.t.\ I = < g(x) >$
$f(x) \in < g(x) >$이므로 $\exists h(x) \in F[x]\ s.t.\ f(x) = g(x)h(x)$
$f(x) = g(x)h(x) \in < f(x) >, g(x) \notin < f(x) > \Rightarrow h(x) \in < f(x) >$
($\because < f(x) >$: 소아이디얼)
그러면 $\exists k(x) \in F[x]\ s.t.\ h(x) = f(x)k(x)$ 그러면 $f(x) = g(x)h(x) = f(x)g(x)k(x)$이고 0인자가 존재하지 않으므로 따라서 $1 = g(x)k(x) \in < g(x) >$이다.

그러면 임의의 $h(x)\in F[x]$에 대하여 $h(x)\cdot 1\in <g(x)>$이다. 따라서 $<g(x)>=F[x]$이다.
그러므로 $\deg f(x)\geq 1$일 때 $P=<f(x)>, f(x)\in F[x]$은 극대 아이디얼이다.

(2) (다른풀이)
$\deg f(x)\geq 1$인 $P=<f(x)>, f(x)\in F[x]$는 극대 아이디얼임을 보이자.
$<f(x)>\subsetneq I\subseteq F[x]$인 F[x]의 아이디얼 I에 대하여 $I=F[x]$임을 보인다.
$F[x]$가 PID이므로 $\exists g(x)\in F[x] s.t. I=<g(x)>$
$<f(x)>$가 소아이디얼이므로 기약다항식이고 $g(x)\notin <f(x)>$이므로
(즉, $f(x)\nmid g(x)$이므로) $\gcd(f(x),g(x))=1$ 이다.
($\because$ 만약 $\gcd(f(x),g(x))=d(x)\neq 1$이면 $f(x)$가 기약다항식이므로 $f(x)=d(x)$이다.
그러면 $f(x)|g(x)\Rightarrow g(x)\in <f(x)> \Rightarrow <g(x)>\subseteq <f(x)>\Rightarrow <f(x)>=<g(x)>$이다.
이는 모순이다. 따라서 $\gcd(f(x),g(x))=1$이다.)
그러면 $\exists s(x),t(x)\in F[x]\ s.t.\ 1=f(x)s(x)+g(x)t(x)\in <g(x)>$이다. 따라서 $1\in <g(x)>$이다.
그러면 임의의 $h(x)\in F[x]$에 대하여 $h(x)\cdot 1\in <g(x)>$이다. 따라서 $<g(x)>=F[x]$이다.
그러므로 $\deg f(x)\geq 1$일 때 $P=<f(x)>, f(x)\in F[x]$은 극대 아이디얼이다.

문 31. F가 체이고 $f(x),g(x)\in F[x]$라 하자. $f(x)$가 $g(x)$를 나누기위한 필요충분조건은 $g(x)\in <f(x)>$일 때임을 보여라.

풀 이

(⇨) F가 체이고 $f(x),g(x)\in F[x]$라 하자. $f(x)\mid g(x)$이므로 $g(x)=f(x)h(x)$를 만족하는 $h(x)\in F[x]$가 존재한다. 따라서 $g(x)=f(x)h(x)\in <f(x)>=\{f(x)k(x)|k(x)\in F[x]$이 성립한다.
(⇦) $g(x)\in <f(x)>$이므로 $g(x)=f(x)h(x)$를 만족하는 $h(x)\in F[x]$가 존재한다. 따라서 $f(x)\mid g(x)$이 성립한다.

문 32. F가 체이고 $f(x),g(x)\in F[x]$라 하자.
$N=\{r(x)f(x)+s(x)g(x)|r(x),s(x)\in F[x]\}$가 $F[x]$의 아이디얼임을 보여라. 만약, $f(x)$와 $g(x)$가 서로 다른 차수를 갖고 $N\neq F[x]$이면 $f(x)$와 $g(x)$는 둘 다 F위에서 기약일 수 없음을 보여라.

풀 이

(a) $<d(x)>=N,\ d(x)\in F[x]$임을 보이자
(⇨) $\gcd(f(x),g(x))=d(x), d(x)\in F[x]$라고 하자. 그러면 유클리드 호제법에 의하여
$f(x)s(x)+g(x)t(x)=d(x)$인 $s(x),t(x)\in F[x]$가 존재한다.
그러면 $d(x)=f(x)s(x)+g(x)t(x)\in N$이고 따라서 $<d(x)>\subseteq N$이 성립한다.
(⇦) 임의의 $k(x)\in N$이라 하자.
그러면 $s_1(x),t_1(x)\in F[x]$가 존재해서$d(x)=f(x)s_1(x)+g(x)t_1(x)$을 만족한다.
$\gcd(f(x),g(x))=d(x), d(x)\in F[x]$이므로 $d(x)|f(x), d(x)|g(x)$이다
그러면 $d(x)|(f(x)s(x)+g(x)t(x))=d(x)|k(x)$을 만족한다.
따라서 $k(x)\in <d(x)>$이다 그러므로 $<d(x)>\supseteq N$ 이 성립한다.
그러므로 N은 F[x]의 아이디얼이다.
(b) $\gcd(f(x),g(x))=1$이라면 유클리드 호제법에 의하여
$1=s(x)f(x)+t(x)g(x)\in N$ 인 $s(x),t(x)\in F[x]$가 존재한다.
이는 $N\neq F[x]$임에 모순이다 따라서 $\gcd(f(x),g(x))\neq 1$이다.
즉 $f(x),g(x)$는 둘 다 기약일수 없다.

문 33. -생 략 함 -

문 34. 만약 A와 B가 환R의 아이디얼이면 A와 B의 합 A+B는

$A+B=\{a+b|a\in A, b\in B\}$

로 정의된다.

(a) A+B 가 R의 아이디얼임을 보여라.

풀 이

$\forall x,y\in A+B\ \exists a_1,a_2\in A, b_1,b_2\in B\ s.t.\ x=a_1+b_1, y=a_2+b_2$

A,B가 R의 아이디얼이므로 각각 다음이 성립한다.

$\forall a_1,a_2\in A\Rightarrow a_1-a_1\in A$
$\forall r\in R, \forall a\in A\Rightarrow ra, ar\in A$
$\forall b_1,b_2\in B\Rightarrow b_1-b_1\in B$
$\forall r\in R, \forall b\in B\Rightarrow rb, br\in B$

그러면

$x-y=(a_1+b_1)-(a_2+b_2)=(a_1-a_2)+(b_1-b_2)\in A+B$
$rx=r(a_1+b_1)=ra_1+rb_1\in A+B$
$xr=(a_1+b_1)r=a_1r+b_1r\in A+B$

을 만족하고 따라서 A+B는 R의 아이디얼이다.

(b) $A\subseteq A+B$이고 $B\subseteq A+B$ 임을 보여라.

풀 이

$A=A+(0)\subseteq A+B,\ B=(0)+B\subseteq A+B$이므로 자명하다.

문 35. A와 B가 환R의 아이디얼이라 하면 A와 B의 곱 AB는

$$AB=\left\{\sum_{i=1}^{n}a_ib_i|\ a_i\in A, b_i\in B, n\in Z^+\right\}$$

로 정의된다.

(a) AB 가 R의 아이디얼임을 보여라.

풀 이

$$\forall x,y\in AB\ \exists a_i\in A, b_i\in B, n,m\in Z^+\ s.t.\ x=\sum_{i=1}^{n}a_ib_i, y=\sum_{i=1}^{m}a_ib_i$$

이때 $x-y=(\sum_{i=1}^{n}a_ib_i)-(\sum_{i=1}^{m}a_ib_i)\in AB$

$$rx=r(\sum_{i=1}^{n}a_ib_i)=\sum_{i=1}^{n}(ra_i)b_i\in AB(\because ra_i\in A)$$

$$xr=(\sum_{i=1}^{n}a_ib_i)r=\sum_{i=1}^{n}a_i(b_ir)\in AB(\because b_ir\in B)$$

이므로 AB는 R의 아이디얼이다.

(b) $AB\subseteq(A\cap B)$임을 보여라.

풀 이

$\forall x\in AB\ \exists a_i\in A, b_i\in B, n\in Z^+\ s.t.\ x=\sum_{i=1}^{n}a_ib_i$이고

$A\cap B=[a|a\in A, a\in B]$이므로 자명하게 $x\subseteq A\cap B=[a|a\in A, a\in B]$이다

따라서 $AB\subseteq A\cap B$가 성립한다.

문 36. A와 B를 가환환 R의 아이디얼이라 하자. A의 B에 의한 몫 A : B는

$A:B=\{r\in R|\text{ 모든 } b\in B\text{에 대하여 } rb\in A\}$

로 정의된다. A : B는 R의 아이디얼임을 증명하라.

풀 이

A:B 가 덧셈에 대하여 가환군임을 보이면 충분하다.

임의의 $r_1,r_2\in(A:B)$에 대하여 $b(r_1-r_2)=br_1-br_2\in A\,(\forall b\in B)$이 성립한다.

따라서 A:B는 R의 아이디얼이다.

문 37. F가 체이고 $a,b\in F$에 대하여 $\begin{pmatrix}a\,b\\0\,0\end{pmatrix}$형태의 모든 행렬들의 집합S는 $M_2(F)$의 우 아이디얼이지만 좌 아이디얼은 아님을 보여라. 즉 S는 $M_2(F)$의 원소를 오른쪽에서 곱하는데 대하여 닫혀 있지만, 왼쪽에 곱하는데 대해서는 닫혀 있지 않은 부분환임을 보이면 된다.

풀 이

$\forall x,y\in S\,\exists a,b,c,d\in F s.t.\, x=\begin{pmatrix}a\,b\\0\,0\end{pmatrix}, y=\begin{pmatrix}c\,d\\0\,0\end{pmatrix}$

이때 $x-y=\begin{pmatrix}a\,b\\0\,0\end{pmatrix}-\begin{pmatrix}c\,d\\0\,0\end{pmatrix}=\begin{pmatrix}a-c\,b-d\\0\quad 0\end{pmatrix}\in S(\because F\text{는 체})$

$\forall r\in M_2(F)\,\exists e,f,g,h\in F s.t.\, r=\begin{pmatrix}e\,f\\g\,h\end{pmatrix}$

$$xr=\begin{pmatrix}a\,b\\0\,0\end{pmatrix}\begin{pmatrix}e\,f\\g\,h\end{pmatrix}=\begin{pmatrix}ae+bg\,af+bh\\0\qquad 0\end{pmatrix}\in S$$
$$rx=\begin{pmatrix}e\,f\\g\,h\end{pmatrix}\begin{pmatrix}a\,b\\0\,0\end{pmatrix}=\begin{pmatrix}ea\,eb\\ga\,gb\end{pmatrix}\notin S$$

를 만족한다.

따라서 집합 S는 $M_2(F)$의 우 아이디얼이지만 좌 아이디얼은 아니다.

문 38. 행렬들의 환 $M_2(Z_2)$는 단순환임을 보여라. 즉 $M_2(Z_2)$는 진부분 비자명 아이디얼을 갖지 않는다.

풀 이

-생 략-

※문제1-8에서 주어진 원소가 기약원인가 아닌가를 결정하라.

문 1. Z에서 5

풀 이

기약원이다. Z에서 5를 나눌 수 있는 값이 +1,-1뿐이고 이는 모두 가역원이기 때문이다.

문 2. Z에서 -17

풀 이

기약원이다. Z에서 -17을 나눌 수 있는 값이 +1,-1뿐이고 이는 모두 가역원이기 때문이다.

문 3. Z에서 14

풀 이

기약원이 아니다. Z에서 14를 나눌수 있는 값이 +1,-1이외의 +2,-2,+7,-7과도 나눌 수 있기 때문이다. 즉 <14>≠<2> 또는 <14>≠<7>이다.

문 4. Z[x]에서 2x-3

풀 이

기약원이다. Z가 정역이므로 D(Z[x])=D(Z)={+1, -1}이고 0이 아닌 값으로 2x-3을 나눌 수 있는 값이 가역원+1, -1 뿐이므로 Z[x]에서 2x-3은 기약원이다.

문 5. Z[x]에서 2x-10

풀 이

기약원이 아니다. Z가 정역이므로 D(Z[x])=D(Z)={+1, -1}이고 0이 아닌 값으로 2x-10을 나눌 수 있는 값이 가역원 이외의 값 2로도 나눌 수 있으므로 기약원이 아니다

문 6. Q[x]에서 2x-3

풀 이

기약원이다. Q가 정역이므로 D(Q[x])=D(Q)=Q-{0}이고 0이 아닌 값으로 2x-3을 나눌 수 있는 값이 가역원 뿐이므로 Q[x]에서 2x-3은 기약원이다

문 7. Q[x]에서 2x-10

풀 이

기약원이다. Q가 정역이므로 D(Q[x])=D(Q)=Q-{0}이고 0이 아닌 값으로 2x-10을 나눌 수 있는 값이 가역원 뿐이므로 Q[x]에서 2x-10은 기약원이다

문 8. $Z_{11}[x]$에서 $2x-10$

풀 이

기약원이다. Z_{11}가 정역이므로 $D(Z_{11}[x])=D(Z_{11}[x])=Z_{11}-\{0\}$ 이고 0이 아닌 값으로 2x-10을 나눌 수 있는 값이 가역원 뿐이므로 $Z_{11}[x]$에서 2x-10은 기약원이다.

문 9. $2x-7$**을** $Z[x]$**의 원소로 간주하여 가능하다면 4개의 서로 다른 동반원소를 구하여라. 또한** $2x-7$**을** $Q[x]$**와** $Z_{11}[x]$**로 간주하여 4개의 동반원소를 구하여라.**

풀 이

(a) Z가 정역이므로 D(Z[x])=D(Z)={+1, -1}이다. 따라서 서로 다른 동반원소 2개 뿐 이고 이는 2x-7, -2x+7이다.

(b) Q가 정역이므로 D(Q[x])=D(Q)=Q-[0]이다.

따라서 서로 다른 동반원소 4개를 찾으면 $2x-7, \frac{2x-7}{2}, \frac{2x-7}{3}, \frac{2x-7}{4}$ 이다.

(c) Z_{11}가 정역이므로 $D(Z_{11}[x]) = D(Z_{11}[x]) = Z_{11} - \{0\}$이다. 따라서 서로 다른 동반원소 4개를 찾으면 $2x-7, 4x-3(=4x-14), 6x+1(=6x-21), 8x-6(=8x-28)$ 이다.

문 10. $4x^2-4x+8$**을 정역** $Z[x]$**의 원소로 간주하여 기약원의 곱으로 인수분해 하여라. 또한** $Q[x]$**와** $Z_{11}[x]$**의 원소로 간주하여 인수분해 하여라.**

풀 이

$4x^2-4x+8 = 4(x^2-x+2)$

(a) Z가 정역이므로 D(Z[x])=D(Z)={+1, -1}이다. 따라서 0과 가역원이 아닌 원소로써 기약원이 될 수 있는 것은 $2, 2, x^2-x+2$ 이다. 그러므로 준 식은 $4x^2-4x+8 = 2 \bullet 2 \bullet (x^2-x+2)$와 같이 기약원의 곱으로 인수분해 할 수 있다.

(b) Q가 정역이므로 D(Q[x])=D(Q)=Q-[0]이다. 따라서 0과 가역원이 아닌 원소로써 기약원이 될 수 있는 것은 자기 자신 뿐이다. 그러므로 준 식은 $4x^2-4x+8$로서 더 이상 인수분해 되지 않는다.

(c) Z_{11}가 정역이므로 $D(Z_{11}[x]) = D(Z_{11}[x]) = Z_{11} - \{0\}$이다. 따라서 0과 가역원이 아닌 원소로써 기약원이 될 수 있는 것은 (x+4), (4x+2)이다. 그러므로 준 식은 $4x^2-4x+8 = (x+4)(4x+2)$와 같이 기약원의 곱으로 인수분해 할 수 있다.

※문제11-14에서 주어진 다항식을 지정된 UFD에서 용량과 원시적 다항식의 곱으로 표현하라.

문 11. $Z[x]$**에서** $18x^2-12x+48$

풀 이

Z가 정역이므로 D(Z[x])=D(Z)={+1, -1}이다. 원시 다항식은 계수들 사이의 공약수가 가역원 이어야 하므로 다음과 같이 용량과 원시적 다항식의 곱으로 표현 할 수 있다.

$18x^2-12x+48 = (6)(3x^2-2x+8)$

문 12. $Q[x]$**에서** $18x^2-12x+48$

풀 이

Q가 정역이므로 D(Q[x])=D(Q)=Q-{0}이다. 원시 다항식은 계수들 사이의 공약수가 Q[x]의 가역원 이므로 그 자신인과 용량의 곱으로 다음과 같이 $(1)(18x^2-12x+48)$ 으로 표현 할 수 있다.

문 13. $Z[x]$**에서** $2x^2-3x+6$

풀 이

Z가 정역이므로 D(Z[x])=D(Z)={+1, -1}이다. 원시 다항식은 계수들 사이의 공약수가 Z[x]의 가역원 이므로 그 자신인과 용량의 곱으로 다음과 같이 $(1)(2x^2-3x+6)$ 으로 표현 할 수 있다.

문 14. $Q[x]$**에서** $2x^2-3x+6$

풀 이

Q가 정역이므로 D(Q[x])=D(Q)=Q-{0}이다. 원시 다항식은 계수들 사이의 공약수가 Q[x]의 가역원이므로 그 자신인과 용량의 곱으로 다음과 같이 $(1)(2x^2-3x+6)$ 으로 표현 할 수 있다.

※ 다음 밑줄 친 부분의 정의가 올바르면 수용하고 그렇지 않으면 옳게 고쳐라.

문 18. 정역 D의 원소 a와 b가 *동반원* 일 필요충분조건은 정역D에서 그들의 잉여 a/b가 가역원이다.

풀 이

맞는 정의이다!!
또한 a와 b가 동반원이면 필요충분하게 <a>=<b>도 성립한다.

문 19. 정역 D의 원소가 D에서 *기약*일 필요충분조건은 D의 두 개의 원소들의 곱으로 인수분해 되어 나타낼 수 없는 것이다.

풀 이

단순히 두 개의 원소들의 곱으로 인수분해 되어 나타 낼 수 없는 것이 아니라. 0과 가역원이 아닌 두 개의 원소들의 곱으로 인수분해 되어 나타낼 수 없는 것이다. 따라서 [0과 가역원이 아닌]이란 조건이 첨가 되어야 한다.

문 20. 정역 D의 원소가 D에서 *소원* 일 필요충분조건은 D에서 보다 작은 두 개의 원소들의 곱으로 인수분해 되어 나타낼 수 없는 것이다.

풀 이

단순히 D에서 보다 작은 두 개의 원소들의 곱으로 인수분해 되어 나타낼 수 없는 것이 아니라. D에서 0과 가역원이 아닌 보다 작은 두 개의 원소들의 곱으로 인수분해 되어 나타낼 수 없는 것이다. 따라서 [0과 가역원이 아닌]이란 조건이 첨가 되어야 한다.

문 21. 참과 거짓을 판단하시오.

(a) 모든 체는 UFD이다.

풀 이 (True)

임의의 체F는 PID 이고 PID는 UFD 이므로 체F는 UFD이다.

(b) 모든 체는 PID이다.

풀 이 (True)

임의의 체F는 아이디얼을 자기 자신F=<1>과 자명아이디얼<0>만을 갖는다. 따라서 체F는 PID이다.

(c) 모든 PID는 UPD이다.

풀 이 (True)

(i) 임의의 D를 PID이라 하고 $a_1 \neq 0, a \not\in U(D)$인 $a_1 \in D$을 유한개의 기약원의 곱으로 나타내어지지 않는 원소라고 가정하자.
이때, a_1은 기약원이 아니므로 a_1은 $a_1 = bc, (b \not\in U(D), c \not\in U(D))$의 꼴로 나타내어진다. 그런데 b와 c가 모두 유한개의 곱으로 나타내어지면 a_1도 유한개의 곱으로 나타내어지므로 a_1의 인수 b와 d 중에서 적어도 하나는 유한개의 곱으로 나타내어지지 않는다.

이제 a_1의 이러한 인수를 a_2라 하면 a_1과 a_2는 서로 다른 원소의 동반원이 아니므로 $< a_1 > \subset < a_2 >$ 이다.

이와 같은 과정을 되풀이 하면, D의 아이디얼로 이루어진 무한열

$< a_1 > \subset < a_2 > \subset \cdots < a_n > \subset \cdots$

을 얻게 된다. 이들 아이디얼의 합집합 $I = \bigcup_{n=1}^{\infty} < a_n >$은 D의 아이디얼이고 D는 PID이므로 $I = < b >$인 원소 $b \in D$가 존재한다.

그런데, b는 적당한 이데알 $< a_n >$에 속하고

이때 $< a_{m+1} > \subset < b > \subset < a_m >$이므로 $< a_{m+1} > = < a_m >$으로 되어 모순이다.

따라서, 0도 아니고 가역원도 아닌 D의 원소는 모두 유한개의 곱으로 나타내어진다.

(ii) 0도 아니고 가역원도 아닌 원소 $a \in D$에 대하여

$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ ($p_1, p_2, \cdots, p_s, q_1, q_2, \cdots, q_t$는 기약원)

이라고 가정하자. 이때 $p_1 | q_1 q_2 \cdots q_t$ 이므로 $p_1 | q_j$ 인 기약원 q_j $(1 \le j \le t)$가 존재하고

이때 이때 $< p_1 >$과 $< q_j >$는 D의 극대 아이디얼이므로 $< p_1 > = < q_j >$이다.

$q_j = u_1 p_1$인 가역원 u_1아 존재하므로 p_1과 q_j는 서로 동반원이다.

이제 $q_1 q_2 \cdots q_t$ 의 순서를 재 조정하여 j=1이라 놓으면

$q_1 = u_1 p_1$이므로

$p_1 p_2 \cdots p_s = u_1 p_1 q_2 \cdots q_t$ 즉, $p_2 \cdots p_s = u_1 q_2 \cdots q_t$

이와 같은 과정을 되풀이 하면 s=t이고 또 각 p_i가 적당한 q_j와 동반원임을 알수 있다.

따라서 PID이면 UFD이다.

(d) 모든 UFD는 PID이다.

풀 이 (False)

Z[x]는 UFD이지만 PID는 아니다.

(e) Z[x]는 UFD이다.

풀 이 (True)

Z가 UFD 이므로 Z[x]는 UFD이다.

(f) UFD에 속하는 임의의 두 기약원은 동반원소이다.

풀 이 (False)

Z에서 3과 5는 기약원이다 하지만 3≠5(+1)또는 3≠5(−1)이다

(g) D가 PID이면 D[x]도 PID이다.

풀 이 (False)

Z는 PID이지만 Z[x]는 PID가 아니다. 즉 $< x^2, 2 > \neq < f(x) >, f(x) \in Z[x]$인 다항식f(x)가 존재하지 않는다. 실제로 $< x^2, 2 > = < f(x) >$이라고 가정하면

$x^2, 2 \in < f(x) > \Rightarrow f(x) | x^2, f(x) | 2 \Rightarrow f(x) | \gcd(x^2, 2) = 1 \Rightarrow 1 \in < f(x) >$

결국 <f(x)>=Z[x]가 된다. 하지만 이때 $x+1 \in Z[x]$ 이지만 $x+1 \in < x^2, 2 >$이 성립하지 않는다. 따라서 Z[x]는 PID가 아니다.

(h) D가 UFD이면 D[x]도 UFD이다.

풀 이 (True)

- (정리45.29) 참조 -

(i) UFD에서 기약원 p에 대하여 p | a 이면 p는 a의 인수분해에서 나타난다.

풀 이 (False)

$Z[2i]$는 UFD이고 $2|2i$이지만 $2i$는 기약원이다. 따라서 $2i$의 인수분해에 2는 나타나지 않는다.

(j) UFD는 0인자를 갖지 않는다.

풀 이 (True)

UFD는 정역이다. 따라서 0인자를 갖지 않는다.

문 22. D를 UFD라 하자. D에서 기약이면 D[x]에서 기약임을 설명하시오. 또한 F를 D의 분수체라 할 때 F[x]에서 기약임을 설명하시오.

풀 이

D가 UFD이면 D[x]는 UFD이므로 D[x]에서 원시적이다. 따라서 D에서 기약이면 D[x]에서 기약이다. 또한 (보조정리45.27)에 의하여 F[x]에서 기약이다.

문 23. (보조정리 45.27)에서 D가 분수체 F를 갖는 UFD이면, D[x]의 상수가 아닌 기약원 f(x)는 F[x]의 기약원임을 알 수 있다. F[x]의 기약원 $g(x)\in D[x]$는 D[x]의 기약원이 될 필요가 없음을 예로 들어 설명하라.

풀 이

$D=Z, F=Q$라 하자. 그러면 $2x+4$는 $Q[x]$에서 기약이지만 $Z[x]$에서는 기약이 아니다.

문 24. 이 절에서의 모든 연구는 정역으로 제한되어 있다. 단위원을 갖는 가환환에 대하여 이절의 모든 정의를 똑같이 택하였을 때 $Z\times Z$에서의 기약원의 인수분해를 생각해보라. 무슨 일이 일어나겠는가? 특히 (1,0)을 생각해 보라.

풀 이

$Z\times Z$에서는 0이 아니고 가역원도 아닌 원소가 기약원으로 인수분해 된다고 볼 수 없다. 왜냐면 $(1,0)$은 가역원이 아니지만 $(\pm 1,0)$의 인수를 갖는다. 여기서 $(\pm 1,0)=(\pm 1,0)(1,2)$이므로 기약이 아니다.

문 25. p가 정역 D의 소원이면 p는 기약원임을 보여라.

풀 이

p가 정역 D의 소원이므로 일단은 0과 가역원이 아닌 원소이다. 이제 p=ab라고 가정하자. 이때 b | p, a | p이고 또 p | ab이므로 소원의 정의에 의하여 p | a 또는 p | b 이다. 따라서 p | a, a | p 또는 p | b, b | p 이므로 a 또는 b 는 p의 동반원이다. 그러므로 p는 기약원이다.

문 26. p가 UFD의 기약원이면 p는 소원임을 보여라.

풀 이

p가 UFD의 기약원이면 0과 가역원이 아닌 원소이다. 또한 p=ab라고 가정할 때 a또는 b는 p의 동반원이다. 따라서 $p|ab \Rightarrow p|a$ 또는 $p|b$ 이 성립한다.
그러므로 p는 소원이다.

문 27. 정역 D에 대하여 a가 b의 동반원소(즉, D의 가역원 u에 대하여 a=bu)이면, 관계 a~b라 하면, ~이 D 위에서 동치관계임을 증명하라.

풀 이

(반사) a~a 이면 a=1a 이고 또한 $a1^{-1}$=a이므로 a~a 가 성립한다.
(대칭) a~b 이면 D의 가역원 u에 대하여 a=bu이 성립하도 $au^{-1}=auu^{-1}=a$이므로 b~a가 성립한다.
(추이) a~b, b~c이면 D의 가역원 u,v에 대하여 a=bu, b=cv 가 성립한다. 따라서 a=c(vu)가 성립하고 이때 vu는 가역원의 원소이므로 따라서 a~c가 성립한다.
따라서 ~이 D 위에서 동치관계임을 알수 있다.

문 28. D를 정역이라 하고 U가 D의 가역원의 집합일 때 (18장 연습문제, 37번)에서 <U,·>는 군이 됨을 보았다. 0을 제외한 D의 가역원이 아닌 원소의 집합 D^*-U 는 곱셈에 대하여 닫혀있음을 보여라. 또, 이 집합 D^*-U는 D의 곱셈에 대하여 군이 되는가?

풀 이

(1) (닫혀있음)
임의의 $a,b\in D^*-U$에 대하여 $ab\in U$라고 가정하여 모순됨을 보이자.
$ab\in U$이면 $c\in U$가 존재해서 $a(bc)=(ab)c=1$이 성립한다. 하지만 이는 a가 가역원이 되게 하는 원소 bc가 존재함을 의미하기 때문에 이는 a가 가역원이 아님에 모순이다. 따라서 $ab\in D^*-U$이다.
(2) 군이 아니다.
$1\in D$이지 $1\notin D^*-U$이다. 따라서 곱셈에 대한 항등원 1이 존재하지 않으므로 집합 D^*-U은 군이 되지는 않는다.

문 29. D를 UFD라 하자. D[x]에 속하는 원시적 다항식의 상수가 아닌 약수도 다시 원시적 다항식임을 보여라.

풀 이

$f(x)$를 $D[x]$에서 원시적 다항식이라 하자. D가 UFD이므로 $D[x]$ 또한 UFD이므로 다음이 성립한다.

$$f(x)=u_1\cdots u_n s_1(x)s_2(x)\cdots s_n(x)u_1\cdots u_n$$
$$(s_1(x),s_2(x),\cdots,s_n(x)\text{는 기약다항식},u_1\cdots u_n\text{는 가역원})$$

$f(x)$가 원시적 다항식이므로 $c(f(x))=c(u_1\cdots u_n s_1(x)s_2(x)\cdots s_n(x))=u_1\cdots u_n=1$이 성립한다. 그러므로 $f(x)=s_1(x)s_2(x)\cdots s_n(x)$이다. 여기서 각각의 $s_i(x)$ $(1\le i\le n)$은 $c(s_i(x))=1$이므로 원시적 다항식이고 이들의 곱셈으로 이루어진 $f(x)$의 상수가 아닌 약수를 $g(x)$라 하면

$$c(g(x))=c(s_{i_1}(x)\cdots s_{i_j}(x))=c(s_{i_1}(x))\cdots c(s_{i_j}(x))=1\cdot\cdots\cdot 1=1$$

이므로 $g(x)$ 또한 원시적 다항식임을 알 수 있다. (여기서 $c(f(x))=(f(x)$의 최고차항의 계수)이다.)

문 30. PID에서 모든 아이디얼은 극대 아이디얼에 포함됨을 보여라.

풀 이

임의의 정역 D를 PID라 하자. $a_1 \in D$를 택할 때

$N_1 \subsetneq D$인 N_1에 대하여 $N_1 = < a_1 >$은 $a_1 \in D$인 D에서의 가장 작은 아이디얼이다.

여기서 $< a_1 >$이 극대 아이디얼이 아니라고 하면

$< a_1 > \subset N_2$을 만족하는 $N_2 \subsetneq D$인 D의 아이디얼 N_2가 존재하고

D는 PID이므로 $N_2 = < a_2 >$인 $a_2 \in D$가 존재함을 알 수 있다.

그러한 과정을 반복하면 $< a_1 > \subset < a_2 > \subset \cdots \subsetneq D$ 와 같은 D의 아이디얼의 증가열을 만들 수 있다.

이때 $S = \{a_i | i \in Z^+\}$라 정의하면 여기서 PID의 상쇄조건(ACC)에 의하여 $< a_1 > \subseteq < a_2 > \subseteq \cdots \subsetneq D$는 유한길이를 갖는다. 즉 $< b > = \bigcup_{i=1}^{\infty} < a_i >$인 $b \in D$가 존재한다.

여기서 $b \in S$이므로 $r \in Z^+$가 존재해서 $< b > = < a_r > = < a_{r+1} > = \cdots$이 성립한다.

그러므로 $< b > \subseteq I \subsetneq D$인 아이디얼 I가 존재하면 $I = < b >$임을 알 수 있다.

따라서 $< b >$는 D에서 극대 아이디얼이고 D의 모든 아이디얼은 극대아이디얼에 포함된다. .

문 31. $x^3 - y^3$을 $Q[x,y]$에서 기약원으로 인수분해하고 각 인자들이 기약임을 보여라.

풀 이

$Q[x,y]$에서 $x^3 - y^3 = (x-y)(x^2 + xy + y^2)$으로 인수분해 할 수 있다. 여기서 $(x-y)$는 기약임이 자명하므로 $(x^2 + xy + y^2)$이 $Q[x,y]$에서 기약임을 보이면 충분하다.

보조정리 23.17에 의하여 $\phi_1(x) = x^2 + x + 1$은 Q에서 기약이다. 만약 $x^2 + xy + y^2$이 $Q[x,y]$에서 가약이면 $\phi_1(x) = x^2 + x + 1$ 또한 $Q[x]$에서 가약이다. 이는 모순이다.

그러므로 $x^2 + xy + y^2$는 $Q[x,y]$에서 기약이다.

문 32. R를 임의의 환이라 하자. R의 아이디얼의 모든 증가열 $N_1 \subseteq N_2 \subseteq \cdots$가 유한 길이를 갖는다면 R에서 아이디얼에 대한 승쇄조건(ACC)을 만족한다고 한다. 만약 R의 아이디얼의 공45집합이 아닌 모든 집합S가 S의 다른 아이디얼에 완전히 포함되지 않는 아이디얼을 가진다면 R의 아이디얼에 대한 극대조건(MC)를 만족한다고 한다. R의 각 아이디얼 N에 대해 B_N을 포함하는 R의 모든 아이디얼의 공통집합이 N이 되는 유한집합 $B_N = [b_1, \cdots b_n] \subseteq N$이 존재한다면 R의 아이디얼애 대한 유한기저조건(FBC)을 만족한다고 하며, B_N을 N에 대한 유한기저라 한다. 모든 환R에 대한 조건 ACC, MC, FBC는 동치임을 보여라.

풀 이

(1) R의 아이디얼의 모든 증가열 $N_1 \subseteq N_2 \subseteq \cdots$가 유한 길이를 갖는다면 R에서 아이디얼에 대한 승쇄조건(ACC)

(2) R의 아이디얼의 공집합이 아닌 모든 집합S가 S의 다른 아이디얼에 완전히 포함되지 않는 아이디얼을 가진다면 R의 아이디얼에 대한 극대조건(MC)

(3) R의 각 아이디얼 N에 대해 B_N을 포함하는 R의 모든 아이디얼의 공통집합이 N이 되는 유한집합 $B_N = [b_1, \cdots b_n] \subseteq N$이 존재한다면 R의 아이디얼에 대한 유한기저조건(FBC)

[(1)ACC ⇨ (2)MC] R의 아디디얼에 대한 승쇄조건(ACC)을 만족하자. 여기서 R의 아디디얼에 대한 극대조건(MC)을 만족하지 않는다고 가정해서 모순됨을 보이자.

즉, R의 아이디얼의 공집합이 아닌 모든 집합S가 S의 다른 아이디얼에 포함된다고 하자. 그러면 S의

임의의 아이디얼을 포함하는 S의 아이디얼이 존재한다. 이제 S의 한 아이디얼을 N_1이라 하자.
그러면 $N_1 \subseteq N_2$인 $N_2 \in S$가 존재한다. 또한 마찬가지로 이유로 $N_2 \subseteq N_3$인 $N_3 \in S$가 존재한다. 이런 과정을 반복하면 $N_1 \subseteq N_2 \subseteq \cdots$인 아이디얼의 무한 증가열을 얻을 수 있다. 이는 ACC에 모순이다. 따라서 R의 아디디얼에 대한 극대조건(MC)을 만족한다.

[(2)MC ⇨ (3)FBC] R의 아디디얼에 대한 극대조건(MC)을 만족한다고 하자. 여기서 R의 아디디얼에 대한 유한기저조건(FBC)을 만족하지 않는다고 가정해서 모순됨을 보이자.
즉, R의 각 아이디얼 N에 대해 B_N을 포함하는 R의 모든 아이디얼의 공통집합이 N이 되는 유한집합 $B_N = [b_1, \cdots b_n] \subseteq N$이 존재하지 않는다고 하자.
$b_1 \in N$이라 하자. 그러면 $N_1 = < b_1 >$은 $b_1 \in N$을 포함하는 N에 포함하는 가장 작은 아이디얼이다.
$N_1 \neq N$또는 $\{b_1\}$는 N에 대한 기저이다. $b_2 \notin N_1$인 $b_2 \in N$을 선택할 수 있다.
이제 N_2를 b_1, b_2를 포함하는 N에 포함하는 가장 작은 아이디얼이자. 그러면 $N_2 \subseteq N$이지만 $\{b_1, b_2\}$는 N에 대한 기저라고 할 수 없으므로 $N_2 \neq N$이다. 그러면 $b_3 \notin N_2$인 $b_3 \in N$을 선택할 수 있다. 그리고 N_3를 b_1, b_2, b_3를 포함하는 N에 포함하는 가장 작은 아이디얼이자. 그런 과정을 반복하면 N이 유한기저를 갖지 않는다는 사실로부터 우리는 R의 아이디얼의 무한 증가열$N_1 \subseteq N_2 \subseteq \cdots$을 구성할 수 있다.
하지만 그러면 $S = \{N_i | i \in Z^+\}$는 아이디얼의 집합이고 $N_i \subseteq N_{i+1}$에 대해 각각은 서로 다른 아이디얼에 포함된다. 이는 R의 아이디얼에 대한 극대조건(MC)에 모순이다. 따라서 R의 아디디얼에 대한 유한기저조건(FBC)을 만족한다.

[(3)FBC ⇨ (1)ACC] R의 아이디얼의 증가열$N_1 \subseteq N_2 \subseteq \cdots$이라 하자. 그리고 $N = \bigcup_{i=1}^{\infty} N_i$이라 하자. 그러면 N은 아이디얼의 합집합이므로 아이디얼임은 자명하다.
이제 $B_N = [b_1, \cdots b_n] \subseteq N$을 N에 대한 유한기저라 하자. 그리고 $b_j \in N_{i_j}$라 하자. r을 첨자 i_j의 극대값이라 하면 $B_N \subseteq N_r$이 성립한다. 여기서 $N_r \subseteq N$이고 N은 B_N을 포함하는 모든 아이디얼의 교집합이다.
그러면 $N_r = N$이다. 그러므로 $N_r = N_{r+1} = N_{r+2} = \cdots$ 이 성립한다. 따라서 R에서 아이디얼에 대한 승쇄조건(ACC)를 만족한다.

문 33. R를 임의의 환이라 하자. R에서 아이디얼의 모든 감소열 $N_1 \supseteq N_2 \supseteq \cdots$가 유한길이를 갖는다면 R의 아이디얼에 대한 감쇄조건(DCC)을 만족한다고 한다. R의 아이디얼의 임의의 집합S에 대하여 집합 S에 속하는 다른 아이디얼을 완전히 포함하지 않는 S의 아이디얼이 존재한다면 R의 아이디얼에 대한 극소조건(mc)을 만족한다고 한다. 모든 환에 대한 조건 DCC와 mc는 동치임을 보여라.

풀 이

(1) R에서 아이디얼의 모든 감소열 $N_1 \supseteq N_2 \supseteq \cdots$가 유한길이를 갖는다면 R의 아이디얼에 대한 감쇄조건(DCC)
(2) R의 아이디얼의 임의의 집합S에 대하여 집합 S에 속하는 다른 아이디얼을 완전히 포함하지 않는 S의 아이디얼이 존재한다면 R의 아이디얼에 대한 극소조건(mc)

[(1)DCC ⇨ (2)mc]R의 아디디얼에 대한 감쇄조건(DCC)을 만족한다고 하자. 여기서 R의 아디디얼에 대한 국소조건(mc)을 만족하지 않는다고 가정해서 모순됨을 보이자.
즉. R의 아이디얼의 임의의 집합S에 대하여 집합 S에 속하는 다른 아이디얼에 포함된다고 하자. 그러면 S의 임의의 아이디얼에 속하는 S의 아이디얼이 존재한다.
이제 S의 한 아이디얼을 N_1이라 하자. 그러면 $N_1 \supseteq N_2$인 $N_2 \in S$가 존재한다.
또한 마찬가지로 이유로 $N_2 \supseteq N_3$인 $N_3 \in S$가 존재한다.
이런 과정을 반복하면 $N_1 \supseteq N_2 \supseteq \cdots$인 아이디얼의 무한 감소열을 얻을 수 있다.

이는 R의 아이디얼에 대한 감쇄조건(DCC)에 모순이다. 그러므로 R의 아디디얼에 대한 극소조건(mc)을 만족한다.

[(2)mc ⇨ (1)DCC] $N_1 \supset N_2 \supset \cdots$을 만족하는 R의 아디디얼의 열을 $N_1, N_2, \cdots$ 라 하자.
그리고 $S = \{N_i | i \in Z^+\}$라 하자. 극소조건(mc)임에 의하여 S의 어떤 원소 N_r은 집합 S에 속하는 다른 아이디얼을 완전히 포함하지 않는다. 그러면 $N_r = N_{r+1} = N_{r+2} = \cdots$ 이므로 따라서 R의 아이디얼에 대한 감쇄조건(DCC)을 만족한다.

문 34. ACC는 성립하지만 DCC는 성립하지 않는 환의 예를 들어라(문제 32와 33을 보라).

풀 이

Z는 PID이므로 ACC를 성립한다. 하지만 $Z, 2Z, 4Z, \cdots, 2^{i-1}Z$는 아이디얼의 열이고
$Z \supseteq 2Z \supseteq 4Z \supseteq \cdots \supseteq 2^{i-1}Z \supseteq \cdots$ 와 같은 무한 감소열임을 알 수 있다.
따라서 DCC는 Z에서 성립하지 않는다.

※ 문제1-5에서 주어진 정역에 대해 다음 함수 ν가 유클리드 부치가 되는가를 설명하라.

문 1. Z에서 0이 아닌 $n \in Z$에 대하여 $\nu(n) = n^2$으로 정의된 함수 ν

풀 이

(1) 임의의 $a,b \in Z, a \neq 0$에 대하여 $\nu(b) = b^2 \leq a^2b^2 = (ab)^2 = \nu(ab)$이 성립함을 알 수 있다.

(2) 임의의 $a,b \in Z, a \neq 0$에 대하여 $b = aq + r, \nu(r) = r^2 < a^2 = \nu(a)$

인 원소 q,r∈Z이 존재한다.

따라서 (1),(2)에 의하여 ν는 유클리드 부치가 된다.

문 2. Z[x]에서 $f(x) \neq 0$인 $f(x) \in Z[x]$에 대하여 $\nu(f(x)) = (f(x)$의 차수$)$로 정의된 함수 ν

풀 이

(1) 임의의 $f(x), g(x) \in Z[x], f(x) \neq 0$에 대하여

$\nu(g(x)) = \deg g(x) \leq \deg f(x) + \deg g(x) = \deg f(x)g(x) = \nu(f(x)g(x))$

이 성립함을 알 수 있다. 하지만

(2) $x+1, 2 \in Z[x]$일 때

$x+1 = 0 \cdot 2 + (x+1)$인 $0, x+1 \in Z[x]$이지만

$\nu(x+1) = \deg(x+1) = 1 > 0 = \deg(2) = \nu(2)$이다.

따라서 (2) 조건이 성립하지 않으므로 ν는 유클리드 부치가 아니다.

문 3. $Z[x]$에서 0이 아닌 $f(x) \in Z[x]$에 대하여

$\nu(f(x)) = (f(x)$의 0이 아닌 최고차 항의 계수의 절대치$)$로 정의된 함수 ν

풀 이

(1) 임의의 $\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{m} b_i x^i \in Z[x], \sum_{i=0}^{n} a_i x^i \neq 0$에 대하여

$\nu(\sum_{i=0}^{m} b_i x^i) = |b_m| \leq |a_n b_m| = \nu((\sum_{i=0}^{m} b_i x^i)(\sum_{i=0}^{n} a_i x^i))$이 성립함을 알 수 있다.

하지만

(2) $x^3 + x + 2, x^2 + 1 \in Z[x]$일 때

$x^3 + x + 2 = x(x^2 + 1) + 2$인 $x, 2 \in Z[x]$존재하지만

$\nu(2) = 2 > 1 = \nu(x^2)$이다.

따라서 조건(2)를 만족하지 않으므로 ν는 유클리드 부치가 아니다.

문 4. Q에서 0이 아닌 $a \in Q$에 대하여 $\nu(a) = a^2$으로 정의된 함수 ν

풀 이

(1) 임의의 $a,b \in Q, a \neq 0, a \leq 1$에 대하여 $\nu(b) = b^2 \geq a^2b^2 = (ab)^2 = \nu(ab)$이다.

따라서 조건(1)를 만족하지 않으므로 ν는 유클리드 부치가 아니다.

문 5. Q에서 0이 아닌 $a \in Q$에 대하여 $\nu(a) = 50$으로 정의된 함수 ν

풀 이

(1) 임의의 $a,b \in Q, a \neq 0$에 대하여 $\nu(b) = 50 = \nu(ab)$이 성립함을 알 수 있다.
(2) 임의의 $a,b \in Q, a \neq 0$에 대하여 Q가 체이므로 $b = aq, \nu(0) = 0 < 50 = \nu(a)$
인 원소 q,r∈Q이 존재한다.
따라서 (1),(2)에 의하여 ν는 유클리드 부치가 된다.

문 6. (예제 46.11)을 참고로 하여 $\lambda, \mu \in Z$일 때 gcd 23을 $\lambda(22,471) + \mu(3,266)$의 형태로 표현하라. [힌트: (예제 46.11)의 계산 끝에서 둘째 줄에 의해 23=(138)3-391이며, 바로 그위 줄에서 138=3,266-(391)8이다. 따라서, 이식을 대입하면 23=[3,266-(391)8]3-391을 얻는다. 이런 식으로 거꾸로 계산하여, λ와 μ의 값을 구한다.

풀 이

23=(138)3-391 이고 138=3,266-(391)8이므로
23=(3,266-(391)8)3-391=3(3,266)-29(391)이고 여기서 391=3,266-(2,875)을 대입하면
23=3(3,266)-29(3,266-(2,875))=-26(3,266)+29(2,875)이다.
끝으로 2875=22471-(3266)6을 대입하면
23=-26(3,266)+29(22,471-(3,266)6)=200(3,266)+29(22,471)임을 알 수 있다.
따라서 $\lambda = 29, \mu = 200$임을 알 수 있다.

문 7. Z에서 49,349와 15,555의 gcd를 구하라.

풀 이

49,349=3(15,555)+2,684
15,555=5(2,684)+2135
2,684=1(2,135)+549
2,135=3(549)+488
549=1(488)+61
488=8(61)+0
따라서 구하고자 하는 49,349와 15,555의 gcd는 61 이다.

문 8. (문제6)의 개념과 (문제7)을 참고하여 Z에서 49,349와 15,555의 양의 gcd를 $\lambda, \mu \in Z$에 대하여 $\lambda(49,349) + \mu(15,555)$의 형태로 표현하라.

풀 이

61=549-1(488)에 2,135-3(549)=488를 대입하면
61=549-1(2,135-3(549))=-(2,135)+4(549)이고
이에 2,684-1(2,135)=549를 대입하면
61=-(2,135)+4(2,684-1(2,135))=-5(2,135)+4(2,684)이고
이에 15,555-5(2,684)=2135을 대입하면
61=-5(15,555-5(2,684))+4(2,684)=-5(15,555)+29(2,684)이고
이에 49,349-3(15,555)=2,684를 대입하면
61=-5(15,555)+29(49,349-3(15,555))=-92(15,555)+29(49,349)임을 알 수 있다.
따라서 $\lambda = 29, \mu = -92$임을 알 수 있다.

문 9. $Q[x]$에서

$x^{10}-3x^9+3x^8-11x^7+11x^6-11x^5+19x^4-13x^3+8x^2-9x+3$과 $x^6-3x^5-3x^4-9x^3+5x^2-5x+2$의 gcd를 구하라.

풀 이

$$x^{10}-3x^9+3x^8-11x^7+11x^6-11x^5+19x^4-13x^3+8x^2-9x+3$$
$$=(x^4+2x)(x^6-3x^5-3x^4-9x^3+5x^2-5x+2)+(-x^4-3x^3-2x^2-5x+3)$$
$$x^6-3x^5-3x^4-9x^3+5x^2-5x+2$$
$$=(-x^2+6x-19)(-x^4-3x^3-2x^2-5x+3)-59(x^3+2x-1)$$
$$-x^4-3x^3-2x^2-5x+3=(x+3)(x^3+2x-1)+0$$

따라서 $\gcd=x^3+2x-1$이다.

문 10. 유클리드 정역의 원소 $a_1,\cdots,a_n$의 n개의 원소의 최대공약수를 유클리드 호제법 사용법을 통하여 설명하시오.

풀 이

$a_1,\cdots,a_n$의 최대공약수를 d라 할 때 $a_1s_1+\cdots+a_ns_n=d$를 만족하는 $s_1,\cdots,s_n$가 존재한다.

문 11. (문제10)을 통하여 발견한 방법을 통하여 2178, 396, 792 그리고 726 의 최대공약수를 찾아라.

풀 이

gcd(2178, 396, 793, 726)=66

문 12. Z[x]에 대해 생각해 보자.

(a) Z[x]는 UFD인가. 그 이유는?

풀 이

Z는 UFD이므로 Z[x]는 UFD이다.

(b) $\{a+xf(x)|a\in 2Z, f(x)\in Z[x]\}$**는 Z[x]의 아이디얼인가?**

풀 이

$I\equiv\{a+xf(x)|a\in 2Z, f(x)\in Z[x]\}$라 정의하고 I가 Z[x]의 아이디얼임을 보이자.

임의의 $s,t\in I$에 대하여 $a,b\in Z, f(x),g(x)\in Z[x]$가 존재해서 다음을 만족한다.

$$s=2a+f(x), t=2b+g(x)$$

이때 $s-t=[2a+xf(x)]-[2b+xg(x)]=2(a-b)+x(f(x)-g(x))\in I$

$(\because a-b\in Z, f(x)-g(x)\in Z[x])$

또한, 임의의 $r(x)=\sum_{i=0}^{n} r_ix^i\in Z[x](r_i\in Z)$와 임의의$s=2a+f(x)\in I$ $(a\in Z, f(x)\in Z[x])$에 대하여

$$r(x)s=sr(x)=[2a+xf(x)]\sum_{i=0}^{n} r_ix^i=2ar(x)+xf(x)\sum_{i=0}^{n} r_ix^i$$
$$=2ar_0+2ax[r_nx^{n-1}+\cdots+r_1]+xf(x)\sum_{i=0}^{n} r_ix^i$$
$$=2(2r_0)+x[r_nf(x)x^n+(2ar_n+r_{n-1}f(x))x^{n-1}+\cdots+(2ar_1+r_0f(x))]\in I$$

$(\because r_0a\in Z, r_nf(x)x^n+(2ar_n+r_{n-1}f(x))x^{n-1}+\cdots+(2ar_1+r_0f(x))\in Z[x])$

이 성립한다. 따라서 I가 Z[x]의 아이디얼임을 알 수 있다.

(c) Z[x]는 PID 인가? ((b)를 참고하라.)

풀 이

아니다. $< x^2, 2 > = < f(x) >$ 인 f(x)∈Z[x]가 존재하지 않는다. 실제로 $< x^2, 2 > \supseteq < f(x) >$이기 위해서는 f(x)는 1이어야 한다. f(x)가 1이면 결국 <f(x)>=Z[x]가 된다. 하지만 이때 $< x^2, 2 > \subseteq < f(x) >$이 성립하지 않는다. 이유인 즉 x+2는 Z[x]의 원소이지만 $< x^2, 2 >$의 원소는 아니기 때문이다.

(d) Z[x]는 유클리드 정역인가? 그 이유는?

풀 이

Z[x]는 PID가 아니다. 따라서 ED가 아니다.

문 13. 참과 거짓을 말하여라.

(a) 모든 유클리드 정역은 PID이다.

풀 이 (True)

임의의 정역D를 ED라 하고 ν를 유클리드 부치라 하자.
또한 I를 D 아이디얼이라 하자.
I={0}이면 I=<0>인 주아이디얼이므로 I⫌{0}이라 하자.
이때 $E \equiv \{\nu(x) | x \in I - \{0\}\}$라 하면 자연수의 정렬성의 원리에 의하여 최소원소 $a(\neq 0)$가 존재한다.
이때 $< a > \subseteq I$이고 유클리드 부치의 정의에 의하여
임의의 $b \in I$에 대하여 $b = aq + r, \nu(r) < \nu(a)$ 또는 r=0 이 성립하는 $q, r \in D$가 존재한다.
여기서 $b, aq \in I$이므로 $r = b - aq \in I$이고 $\nu(a)$의 최소성에 의하여 r=0이다.
따라서 $b = aq \in < a >$이다. 그러므로 $I = < a >$이다. 따라서 ED이면 PID이다.

(b) 모든 PID는 유클리드 정역(ED)이다.

풀 이 (False)

(반례)

$A_{-19} = \left\{ \frac{a + b\sqrt{-19}}{2} | a, b \in Z, a \equiv b (\mathrm{mod} 2) \right\}$는 $Z[\sqrt{-19}] \subseteq A_{-19} \subseteq Q(\sqrt{-19})$이고

따라서 A_{-19}는 정역이다.

한편 A_{-19}는 PID이지만 ED는 아니다.

(Montzkin[42], Wilson[58] 참조)

(c) 모든 유클리드 정역은 UFD이다.

풀 이 (True)

임의의 ED는 PID이고 PID이면 UFD이다. 따라서 ED이면 UFD이다.

(d) 모든 UFD는 유클리드 정역이다.

풀 이 (False)

UFD는 PID가 아니다. PID가 아니면 ED가 아니다. 그러므로 UFD는 ED가 아니다.

(e) Q에서 2와 3의 gcd는 $\frac{1}{2}$이다.

풀 이 (True)

Q에서

(1) $\frac{1}{2}|2, \frac{1}{2}|3$

(2) $d|2, d|3 \Rightarrow d|\frac{1}{2}$

따라서 2와 3의 최대 공약수는 $\frac{1}{2}$이다.

** Q가 체이므로 최대공약수는 무의미하다? 는 생각이 듬!! 왜냐면 유일하지 않으니까..*

(f) 유클리드 호제법은 두 정수의 gcd를 구하기 위한 실질적 방법이다.

풀 이 (True)

유클리드 호제법에 의하여 쉽게 두 정수의 최대공약수를 찾을 수 있으므로 실질적인 방법이라고 볼 수 있다. (정리46.9)참조!!

(g) ν가 유클리드 정역 D의 유클리드 부치이면 0이 아닌 모든 $a \in D$에 대하여 $\nu(1) \leqq \nu(a)$이다.

풀 이 (True)

ν가 유클리드 부치이므로 정의에 의하여 다음이 성립한다. $\nu(1) \leqq \nu(1 \cdot a) = \nu(a)$

(h) ν가 유클리드 정역 D의 유클리드 부치이면 0이 아닌 모든 $a \in D, a \neq 1$에 대하여 $\nu(1) < \nu(a)$이다.

풀 이 (False)

ν가 유클리드 부치이므로 정의에 의하여 다음이 성립한다.

$\nu(1) \leqq \nu(1 \cdot a) = \nu(a)$

a가 가역원인 경우 $\nu(a) \leqq \nu(a \cdot a') = \nu(1)$을 만족하는 a' 이 존재한다. 따라서 $\nu(a) = \nu(1)$이 성립한다.

(i) ν가 유클리드 정역 D의 유클리드 부치이면 0이 아니고 가역원도 아닌 모든 $a \in D$에 대하여 $\nu(1) < \nu(a)$이다.

풀 이 (True)

임의의 0이 아니고 가역원도 아닌 모든 $a \in D$에 대하여 $\nu(1) = \nu(a)$이라 가정해서 모순됨을 보이자.

D가 ED이므로 유클리드 호제법에 의하여 $1 = qa + r, r = 0$또는$\nu(r) < \nu(a)$ 이 성립하는 $q, r \in D$가 존재한다. 여기서 $\nu(r) < \nu(a) = \nu(1)$이 성립하면 이는 $\nu(1) \leqq \nu(a)$임에 모순된다. 따라서 $r = 0$이고 $aq = 1$가 된다. 이는 a가 가역원이 아님에 모순된다. 그러므로 $\nu(1) < \nu(a)$이다.

(j) 임의의 체 F에 대하여 F[x]는 유클리드 정역이다.

풀 이 (True)

$\nu : F[x] \to Z, \nu(f(x)) = 2^{\deg(f(x))}$(단, $2^{-\infty} = 0$)이라 하면 다음이 성립하여 ν는 유클리드 부치이다.

(1) 임의의 $f(x), g(x) \in F[x], f(x) \neq 0$ 에 대하여 $\nu(g(x)) = 2^{\deg(g(x))} \leq 2^{\deg(f(x)g(x))} = \nu(f(x)g(x))$이 성립한다.

(2) 임의의 $f(x), g(x) \in F[x], f(x) \neq 0$ 에 대하여

$g(x) = q(x)f(x) + r(x), \nu(r(x)) = 2^{\deg r(x)} < 2^{\deg f(x)} = \nu(f(x))$인 $q(x), r(x) \in F[x]$가 존재한다.

그러므로 $F[x]$는 ED이다.

문 14. 유클리드 정역 D의 연산구조는 특정한 유클리드 부치 ν의 선택에 어떤 방법으로 영향으로 미치는가? 그 이유는?

풀 이

유클리드 정역 D의 연산구조는 특정한 유클리드 부치 ν의 선택에 영향을 미치지 않는다. 정역 D의 연산구조는 덧셈과 곱셈에 관한 이항연산에 의해서 완전히 결정된다. 유클리드 부치 ν가 존재한다면 유클리드 부치 ν를 통해 연산의 구조를 이해하는데 도움을 줄 수는 있지만 유클리드 부치 ν의 선택에 연산구조가 어떤 방법으로 영향을 미친다고 볼 수 없다. 즉, 유클리드 부치 ν의 선택은 유클리드 부치가 되기 위한 두 가지 조건에만 부합하면 어떤 값을 같던지 연산구조와 상관없이 선택 할 수 있다.

문 15. D를 유클리드 정역, 그리고 ν를 D의 유클리드 부치라고 하고 a와 b가 D에서 동반원소이면 $\nu(a)=\nu(b)$임을 보여라.

풀 이

ν을 유클리드 부치라 하고 a와 b가 동반원소라 하자. 그러면

$\nu(a) \le \nu(au) = \nu(b)$
$\nu(b) \le \nu(bu') = \nu(a) (\because u, u' \text{은 가역원})$

이 성립한다. 따라서 $\nu(a)=\nu(b)$이다.

문 16. D를 유클리드 정역, 그리고 ν를 D의 유클리드 부치라 하자. 0이 아닌 $a,b \in D$에 대해 $\nu(a) < \nu(ab)$일 필요충분조건은 b가 D의 가역원이 아님을 보여라.
[힌트: (문제15)을 이용하여 $\nu(a) < \nu(ab)$일 필요충분조건은 b가 D의 가역원이 아님을 보여라. 유클리드 호제법을 이용하여 $\nu(a)=\nu(ab)$에서 $< a > = < ab >$임을 보인다. 따라서, b가 가역원이 아니면, $\nu(a) < \nu(ab)$임으로 결론짓는다.]

풀 이

(⇨) 대우 증명한다!!
b가 가역원이라 가정하자 여기서 b가 가역원이면 a와 ab는 동반원이다. 그러면 (문제15)번에 의하여 $\nu(a)=\nu(b)$이다.
(⇦) b가 가역원이 아니라고 하자. 또한 유클리드 부치의 정의에 의하여 $\nu(a) < \nu(ab)$을 부정해서 $\nu(a)=\nu(ab)$이라 가정해서 $< a > = < ab >$임을 보여 가정에 모순됨을 보인다.
$a|ab$가 성립하므로 $< ab > \subseteq < a >$가 성립한다.
유클리드 호제법에 의하여 $a=(ab)q+r, r=0 \text{ or } \nu(r) < \nu(ab)$인 $q,r \in D$가 존재한다.
여기서 $r \neq 0$이면 $\nu(r) < \nu(ab) = \nu(a)$이므로 $a=a(bq)+r, \nu(r) < \nu(a)$이 성립한다.
b가 가역원이 아니므로 $r=a-a(bq)=a[1-bq] \neq 0$이고 따라서 $\nu(r)=\nu(a-a(bq))=\nu(a[1-bq]) \ge \nu(a)$이 성립한다. 이는 모순이다.
그러므로 $r=0$이다. 그러면 $a=(ab)q$이고 $ab|a$이 성립해서 $< ab > \supseteq < a >$임을 알 수 있다. 따라서 $< ab > = < a >$이 성립한다. 그러면 ab,a는 동반원이다. 이는 b가 가역원이 아님에 모순이다. 따라서 $\nu(a) < \nu(ab)$이다.

문 17. 다음 명제가 참이면 증명하고, 거짓이면 반례를 들어라. ν가 유클리드 정역 D의 유클리드 부치이면 $\{a\in D|\nu(a)>\nu(1)\}\cup\{0\}$은 D의 아이디얼이다.

풀 이

거짓이다.

(반례) $D=Z,\nu(x)=\begin{cases}0 & ,x=0\\ |x| & ,x\neq 0\end{cases}$이라 하자.

$\lambda(2)=|2|=2>1=\lambda(1)$
$\lambda(-3)=|-3|=3>1=\lambda(1)$
이지만 $\lambda(2-3)=|2-3|=1=1=\lambda(1)$이 성립한다. 따라서 주어진 집합은 덧셈에 관한 연산에 닫혀 있지 않기 때문에 Z의 아이디얼이 아니다.

문 18. 모든 체는 유클리드 정역임을 증명하라.

풀 이

임의의 $x\in F$에 대하여 유클리드 부치를 $\nu(x)=\begin{cases}0 & ,x=0\\ 1 & ,x\neq 0\end{cases}$라 정의하면

(1) 임의의 $a,b\in F,a\neq 0$에 대하여 $\nu(b)=1=\nu(ab)$가 성립한다.

(2) 임의의 $a,b\in F,a\neq 0$에 대하여 $b=aq+0,\nu(0)=0<1=\nu(a)$인 $q,0\in F$가 존재한다.

따라서 유클리드 부치가 존재하므로 임의의 체는 ED이다.

문 19. ν가 유클리드 정역 D의 유클리드 부치라 하자.

(a) $s\in Z$이고 $s+\nu(1)>0$이면 0이 아닌 모든 $a\in D$에 대하여 $\eta(a)=\nu(a)+s$로 정의된 $\eta:D^*\to Z$는 D의 유클리드 부치임을 보여라. 여기서 D^*는 D의 0이 아닌 원소들의 집합이다.

풀 이

임의의 $a\in D,a\neq 0$에 대하여 $\eta(a)=\nu(a)+s\geq\nu(1)+s>0$이므로 $\eta(a)>0$가 성립한다.

또한 ν가 유클리드 부치이므로 다음이 성립한다.

(1) 임의의 $a,b\in D,a\neq 0$에 대하여 $\eta(b)=\nu(b)+s\leq\nu(ab)+s=\eta(ab)$이 성립한다.

(2) 임의의 $a,b\in D,a\neq 0$에 대하여

$b=aq+r,\eta(r)=s+\nu(r)<s+\nu(a)=\eta(a)$인 $q,r\in D$가 존재한다.

(b) $r\in Z^+$에 대해 0이 아닌 $a\in D$에서 $\lambda(a)=r\cdot\nu(a)$로 정의된 $\lambda:D^*\to Z$는 D의 유클리드 부치임을 보여라.

풀 이

$r\in Z^+$이므로 $\lambda(a)=r\cdot\nu(a)>0$이 성립한다.

또한 ν가 유클리드 부치이므로 다음이 성립한다.

(1) 임의의 $a,b\in D,a\neq 0$에 대하여 $\lambda(b)=r\cdot\nu(b)\leq r\cdot\nu(ab)=\lambda(ab)$이 성립한다.

(2) 임의의 $a,b\in D,a\neq 0$에 대하여

$b=aq+r,\lambda(r)=r\cdot\nu(r)<r\cdot\nu(a)=\lambda(a)$인 $q,r\in D$가 존재한다.

(c) 0이 아니며 가역원도 아닌 모든 $a\in D$에 대하여 $\mu(1)=1$이면 $\mu(a)>100$인 D의 유클리드 부치가 존재함을 보여라.

풀 이

$\lambda(a)=100\cdot\nu(a)$이라 하자. 그러면 (b)에 의하여 λ는 유클리드 부치이다.
그리고 $\mu(a)=\lambda(a)+s$라 하자. 그러면 (a)에 의하여 μ 또한 유클리드 부치이다.
여기서 $s=1-\lambda(1)$이라 하자.
그러면 $\mu(1)=1$이 성립함을 알 수 있어 주어진 조건을 만족한다.
이제 0이 아니며 가역원도 아닌 임의의 $a\in D$에 대하여

$\nu(a)\geq\nu(1)+1$
$\Rightarrow\lambda(a)=100\nu(a)\geq 100[\nu(1)+1]$
$\Rightarrow\mu(a)=\lambda(a)+1-\lambda(1)\geq 100[\nu(1)+1]+1-100\nu(1)=101$

따라서 $\mu(a)\geq 101>100$인 D의 유클리드 부치가 존재함을 알 수 있다.

문 20. D를 UFD라 하자. D의 원소 c에 대하여, 만약 a | c, b | c이며, c가 a와 b를 둘 다 나누는 모든 D의 원소 c를 두 원소 a와 b의 최소공배수(lcm)라 한다. 유클리드 정역 D의 0이 아닌 두 원소 a와 b는 D에서 lcm을 가짐을 보여라.
[힌트: a와 b의 모든 공배수는 D의 아이디얼을 이룸을 보여라.]

풀 이

$<c>=<a>\cap<b>$인 $c\in D$가 존재함을 보인다. $<a>$는 a를 포함하고 a의 배수들을 원소로 갖는 아이디얼이고 $<b>$는 b를 포함하고 b의 배수들을 원소로 갖는 아이디얼이다. 또한 아이디얼의 교집합은 아이디얼임이므로 $<a>\cap<b>$는 아이디얼이다. 여기서 $a|ab, b|ab$ 이므로 $ab\in<a>\cap<b>\neq 0$임은 자명하게 알 수 있다. 또한 주어진 조건에서 D는 ED이므로 PID이다.
따라서 $<a>\cap<b>=<c>$인 $0<c\leq ab$, $c\in D$가 존재한다. 여기서 c는 주 아이디얼의 정의에 의하여 a의 배수들과 b의 배수들의 교집합의 가장 작은 원소이다. 따라서 위의 정의 [만약 a | c, b | c이며, c가 a와 b를 둘 다 나누는 모든 D의 원소 c를 두 원소 a와 b의 최소공배수(lcm)라 한다.]가 성립하여 c가 최소공배수가 됨을 알 수 있다.

문 21. (정리46.9)의 마지막 명제를 사용하여 두 개의 0이 아닌 $r,s\in Z$가 군$<Z,+>$를 생성할 필요충분조건은 r와 s가 (정역 Z에 속하는 정수로 간주하여) 서로소, 즉 gcd가 1을 가짐을 보여라.

풀 이

$<r,s>\equiv\{rn+sm|n,m\in Z\}$
$<<r,s,>,+>=<Z,+>\Leftrightarrow\gcd(r,s)=1(r,s\in Z)$
(⇦) 임의의 $r,s\in Z$에 대하여 $\gcd(r,s)=1$이라 하자.
$<<r,s,>,+>\subseteq<Z,+>$ 임은 자명하므로 $<<r,s,>,+>\supseteq<Z,+>$ 임을 보인다.
임의의 $a\in Z$에 대하여 (정리 46.9)의 마지막 유클리드 호제법에 의해 $rx+sy=1$를 만족하는 $x,y\in Z$가 존재하고 그러면 $a=a\cdot 1=a\cdot(rx+sy)=r(ax)+s(ay)\in<r,s>$이 성립한다.
따라서 $<<r,s,>,+>=<Z,+>$ 임을 알 수 있다.
(⇨) $<<r,s,>,+>=<Z,+>$ 이므로 $1\in Z$에 대하여 $n,m\in Z$가 존재해서 $rn+sm=1$을 만족한다.
이제 1이 r,s의 최대 공약수 임을 보이자.
(1) $1|r, 1|s$임은 자명하다.
(2) $d|r, d|s\Rightarrow d|(rn+sm)=1$
따라서 $\gcd(r,s)=1$이다.

문 22. (정리46.9)의 마지막 명제를 사용하여 0이 아닌 $a,b,n\in Z$에 대해 합동방정식 $ax\equiv b(\mathrm{mod}n)$는 a와 n이 서로소일 때 Z에서 해를 가짐을 증명하라.

풀 이

$\gcd(a,n)=1$이라 하자. 그러면 $ax_1+ny_1=1$을 만족하는 $x_1,y_1\in Z$가 존재한다. 양변에 b를 곱하면 $a(bx_1)+n(by_1)=b$이고 $a(bx_1)+n(by_1)\equiv a(bx_1)\equiv b(\mathrm{mod}n)$이다. 이로부터 $x=bx_1\in Z$가 $ax\equiv b(\mathrm{mod}n)$의 하나의 해가 될 수 있음을 알 수 있다. 그러므로 $ax\equiv b(\mathrm{mod}n)$는 Z에서 해를 가진다.

문 23. (문제22)를 일반화하여 0이 아닌 $a,b,n\in Z$에 대해 합동방정식 $ax\equiv b(\mathrm{mod}n)$가 Z에서 해를 가질 필요충분조건은 Z에서 a와 n의 양의 gcd가 b를 나눔을 증명하라.
이 결과를 환 Z_n에서 해석해 보아라.

풀 이

$\gcd(a,n)=1$이면 (문제22)번에 의하여 자명하므로 $\gcd(a,n)=d>1$이 경우에 한하여 성립하는지 보이자.
(⇦) $\gcd(a,n)=d>1$이라 하자. 그러면 $ax_1+ny_1=d$을 만족하는 $x_1,y_1\in Z$가 존재한다. 양변에 b를 곱하고 d로 나누면 $a(\frac{bx_1}{d})+n(\frac{by_1}{d})=b$이고 d는 a, n이 최대 공약수 이므로 $\frac{bx_1}{d},\frac{by_1}{d}\in Z$이 성립한다.
이로부터 $x=x_1\frac{b}{d}\in Z$가 $ax\equiv b(\mathrm{mod}n)$의 하나의 해가 될 수 있음을 알 수 있다.
그러므로 $ax\equiv b(\mathrm{mod}n)$는 Z에서 해를 가진다.
(⇨) $\gcd(a,n)=d>1$이라 하자. $ax\equiv b(\mathrm{mod}n)$가 해를 갖는다면 $ax_2-b=ny_2$인 $x_2,y_2\in Z$가 존재한다.
그러면 $b=ax_2-ny_2$가 성립해서 $d|a,d|b$이므로 $d|b$가 성립한다.

환 Z_n에서 말한다면...
[0이 아닌 $a,b,n\in Z$에 대해 일차방정식 $ax=b$가 Z_n에서 해를 가질 필요충분조건은 Z_n에서 a와 n의 양의 gcd가 b를 나눌 수 있어야 한다.]
로 볼 수 있다.

문 24. (문제6)와 (문제23)의 개념에 따라 0이 아닌 $a,b,n\in Z$에 대해 합동방정식 $ax\equiv b(\mathrm{mod}n)$가 해를 갖는다면 Z에서 해를 구하는 실질적 방법을 개괄적으로 설명하고, 이 방법을 이용하여 합동방정식 $22x\equiv 18(\mathrm{mod}42)$의 해를 구하라.

풀 이

(1) 유클리드 호제법에 의하여 a, n의 최대 공약수 d를 찾는다.

(2) $d=x_0a+y_0n$을 만족하는 $x_0,y_0\in Z$를 찾고 $d=x_0a+y_0n$의 형태로 표현한다.

(3) $x=x_0\frac{b}{d}$는 $ax\equiv b(\mathrm{mod}n)$의 해가 된다.

$22x\equiv 18(\mathrm{mod}42)$의 경우에 위의 방법을 적용하면

$a=22,b=18,n=42$라 하자. 이제

(1) 22,42의 최대 공약수를 찾는다.

42=1(22)+20

22=1(20)+2

20=10(2)+0

따라서 최대 공약수는 2이다.

(2) 2=22-1(20)=22-(42-22)=2(22)-42

가 성립한다. 따라서 $x_0=2,y_0=-1$이다.

(3) 그러면 $x=2\frac{18}{2}=18$임을 알 수 있다.

그러므로 구하고자 하는 해는 $x\equiv 18(\mathrm{mod}42)$이다.

※ 문제 1~4에서 가우스 정수 $Z[i]$에 속하는 기약원의 곱으로 인수분해 하라.
[힌트: α $Z[i]$의 기약인 인수는 노름을 1보다 크게 가지고 $N(\alpha)$를 나누기 때문에 주어진 α의 가능한 기약인수로 간주되는 가우스 정수 $a+bi$는 유한개만이 존재한다. C에서 α를 그들 각각으로 나누고 그 몫이 다시 $Z[i]$에 속하는 가를 알아보라.

문 1. 5

풀 이

$N(5)=25$이므로 $N(\alpha)=1,5,25$이어야만 한다.
(1) $N(\alpha)=1$이면 α는 $Z[i]$의 가역원이다.

(2) $N(\alpha)=25$이면 $N(\frac{5}{\alpha})$이 $Z[i]$의 가역원이다.

(3) $\alpha=a+bi$일 때 $N(\alpha)=5$이면 $a^2+b^2=5$이므로 $a=\pm 1, b=\pm 2$ or $a=\pm 2, b=\pm 1$이다.
$(1+2i)(1-2i)=5$이고 여기서 $1+2i, 1-2i$은 $N(1+2i)=5, N(1-2i)=5$이므로 노름이 5인 소수이므로 기약원이다.

문 2. 7

풀 이

$N(7)=49$이므로 $N(\alpha)=1,7,49$이어야만 한다.
(1) $N(\alpha)=1$이면 α는 $Z[i]$의 가역원이다.

(2) $N(\alpha)=49$이면 $N(\frac{7}{\alpha})$이 $Z[i]$의 가역원이다.

(3) $\alpha=a+bi$일 때 $N(\alpha)=7$이면 $a^2+b^2=7$이다.
하지만 $a^2+b^2=7$을 만족하는 정수해는 존재하지 않는다. 따라서 7은 $Z[i]$에서 기약원이다.

문 3. $4+3i$

풀 이

$N(4+3i)=25$이므로 $N(\alpha)=1,5,25$이어야만 한다.
(1) $N(\alpha)=1$이면 α는 $Z[i]$의 가역원이다.

(2) $N(\alpha)=25$이면 $N(\frac{5}{\alpha})$이 $Z[i]$의 가역원이다.

(3) $\alpha=a+bi$일 때 $N(\alpha)=5$이면 $a^2+b^2=5$이므로 $a=\pm 1, b=\pm 2$ or $a=\pm 2, b=\pm 1$이다.
여러 가지 경우를 통하여 $(4+3i)=(1+2i)(2-i)$임을 알 수 있다.
여기서 $(1+2i),(2-i)$의 노름이 각각 5인 소수이므로 기약원이다.

문 4. $6-7i$

풀 이

- 생략 -

문 5. 6은 $Z[\sqrt{-5}]$에서 유일하게 (동반원에 관계없이) 기약원들로 인수분해되지 않음을 보여라. 두 개의 서로 다른 인수분해를 나타내 보여라.

풀 이

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

(1) $a^2+5b^2=2$ 와 $a^2+5b^2=3$ 은 정수해를 갖지 않으므로 2와 3은 둘 다 $Z[\sqrt{-5}]$에서 기약원이다.

(2) $-1+\sqrt{-5}$ 를 기약원이 아니라면

α가 가역원이 아니고 β가 가역원이 아닐 때 $-1+\sqrt{-5}=\alpha\beta$이 성립한다.

$N(\alpha\beta)=N(\alpha)N(\beta)=6$이고 $N(\alpha)=2\text{ or }3$일 때는 해를 갖지 않으므로 $N(\alpha)=1\text{ or }6$이다. 그러면 $N(\alpha)$ 또는 $N(\beta)$은 가역원이다. 이는 모순이다.

따라서 $-1+\sqrt{-5}$ 은 기약원이다.

(3) $Z[\sqrt{-5}]$에서 가역원은 ± 1뿐이다.

하지만 2도 3도 $\pm(-1+\sqrt{-5})$가 아니므로 $Z[\sqrt{-5}]$은 UFD가 아니다.

(4) 따라서 $6=2\cdot 3=(-1+\sqrt{-5})(-1-\sqrt{-5})$은 서로 다른 인수분해이다.

문 6. $Z[i]$에 속하는 $\alpha=7+2i$와 $\beta=3-4i$를 생각해 보자.

$\alpha=\beta\sigma+\rho$이며 $N(\rho)<N(\beta)$

를 만족하는 $Z[i]$에 속하는 σ와 ρ를 구하라.

[힌트: 문제 14의 힌트에서 주어진 구성방법을 이용하라.]

풀 이

$\frac{7+2i}{3-4i}=\frac{(7+2i)(3+4i)}{25}=\frac{13+34i}{25}=\frac{13}{25}+\frac{34}{25}i\in Q[i]$이라고 하면

$\sigma=1+i\in Z[i]$

$\rho=\alpha-\beta\sigma=(7+2i)-(3-4i)(1+i)=3i$

$\alpha=\beta\sigma+\rho\Leftrightarrow(7+2i)=(3-4i)(1+i)+(3i)$ 이고 $N(\rho)=9<25=N(\beta)$이다.

따라서 $\sigma=1+i,\rho=3i$ 이다.

문 7. $Z[i]$의 유클리드 호제법을 사용하여 $Z[i]$에서 $8+6i$와 $5-15i$의 $\gcd$를 구하여라.

풀 이

(1) $\frac{5-15i}{8+6i}=\frac{(5-15i)(8-6i)}{100}=-\frac{1}{2}-\frac{3}{2}i\in Q[i]$이라고 하면

$\nu=-1-2i\in Z[i]$

$\epsilon=\beta-\alpha\nu=(5-15i)+(8+6i)(1+2i)=1+7i\in Z[i]$

$\beta=\alpha\nu+\epsilon\Leftrightarrow(5-15i)=(8+6i)(-1-2i)+(1+7i)$

(2) $\frac{8+6i}{1+7i}=\frac{(8+6i)(1-7i)}{50}=1-i\in Q[i]$이라고 하면

$\nu=1-i\in Z[i]$

$\epsilon=\beta-\alpha\nu=(8+6i)-(1+7i)(1-i)=0\in Z[i]$

$\beta=\alpha\nu+\epsilon\Leftrightarrow(8+6i)=(1+7i)(1-i)+0$

따라서 $8+6i$와 $5-15i$의 $\gcd$는 $1+7i$이다.

그 밖에 최대 공약수로는 단원인 $-1,\pm i$을 곱한 $-1-7i,1+7i,-7+i$ 도 될 수 있다.

문 8. 참, 거짓을 판정하라.

(a) $Z[i]$는 PID이다.

풀 이 True

$Z[i]$는 ED이고 ED는 PID이므로 $Z[i]$는 PID이다.

(b) $Z[i]$는 유클리드 정역이다.

풀 이 True

$\alpha = a+b\sqrt{-1} \in Q(\sqrt{-1})$에 대하여 $\delta(\alpha) = |N(\alpha)| = |a^2+b^2|$이라고 정의하면,

임의의 $\alpha, \beta \in Q(\sqrt{-1})$에 대하여 다음이 성립한다.

$\delta(\alpha\beta) = |N(\alpha\beta)| = |N(\alpha)||N(\beta)| = \delta(\alpha)\delta(\beta)$

특히 각 $\alpha = a+b\sqrt{-1} \in Z[\sqrt{-1}]$에 대하여

$\delta(\alpha) = |N(\alpha)| = |a^2+b^2| \in W = \{n \in Z \mid n \geq 0\}$

이므로 함수 $\delta : Z[\sqrt{-1}] \to W$ 가 정의되고 또 다음이 성립한다.

$\delta(\alpha) = 0 \Leftrightarrow \alpha = 0$

$\alpha, \beta \in Z[\sqrt{-1}], \alpha = 0 \Rightarrow \delta(\beta) \leq \delta(\alpha)\delta(\beta) = \delta(\alpha\beta)$

이제 $\alpha, \beta \in Z[\sqrt{-1}], \alpha \neq 0$에 대하여 $\frac{\beta}{\alpha} = c+d\sqrt{-1} \in Q[\sqrt{-1}]$ 이라고 하고

x, y를 각각 유리수 c, d에 가장 가까운 정수라고 하자. 즉

$0 \leq |c-x| \leq \frac{1}{2}, 0 \leq |d-y| \leq \frac{1}{2}$

이때 $\nu = x+y\sqrt{-1} \in Z[\sqrt{-1}], \epsilon = \beta - \alpha\nu \in Z[\sqrt{-1}]$이라고 하면

$\epsilon = \beta - \alpha\nu = \alpha(\frac{\beta}{\alpha} - \nu) = \alpha\{(c-x)+(d-y)\sqrt{-1}\},$

$\delta(\epsilon) = \delta(\alpha)\delta(\frac{\beta}{\alpha} - \nu) = \delta(\alpha)|(c-x)^2+(d-y)^2|$

이고 또 다음이 성립한다.

$0 \leq (c-x)^2+(d-y)^2 \leq \frac{1}{2}$

따라서 $\beta = \alpha\nu + \epsilon$, $\delta(\epsilon) < \delta(\alpha)$이므로 $Z[\sqrt{-1}]$은 ED이다.

(c) Z에 속하는 모든 정수는 가우스 정수이다.

풀 이 True

$Z[i]$를 가우스 정수들의 집합이라 하자. 임의의 $\alpha \in Z$에 대하여 $\alpha = \alpha + 0 \cdot i \in Z[i]$이 성립한다. 따라서 Z에 속하는 모든 정수는 가우스 정수이다.

(d) 모든 복소수는 가우스 정수이다.

풀 이 F

$\sqrt{2} \notin Z$이므로 $\sqrt{2}\,i \notin Z[i]$이다. 따라서 모든 복소수가 가우스 정수인 것은 아니다.

(e) $Z[i]$에서 유클리드 호제법이 성립된다.

풀 이 T

$Z[i]$는 ED이므로 유클리드 호제법이 성립한다.

(f) 정역의 승법노름은 때때로 정역의 기약원을 구하는데 도움이 된다.

풀 이 T

[정리 47.7]에 의하여 때때로 정역의 승법노름은 때때로 정역의 기약원을 구하는데 도움이 될 수 있음을 알 수 있다.

(g) N이 정역 D의 승법노름이면 D의 모든 가역원 u에 대하여 $|N(u)|=1$이다.

풀 이 T

D를 승법노름 N을 갖는 정역이라 하면 $N(1)=N(1\cdot 1)=N(1)N(1)$이고 $N(1)>0$이므로 $N(1)=1$이다. 또한 u가 D의 가역원이면 $1=N(1)=N(u\cdot u^{-1})=N(u)N(u^{-1})$이고 $N(u)$는 음이 아닌 정수이므로 $|N(u)|=1$이다.

(h) F가 체이면 $N(f(x))=(f(x)$의차수$)$로 정의된 함수 N은 $F[x]$ 위에서 승법노름이 된다.

풀 이 F

$N(1)=\deg(1)=0$이지만 $1\neq 0$이다.

(i) F가 체이면 $f(x)\neq 0$에 대하여 $N(f(x))=2^{(f(x)의\ 차수)}$이고, $N(0)=0$로 정의된 함수는 정의에 의하여 $F[x]$에서 승법노름이다.

풀 이 T

(a) 임의의 $f(x)\in F[x]$에 대하여 $N(f(x))=2^{(f(x)의\ 차수)}\geq 0$이다.

(b) $N(f(x))=2^{(f(x)의\ 차수)}=0\Leftrightarrow f(x)=0\ (\because N(0)=0)$

(c) 임의의 $f(x),g(x)\in F[x]$에 대하여

$N(f(x)g(x))=2^{\deg f(x)g(x)}=2^{\deg f(x)+\deg g(x)}=2^{\deg f(x)}\cdot 2^{\deg g(x)}=N(f(x))N(g(x))$

이다. 따라서 N은 $F[x]$위에서 승법노름이 된다.

(j) $Z[\sqrt{-5}]$는 정역이지만 UFD는 아니다.

풀 이 T

(a) $Z[\sqrt{-5}]$은 정역이다.

($\because Z[\sqrt{-5}]$은 0과 1을 포함하는 복소수의 부분집합이므로 정역임은 당연하다.)

(b) $Z[\sqrt{-5}]$는 UFD가 아니다.

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

(1) $a^2+5b^2=2$와 $a^2+5b^2=3$은 정수해를 갖지 않으므로 2와 3은 둘 다 $Z[\sqrt{-5}]$에서 기약원이다.

(2) $-1+\sqrt{-5}$를 기약원이 아니라면

α가 가역원이 아니고 β가 가역원이 아닐 때 $-1+\sqrt{-5}=\alpha\beta$이 성립한다.

$N(\alpha\beta)=N(\alpha)N(\beta)=6$이고 $N(\alpha)=2\text{ or }3$일 때는 해를 갖지 않으므로 $N(\alpha)=1\text{or}6$이다. 그러면 $N(\alpha)$ 또는 $N(\beta)$은 가역원이다. 이는 모순이다. 따라서 $-1+\sqrt{-5}$은 기약원이다.

(3) $Z[\sqrt{-5}]$에서 가역원은 ± 1뿐이다. 하지만 2도 3도 $\pm(-1+\sqrt{-5})$가 아니므로 $Z[\sqrt{-5}]$은 UFD가 아니다.)

문 9. D를 $\alpha \in D$에 대하여 $|N(\alpha)|=1$이 될 필요충분 조건이 α가 D의 가역원임을 만족하는 승법노름 N을 갖는 정역이라 하자. π가 $\beta \in D$에 대하여 $|N(\beta)|>1$을 만족하는 β중에서 $|N(\pi)|$가 최소가 되는 원소라 하면 π는 D의 기약원임을 보여라.

풀 이

$\pi=\alpha\beta$라 하면 $|N(\pi)|=|N(\alpha\beta)|=|N(\alpha)||N(\beta)|>1$을 얻게 된다.
이때 $|N(\alpha)|>1$ 이고 $|N(\beta)|>1$이라고 하면 $|N(\alpha)|<|N(\pi)|$ 또는 $|N(\beta)|<|N(\pi)|$이므로 가정에서 π가 $|N(\pi)|$이 최소가 되는 원소라는 가정에 모순된다.
따라서 $|N(\alpha)|=1$ 또는 $|N(\beta)|=1$이다. 이는 조건에 의하여 필요충분하게 α가 D의 가역원이거나 β가 D의 가역원이다. 그러므로 π는 D의 기약원이다.

문 10.
(a) Show that 2 is equal to the product of a unit and square of an irreducible in Z[i].

풀 이

- 생 략 -

(b) Show that an odd prime p in Z is irreducible in Z[i] iff p≡3(mod4).
(Use Thm 47.10)

풀 이

- 생 략 -

문 11. 보조정리 47.2를 증명하라.

풀 이

$\alpha=a+bi, \beta=c+di \in Z[i]$라 할 때

(1) $N(\alpha)=a^2+b^2 \geq 0$

(2) $N(\alpha)=a^2+b^2=0 \Leftrightarrow a=b=0 \Leftrightarrow \alpha=a+bi=0$

(3)
$$\begin{aligned} N(\alpha\beta) &= N((a+bi)(c+di)) \\ &= N((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2+(ad+bc)^2 \\ &= (ac)^2+(bd)^2+(ad)^2+(bc)^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(a+bi)N(c+di) \\ &= N(\alpha)N(\beta) \end{aligned}$$

따라서 [보조정리 47.2]는 성립한다.

문 12. 예제 47.9의 N이 승법 즉, $\alpha,\beta \in Z[\sqrt{-5}]$에 대하여 $N(\alpha\beta)=N(\alpha)N(\beta)$임을 증명하라.

풀 이

$\alpha=a+b\sqrt{-5}, \beta=c+d\sqrt{-5} \in Z[\sqrt{-5}]$에 대하여

$$\begin{aligned} N(\alpha\beta) &= N((a+b\sqrt{-5})(c+d\sqrt{-5})) \\ &= N((ac-5bd)+(ad+bc)\sqrt{-5}) \\ &= (ac-5bd)^2+5(ad+bc)^2 \\ &= (ac)^2+25(bd)^2+5(ad)^2+5(bc)^2 \\ &= (a^2+5b^2)(c^2+5d^2) \\ &= N(a+b\sqrt{-5})N(c+d\sqrt{-5}) \\ &= N(\alpha)N(\beta) \end{aligned}$$

이 성립함을 알 수 있다.

문 13. D**를** $\alpha \in D$**에 대하여** $|N(\alpha)|=1$**이 될 필요충분조건은** α**가** D**의 가역원임을 만족하는 승법노름** N**를 갖는 정역이라 하자. 0이 아니고 가역원도 아닌 모든** D**의 원소는** D**의 기약원으로 인수분해됨을 보여라.**

풀 이

$\alpha \in D$라 하자. 수학적 귀납법에 의하여 증명한다.
(1) $N(\alpha)=2$인 경우
2가 소수이므로 정리 47.7에 의하여 α 자신이 기약원이다.
(2) $1 < N(\delta) < k$에서 모든 D의 원소δ는 기약원으로 인수분해된다고 가정하자. 그리고 $N(\alpha)=k$라고 하자. 만약 α가 기약원이면 당연하다.
α가 기약원이 아니라면 $\alpha=\beta\gamma$ (단, β,γ는 둘 다 가역원이 아니다.)이라 둘 수 있다.
그러면 $N(\beta)>1, N(\gamma)>1$이고 $N(\alpha)=N(\beta)N(\gamma)=k$이므로 $N(\beta)<k, N(\gamma)<k$이다.
즉 $1<N(\beta)<k, 1<N(\gamma)<k$이다.
가정에 의하여 β,γ는 기약원으로 인수분해된다.
따라서 이 둘의 곱은 α 또한 기약원으로 인수분해 됨을 알 수 있다.

문 14. $Z[i]$**의 유클리드 호제법을 사용하여** $Z[i]$**에서** $16+7i$**와** $10-5i$**의** gcd**를 구하여라.**
[힌트: 정리 47.4의 증명에서의 모순을 사용한다.]

풀 이

[문제7]번과 같은 방법으로... (-생략-)
따라서 $\gcd(16+7i, 10-5i)=1+2i$이다.
그 밖에 최대 공약수로 $-1-2i, -2+i, 2-i$ 도 될 수 있다.

문 15. $<\alpha>$**를** $Z[i]$**에서 0이 아닌 주 아이디얼이라 하자.**
(a) $Z[i]/<\alpha>$**가 유한환임을 보여라.**
[힌트: 호제법을 이용하라.]

풀 이

정역 $Z[i]$에 대해서 주 아이디얼$<\alpha>$에 의한 $Z[i]/<\alpha>$이 환임은 당연하다.
이제 유환환임을 보이자.
임의의 $\gamma+<\alpha> \in Z[i]/<\alpha>$에 대하여 $Z[i]$가 UFD이므로
유클리드 호제법에 의하여 $\gamma=\alpha\sigma+\rho, \rho=0 \text{ or } N(\rho)<N(\alpha)$를 만족한다.
그러면 $\gamma+<\alpha> = (\alpha\sigma+\rho)+<\alpha>$
$\Rightarrow \alpha\sigma \in <\alpha>$ 이므로 $\gamma+<\alpha> = \rho+<\alpha>$
그러므로 $<\alpha>$에 의한 모든 잉여류는 $N(\alpha)$보다 작은 노름을 갖는다.
$Z[i]$에서 $N(\alpha)$보다 작은 노름을 갖는 원소가 유한 개 뿐이므로
따라서 $Z[i]/<\alpha>$은 유한환이다.

(b) π**가** $Z[i]$**의 기약원이면** $Z[i]/<\pi>$**는 체임을 보여라.**

풀 이

$Z[i]$가 PID이므로 다음은 서로 동치이다.
π가 $Z[i]$의 기약원이다
$\Leftrightarrow$ $<\pi>$는 $Z[i]$의 극대 아이디얼이다.
$\Leftrightarrow$ $Z[i]/<\pi>$는 체이다.

(c) b)를 참고로 하여 다음 각 체들의 위수와 표수를 구하라.

ⅰ) $Z[i]/<3>$

풀 이

위수는 9이고 표수는 3이다.

ⅱ) $Z[i]/<1+i>$

풀 이

위수는 2이고 표수는 2이다.

ⅲ) $Z[i]/<1+2i>$

풀 이

위수는 5이고 표수는 5이다.

문 16. $n \in Z^+$**를 어떤 소수의 제곱으로 나누어지지 않는 수(이런 수를 square free라 한다.)라 할 때** $Z[\sqrt{-n}] = \{a+bi \mid a,b \in Z\}$**라 하자.**

(a) $\alpha = a+ib\sqrt{n}$**에 대하여** $N(\alpha) = a^2+nb^2$**으로 정의된 노름** N**이** $Z[\sqrt{-n}]$**에서 승법노름임을 보여라.**

풀 이

$\alpha = a+ib\sqrt{n}$, $\beta = c+id\sqrt{n} \in Z[\sqrt{-n}]$에 대하여

(1) $N(\alpha) = a^2+nb^2 \geq 0$임은 당연하다.

(2) $N(\alpha) = a^2+nb^2 = 0 \Leftrightarrow a^2 = 0 \text{ and } nb^2 = 0 (n \neq 0) \Leftrightarrow a = b = 0 \Leftrightarrow \alpha = 0$ 임을 알 수 있다.

(3) $$\begin{aligned} N(\alpha\beta) &= N((a+ib\sqrt{n})(c+id\sqrt{n})) \\ &= N((ac-nbd)+i(ad+bc)\sqrt{n}) \\ &= (ac-nbd)^2+n(ad+bc)^2 \\ &= (ac)^2+n^2(bd)^2+n(ad)^2+n(bc)^2 \\ &= (a^2+nb^2)(c^2+nd^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

임을 알 수 있다.

따라서 노름N이 $Z[\sqrt{-n}]$에서 승법노름이다.

(b) $\alpha \in Z[\sqrt{-n}]$**에 대하여** $N(\alpha) = 1$**일 필요충분조건은** α**가** $Z[\sqrt{-n}]$**의 가역원임을 보여라.**

풀 이

☞) $\alpha \in Z[\sqrt{-n}]$에 대하여 $N(\alpha) = 1$이면 $\alpha = a+bi$일 때 $a^2+nb^2 = 1$이다.

그러면 $a = \pm 1, b = 0$ 또는 $a = 0, b = \pm 1$이다.

(1) $a = \pm 1, b = 0$인 경우

± 1은 $Z[\sqrt{-n}]$의 가역원이므로 α는 $Z[\sqrt{-n}]$의 가역원이다.

(2) $a = 0, n = 1, b = \pm 1$인 경우

$Z[\sqrt{-1}]$은 가우스 정수이므로 유클리드 정역이다.

따라서 $N(\alpha) = 1$이면 α는 $Z[\sqrt{-n}]$의 가역원이다.

☜) $\alpha \in U(Z[\sqrt{-n}])$이면

$1 = N(1) = N(\alpha \cdot \alpha^{-1}) = N(\alpha)N(\alpha^{-1})$이고 $N(\alpha)$는 양의 정수이므로 $N(\alpha) = 1$이다.

(c) 가역원도 아니고 0이 아닌 모든 $\alpha\in Z[\sqrt{-n}]$은 $Z[\sqrt{-n}]$에서 기약원으로 인수분해를 가짐을 보여라.

[힌트: b)를 이용하라.]

풀 이

(a),(b)에 의하여 $Z[\sqrt{-n}]$은 승법노름 N을 갖는다는 사실과 $N(\alpha)=1\Leftrightarrow\alpha:units$ 라는 사실을 알 수 있다. 그러면 [문제13]에 의하여 가역원도 아니고 0이 아닌 모든 $\alpha\in Z[\sqrt{-n}]$은 $Z[\sqrt{-n}]$에서 기약원으로 인수분해를 가짐을 알 수 있다.

문 17. $Z[\sqrt{n}]$에 속하는 $\alpha=a+b\sqrt{n}$에 대하여
$N(\alpha)=|a^2-nb^2|$으로 정의된 N을 갖는 $Z[\sqrt{n}]=\{a+b\sqrt{n}\,|\,a,b\in Z\}$에 대하여 문제 16을 반복하라.

(a) $\alpha=a+b\sqrt{n}$에 대하여 $N(\alpha)=|a^2-nb^2|$으로 정의된 노름 N이 $Z[\sqrt{n}]$에서 승법노름임을 보여라.

풀 이

$\alpha=a+b\sqrt{n}$, $\beta=c+d\sqrt{n}\in Z[\sqrt{n}]$에 대하여

(1) $N(\alpha)=|a^2-nb^2|\geq 0$임은 당연하다.

(2) $N(\alpha)=|a^2-nb^2|=0\Leftrightarrow a^2=nb^2$ 임을 알 수 있다.

(i) $b=0$이면 $a=0$이다.

(ii) $b\neq 0$이면 $n=\dfrac{a^2}{b^2}=(\dfrac{a}{b})^2$이다. 하지만 이는 n이 제곱수가 아닌 가정에 모순이다.

따라서 $\alpha=0$이다.

(3)
$$\begin{aligned}N(\alpha\beta)&=N((a+b\sqrt{n})(c+d\sqrt{n}))\\&=N((ac+nbd)+(ad+bc)\sqrt{n})\\&=|(ac+nbd)^2-n(ad+bc)^2|\\&=|(a^2-nb^2)||(c^2-nd^2)|\\&=N(\alpha)N(\beta)\end{aligned}$$

임을 알 수 있다.

따라서 노름N이 $Z[\sqrt{n}]$에서 승법노름이다.

(b) $\alpha\in Z[\sqrt{n}]$에 대하여 $N(\alpha)=1$일 필요충분조건은 α가 $Z[\sqrt{n}]$의 가역원임을 보여라.

풀 이

☞) $\alpha\in Z[\sqrt{n}]$에 대하여 $N(\alpha)=1$이면 $\alpha=a+bi$일 때 $|a^2-nb^2|=1$이다.

즉, $a^2-nb^2=\pm 1$이다.

그러면

$\dfrac{1}{\alpha}=\dfrac{1}{a+b\sqrt{n}}=\dfrac{a-b\sqrt{n}}{a^2-nb^2}=\pm(a-b\sqrt{n})$이고 $a-b\sqrt{n}\in Z[\sqrt{n}]$이다.

따라서 α는 가역원이다.

☜) $\alpha\in U(Z[\sqrt{n}])$이면

$1=N(1)=N(\alpha\cdot\alpha^{-1})=N(\alpha)N(\alpha^{-1})$이고 $N(\alpha)$는 양의 정수이므로 $N(\alpha)=1$이다.

(c) 가역원도 아니고 0이 아닌 모든 $\alpha \in Z[\sqrt{n}]$은 $Z[\sqrt{n}]$에서 기약원으로 인수분해를 가짐을 보여라. [힌트: b)를 이용하라.]

풀 이

(a),(b)에 의하여 $Z[\sqrt{n}]$은 승법노름 N을 갖는다는 사실과 $N(\alpha)=1 \Leftrightarrow \alpha : units$ 라는 사실을 알 수 있다. 그러면 [문제13]에 의하여 가역원도 아니고 0이 아닌 모든 $\alpha \in Z[\sqrt{-n}]$은 $Z[\sqrt{n}]$에서 기약원으로 인수분해를 가짐을 알 수 있다.

문 18. $Z[\sqrt{-2}]$에서 이 정역의 0이 아닌 원소 α에 대하여 $\nu(\alpha)=N(\alpha)$로 정의하면 ν에 대하여 호제법이 성립됨을 정리 47.4의 증명에 있어서 모순됨을 이용하여 보여라. (문제 16 참조). (따라서, 이들 정역은 유클리드정역이다. 정역$Z[\sqrt{n}]$ an와 $Z[\sqrt{-n}]$이 유클리드 정역임을 Hardy 와 Wright [29]에 잘 설명되어 있다.)

풀 이

$Z[\sqrt{-2}]$이 ED임을 보이면 충분하다.

$\alpha = a+b\sqrt{-2} \in Q(\sqrt{-2})$에 대하여 $\delta(\alpha)=|N(\alpha)|=|a^2+2b^2|$이라고 정의하면, 임의의 $\alpha, \beta \in Q(\sqrt{-2})$에 대하여 다음이 성립한다.

$$\delta(\alpha\beta)=|N(\alpha\beta)|=|N(\alpha)||N(\beta)|=\delta(\alpha)\delta(\beta)$$

특히 각 $\alpha = a+b\sqrt{-2} \in Z[\sqrt{-2}]$에 대하여 $\delta(\alpha)=|N(\alpha)|=|a^2+2b^2| \in W=\{n \in Z \mid n \geq 0\}$이므로 함수 $\delta : Z[\sqrt{-2}] \to W$ 가 정의되고 또 다음이 성립한다.

$$\delta(\alpha)=0 \Leftrightarrow \alpha=0$$
$$\alpha, \beta \in Z[\sqrt{-2}], \alpha=0 \Rightarrow \delta(\beta) \leq \delta(\alpha)\delta(\beta)=\delta(\alpha\beta)$$

이제 $\alpha, \beta \in Z[\sqrt{-2}], \alpha \neq 0$에 대하여 $\frac{\beta}{\alpha}=c+d\sqrt{-2} \in Q[\sqrt{-2}]$ 이라고 하고 x, y를 각각 유리수 c, d에 가장 가까운 정수라고 하자. 즉,

$$0 \leq |c-x| \leq \frac{1}{2}, 0 \leq |d-y| \leq \frac{1}{2}$$

이때 $\nu = x+y\sqrt{-2} \in Z[\sqrt{-2}], \epsilon = \beta - \alpha\nu \in Z[\sqrt{-2}]$이라고 하면

$$\epsilon = \beta - \alpha\nu = \alpha(\frac{\beta}{\alpha}-\nu) = \alpha\{(c-x)+(d-y)\sqrt{-2}\},$$

$$\delta(\epsilon)=\delta(\alpha)\delta(\frac{\beta}{\alpha}-\nu)=\delta(\alpha)|(c-x)^2+2(d-y)^2|$$

이고 또 다음이 성립한다.

$$0 \leq (c-x)^2+2(d-y)^2 \leq \frac{3}{4}$$

따라서 $\beta = \alpha\nu+\epsilon$, $\delta(\epsilon) < \delta(\alpha)$이므로 $Z[\sqrt{-2}]$은 ED이다.

※ 문제1~5에서 $f(\alpha)=0$를 만족하는 $f(x)\in Q[x]$를 찾음으로서 주어진 수 $\alpha\in C$가 Q위에서 대수적임을 보여라.

문 1. $1+\sqrt{2}$

풀 이

$\alpha=1+\sqrt{2}$일 때 $\alpha-1=\sqrt{2}$이고 여기서 양변을 제곱하면 $(\alpha-1)^2=2$이다.
이를 정리하면 $\alpha^2-2\alpha-1=0$을 얻는다. 따라서 $f(x)=x^2-2x-1$임을 알 수 있다.

문 2. $\sqrt{2}+\sqrt{3}$

풀 이

$\alpha=\sqrt{2}+\sqrt{3}$일 때 $\alpha-\sqrt{3}=\sqrt{2}$이고 여기서 양변을 제곱하면 $(\alpha-\sqrt{3})^2=2$이다.
이를 정리하면 $\alpha^2+1=2\sqrt{3}\alpha$을 얻는다. 또한 이를 양변 제곱하면 $(\alpha^2+1)^2=12\alpha^2$이다.
이를 정리하면 $\alpha^4-10\alpha^2+1=0$이고 따라서 $f(x)=x^4-10x^2+1$임을 알 수 있다.

문 3. $1+i$

풀 이

$\alpha=1+i$일 때 $\alpha-1=i$이고 여기서 양변을 제곱하면 $(\alpha-1)^2=-1$이다.
이를 정리하면 $\alpha^2-2\alpha+2=0$을 얻는다. 따라서 $f(x)=x^2-2x+2$임을 알 수 있다.

문 4. $\sqrt{1+\sqrt[3]{2}}$

풀 이

$\alpha=\sqrt{1+\sqrt[3]{2}}$일 때 양변을 제곱하면 $\alpha^2=1+\sqrt[3]{2}$이다.
이를 정리하면 $\alpha^2-1=\sqrt[3]{2}$이고 이를 양변 세제곱하면 $\alpha^6-3\alpha^4+3\alpha^2-3=0$을 얻는다.
따라서 $f(x)=x^6-3x^4+3x^2-3$임을 알 수 있다.

문 5. $\sqrt{\sqrt[3]{2}-i}$

풀 이

$\alpha=\sqrt{\sqrt[3]{2}-i}$일 때 양변을 제곱하면 $\alpha^2=\sqrt[3]{2}-i$이다.
이를 정리하면 $\alpha^2+i=\sqrt[3]{2}$이고 이를 양변 세제곱하면 $\alpha^6-3\alpha^2-2=(1-3\alpha^4)i$을 얻을 수 있다.
여기서 양변 제곱하여 정리하면 $\alpha^{12}+3\alpha^8-4\alpha^6+3\alpha^4+12\alpha^2+5=0$을 얻는다.
따라서 $f(x)=x^{12}+3x^8-4x^6+3x^4+12x^2+5$임을 알 수 있다.

※ 문제6~8에서 주어진 대수적 수 $\alpha \in C$에 대하여 $irr(\alpha, Q)$와 $\deg(\alpha, Q)$를 구하라. 또한 다항식이 Q 위에서 기약임을 보여라.

문 6. $\sqrt{3-\sqrt{6}}$

풀 이

$\alpha = \sqrt{3-\sqrt{6}}$ 일 때 양변을 제곱하면 $\alpha^2 = 3-\sqrt{6}$ 이다. 이를 정리하면 $\alpha^2 - 3 = -\sqrt{6}$ 이고 이를 양변 제곱하면 $(\alpha^2-3)^2 = 6$ 이고 이를 정리하면 $\alpha^4 - 6\alpha^2 + 3 = 0$이다.

이제 $f(x) = x^4 - 6x^2 + 3$이라 하면 $f(x)$는 $3 \nmid 1, 3|6, 3^2 \nmid 3$이므로 Eisenstein 판정법에 의하여 Q위에서 기약이다. 따라서 $irr(\alpha, Q) = f(x) = x^4 - 6x^2 + 3$이고 $\deg(\alpha, Q) = \deg f(x) = 4$이다.

문 7. $\sqrt{(\frac{1}{3}) + \sqrt{7}}$

풀 이

$\alpha = \sqrt{(\frac{1}{3}) + \sqrt{7}}$ 일 때 양변을 제곱하면 $\alpha^2 = (\frac{1}{3}) + \sqrt{7}$ 이다. 이를 정리하면 $\alpha^2 - (\frac{1}{3}) = \sqrt{7}$ 이고 이를 양변 제곱하면 $\alpha^4 - (\frac{2}{3})\alpha^2 + \frac{1}{9} = 7$이다. 여기서 양변에 9를 곱하고 정리하면 $9\alpha^4 - 6\alpha^2 - 62 = 0$이다.

이제 $f(x) = 9x^4 - 6x^2 - 62$이라 하면 $f(x)$는 $2 \nmid 9, 2|6, 2^2 \nmid 62$이므로 Eisenstein 판정법에 의하여 Q위에서 기약이다. 따라서 $irr(\alpha, Q) = f(x) = 9x^4 - 6x^2 - 62$이고 $\deg(\alpha, Q) = \deg f(x) = 4$이다.

문 8. $\sqrt{2} + i$

풀 이

$\alpha = \sqrt{2} + i$일 때 $\alpha - \sqrt{2} = i$이고 이를 양변 제곱하면 $\alpha^2 - 2\sqrt{2}\alpha + 2 = -1$이다. 이를 정리하면 $\alpha^2 + 3 = 2\sqrt{2}\alpha$이고 이를 양변 제곱하면 $\alpha^4 + 6\alpha^2 + 9 = 8\alpha^2$이다. 이를 정리하면 $\alpha^4 - 2\alpha^2 + 9 = 0$이다.

이제 $f(x) = x^4 - 2x^2 + 9$이라 하면 $f(x)$는 Q위에서 기약이다.

(∵

(1) 일차항을 인수로 갖지 않는다.

(∵ $\frac{(\text{상수항})}{(\text{첫째항})}$의 약수: $\pm 1, \pm 3, \pm 9$ 이지만

$f(\pm 1) = 1 - 2 + 9 = 8 \neq 0$,

$f(\pm 3) = 81 - 18 + 9 = 72 \neq 0$,

$f(\pm 9) = 9^4 - 162 + 9 = 6408 \neq 0$

이므로 Q위에서 일차항을 인수로 갖지 않는다.)

(2) 이차항을 인수로 갖지 않는다.

(∵이차항을 인수로 갖는다면 $f(x) = (\text{이차항}) \times (\text{이차항})$의 꼴이다.

그러면 $f(x) = (x^2 - \alpha)(x^2 - \beta) = x^4 - 2x^2 + 9$ $(\alpha, \beta \in Q)$이다. 즉, $\alpha + \beta = 2, \alpha\beta = 9$이다. 하지만 α, β를 근으로 갖는 이차 방정식은 존재하지 않는다. 이는 모순이다. 따라서 이차항을 인수로 갖지 않는다.)

(1),(2)로부터 $f(x)$는 Q위에서 기약이다.)

따라서 $irr(\alpha, Q) = f(x) = x^4 - 2x^2 + 9$이고 $\deg(\alpha, Q) = \deg f(x) = 4$이다.

※ 문제9~16에서 주어진 $\alpha \in C$가 주어진 체 위에서 대수적인지 초월적인지를 분류하라. 만약, α가 F 위에서 대수적이면 $\deg(\alpha, F)$를 구하라.

문 9. $\alpha = i, F = Q$

풀 이

대수적이고 이때 $\deg(i, Q) = \deg(x^2 + 1) = 2$이다.

문 10. $\alpha = 1 + i, F = R$

풀 이

대수적이고 이때 $\deg(1 + i, R) = \deg(x^2 - 2x + 2) = 2$이다.

문 11. $\alpha = \sqrt{\pi}, F = Q$

풀 이

초월적이다.

문 12. $\alpha = \sqrt{\pi}, F = R$

풀 이

대수적이고 이때 $\deg(\sqrt{\pi}, R) = \deg(x^2 - \pi)\,(\because \pi \in R) = 2$이다.

문 13. $\alpha = \sqrt{\pi}, F = Q(\pi)$

풀 이

대수적이고 이때 $\deg(\sqrt{\pi}, Q(\pi)) = \deg(x^2 - \pi)\,(\because \pi \in Q(\pi)) = 2$이다.

문 14. $\alpha = \pi^2, F = Q$

풀 이

초월적이다.

문 15. $\alpha = \pi^2, F = Q(\pi)$

풀 이

대수적이고 이때 $\deg(\pi^2, Q(\pi)) = \deg(x - \pi^2)\,(\because \pi^2 \in Q(\pi)) = 1$ 이다.

문 16. $\alpha = \pi^2, F = Q(\pi^3)$

풀 이

대수적이고 이때 $\deg(\pi^2, Q(\pi^3)) = \deg(x^3 - \pi^6)(\because \pi^6 \in Q(\pi^3)) = 3$이다.

문 17. 예제 29.19를 참고하여, 다항식 x^2+x+1은 $Z_2(\alpha)$에서 근 α를 가지며 $(Z_2(\alpha))[x]$에서 일차 인수들의 곱으로 인수분해 되어야 한다. 이 인수분해를 구하라.

[힌트: $\alpha^2=\alpha+1$임을 이용하여 x^2+x+1을 $x-\alpha$로 나누어라].

풀 이

$f(x)=x^2+x+1$이라 할 때 $f(\alpha)=0$라 하자.

$\alpha^2=\alpha+1$이라 할 때 $f(\alpha^2)=\alpha^4+\alpha^2+1=\alpha^2+\alpha+1(\because \alpha^3=1)=0$이므로

따라서 $f(x)$는 α^2을 인수로 갖는다. 따라서 $f(x)=(x-\alpha)(x-\alpha^2)$으로 인수 분해 된다.

여기서 $\alpha\neq\alpha^2$이다. ($\because \alpha=\alpha^2$이면 $\alpha^2=\alpha+1$인 조건으로부터 $0=1$이 되어 모순이다.)

문 18.

(a) 다항식 x^2+1이 $Z_3[x]$에서 기약임을 보여라.

풀 이

$\phi_\alpha : Z_3[x]\to Z_3, \phi_\alpha(f(x))=f(\alpha)\in Z_3$인 평가 준동형사상이라 하자.

그러면 $f(x)=x^2+1$에 대하여 $\phi_0(f(x))=1\neq 0, \phi_1(f(x))=2\neq 0, \phi_2(f(x))=5=2\neq 0$을 만족한다.

따라서 x^2+1은 $Z_3[x]$에서 기약이다.

(b) α가 Z_3의 확대체에서 x^2+1의 근이라 하자. 예제 29.19에서 처럼 $0,1,2,\alpha,2\alpha,1+\alpha,1+2\alpha,2+\alpha$ 그리고 $2+2\alpha$의 순서로 쓰여진 $Z_3(\alpha)$의 9개 원소들의 곱셈과 덧셈 연산표를 만들어라.

풀 이

(a)에 의하여 x^2+1은 $Z_3[x]$에서 기약이므로 $\alpha\neq 0,1,2$이다. 또한 조건에 의하여 $\alpha^2=-1=2$이다.

이 때 9개의 원소들의 곱셈과 덧셈 연산표는 다음과 같다.

•	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	0	α	2α	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
2α	0	2α	α	1	2	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	$2+\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	α	0	1	2α
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	0	α	2α	0
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	1	2α	α	2
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	2α	0	2	α

+	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	2α
2	2	0	1	$2+\alpha$	$2+2\alpha$	α	2α	$1+\alpha$	$1+2\alpha$
α	α	$1+\alpha$	$2+\alpha$	2α	0	$1+2\alpha$	1	$2+2\alpha$	2
2α	2α	$1+2\alpha$	$2+2\alpha$	0	α	1	$1+\alpha$	2	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	1	$2+2\alpha$	2	2α	0
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	2α	1	$1+\alpha$	2	$2+\alpha$	0	α
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2	2α	0	$1+2\alpha$	1
$2+2\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	$2+\alpha$	0	α	1	$1+\alpha$

※ 문제19~22 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 19. An element α of an extension field E of a field F if *algebraic* over F iff α is a zero of some polynomial.

풀 이

어떤 다항식에 대한 구분이 명확하지 않다.
따라서 옳은 정의로는 E가 체 F의 확대체일 때 $\alpha \in E$가 F위에서 *대수적*일 필요충분조건은 $\alpha \in E$가 $F[x]$상의 다항식 $f(x) \in F[x]$이 존재해서 $f(\alpha) = 0$을 만족하는 것이다.

문 20. An element β of an extension field E of a field F is *transcendental* over F iff β is not a zero of any polynomial in $F[x]$.

풀 이

E가 체 F의 확대체일 때 $\beta \in E$가 F위에서 *초월적*일 필요충분조건은 $\beta \in E$가 $F[x]$상의 임의의 다항식 $f(x) \in F[x]$에 대하여 $f(\beta) \neq 0$을 만족하는 것이다.
따라서 주어진 표현은 옳은 표현이다.

문 21. A *monic polynomial* in $F[x]$ is one having all coefficients equal to 1.

풀 이

모든 계수가 1인 다항식을 말하는 것이 아니라. 최고차항의 계수가 1인 다항식을 말한다.
즉, $F[x]$상에서 *모닉다항식*은 최고차항의 계수가 1인 다항식을 말한다.

문 22. A field E is *simple extension* of a subfield F iff there exists some $\alpha \in E$ such that on proper subfiled of E contains α.

풀 이

α를 포함하는 E의 진부분체가 아니라 E가 부분체 F와 $\alpha \in E$를 포함하는 최소의 체와 같아야 한다.
즉, 체 E가 부분체 F의 *단순 확대체*일 필요충분조건은 $E = F(\alpha)$를 만족하는 $\alpha \in E$가 존재하는 것이다.

문 23. 참, 거짓을 판정하라.

(a) 수 π는 Q위에서 초월적이다.

풀 이 T

$\nexists f(x) \in Q[x]\ s.t.\ f(\pi) = 0$

(b) C는 R의 단순 확대체이다.

풀 이 T

$C = R(i)$이므로 C는 r의 단순 확대체이다.

(c) 체 F의 모든 원소는 F위에서 대수적이다.

풀 이 T

임의의 $\alpha \in F$에 대하여 $\exists f(x) = x - \alpha \in F[x]$이다. 따라서 체 F의 모든 원소는 F위에서 대수적이다.

(d) R는 Q의 확대체이다.

풀 이 T

$Q \subseteq R$임은 자명하고 둘 다 표수가 0인 체이므로 R는 Q의 확대체이다.

(e) Q는 Z_2의 확대체이다.

풀 이 F

Q를 Z_2의 확대체하고 하자. 그러면 Q의 표수는 Z_2의 표수와 같다. 그러면 $0=2$가 된다. 이는 모순이다. 따라서 Q는 Z_2의 확대체가 아니다.

(f) $\alpha \in C$가 Q위에서 차수 n인 대수적인 원소라 하자. 만약 0이 아닌 $f(x) \in Q[x]$에 대해 $f(\alpha)=0$이면 $\deg f(x) \geq n$이다.

풀 이 T

$\alpha \in C$에 대하여 $irr(\alpha, Q)=n$일 때 α를 포함하는 최소차 다항식을 $g(x) \in Q[x]$라 하면 $f(x) \in Q[x]$에 대하여 $f(\alpha)=0$이면 $g(x) | f(x)$을 만족한다. 따라서 $\deg f(x) \geq \deg g(x)=n$이다.

(g) $\alpha \in C$가 Q위에서 차수가 n인 대수적인 원소라 하자. 만약 0이 아닌 $f(x) \in R[x]$에 대해 $f(\alpha)=0$이면 $\deg f(x) \geq n$이다.

풀 이 F

$\sqrt{2} \in C$는 Q위에서 2차인 대수적인 원소이지만 $f(x)=x-\sqrt{2} \in R[x]$에 대해 $f(\sqrt{2})=0$이지만 $\deg f(x)=1 \leq 2$이다.

(h) $F[x]$에 속하는 상수가 아닌 모든 다항식은 F의 적당한 확대체에서 근을 갖는다.

풀 이 T

E를 F의 대수적 폐체라고 하자. 그러면 $\deg f(x) \geq 1$인 $f(x) \in F[x]$에 대해 $f(\alpha)=0$을 만족하는 $F \leq E$인 $\alpha \in E$이 존재한다. 따라서 $f(x)$는 F의 적당한 확대체 $F(\alpha)(\leq E)$에서 근을 갖는다.

(i) $F[x]$에 속하는 상수가 아닌 모든 다항식은 F의 모든 확대체에서 근을 갖는다.

풀 이 F

$F=Q$일 때 $Q \leq Q(\sqrt{2})$인 확대체 $Q(\sqrt{2})$에서 $f(x)=x^2-3$은 근을 갖지 않는다.

(j) 만약 x가 부정원이면 $Q[\pi] \simeq Q[x]$이다.

풀 이 T

만약 x가 부정원이라 할 때, $\phi_\pi : Q[x] \to Q[\pi], \phi_\pi(f(x))=f(\pi) \in Q[\pi]\ (f(x) \in Q[x])$로 정의된 전사인 평가준동형사상이라 하자.($\because$ 전사임과 준동형사상은 자명하다.) 또한 $\ker\phi=\{0\}$이다. ($\because \ker\phi \neq \{0\}$이라 가정하면 $f(x) \neq 0$인 $f(x) \in \ker\phi$에 대하여 $\phi_\pi(f(x))=f(\pi)=0$이다. 하지만 Q에서 π는 초월적이므로 $f(x) \neq 0$인 가정에 모순이다.) 따라서 $Q[x] \simeq Q[\pi]$이다.

문 24. 앞에서 π와 e가 Q위에서 초월적임을 증명없이 진술만 하였다.

(a) π가 F위에서 차수 3인 대수적인 원소가 되도록 R의 부분체 F를 구하라.

풀 이

$F = Q(\pi^3)$이다.

($\because$ $irr(\pi, Q(\pi^3)) = \deg(x^3 - \pi^3) = 3$이고 $Q(\pi^3) \leq R$)

(b) e^2이 E위에서 차수 5인 대수적인 원소가 되도록 R의 부분체 E를 구하라.

풀 이

$E = Q(e^{10})$이다.

($\because$ $irr(e^2, Q(e^{10})) = \deg(x^5 - e^{10}) = 5$이고 $Q(e^{10}) \leq R$)

문 25.

(a) $x^3 + x^2 + 1$이 Z_2위에서 기약임을 보여라.

풀 이

$\phi_\alpha : Z_2[x] \to Z_2, \phi_\alpha(f(x)) = f(\alpha) \in Z_2$인 평가 준동형사상이라 하자.

그러면 $f(x) = x^3 + x^2 + 1$에 대하여 $\phi_0(f(x)) = 1 \neq 0$, $\phi_1(f(x)) = 3 = 1 \neq 0$을 만족한다.

따라서 $x^3 + x^2 + 1$은 Z_2위에서 기약이다.

(b) α를 Z_2의 확대체에서 $x^3 + x^2 + 1$의 하나의 근이라 하자. 실제로 인수분해해 보임으로서 $x^3 + x^2 + 1$이 $(Z_2(\alpha))[x]$에서 일차 인수들로 인수분해 됨을 보여라.

[힌트: $Z_2(\alpha)$의 모든 원소는 $a_i = 0,1$에 대해 $a_0 + a_1\alpha + a_2\alpha^2$의 형태이다. $x^3 + x^2 + 1$을 $x - \alpha$로 나누면 그 몫도 $Z_2(\alpha)$에서 군을 가짐을 $Z_2(\alpha)$의 여덟 개의 원소를 조사해 봄으로서 보이고 인수분해를 완성하라].

풀 이

$f(x) = x^3 + x^2 + 1$이라 할 때 α가 $x^3 + x^2 + 1$의 하나의 근이므로 $\alpha^3 + \alpha^2 + 1 = 0$을 만족한다.

다른 근을 β라 하면

⑴ $\beta = 0$인 경우, $f(\beta) = f(0) = 1 \neq 0$이므로 근이 아니다.(×)

⑵ $\beta = 1$인 경우, $f(\beta) = f(1) = 3 = 1 \neq 0$이므로 근이 아니다.(×)

⑶ $\beta = \alpha$인 경우, $f(\beta) = f(\alpha) = 0$이므로 조건에 의해 근이다.(○)

⑷ $\beta = \alpha^2$인 경우, $f(\beta) = f(\alpha^2) = \alpha^6 + \alpha^4 + 1 = (\alpha^2 - \alpha) + (\alpha^2 - \alpha + 1) + 1 = 0$이므로 근이다.(○)

⑸ $\beta = \alpha^2 + 1$인 경우,

$f(\beta) = f(\alpha^2 + 1) = f(-\alpha^3) = f(\alpha^3) = \alpha^9 + \alpha^6 + 1 = (-\alpha^2) + (\alpha^2 - \alpha) + 1 = 1 - \alpha$이므로 근이 아니다.(×)

⑹ $\beta = \alpha + 1$인 경우,

$f(\beta) = f(\alpha + 1) = (\alpha + 1)^3 + (\alpha + 1)^2 + 1 = \alpha^3 + \alpha + 1 = -\alpha^2 + \alpha$이므로 근이 아니다.(×)

⑺ $\beta = \alpha^2 + \alpha$인 경우,

$f(\beta) = f(\alpha^2 + \alpha) = \alpha^3(\alpha + 1)^3 + \alpha^2(\alpha + 1)^2 + 1 = \alpha^2 + 1 = -\alpha^3$이므로 근이 아니다.(×)

⑻ $\beta = \alpha^2 + \alpha + 1$인 경우, $f(\beta) = f(\alpha^2 + \alpha + 1) = 0$이므로 근이다.(○)

따라서 $f(x) = (x - \alpha)(x - \alpha^2)(x - (\alpha^2 + \alpha + 1))$으로 인수분해 될 수 있다.

문 26. E**를** Z_2**의 확대체 그리고** $\alpha \in E$**를** Z_2**위에서 차수가 3인 대수적인 원소라 하자. 유한 생성된 가환군의 기본정리를 따라 군** $\langle Z_2(\alpha), + \rangle$**와** $\langle (Z_2(\alpha))^*, \bullet \rangle$**을 분류하여라. 단,** $(Z_2(\alpha))^*$**는** $Z_2(\alpha)$**의 0이 아닌 원소들의 집합이다.**

풀 이

$\langle Z_2(\alpha), + \rangle$는 유한인 가환군이다. 또한 $irr(\alpha, Z_2) = 3$이므로 유한 생성된 가환군의 기본정리에 의하여 $Z_2(\alpha) \simeq Z_2 \times Z_2 \times Z_2$임을 알 수 있고 $\langle (Z_2(\alpha))^*, \bullet \rangle$는 위수 7인 가환군이므로 순환군 Z_7과 동형이다.

문 27. E**를 체** F**의 확대체 그리고** $\alpha \in E$**가** F**위에서 대수적이라 하자.** $irr(\alpha, F)$**를** F**위에서** α**에 대한 최소차 다항식이라고 한다. 이 용어가 왜 적당한가 그 이유를 설명하라.**

풀 이

적당하다. 그 이유는 α을 대입했을 때 0이 되는 최소차수 다항식이기 때문이다.

문 28. -생략-

문 29. E**를** F**의 확대체, 그리고** $\alpha, \beta \in E$**라 하자.** α**가** F**위에서 초월적이지만** $F(\beta)$**위에서 대수적이라 가정하면** β**는** $F(\alpha)$**위에서 대수적임을 보여라.**

풀 이

(1) β기 F에서 대수적이라 가정하자 그러면 $F(\beta)$는 F위에서의 대수적 확대체이다.
⇒ $F(\beta)$가 대수적확대체이므로 $(F(\beta))(\alpha)$는 $F(\beta)$의 대수적확대체이다.
⇒ $(F(\beta))(\alpha)$는 $F(\beta)$의 대수적확대체이고 $F(\beta)$는 F위에서의 대수적 확대체이다.
⇒ $(F(\beta))(\alpha)$는 F위에서의 대수적 확대체이다.
⇒ 대수적확대체의 정의에 의하여 α는 F에서 대수적 확대체이다. 이는 모순이다.
그러므로 β는 F에서 초월적이다.

(2) β는 F에서 초월적이므로 $F(\beta) = \left\{ \frac{f(\beta)}{g(\alpha)} | f(x), g(x) \in F[x], g(x) \neq 0 \right\}$이다.
가정에 의하여 α기 $F(\beta)$에서 대수적이므로 $\exists\, h(x) \in (F(\beta))[x]\ s.t.\ h(\alpha) = 0$ 이다.
이제 $h(x) = \frac{f_0(\beta)}{g_0(\beta)} + \frac{f_1(\beta)}{g_1(\beta)}x + \cdots + \frac{f_n(\beta)}{g_n(\beta)}x^n$이라고 두자. 그러면

$$h(\alpha) = \frac{f_0(\beta)}{g_0(\beta)} + \frac{f_1(\beta)}{g_1(\beta)}\alpha + \cdots + \frac{f_n(\beta)}{g_n(\beta)}\alpha^n = 0$$

$$\Rightarrow\ h(\alpha)[g_0(\beta)g_1(\beta)\cdots g_n(\beta)] = [\frac{f_0(\beta)}{g_0(\beta)} + \frac{f_1(\beta)}{g_1(\beta)}\alpha + \cdots + \frac{f_n(\beta)}{g_n(\beta)}\alpha^n][g_0(\beta)g_1(\beta)\cdots g_n(\beta)] = 0$$

$$\Rightarrow\ \overline{g_0}(\beta)f_0(\beta) + \overline{g_1}(\beta)f_1(\beta)\alpha + \cdots + \overline{g_n}(\beta)f_n(\beta)\alpha^n = 0 \quad (\text{단},\ \overline{g_i}(\beta) = g_1(\beta)\cdots g_{i-1}(\beta)g_{i+1}(\beta)\cdots g_n(\beta))$$

⇒ 위의 식을 β 에 관하여 정리하면 $k_0(\alpha) + k_1(\alpha)\beta + \cdots + k_m(\alpha)\beta^m = 0$
이제 $f(x) = k_0(\alpha) + k_1(\alpha)x + \cdots + k_m(\alpha)x^m$라 두자.
그러면 $f(x) \in (F(\alpha))[x]$이고 또한 $f(\beta) = 0$이다.
따라서 β는 $F(\alpha)$에서 대수적이다.

문 30. E**를** q**개의 원소를 갖는 유한체** F**의 확대체, 그리고** $\alpha \in E$**는** F**위에서 차수**n**인 대수적인 원소라 하자.** $F(\alpha)$**는** q^n**개의 원소를 가짐을 보여라.**

풀 이

체 F와 $F \le F(\alpha) \le E$인 확대체 $F(\alpha)$에 대하여
$|F| = q$이고 $[F(\alpha) : F] = n$이므로 $F(\alpha) = \{(a_1, \cdots, a_n) | a_i \in F, 1 \le i \le n\}$이다.
여기서 a_i는 서로 일차독립이므로 따라서 $|F(\alpha)| = q^n$이다.

문 31.

(a) $Z_3[x]$**에서 차수 3인 기약 다항식이 존재함을 보여라.**

풀 이

$f(x) = x^3 + x^2 - x + 1 \in Z_3[x]$라 할 때 $f(0) = 1, f(1) = 2, f(2) = 2$이므로 $f(x)$는 일차항을 인수로 갖지 않는다. 따라서 $Z_3[x]$에서 기약 다항식 $f(x)$가 존재함을 알 수 있다.

(b) (a)로부터 27개의 원소를 갖는 유한체가 존재함을 보여라[힌트: 문제30를 이용하라].

풀 이

Z_3의 원소의 개수는 3개이고 (a)로부터 차수 3인 기약 다항식이 존재함을 알 수 있다.
$\Rightarrow$ $\alpha \notin Z_3$가 존재해서 $f(\alpha) = 0$을 만족한다.
$\Rightarrow$ $Z_3(\alpha)$는 Z_3의 유한확대체이고 차수는 $[Z_3(\alpha) : Z_3] = irr(\alpha, Z_3) = \deg(f(x)) = 3$이다.
$\Rightarrow$ 문제 30에 의하여 $|Z_3(\alpha)| = 3^3 = 27$개의 원소를 갖는다.
따라서 27개의 원소를 갖는 유한체가 존재함을 알 수 있다.

문 32. 표수 $p \neq 0$**인 소체** Z_p**에 대하여 생각해 보자.**

(a) $p \neq 2$**에 대하여** Z_p**의 모든 원소가** Z_p**의 원소의 제곱이 아님을 보여라.**

[힌트: Z_p**에서** $1^2 = (p-1)^2 = 1$**이다. 헤아림에 의해 원하는 결론을 유추하여라]**

풀 이

$\phi : Z_p \to Z_p, \phi(a) = a^2 \ (a \in Z_p)$인 군 준동형사상을 생각해 보자.
그러면 $1^2 = (p-1)^2 = 1$이므로 $im\phi \neq Z_p$이다. 즉, $im\phi \subsetneq Z_p$이다.
따라서 Z_p의 원소 중에는 Z_p의 원소의 제곱이 아닌 원소가 존재함을 알 수 있다.

(b) (a)를 이용하여 Z^+**의 모든 소수** p**에 대하여** p^2**개의 원소를 갖는 유한체가 존재함을 보여라.**

풀 이

(a)에 의하여 $x^2 - \alpha \neq 0$인 $\alpha \in Z_p$가 존재한다. 그러므로 $f(x) = x^2 - \alpha$라 할 때 $f(x)$는 $Z_p[x]$에서 기약이다. 이제 Z_p이 확대체를 E라 할 때 $\beta \in E$에 대해 $f(\beta) = 0$이라고 하자.
그러면 $[Z_p(\beta) : Z_p] = irr(\beta, Z_p) = \deg f(x) = 2$이고, 문제30번에 의하여 $Z_p(\beta)$는 p^2개의 원소를 갖는 유한체이다. 따라서 Z^+의 모든 소수 p에 대하여 p^2개의 원소를 갖는 유한체 $Z_p(\beta)$가 존재함을 알 수 있다.

문 33. E를 체 F의 확대체, 그리고 $\alpha\in E$를 F위에서 초월적이라 하자. F에 속하지 않는 $F(\alpha)$의 모든 원소는 또한 F위에서 초월적임을 보여라.

풀 이

$\beta\in F(\alpha)-F$에 대하여 F에서 대수적이라고 가정하여 $\alpha\in E$가 F에서 초월적임에 모순됨을 보인다.
$\beta\in F(\alpha)-F$에 대하여 $\alpha\in E$가 F에서 초월적이므로 다음이 성립한다.

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}\,|\,f(x),g(x)\in F[x],g(x)\neq 0\right\}$$

그러면 어떤 $f(x),g(x)\in F[x],g(x)\neq 0$에 대하여 $\beta=\frac{f(\alpha)}{g(\alpha)}$이다.
$\alpha\in E$가 F에서 초월적이고 $g(x)\neq 0$이므로 β가 F에서 대수적이라고 가정하자.
그러면 $\exists\, h(x)\in F[x]\setminus\{0\}\, s.t.\quad h(\beta)=0$
이제 $h(x)=a_0+a_1x+\cdots+a_nx^n$이라 두자.
그러면 $0=h(\beta)=a_0+a_1\beta+\cdots+a_n\beta^n=a_0+a_1\frac{f(\alpha)}{g(\alpha)}+\cdots+a_n(\frac{f(\alpha)}{g(\alpha)})^n$이다.
여기에 양변에 $g(\alpha)^n$을 곱하면 $a_0g(\alpha)^n+a_1f(\alpha)g(\alpha)^{n-1}+\cdots+a_nf(\alpha)^n=0$이다.
위의 식을 α에 관하여 정리하면 $b_i\neq 0$인 $b_i\in F$에 대하여 $b_0+b_1\alpha+\cdots+b_m\alpha^m=0$이다.
이제 $p(x)=b_0+b_1x+\cdots+b_mx^m=0$라 두자.
그러면 $p(x)\in F[x]$이고 $p(\alpha)=0$이다. 따라서 α가 F에서 대수적이다. 이는 모순이다.
그러므로 $\beta\in F(\alpha)-F$는 F위에서 초월적이다.

문 34. 체의 공리들을 보이는 것 대신에
이 절에서 사용된 개념을 이용하여 $\{a+b(\sqrt[3]{2})+c(\sqrt[3]{2})^2\,|\,a,b,c\in Q\}$가 R의부분체임을 보여라.

풀 이

$\{a+b(\sqrt[3]{2})+c(\sqrt[3]{2})^2\,|\,a,b,c\in Q\}=Q(\sqrt[3]{2})$이고 $x^3-2=0$은 $Q[x]$에서 기약이다. 그러므로 $Q(\sqrt[3]{2})$는 Q의 확대체임을 알 수 있다. 또한 $Q\subseteq R,\sqrt[3]{2}\in R$이고 Q,R은 모두 체이므로 $Q\leq Q(\sqrt[3]{2})\leq R$이 성립한다. 따라서 $Q(\sqrt[3]{2})$은 체 R의 부분체이다.

문 35. 문제31의 방법에 의해 각각 8개, 16개, 그리고 25개의 원소를 갖는 체가 존재함을 보여라.

풀 이

(1) Z_2위에서 $f(x)=x^3+x+1$은 기약이다.($\because f(0)=1,f(1)=1$) 그러므로 $f(x)=0$이 되는 근을 α라 할 때 $irr(\alpha,Z_2)=3$이다. 따라서 문제31의 방법에 의하여 $2^3(=8)$개의 원소를 갖는 체 $Z_2(\alpha)$가 존재함을 알 수 있다.
(2) Z_2위에서 $g(x)=x^4+x+1$은 기약이다.($\because g(0)=1,g(1)=1$) 그러므로 $g(x)=0$이 되는 근을 β라 할 때 $irr(\beta,Z_2)=4$이다. 따라서 문제31의 방법에 의하여 $2^4(=16)$개의 원소를 갖는 체 $Z_2(\beta)$가 존재함을 알 수 있다.
(3) Z_5위에서 $h(x)=x^2+2$은 기약이다.($\because h(0)=2,h(1)=3,h(2)=1,h(3)=1,h(4)=3$) 그러므로 $f(x)=0$이 되는 근을 γ라 할 때 $irr(\gamma,Z_5)=2$이다. 따라서 문제31의 방법에 의하여 $5^2(=25)$개의 원소를 갖는 체 $Z_5(\gamma)$가 존재함을 알 수 있다.

문 36. F는 표수 p를 갖는 유한체라 하자. F의 모든 원소는 F의 소체 Z_p 위에서 대수적임을 보여라.
[힌트: F^*를 F의 0이 아닌 원소들이라 하면 F^*가 순환군을 이룸을 이용하여 $\alpha \in F^*$가 x^n-1의 형태의 $Z_p[x]$의 다항식의 근임을 보여라.]

풀 이

F는 표수 p를 갖는 유한체이므로 Z_p와 동형인 소체 K가 존재한다.
그리고 F는 유한체이므로 $\exists m \in Z^+ \; s.t. \; |F| = m$
그러면 $< F^*, \bullet >$는 위수 $m-1$인 순환군이다.
임의의 $a \in F^*$에 대하여 위수의 정의에 의하여 $a^{m-1} = 1$이고 $a^m = a$이다. 즉, $a^m - a = 0$이다.
이제 $f(x) = x^m - x \in K[x]$라 두자.
그러면 F위에서 $f(a) = 0$이고 $f(0) = 0$이다.
그러므로 임의의 $a \in F$에 대하여 K위에서 대수적이다.

[다른풀이]
F는 유한체, F는 K의 유한차원 확대체이므로 $\exists n \in N \, s.t. \; [F:K] = n$
$\Rightarrow$ F는 K위의 벡터공간으로서 $F = \{(a_1, a_2, \cdots, a_n) | a_i \in K\}$이고 $|F| = p^n$이다.
$\Rightarrow$ $< F^*, \bullet >$는 위수 $p^n - 1$인 순환군이다.
임의의 $a \in F^*$에 대하여 위수의 정의에 의하여 $a^{p^n-1} = 1$이고 $a^{p^n} = a$이다.
이제 $f(x) = x^{p^n} - x \in K[x]$라 두자.
그러면 F위에서 $f(a) = 0$이고 $f(0) = 0$이다.
그러므로 임의의 $a \in F$에 대하여 K위에서 대수적이다.

문 37. 문제30와 36을 이용하여, 모든 유한체는 소수의 멱을 위수로 가짐을 보여라. 즉, 그 체는 어떤 소수의 멱의 개수를 원소로 갖는다.

풀 이

F는 임의의 유한체라 하자. F가 체이므로 표수는 0 또는 적당한 소수 p이다.
여기서 F가 유한체이므로 F의 표수는 p를 만족한다.
($\because$ F의 표수가 0이면 Q와 동형인 소체를 갖고 이는 유한임에 모순)
그러면 Z_p와 동형인 소체 K가 유일하게 존재한다.
F는 유한체이고 F는 K의 유한확대체이므로 $\exists n \in N \; s.t. \; [F:K] = n$
그러면 F는 K위의 벡터공간으로서 $F = \{(a_1, a_2, \cdots, a_n) | a_i \in K\}$이므로 따라서 $|F| = p^n$이다.

문 1. 어느 두 개의 기저에도 공통으로 벡터를 갖지 않는 R위에서 R^2의 기저들을 세 개 구하라.

풀 이

- 생략함 -

※ 문제2~3에서 벡터들의 주어진 집합의 R위에서 R^3에 대한 기저가 되는지 결정하라.

문 2. $\{(1,1,0),(1,0,1),(0,1,1)\}$

풀 이

주어진 벡터로 이루어진 행렬A의 기본행변환에 의하여

$$A=\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&0\\0&-1&1\\0&1&1\end{pmatrix}\sim\begin{pmatrix}1&0&1\\0&1&-1\\0&0&2\end{pmatrix}\sim\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

이다. 따라서 주어진 벡터는 R^3에 대한 기저임을 알 수 있다.

※ 기저가 되는지 알아보기 위해서는 생성조건과 일차독립임을 확인하면 된다.

문 3. $\{(-1,1,2),(2,-3,1),(10,-14,0)\}$

풀 이

주어진 벡터로 이루어진 행렬A의 기본행변환에 의하여

$$A=\begin{pmatrix}-1&2&10\\1&-3&-14\\2&1&0\end{pmatrix}\sim\begin{pmatrix}0&-1&-4\\1&3&-14\\0&7&28\end{pmatrix}\sim\begin{pmatrix}1&0&-26\\0&1&4\\0&0&0\end{pmatrix}$$

이다. 그러면 주어진 벡터는 R^3를 생성할 수 없다. 따라서 주어진 벡터는 R^3에 대한 기저가 아니다.

※ 문제4~9에서 체 위에서 주어진 벡터공간에 대한 기저를 구하라.

문 4. Q위에서 $Q(\sqrt{2})$

풀 이

$[Q(\sqrt{2}):Q]=irr(\sqrt{2},Q)=\deg(x^2-2)=2$이고 이 때 벡터공간에 대한 기저는 $\{1,\sqrt{2}\}$이다.

문 5. R위에서 $R(\sqrt{2})$

풀 이

$[R(\sqrt{2}):R]=irr(\sqrt{2},R)=\deg(x-\sqrt{2})=1$이고 이 때 벡터공간에 대한 기저는 $\{1\}$이다.

문 6. Q위에서 $Q(\sqrt[3]{2})$

풀 이

$[Q(\sqrt[3]{2}):Q]=irr(\sqrt[3]{2},Q)=\deg(x^3-2)=3$이고 이 때 벡터공간에 대한 기저는 $\{1,\sqrt[3]{2},\sqrt[3]{2^2}\}$이다.

문 7. R**위에서** C

풀 이

$[C:R]=irr(i,R)=\deg(x^2+1)=2$이고 이 때 벡터공간에 대한 기저는 $\{1,i\}$이다.

문 8. Q**위에서** $Q(i)$

풀 이

$[Q(i):Q]=irr(i,Q)=\deg(x^2-1)=2$이고 이 때 벡터공간에 대한 기저는 $\{1,i\}$이다.

문 9. Q**위에서** $Q(\sqrt[4]{2})$

풀 이

$[Q(\sqrt[4]{2}):Q]=irr(\sqrt[4]{2},Q)=\deg(x^4-2)=4$이고
이 때 벡터공간에 대한 기저는 $\left\{1,\sqrt[4]{2},\sqrt[4]{2^2},\sqrt[4]{2^3}\right\}$이다.

문 10. 정리 30.23에 의해 예제 29.19에서 주어진 $Z_2(\alpha)$**의 원소** $1+\alpha$**는** Z_2**위에서 대수적이다.** $Z_2[x]$**에서** $1+\alpha$**에 대한 기약 다항식을 구하라.**

풀 이

$f(x)=x^2+x+1\in Z_2[x]$에 대하여 예제 29.19에서 $f(\alpha)=0$를 만족한다.
그러면 Z_2위에서 $Z_2(\alpha+1)$의 기저는 다음과 같다.

$(1+\alpha)=-\alpha^2=\alpha^2$
$(1+\alpha)^2=\alpha^2+2\alpha+1=\alpha^2+1=-\alpha=\alpha$
$(1+\alpha)^3=\alpha^3+3\alpha^2+3\alpha+1=\alpha^3+\alpha^2+\alpha+1=\alpha^3=1$

즉, 기저는 $\{1,\alpha+1,\alpha\}$이다. 그러면 $Z_2[x]$에서 $1+\alpha$에 대한 기약 다항식은 예제 29.19에서 주어진 α에 대한 기약 다항식과 같은 x^2+x+1이다.

※11~14 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 11. The vectors in a subset S **of a vector space** V **over a field** F ***span*** V **iff each** $\beta\in V$ **can be expressed uniquely as a linear combination of the vectors in** S**.**

풀 이

체 F위의 벡터공간 V의 부분집합 S안의 벡터가 V를 *생성*할 필요충분조건은 각각의 $\beta\in V$가 S안의 벡터들의 유일한 일차결합으로 나타낼 수 있는 것이다.
⇒ 맞는 정의인듯!!

문 12. The vectors in a subset S **of a vector space** V **over a field** F **are** ***linearly independent*** **over** F **iff the zero vector cannot be expressed as a linear combination of vectors in** S**.**

풀 이

체 F위의 벡터공간 V의 부분집합 S안의 벡터가 F위에서 *일차독립*일 필요충분조건은 영벡터가 S안의 벡터들의 일차결합으로 나타낼 수 없는 것이다.
⇒ 영벡터가 S안의 벡터들의 일차결합으로 나태낼 수 없는 것이 아니라. 영벡터가 S안의 벡터들의 일차결합으로 표현되는 유일한 방법은 모든 스칼라가 0일 때이다.

문 13. The ***dimension*** over F of a finite-demensional vector space V over a field F is the minimun number of vectors requires to span V.

풀 이

체 F위의 유한 차원 벡터공간 V의 F위의 *차원*은 V를 생성할 수 있는 최소의 벡터수와 같다.
⇒ 맞는 정의인듯!!

문 14. A ***basis*** for a vector space V over a field F is a set of vectors in V that span V and are linearly dependent.

풀 이

체 F위의 벡터공간 V의 *기저*는 V를 생성하고 일차종속인 V에서의 벡터들의 집합이다.
⇒ 일차종속이 아니고 일차독립이다.

문 15. 참, 거짓을 판정하라.

(a) 두 벡터의 합은 벡터이다.

풀 이 T

체 F위에서 벡터공간을 V라 할 때, 두 벡터의 합은 연산에 대해 닫혀 있으므로 벡터이다.

(b) 두 스칼라의 합은 벡터이다.

풀 이 F

체 F위에서 벡터공간을 V라 할 때, 스칼라는 체 F의 원소이고 덧셈연산에 관하여 닫혀 있으므로 F의 원소이다. 따라서 벡터공간이 아니고 스칼라이다.

(c) 두 스칼라의 곱은 스칼라이다.

풀 이 T

체 F위에서 벡터공간을 V라 할 때, 스칼라는 체 F의 원소이고 곱셈 연산에 관하여 닫혀 있으므로 F의 원소이다. 따라서 두 스칼라의 곱은 스칼라이다.

(d) 스칼라와 벡터와의 곱은 벡터이다.

풀 이 T

벡터공간의 정의에 의하여 스칼라와 벡터의 곱은 벡터이다.

(e) 모든 벡터공간은 유한기저를 갖는다.

풀 이 F

Q위에서 R는 유한기저를 갖지 않는다.

(f) 기저에 속하는 벡터는 일차종속이다.

풀 이 F

S가 기저이면 S에 속하는 원소는 일차독립이다.

(g) 0-벡터는 기저의 원소가 될 수 있다.

풀 이 F

벡터공간 V에 대하여 0-벡터가 기저의 원소가 될 수 있다면 그 기저는 일차종속이다. 이는 모순이다.

(h) $F \leq E$이고, $\alpha \in E$가 체 F위에서 대수적이면 α^2도 F위에서 대수적이다.

풀 이 T

$\alpha \in F$이면 $\alpha^2 \in F$이므로 체 F위에서 대수적이다.

$\alpha \notin F$일 때, $[F(\alpha):F] = n \in N$이라 하자. α가 F위에서 대수적이므로

$\exists f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \in F[x], a_i \in F \; s.t. \; f(\alpha) = 0$

(1) n이 짝수인 경우

$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \cdots + a_n\alpha^n = 0$

$\Rightarrow (a_0 + a_2\alpha^2 + \cdots a_n\alpha^n) + \alpha(a_1 + a_3\alpha^2 + \cdots + a_{n-1}\alpha^{n-2}) = 0$

$\Rightarrow \alpha = -\dfrac{(a_0 + a_2\alpha^2 + \cdots a_n\alpha^n)}{(a_1 + a_3\alpha^2 + \cdots + a_{n-1}\alpha^{n-2})}$

$\Rightarrow f(\alpha) = f(-\dfrac{(a_0 + a_2\alpha^2 + \cdots a_n\alpha^n)}{(a_1 + a_3\alpha^2 + \cdots + a_{n-1}\alpha^{n-2})}) = 0$

이를 α^2에 관하여 정리하면 $\exists b_i \in F \; s.t. \; f(\alpha) = b_0 + b_1(\alpha^2) + b_2(\alpha^2)^2 + \cdots + b_k(\alpha^2)^k$

이제 $g(x) = b_0 + b_1 x + \cdots + b_k x^k$라고 하면

$g(x) \in F[x]$이고 $g(\alpha^2) = 0$을 만족한다. 따라서 α^2도 F위에서 대수적이다.

(2) n이 홀수인 경우

$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \cdots + a_n\alpha^n = 0$

$\Rightarrow (a_0 + a_2\alpha^2 + \cdots a_{n-1}\alpha^{n-1}) + \alpha(a_1 + a_3\alpha^2 + \cdots + a_n\alpha^{n-1}) = 0$

$\Rightarrow \alpha = -\dfrac{(a_0 + a_2\alpha^2 + \cdots a_{n-1}\alpha^{n-1})}{(a_1 + a_3\alpha^2 + \cdots + a_n\alpha^{n-1})}$

$\Rightarrow f(\alpha) = f(-\dfrac{(a_0 + a_2\alpha^2 + \cdots a_{n-1}\alpha^{n-1})}{(a_1 + a_3\alpha^2 + \cdots + a_n\alpha^{n-1})}) = 0$

이를 α^2에 관하여 정리하면 $\exists c_i \in F \; s.t. \; f(\alpha) = c_0 + c_1(\alpha^2) + c_2(\alpha^2)^2 + \cdots + c_l(\alpha^2)^l$

이제 $h(x) = c_0 + c_1 x + \cdots + c_l x^l$라고 하면

$h(x) \in F[x]$이고 $h(\alpha^2) = 0$을 만족한다. 따라서 α^2도 F위에서 대수적이다.

위의 경우에 의하여 α^2도 F위에서 대수적이다.

[다른 풀이]

$\alpha^2 \in F(\alpha)$이고 $F(\alpha)$는 F위의 대수적 확대체이므로 $F(\alpha^2)$ 또한 F위의 대수적확대체이다.

따라서 α^2는 F위에서 대수적이다.

(i) $F \leq E$이고, $\alpha \in E$가 체 F위에서 대수적이면 $\alpha + \alpha^2$도 F위에서 대수적이다.

풀 이 T

$\alpha, \alpha + 1 \in F(\alpha)$이므로 $\alpha + \alpha^2 \in F(\alpha)$이고 $F(\alpha)$는 F위의 대수적 확대체이므로

$F(\alpha^2 + \alpha)$ 또한 F위의 대수적확대체이다.

따라서 $\alpha^2 + \alpha$는 F위에서 대수적이다.

(j) 모든 벡터공간은 기저를 갖는다.

풀 이 T

기저는 벡터공간을 이루는 가장 기본적인 원소들의 모임이다. 따라서 모든 벡터공간은 기저를 갖는다.

※ 다음 연습문제들은 벡터공간에 대해서 다룬 것이다. 다른 대수적 구조에 대하여 공부한 것과 비슷한 개념을 벡터공간에 대해서 정의하도록 해보자. 이들 연습문제들은 대수에 관련된 상황들을 이해하는 능력을 향상시켜 줄 것으로 믿는다. 이 연습문제에서는 앞 장에서 정의된 개념을 알고 있다고 가정한다.

문 16. V가 체 F위에서 벡터공간이라 하자.
(a) F위에서 벡터공간 V의 부분공간을 정의하라.

풀 이

체 F위의 벡터공간 V의 부분집합 $W(\neq \varnothing)$가 V의 덧셈과 스칼라 곱셈에 관하여 벡터공간을 이룰 때, W를 V의 부분공간이라고 한다. ($\leftrightarrow\ w_1, w_2 \in W \Rightarrow w_1 - w_2 \in W\ ;\ a \in F,\ w \in W \Rightarrow aw \in W$)

(b) V의 부분공간의 공통집합은 다시 F위에서 부분공간임을 증명하라.

풀 이

$\{A_i | i \in I\}$를 벡터공간 V의 부분공간들의 집합족이라 하자. 그러면

$w_1, w_2 \in \bigcap_{i \in I} A_i \Rightarrow w_1, w_2 \in A_i (\forall\, i \in I) \Rightarrow\ w_1 - w_2 \in A_i (\forall\, i \in I) \Rightarrow\ w_1 - w_2 \in \bigcap_{i \in I} A_i$

$a \in F,\ w \in \bigcap_{i \in I} A_i \Rightarrow a \in F,\ w \in A_i (\forall\, i \in I) \Rightarrow\ aw \in A (\forall\, i \in I) \Rightarrow aw \in \bigcap_{i \in I} A_i$

이다. 따라서 $\bigcap_{i \in I} A_i$ 또한 V의 부분공간이다.

문 17. V를 체 F의 벡터공간, 그리고 $S = \{\alpha_i | i \in I\}$를 V에 속하는 벡터의 공집합이 아닌 모임이라 하자.
(a) 문제 16의 (b)를 이용하여 S에 의해 생성된 V의 부분공간을 정의하라.

풀 이

S에 의하여 생성된 부분공간은 S의 모든 원소를 포함하는 가장 작은 V의 부분공간을 말한다.
즉, $< S > = \cap \{ W | a_i \in W (\forall\, i \in I),\ W \leq V \}$이다.

(b) S에 의하여 생성된 V의 부분공간에 속하는 벡터들은 S에 속하는 벡터들의 (유한) 일차결합임을 증명하라. (정리 7.6과 비교하라)

풀 이

- 생략함 -

문 18. $V_1, \cdots, V_n$을 체 F위에서 벡터공간이라 하자. $i = 1, 2, \cdots, n$에 대해서 벡터공간 V_i의 직합 $V_1 \oplus \cdots \oplus V_n$을 정의하고 그 직합은 다시 F위에서 벡터공간임을 보여라.

풀 이

$V_1 \oplus \cdots \oplus V_n = \{(v_1, v_2, \cdots, v_n) | v_i \in V_i\ (i \in I)\}$라고 덧셈과 스칼라 곱셈을 다음과 같이 정의하자.

$\forall\, \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n), \beta = (\beta_1, \beta_2, \cdots, \beta_n) \in V_1 \oplus \cdots \oplus V_n\ s.t.\ \ \alpha + \beta = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \cdots, \alpha_n + \beta_n)$

$\forall\, (\alpha_1, \alpha_2, \cdots, \alpha_n) \in V_1 \oplus \cdots \oplus V_n, \forall\, a \in F\ \ s.t.\ \ \ a(\alpha_1, \alpha_2, \cdots, \alpha_n) = (a\alpha_1, a\alpha_2, \cdots, a\alpha_n)$

그러면 벡터공간 V_i의 직합 $V_1 \oplus \cdots \oplus V_n$은 F위의 벡터공간임이 명백하다.

문 19. 임의의 체 F에 대해서 체 F위에서 F의 원소의 $n-$순서쌍의 벡터공간 F^n을 얻기 위해 예제 30.2을 일반화 하라. 또, F^n에 대한 하나의 기저를 구하라.

풀 이

체 F위에서 F의 원소의 $n-$순서쌍의 벡터공간 F^n은 $F^n=\{(\alpha_1,\alpha_2,\cdots,\alpha_n)|\alpha_i\in F\}$와 같이 일반화 할 수 있고, 이때 하나의 기저로는 $\{(1,0,0,\cdots,0),(0,1,0,\cdots,0),\cdots,(0,0,0,\cdots,1)\}$이 있다.

문 20. 체 F에서 벡터공간 V에서와 같은 체 F위에서 벡터공간 V'로 대응하는 동형사상을 정의하라.

풀 이

F위에서 두 벡터공간 V와 V'에 대하여 사상 $\phi: V\rightarrow V'$가 벡터공간의 덧셈과 스칼라 곱셈을 보존시킬 때, 즉 다음 두 조건을 만족시킬 때, ϕ를 V에서 V'으로의 선형사상이라고 한다.

(1) $\alpha,\beta\in V\ s.t.\ \phi(\alpha+\beta)=\phi(\alpha)+\phi(\beta)$

(2) $\alpha\in V,\ a\in F\ s.t.\ \phi(a\alpha)=a\phi(\alpha)$

사상 ϕ가 선형사상인 동시에 일대일 대응일 때, ϕ를 V에서 V'위로의 벡터공간의 동형사상이라고 한다.

문 21. V가 체 F위에서 유한차원 벡터공간이면 V의 부분집합 $\{\beta_1,\cdots,\beta_n\}$이 F에서 V에 대한 기저가 되기 위한 필요충분조건은 V에 속하는 모든 벡터가 β_i의 일차결합으로 유일하게 표현됨을 증명하라.

풀 이

V가 체 F위의 유한차원 벡터공간이라 하자.

(⇨)

(1) 일차결합으로 나타낼 수 있음을 보이자.

벡터공간 V의 부분집합 $\{\beta_1,\cdots,\beta_n\}$이 F에서 V에 대한 기저라고 하자.

그러면 $V=<\beta_1,\beta_2,\cdots,\beta_n>$이므로 임의의 $\beta\in V$에 대하여

$\beta=c_1\beta_1+c_2\beta_2+c_3\beta_3+\cdots+c_n\beta_n(c_i\in F)$와 같은 일차결합으로 표현된다.

(2) 유일성에 대하여 보이자.

$\beta=c_1\beta_1+c_2\beta_2+c_3\beta_3+\cdots+c_n\beta_n=d_1\beta_1+d_2\beta_2+d_3\beta_3+\cdots+d_n\beta_n\ (c_i,d_i\in F)$라고 하자.

그러면 $(c_1-d_1)\beta_1+(c_2-d_2)\beta_2+(c_3-d_3)\beta_3+\cdots+(c_n-d_n)\beta_n=0$이고

여기서 $\{\beta_1,\cdots,\beta_n\}$는 일차독립이므로 $c_1=d_1,c_2=d_2,\cdots,c_n=d_n$ 이다.

따라서 $\beta=c_1\beta_1+c_2\beta_2+c_3\beta_3+\cdots+c_n\beta_n(c_i\in F)$를 나타내는 방법은 유일하다.

(⇦)

V에 속하는 모든 벡터가 β_i의 일차결합으로 유일하게 표현된다고 하자.

그러면 $V=<\beta_1,\beta_2,\cdots,\beta_n>$임은 자명하다.

그러므로 $\{\beta_1,\cdots,\beta_n\}$가 일차독립임을 보이면 충분하다.

$c_1\beta_1+c_2\beta_2+c_3\beta_3+\cdots+c_n\beta_n=0=0\beta_1+0\beta_2+0\beta_3+\cdots+0\beta_n\ (c_i\in F)$이라 하자.

그러면 일차결합의 유일성에 의하여 $c_1=c_2=\cdots=c_n=0$이다.

따라서 $\{\beta_1,\cdots,\beta_n\}$는 일차독립이다.

그러므로 $\{\beta_1,\cdots,\beta_n\}$는 V에 대한 기저이다.

문 22. F**가 체일 때** n**개의 미지수를 갖는** m**개의 연립 일차방정식**

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n &= b_2 \\ &\vdots \\ a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n &= b_m \end{aligned}$$

을 생각해 보자. 단, $a_{ij}, b_i \in F$**이다.**

(a) 이 연립방정식이 해를 가질 필요충분조건은 F^m**의 벡터** $\beta = (b_1, \cdots, b_m)$**이 벡터** $a_j = (a_{1j}, \cdots, a_{mj})$**가 생성하는** F^m**의 부분공간에 속함을 보여라.**
(해의 정의에 의해 이 결과를 증명하기는 쉽지만, 실제로 연립 방정식의 공통해의 기본존재 정리를 고려해 보아야 한다.)

풀 이

– 생략함 –

(b) (a)로 부터 $n = m$**이고** $\{\alpha_j | j = 1, \cdots, n\}$**이** F^n**에 대한 기저이면 이 연립방정식은 항상 단 하나의 해를 가짐을 보여라.**

풀 이

$\{\alpha_j | j = 1, \cdots, n\}$이 F^n상의 기저이면 (문제21)에 의하여 $\{\alpha_j | j = 1, \cdots, n\}$들의 일차결합으로 유일하게 표현된다. 이는 (a)부분에 의하여 이 연립방정식이 단 하나의 해를 가짐을 의미한다.
따라서 $\{\alpha_j | j = 1, \cdots, n\}$이 F^n의 기저이면 이 연립방정식은 항상 단 하나의 해를 갖는다.

문 23. 체 F**위에서 차수가** n**인 모든 유한차수의 벡터공간은 (문제19)의** F^n**과 동형임을 증명하라.**

풀 이

체 F위에서 차수가 n인 유한차수의 벡터공간을 V라 하자.
$\{\gamma_1, \cdots, \gamma_n\}$을 V에서의 기저라고 하고 $\phi : F^n \to V, \phi(\alpha_1, \cdots, \alpha_n) = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$인 사상으로 정의하자.
그러면 F^n에서의 덧셈과 스칼라 곱셈에 대하여 다음이 성립한다.

$$\begin{aligned} \phi(\alpha + \beta) &= \phi(\alpha_1 + \beta_1, \cdots, \alpha_n + \beta_n) = \gamma_1(\alpha_1 + \beta_1) + \cdots + \gamma_n(\alpha_n + \beta_n) \\ &= (\gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n) + (\gamma_1\alpha_1 + \cdots + \gamma_n\beta_n) = \phi(\alpha_1, \cdots, \alpha_n) + \phi(\beta_1, \cdots, \beta_n) = \phi(\alpha) + \phi(\beta) \end{aligned}$$

$$a\phi(\alpha) = a\phi(\alpha_1, \cdots, \alpha_n) = a(\gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n) = \gamma_1 a\alpha_1 + \cdots + \gamma_n a\alpha_n = \phi(a\alpha_1, \cdots, a\alpha_n) = \phi(a\alpha)$$

$(\forall\, a \in F, \forall\, \alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n) \in F^n)$
$\{\gamma_1, \cdots, \gamma_n\}$는 V에서의 기저이므로 V에서의 모든 벡터는 이들의 일차결합에 의하여 나타낼 수 있다. 그러므로 ϕ는 F^n에서 V위로의 사상이다. 또한 (문제21)에 의하여 V안의 벡터는 $\{\gamma_1, \cdots, \gamma_n\}$의 유일한 일차결합으로 나타낼 수 있다. 그러므로 ϕ는 F^n에서 V로의 일대일 사상이다.
따라서 ϕ는 동형사상임을 알 수 있다.

문 24. V와 V'를 같은 체 F위에서 벡터공간이라 하자. 함수 $\phi: V \to V'$가 모든 $\alpha, \beta \in V$와 $a \in F$에 대해 다음 조건을 만족하면 ϕ를 V에서 V'로 대응하는 일차변환이라 한다.

$\phi(\alpha+\beta) = \phi(\alpha) + \phi(\beta)$

$\phi(a\alpha) = a(\phi(\alpha))$

(a) 만약 $\{\beta_i | i \in I\}$가 F위에서 V에 대한 기저이면 일차변환 $\phi: V \to V'$는 벡터 $\phi(\beta_i) \in V'$에 의해서 결정됨을 보여라.

풀 이

$\{\beta_1, \cdots, \beta_n\}$가 V위의 기저이므로

임의의 $\alpha \in V$에 대하여 $c_i \in F$가 존재해서 $\alpha = c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n$이다.

이 때, ϕ는 일차변환이므로 $\phi(\alpha) = \phi(c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n) = c_1\phi(\beta_1) + c_2\phi(\beta_2) + \cdots + c_n\phi(\beta_n)$이다.

이는 ϕ가 $\{\phi(\beta_1), \cdots, \phi(\beta_n)\}$에 의하여 결정됨을 보여준다.

따라서 일차변환 $\phi: V \to V'$는 벡터 $\phi(\beta_i) \in V'$에 의해서 결정된다.

(b) $\{\beta_i | i \in I\}$를 V에 대한 기저, 그리고 $\{\beta_i' | i \in I\}$를 V'의 서로 다를 필요가 없는 임의의 벡터들의 집합이라 하자. $\phi(\beta_i) = \beta_i'$을 만족하는 일차변환 $\phi: V \to V'$가 단 하나 존재함을 증명하라.

풀 이

- 생략함 -

문 25. V와 V'를 체 F위에서 벡터공간 그리고, $\phi: V \to V'$를 일차변환이라 하자.

(a) 군과 환의 대수적 구조에서 배운 어떤 개념이 일차변환의 개념에 대응하는가?

풀 이

벡터공간에서의 일차변환의 개념은 군에서의 준동형사상의 개념에 대응할 수 있다.

(b) ϕ의 핵(kernel)을 정의하고 그것이 V의 부분공간임을 보여라.

풀 이

ϕ의 핵의 정의는 $\ker\phi = \{v \in V | \phi(v) = 0\}$이다.

$\phi(0) = 0$이므로 $\ker\phi \neq \varnothing$이고 $\ker\phi \subseteq V$임은 자명하다. 이제 V의 부분공간임을 보이자.

(1) 임의의 $w_1, w_2 \in \ker\phi$ 에 대하여 $\phi(w_1 - w_2) = \phi(w_1) - \phi(w_2) = 0 - 0 = 0$이다.

따라서 $w_1 - w_2 \in \ker\phi$이다.

(2) 임의의 $a \in F$와 임의의 $w \in W$에 대하여 $\phi(a\omega) = a\phi(w) = a0 = 0$이다.

따라서 $a\omega \in \ker\phi$이다.

(1)과 (2)에 의하여 $\ker\phi$는 V의 부분공간이다.

(c) ϕ가 V에서 V'로 대응하는 동형사상이 될 때를 설명하라.

풀 이

ϕ가 일대일 대응인 일차변환이면 ϕ는 V에서 V'으로 대응하는 동형사상이다.

문 26. V가 체 F위에서 벡터공간, 그리고 S가 V의 부분공간이다.
잉여공간 V/S를 정의하고 그것이 F위에서 벡터공간임을 보여라.

풀 이

잉여공간 V/S는 $V/S=\{v+S \mid v\in V\}$이라고 정의할 수 있다.
그리고 잉여공간 V/S 위에 덧셈과 스칼라 곱셈을 다음과 같이 정의하자.

$(v+S)+(v'+S)=(v+v')+S$, $a(v+S)=av+S \quad (\forall v,v'\in V, \forall a\in F)$

이제 F위에서 벡터공간임을 보이자. 먼저 $(V/S,+)$는 아벨군이다. 또 위에서 정의한 스칼라 곱셈은 잘 정의된다. 즉, $v+S=v'+S \Rightarrow v-v'\in S \Rightarrow a(v-v')\in S \Rightarrow av+S=av'+S \Rightarrow a(v+S)=a(v'+S)$이다.
또한 스칼라 곱셈에 관하여 다음을 만족한다.

$a\{v+w\}=av+aw, (ab)(v)=a\{b(v)\}, (a+b)(v)=av+bv, 1v=v \quad (\forall a,b\in F, \forall v\in V/S)$

따라서 V/S는 F위에서 벡터공간이다.

문 27. V와 V'를 체 F위에서 벡터공간, 그리고 V가 F위에서 유한차원이라 하자.
$\dim V$는 F위에서 벡터공간 V의 차원을 나타내며 $\phi: V\rightarrow V'$가 일차변환이라 하자.
(a) $\phi(V)$가 V'의 부분공간임을 보여라.

풀 이

이제 $\varnothing \neq \phi(V)\subseteq V'$임은 자명하다.
이제 $\phi(V)$가 V'의 부분공간임을 보이자.
(1) $\forall w_1,w_2\in\phi(V)\ \exists v_1,v_2\in V\ s.t.\ \omega_1=\phi(v_1),\ \omega_2=\phi(v_2)$
$\Rightarrow\ \omega_1-\omega_2=\phi(v_1)-\phi(v_2)=\phi(v_1-v_2)\in\phi(V)\ \ (\because v_1-v_2\in V)$
따라서 $\omega_1-\omega_2\in\phi(V)$이다.
(2) $\forall a\in F$와 $\forall w_1\in\phi(V)\ \exists v_1\in V\ s.t.\ \omega_1=\phi(v_1)$
따라서 $aw_1\in\phi(V)$이다.
그러므로 $\phi(V)$는 V'은 부분공간이다.

(b) $\dim\phi(V)=\dim V-\dim\ker\phi$임을 보여라.
[힌트: 정리30.19에서 사용된 V에 대한 편리한 기저를 택하라.
예를 들어 $\ker\phi$에 대한 기저를 V에 대한 기저로 확대하라.]

풀 이

V가 F위의 n차원 벡터공간이라 하자.
그러면 $\dim\ker\phi=0$이면 $\ker\phi=\{0\}$이므로 $im\phi\approx V$이다.
따라서 $\dim\ker\phi=0$이면 다음이 성립한다.
$\dim\phi(V)=\dim V=n,\ \dim\phi(V)=n=n-0=\dim V-\dim\ker\phi$
그리고 $\dim\ker\phi=n$이면,
분명히 $\ker\phi=V, im\phi=\{0\}$이므로 $\dim\phi(V)=0$이고
따라서 $\dim\phi(V)=0=n-n=\dim V-\dim\ker\phi$ 이다.
이제 $im\ker\phi=m, 1\leq m\leq n$이라 하고, $\beta=\{\beta_1,\beta_2,\cdots,\beta_m\}$을 $\ker\phi$의 기저라고 하자.
이 때 β에 r개 $(r=n-m)$의 벡터 $\alpha_1,\cdots,\alpha_r$를 첨가하여
V의 기저 $\beta'=\{\beta_1,\cdots,\beta_m,\alpha_1,\cdots,\alpha_r\}$을 얻을 수 있다.
이제 $\{\phi(\alpha_1),\cdots,\phi(\alpha_r)\}$가 $im\phi$의 기저임을 증명한다.
먼저 $\phi(\beta_1)=\cdots=\phi(\beta_m)=0$이므로
$im\phi=\langle\phi(\beta_1),\cdots,\phi(\beta_m),\phi(\alpha_1),\cdots,\phi(\alpha_r)\rangle=\langle\phi(\alpha_1),\cdots,\phi(\alpha_r)\rangle$이다.

다음에 $c_1\phi(\alpha_1)+\cdots+c_r\phi(\alpha_r)=0$이라고 가정하면 $\phi(c_1\alpha_1+\cdots+c_r\alpha_r)=0$

즉, $c_1\alpha_1+\cdots+c_r\alpha_r\in\ker\phi$이므로 적당한 $d_1,\cdots,d_m\in F$에 대하여

$c_1\alpha_1+\cdots+c_r\alpha_r=d_1\beta_1+\cdots+d_m\beta_m$으로 나타내어진다.

그런데 위의 등식에 의하여 $(-c_1)\alpha_1+\cdots+(-c_r)\alpha_r+d_1\beta_1+\cdots+d_m\beta_m=0$이고

β'는 V의 기저이므로 $c_1=\cdots=c_r=d_1=\cdots=d_m=0$이다.

따라서 $\phi(\alpha_1),\cdots,\phi(\alpha_r)$는 일차독립이다.

그러므로 $\{\phi(\alpha_1),\cdots,\phi(\alpha_r)\}$는 $im\phi$의 기저이고 $\dim\phi(V)=r$이다.

따라서 $\dim\phi(V)=r=n-m=\dim V-\dim\ker\phi$이다.

※ 문제 1~13에서 주어진 확대체의 차원과 기저를 구하라.

문 1. Q**위에서** $Q(\sqrt{2})$

풀 이

주어진 확대체의 차원은 $irr(\sqrt{2}, Q) = x^2 - 2$이므로 $[\sqrt{2}, Q] = \deg irr(\sqrt{2}, Q) = 2$이다.
또한 주어진 확대체에서의 기저는 $\{1, \sqrt{2}\}$이다.

문 2. Q**위에서** $Q(\sqrt{2}, \sqrt{3})$

풀 이

$[\sqrt{2}, \sqrt{3} : Q] = [\sqrt{2} + \sqrt{3} : Q]$이므로
주어진 확대체의 최소차 다항식은 $irr(\sqrt{2} + \sqrt{3}, Q) = x^4 - 10x^2 + 1$이다.
따라서 $[\sqrt{2} + \sqrt{3} : Q] = 4$이다. 또한, 이 때 기저는 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$이다.

문 3. Q**위에서** $Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$

풀 이

주어진 확대체의 기저는 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$이므로
확대체의 차수는 $[\sqrt{2}, \sqrt{3}, \sqrt{5} : Q] = 8$이다.

문 4. Q**위에서** $Q(\sqrt[3]{2}, \sqrt{3})$

풀 이

Q 위에서 $Q(\sqrt[3]{2})$의 기저는 $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$이고, $Q(\sqrt[3]{2})$ 위에서 $Q(\sqrt[3]{2}, \sqrt{3})$의 기저는 $\{1, \sqrt{3}\}$이므로 Q 위에서 $Q(\sqrt[3]{2}, \sqrt{3})$의 기저는 $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}, \sqrt{3}, \sqrt[3]{2}\sqrt{3}, \sqrt[3]{2^2}\sqrt{3}\}$이다.
이 때 차원은 $[\sqrt[3]{2}, \sqrt{3} : Q] = 6$이다.

문 5. Q**위에서** $Q(\sqrt{2}, \sqrt[3]{2})$

풀 이

Q 위에서 $Q(\sqrt{2})$의 기저는 $\{1, \sqrt{2}\}$이고 $Q(\sqrt{2})$ 위에서 $Q(\sqrt{2}, \sqrt[3]{2})$의 기저는 $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$이므로 Q 위에서 $Q(\sqrt{2}, \sqrt[3]{2})$의 기저는 $\{1, \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{2^2}, \sqrt{2}\sqrt[3]{2}, \sqrt{2}\sqrt[3]{2^2}\}$이다.
이 때, 차원은 $[\sqrt{2}, \sqrt[3]{2} : Q] = 6$이다.

문 6. Q**위에서** $Q(\sqrt{2} + \sqrt{3})$

풀 이

$[\sqrt{2}, \sqrt{3} : Q] = [\sqrt{2} + \sqrt{3} : Q]$이므로
주어진 확대체의 최소차 다항식은 $irr(\sqrt{2} + \sqrt{3}, Q) = x^4 - 10x^2 + 1$이다.
따라서 $[\sqrt{2} + \sqrt{3} : Q] = 4$이다. 또한, 이 때 기저는 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$이다.

문 7. Q**위에서** $Q(\sqrt{2}\,\sqrt{3})$

풀 이

$Q(\sqrt{2}\,\sqrt{3}) = Q(\sqrt{6})$이므로 $irr(\sqrt{6}, Q) = x^2 - 6$이므로 차원은 $[\sqrt{6}: Q] = 2$이다.
또한 기저는 $\{1, \sqrt{6}\}$이다.

문 8. Q**위에서** $Q(\sqrt{2}, \sqrt[3]{5})$

풀 이

Q 위에서 $Q(\sqrt{2})$의 기저는 $\{1, \sqrt{2}\}$이고 $Q(\sqrt{2})$ 위에서 $Q(\sqrt{2}, \sqrt[3]{5})$의 기저는 $\{1, \sqrt[3]{5}, \sqrt[3]{5^2}\}$이므로
Q 위에서 $Q(\sqrt{2}, \sqrt[3]{5})$의 기저는 $\{1, \sqrt{2}, \sqrt[3]{5}, \sqrt[3]{5^2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{5^2}\}$이다.
이 때, 차원은 $[\sqrt{2}, \sqrt[3]{5}: Q] = 6$이다.

문 9. Q**위에서** $Q(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24})$

풀 이

$[Q(\sqrt[3]{2}): Q] = 3$, $[Q(\sqrt[3]{6}, \sqrt[3]{2}), Q(\sqrt[3]{2})] = 3$ 그리고 $[Q(\sqrt[3]{24}, \sqrt[3]{6}, \sqrt[3]{2}): Q(\sqrt[3]{6}, \sqrt[3]{2})] = 1$이다.
따라서 $[Q(\sqrt[3]{24}, \sqrt[3]{6}, \sqrt[3]{2}): Q] = 3 \cdot 3 \cdot 1 = 9$이다.
이 때 기저는 $\{1, \sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{4}, \sqrt[3]{6}, \sqrt[3]{9}, \sqrt[3]{12}, \sqrt[3]{18}, \sqrt[3]{36}\}$이다.

문 10. $Q(\sqrt{3})$**위에서** $Q(\sqrt{2}, \sqrt{6})$

풀 이

$Q(\sqrt{2}, \sqrt{6}) = Q(\sqrt{2}, \sqrt{3})$이므로 $Q(\sqrt{3})$ 위에서 $Q(\sqrt{2}, \sqrt{6})$ 의 차원은 $[Q(\sqrt{2}, \sqrt{6}): Q(\sqrt{3})] = 2$
이고 이때 기저는 $\{1, \sqrt{2}\}$이다.

문 11. $Q(\sqrt{3})$**위에서** $Q(\sqrt{2} + \sqrt{3})$

풀 이

$Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$이므로 $Q(\sqrt{3})$ 위에서 $Q(\sqrt{2} + \sqrt{3})$의 차원은 $[Q(\sqrt{2} + \sqrt{3}): Q(\sqrt{3})] = 2$
이고 이때 기저는 $\{1, \sqrt{2}\}$이다.

문 12. $Q(\sqrt{2} + \sqrt{3})$**위에서** $Q(\sqrt{2}, \sqrt{3})$

풀 이

$Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$이므로 $[Q(\sqrt{2}, \sqrt{3}): Q(\sqrt{2} + \sqrt{3})] = 1$이고 이때 기저는 $\{1\}$이다.

문 13. $Q(\sqrt{3} + \sqrt{5})$**위에서** $Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$

풀 이

$Q(\sqrt{2}, \sqrt{6} + \sqrt{10}) = Q(\sqrt{2}, \sqrt{2}(\sqrt{3} + \sqrt{5})) = Q(\sqrt{2}, \sqrt{3} + \sqrt{5}) = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$이고
$Q(\sqrt{3} + \sqrt{5}) = Q(\sqrt{3}, \sqrt{5})$이므로 $Q(\sqrt{3} + \sqrt{5})$ 위에서 $Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$의 차원은
$[Q(\sqrt{2}, \sqrt{6} + \sqrt{10}): Q(\sqrt{3} + \sqrt{5})] = 2$이고 이때 기저는 $\{1, \sqrt{2}\}$이다.

※14~17 correct the definition of the italicized term without reference to the text. if correction. so that it is in a form acceptable for publication.

문 14. An *algebraic extension* filed F is a field $F(\alpha_1,\cdots,\alpha_n)$ where each α_i is a zero of some polynomial in $F[x]$.

풀 이

체 F의 대수적 확대체는 $F(\alpha_1,\cdots,\alpha_n)$에서 각각의 α_i가 $\alpha_i=0$인 $F[x]$에서의 어떤 다항식을 갖는다???
⇒ 번역이 미숙하여 이해 못함. ㅜ

문 15. A *finite extension field* of a field F is one that can be obtained by adjoining a finite number of elements to F.

풀 이

체 F의 *유한확대체*는 F에 유한번의 원소를 첨가하여 얻을 수 있는 체이다.
⇒ 맞는 정의인 듯!!
보충 설명하자면 유한확대체는 대수적확대체이고 차원이 유한차원이므로 유한개의 원소를 첨가하여 얻을 수 있는 단순확대체 이기도 하다.

문 16. *An algebraic closure $\overline{F_E}$ of a field F in an extension field E of F* is the field consisting of all elements of E that are algebraic over F.

풀 이

*체 F의 확대체 E라 할 때, F의 대수적 폐체 $\overline{F_E}$*는 F위에서 대수적인 E의 모든 원소로 이루어진 체이다.
⇒ 맞는 정의인 듯!!!

문 17. A field F is *algebraically closed* iff every polynomial has a zero in F.

풀 이

체 F가 *대수적으로 닫혀 있을* 필요충분조건은 F위에서 모든 다항식이 영점을 갖는 것이다.
⇒ 모든 다항식이 영점을 갖는 것이 아니라. 일차 이상의 다항식이 영점을 갖는 것이다. 그러므로 옳은 정의로는 체 F가 *대수적으로 닫혀 있을* 필요충분조건은 F위의 상수가 아닌 모든 다항식이 근을 갖는 것이다.

문 18. 체 F의 확대체 E에 대하여 E에서 F의 대수적 폐포가 대수적으로 닫혀 있을 필요가 없음을 예를 들어 보아라. 단, $E\neq F$이다.

풀 이

$F=Q$, $E=Q(\sqrt{2})$이라고 하자.
그러면 $Q(\sqrt{2})$에서 Q의 대수적 폐포이지만 x^2+1은 $Q(\sqrt{2})$에서 근을 갖지 않는다.
즉, 대수적으로 닫혀있지 않다.

문 19. 참, 거짓을 판정하라.

(a) 체의 모든 유한확대체는 대수적 확대체이다.

풀 이 T

체 F의 임의의 유한확대체를 E라 하자. 그러면 $\exists n \in N \; s.t. \; [E:F]=n$

임의의 $\alpha \in E$에 대하여 $1, \alpha, \alpha^2, \cdots, \alpha^n$은 $n+1$개의 원소이므로 일차종속이다.

그러면 $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$ (적어도 한 k에 대하여 $c_k \neq 0$)인 $c_i \in F$가 존재한다.

이제 $f(x) = c_0 + c_1x + \cdots + c_nx^n$이라 하자. 그

러면 $f(x) \neq 0$인 체 F위의 다항식이고 $f(\alpha) = 0$이므로 $\deg f(x) \geq 1$이다.

따라서 α는 체 F 위에서 대수적이다.

그러므로 E는 체 F 위의 대수적확대체이다.

(b) 체의 모든 대수적 확대체는 유한확대체이다.

풀 이 F

Q위에서 R는 대수적확대체이지만 Q 위에서 R은 유한확대체가 아니다.

(c) 체의 유한확대체들의 유한 탑에서 맨 위의 체는 맨 아래 체의 유한 확대체이다.

풀 이 T

$F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$이 체라고 하고 각 $i = 1,2,\cdots,n$에 대하여 F_{i+1}은 F_i의 유한확대체라고 하자.

그러면 $[F_n : F_1] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_2 : F_1]$이 성립하므로 F_n 은 F_1의 유한확대체임을 알 수 있다.

(d) R는 대수적으로 닫혀 있다.

풀 이 F

x^2+1은 체 R 위에서 근이 존재하지 않는다. 그러므로 R은 대수적으로 닫혀 있지 않다.

(e) Q는 자신이 R에서 대수적 폐포이다. 즉, Q는 R에서 대수적으로 닫혀 있다.

풀 이 F

R가 Q의 대수적 폐포라고 하자. 하지만 x^2+1은 Q위에서의 다항식이지만 R위에서 해가 존재하지 않는다. 이는 대수적으로 닫혀 있음에 모순된다. 따라서 R은 Q의 대수적 폐포가 아니다.

(f) C는 $C(x)$에서 대수적으로 닫혀 있다. 단, x는 부정원이다.

풀 이 T

C는 대수적 폐체임은 자명하다. 이제 $f(x) \in C(x) \; s.t. \deg f(x) \geq 1$이라 하자.

이 때, 대수학의 기본정리에 의하여 $f(x)$는 근 $\alpha \in C$에서 근을 가지므로 $(x-\alpha) | f(x)$이다.

즉, $\exists \, g(x) \in C(x) \; s.t. \; f(x) = (x-\alpha)g(x)$

여기서 $\deg g(x) = 0$이면 자명하고

$\deg g(x) \geq 1$이면 $g(x)$는 대수학의 기본정리에 의하여 근 $\beta \in C$를 가지고

이 때 $\exists \, h(x) \; s.t. \; f(x) = (x-\alpha)(x-\beta)$

이 과정을 반복함으로써 $C(x)$에서 $f(x)$는 일차인수들의 곱으로 분해된다.

따라서 C는 $C(x)$에서 대수적으로 닫혀 있다.

(g) $C(x)$는 대수적으로 닫혀 있다. 단, x는 부정원이다.

풀 이 F

반례를 찾기가 쉽지 않아서 잘 모르겠다.
다만, 어디에서 성립하는지 조건이 불명확한게 오류가능성을 내포한다는 생각이 들뿐. ㅎㅎ

(h) C가 모든 대수적 수들을 포함하기 때문에 체 $C(x)$는 대수적 폐포를 갖지 않는다.

풀 이 F

$C(x)$는 C를 대수적 폐포로 갖는다.

(i) 대수적으로 닫혀 있는 체는 표수 0이어야 한다.

풀 이 F

(반례) 모든 체는 대수적 폐포를 가지므로 Z_p에 대하여 $\overline{Z_p}$를 대수적 폐포라 하자. 그러면 $\overline{Z_p}$는 무한체이다. 하지만 표수는 p이다. 단, p는 임의의 소수

(j) E가 F의 대수적으로 닫혀 있는 확대체이면 E는 대수적 확대체이다.

풀 이 F

(반례) C는 Q의 대수적으로 닫혀 있는 확대체이지만 C는 Q의 대수적 확대체가 아니다.
(→ 문제 36번 참조)

문 20. 21. - 생략함 -

문 22. $a,b\in R$이며 $b\neq 0$에 대하여 $a+bi\in C$이면 $C=R(a+bi)$임을 보여라.

풀 이

$a,b\in R$이며 $b\neq 0$에 대하여 $R\subseteq C, a+bi\in C$이고 $R(a+bi)$는 체 R과 $a+bi$를 포함하는 최소의 체이므로 $R(a+bi)\subseteq Q$이다.
역으로 $\forall x\in C\ \exists c,d\in R\ s.t.\ x=c+di$ 그러면 $x=c+di\in R(i)=R(bi)=R(a+bi)$이다.
따라서 $C\subseteq R(a+bi)$이다.
그러므로 $C=R(a+bi)$이다.

[다른 풀이1]
$a+bi$와 $a-bi$는 R상의 다항식 $x^2-2ax+(a^2+b^2)$의 영점이다.
그래서 $x^2-2ax+(a^2+b^2)$는 R에서 영점을 갖지 않고 $\deg(x^2-2ax+(a^2+b^2))=2$ 이다.
그러면 $x^2-2ax+(a^2+b^2)$는 R위에서 기약이다. 즉, $\deg(a+bi,R)=2$
따라서 $R(a+bi)=\{a_0+a_1(a+bi)|a_i\in R\}=\{x+yi|x,y\in R\}=C$

[다른 풀이2]
$C=R(i)$는 명백하다. 즉, $[C:R]=[R(i):R]=\deg(i,R)=2$ ($\because\ irr(i,R)=x^2+1$)
그러므로 C는 R의 유한확대체이다. 한편 $a+bi\in C$이므로 $R\leq R(a+bi)\leq C$이다.
그러면 $[C:R]=[C:R(a+bi)][R(a+bi):R]$ 이 성립한다.
여기서 $[R(a+bi):R]=\deg(a+bi,R)=2$이고 $[C:R]=2$ 이다.
그러면 $[C:R(a+bi)]=1$이고 따라서 $C=R(a+bi)$

문 23. E**가 체** F**의 유한 확대체이고** $[E:F]$**가 소수이면** E**가** F**의 단순확대체이며 실제로** F**에 속하지 않는 모든** $\alpha \in E$**에 대하여** $E = F(\alpha)$**이다.**

풀 이

E가 체 F의 유한확대체라고 하고 $[E:F] = p$ (단, p는 소수)라고 하자. 그러면 $F \subsetneq E$임은 자명하다.
임의의 $\alpha \in E - F$에 대하여 $F(\alpha)$는 F의 유한확대체이고 E는 $F(\alpha)$의 유한확대체이다.
그러면 다음이 성립한다.

$p = [E:F] = [E:F(\alpha)][F(\alpha):F]$

$\Rightarrow [F(\alpha):F] = 1 \text{ or } [F(\alpha):F] = p$

$\Rightarrow \alpha \in E - F$이므로 $[F(\alpha):F] \neq 1$이다.

따라서 $[F(\alpha):F] = p$이고 이는 즉, $[E:F(\alpha)] = 1$이므로 $E = F(\alpha)$이다.

문 24. $x^2 - 3$**이** $Q(\sqrt[3]{2})$ **위에서 기약임을 보여라.**

풀 이

$irr(\sqrt[3]{2}, Q) = x^3 - 2, \deg(\sqrt[3]{2}, Q) = 3$이므로 $Q(\sqrt[3]{2})$는 Q위에서 유한확대체이다.
또한 $irr(\sqrt{3}, Q) = x^2 - 3, \deg(\sqrt{3}, Q) = 2$이므로 $Q(\sqrt{3})$는 Q위에서 유한확대체이다.
그러면 $[Q(\sqrt{3}):Q] = \deg(\sqrt{3}, Q) = 2$ 이고 $[Q(\sqrt[3]{2}):Q] = \deg(\sqrt[3]{2}, Q) = 3$ 이다.
$\sqrt{3} \in Q(\sqrt[3]{2})$라 가정하자. 그러면 $Q \leq Q(\sqrt{3}) \leq Q(\sqrt[3]{2})$이 성립한다.
$[Q(\sqrt[3]{2}):Q] = [Q(\sqrt[3]{2}):Q(\sqrt{3})][Q(\sqrt{3}):Q]$이므로 $[Q(\sqrt{3}):Q] \mid [Q(\sqrt[3]{2}):Q]$가 성립한다.
즉, $2 \mid 3$이다. 하지만 이는 모순이다. 그러므로 $\sqrt{3} \notin Q(\sqrt[3]{2})$ 이다.
그러면 $x^2 - 3$은 $Q(\sqrt[3]{2})$에서 영점을 갖지 않고 차수는 2차이다.
그러므로 $x^2 - 3$는 $Q(\sqrt[3]{2})$에서 기약이다.

문 25. F**에서 제곱수가 아닌** F**의 원소의 제곱근을 체** F**에 첨가시키고, 이렇게 하여 얻어진 새로운 체에 제곱수가 아닌 원소의 제곱근을 첨가시키는 등의 작업을 계속하여 얻어지는 확대체의 차수는 얼마인가? 이 사실에서** Q**에서** $x^4 - 3x^2 + 12$**의 근은** Q**의 원소들의 제곱근들의 유리함수, 제곱근들의 유리함수의 제곱근등등으로 표현될 수 없음을 보여라.**

풀 이

① $a_1 \in \overline{F} - F$는 어떤 $b_1 \in F$의 제곱근이라 하자. $(a_1^2 = b_1)$

그러면 a_1는 $x^2 - b_1$의 영점이다.

$a_1 \notin F$이므로 F위에서 $x^2 - b_1$는 기약이다.

그러면 $\deg(a_1, F) = 2$이고 $[F(a_1):F] = 2$이다.

② $a_2 \in \overline{F} - F(a_1)$는 어떤 $b_2 \in F(a_1)$의 제곱근이라 하자. $(a_2^2 = b_2)$

그러면 a_2는 $x^2 - b_2$의 영점이다.

$a_2 \notin F(a_1)$이므로 $F(a_1)$위에서 $x^2 - b_2$는 기약이다.

그러면 $\deg(a_2, F(a_1)) = 2$이고 $[F(a_1, a_2):F(a_1)] = 2$이다.

이제 $F \leq F(a_1) \leq F(a_1, a_2)$이므로 $[F(a_1, a_2):F] = [F(a_1, a_2):F(a_1)][F(a_1):F]$가 성립해서 위의 사실로부터 $[F(a_1, a_2):F] = 2^2$을 얻을 수 있다.

③ 위의 과정을 반복하면 $[F(a_1, a_2, \cdots, a_n):F] = 2^n$을 얻을 수 있다.

단, $a_i \in \overline{F} - F(a_1, \cdots, a_{i-1})$는 어떤 $b_i \in F(a_1, \cdots, a_{i-1})$의 제곱근이다.

따라서 제곱근에 의하여 얻을 수 있는 확대체의 위수는 어떤 $n \in N$에 대하여 2^n의 꼴이어야 한다.

④ $p=3$일 때, 아이젠스타인 판정법에 의하여 Q에서 $x^{14}-3x^2+12$는 기약이다.
그러므로 이 다항식의 임의의 근을 α라 할 때, $[Q(\alpha):Q]=14$이다.
14는 임의의 $n\in Z$에 대하여 2^n를 나누지 않는다는 사실로부터 제곱근에 의하여 얻을 수 있는 임의의 체에 놓여 있다고 볼 수 없다. 그러므로 α는 제곱근들의 유리함수, 제곱근들의 유리함수의 제곱근 등등으로 표현될 수 없다.

문 26. E가 F의 유한확대체이고 D가 $F\subseteq D\subseteq E$를 만족하는 정역이면 D가 체임을 보여라.

풀 이

우선 D가 정역이므로 단위원 1을 갖는 가환환이다.
그러면 $\alpha\in D-\{0\}$에 대하여 가역원이 존재함을 보이면 충분하다.
임의의 $\alpha\in D-\{0\}\subseteq E$에 대하여 $F(\alpha)$는 체 F위의 유한확대체이므로 대수적 확대체이다.
그러면 $\exists f(x)=a_0+a_1x+\cdots+a_nx^n\in F[x]\,s.t.\ irr(\alpha,F)=f(x)$
$a_0\neq 0$이므로 ($\because a_0=0$이면 $irr(\alpha,F)=f(x)$임에 모순이다.)

$f(\alpha)=0$으로부터 $\alpha(-\dfrac{a_1+a_2\alpha+\cdots+a_n\alpha^{n-1}}{a_0})=1$임을 알 수 있다.

그러면 $\alpha^{-1}=-\dfrac{a_1+a_2\alpha+\cdots+a_n\alpha^{n-1}}{a_0}\in D$

($\because$ $\dfrac{a_i}{a_0}\in F\subseteq D\ (i=1,2,\cdots,n)$이고 $\alpha\in D$이므로 $\alpha^i\in D(i=1,2,\cdots,n)$이다.)
따라서 가역원이 존재하므로 D는 체이다.

문 27. $Q(\sqrt{3}+\sqrt{7})=Q(\sqrt{3},\sqrt{7})$임을 상세히 증명하라.

풀 이

$\sqrt{3}+\sqrt{7}\in Q(\sqrt{3},\sqrt{7})$이므로 $Q(\sqrt{3}+\sqrt{7})\subseteq Q(\sqrt{3},\sqrt{7})$임은 자명하다.
이제 $\alpha=\sqrt{3}+\sqrt{7}$이라 하자. 그러면 $\dfrac{1}{\alpha}=\dfrac{1}{\sqrt{3}+\sqrt{7}}=\dfrac{\sqrt{7}-\sqrt{3}}{4}$이므로 $\dfrac{4}{\alpha}=\sqrt{7}-\sqrt{3}$이다.
또한 다음이 성립한다.

$$\sqrt{7}=\frac{1}{2}\left(\alpha+\frac{4}{\alpha}\right)\in Q(\sqrt{3}+\sqrt{7}),\ \ \sqrt{3}=\frac{1}{2}\left(\alpha-\frac{4}{\alpha}\right)\in Q(\sqrt{3}+\sqrt{7})$$

따라서 $Q(\sqrt{3},\sqrt{7})$은 체 Q와 $\sqrt{3},\sqrt{7}$을 포함하는 최소의 체이므로 $Q(\sqrt{3}+\sqrt{7})\supseteq Q(\sqrt{3},\sqrt{7})$이다. 그러므로 $Q(\sqrt{3}+\sqrt{7})=Q(\sqrt{3},\sqrt{7})$이다.

문 28. 문제27을 일반화하여
Q에 속하는 모든 a,b에 대하여 $\sqrt{a}+\sqrt{b}\neq 0$이면 $Q(\sqrt{a}+\sqrt{b})=Q(\sqrt{a},\sqrt{b})$임을 증명하라.
[힌트: $(\sqrt{a}+\sqrt{b})^2$을 계산하라.]

풀 이

임의의 $a,b\in Q$에 대하여 $a=b$이면 자명하다. 그러므로 $a\neq b$인 경우에 성립함을 보이면 충분하다.
$\sqrt{a}+\sqrt{b}\in Q(\sqrt{a},\sqrt{b})$이므로 $Q(\sqrt{a}+\sqrt{b})\subseteq Q(\sqrt{a},\sqrt{b})$임은 자명하다.
이제 $\alpha=\sqrt{a}+\sqrt{b}$이라 하자. 그러면 $\dfrac{1}{\alpha}=\dfrac{1}{\sqrt{a}+\sqrt{b}}=\dfrac{\sqrt{a}-\sqrt{b}}{a^2-b^2}$이므로 $\dfrac{a^2-b^2}{\alpha}=\sqrt{a}-\sqrt{b}$이다.
또한 다음이 성립한다.

$\sqrt{a}=\frac{1}{a^2-b^2}\left(\alpha+\frac{a^2-b^2}{\alpha}\right)\in Q(\sqrt{a}+\sqrt{b})$, $\sqrt{b}=\frac{1}{a^2-b^2}\left(\alpha-\frac{a^2-b^2}{\alpha}\right)\in Q(\sqrt{a}+\sqrt{b})$

따라서 $Q(\sqrt{a},\sqrt{b})$은 체 Q와 $\sqrt{a},\sqrt{b}$을 포함하는 최소의 체이므로 $Q(\sqrt{a}+\sqrt{b})\supseteq Q(\sqrt{a},\sqrt{b})$이다. 그러므로 $Q(\sqrt{a}+\sqrt{b})=Q(\sqrt{a},\sqrt{b})$이다.

문 29. E가 체 F의 유한확대체이고 $p(x)\in F[x]$가 F위에서 기약이고, $[E:F]$의 약수가 아닌 차수를 갖는다면 $p(x)$는 E에서 근을 가질 수 없음을 보여라.

풀 이

$p(x)$가 E에서 근을 갖는다고 가정하여 모순됨을 보이자.

$p(x)$가 E에서 근을 갖는다고 가정하자. 즉, $\exists\,\alpha\in E\ s.t.\ p(\alpha)=0$

주어진 가정에 의하여 $p(x)$는 F위에서 기약이므로 $irr(\alpha,F)=p(x)$이고 따라서 $F(\alpha)$는 F 위의 유한확대체이다. 그러면 $F\subseteq F(\alpha)\subseteq E$이므로 $[F(\alpha):F]\,|\,[E:F]$이다.

하지만 이는 $[F(\alpha):F]=\deg p(x)\nmid[E:F]$인 가정에 모순이다.

따라서 $p(x)$는 E에서 근을 가질 수 없다.

문 30. E가 체 F의 유한확대체이고 $\alpha\in E$가 F위에서 홀수 차수를 갖는 대수적 원소이면 α^2도 F위에서 홀수 차수를 갖는 대수적 원소이고 $F(\alpha)=F(\alpha^2)$임을 보여라.

풀 이

α가 F위에서 대수적이면 α^2이 F 위에서 대수적임은 자명하다. 그리고 $\alpha^2\in F(\alpha)$이므로 $F(\alpha^2)\subseteq F(\alpha)$임이 자명하다. 이제 $F(\alpha^2)\supseteq F(\alpha)$임을 보이면 충분하다. 주어진 가정에 의하여

$\deg irr(\alpha,F)=2n-1\,(n\in N)$이므로 $\exists f(x)=a_0+a_1x+\cdots+a_{2n-1}x^{2n-1}\ s.t.\ irr(\alpha,F)=f(x)$

$f(\alpha)=a_0+a_1\alpha+\cdots+a_{2n-1}\alpha^{2n-1}=0$

$\Rightarrow\ \alpha(a_1+a_3(\alpha^2)+\cdots+a_{2n-1}(\alpha^2)^{n-1})+(a_0+a_2(\alpha^2)+\cdots+a_{2n-2}(\alpha^2)^{n-1})=0$

$\Rightarrow\ \alpha=-\frac{a_0+a_2(\alpha^2)+\cdots+a_{2n-2}(\alpha^2)^{n-1}}{a_1+a_3(\alpha^2)+\cdots+a_{2n-1}(\alpha^2)^{n-1}}\in F(\alpha^2)$

$F(\alpha)$는 체 F와 α를 포함하는 최소의 체이므로 $F(\alpha^2)\supseteq F(\alpha)$이다. 따라서 $F(\alpha)=F(\alpha^2)$이다.

[다른풀이]

$F(\alpha)\neq F(\alpha^2)$이라 가정하여 모순됨을 보이자. $f(x)=x^2-\alpha^2$은 $F(\alpha^2)$위에서 기약이지만 $F(\alpha)$ 위에서 $f(\alpha)=0$이므로 기약이 아니다. 그러므로 $F(\alpha)$는 $F(\alpha^2)$의 대수적 확대체이고 $irr(\alpha,F(\alpha^2))=x^2-\alpha^2$이므로 $[F(\alpha):F(\alpha^2)]=2$이다. 그러면 $[F(\alpha):F(\alpha^2)]=2\,|\,[F(\alpha):F]$이다. 하지만 가정에서 $[F(\alpha):F]$는 홀수이므로 모순이다. 따라서 $F(\alpha)=F(\alpha^2)$이다.

문 31. E,F 그리고, K가 $F\le E\le K$를 만족하는 체이면 K가 F위에서 대수적일 필요충분조건은 E가 F위에서 대수적이고 K가 E위에서 대수적임을 보여라. (유한확대체라고 가정해서는 안된다.)

풀 이

(→) K를 F의 대수적 확대체라 하자.

그러면 임의의 $\alpha\in K$에 대하여 $f(\alpha)=0$를 만족하는 다항식 $f(x)\in F[x], f(x)\neq 0$이 존재한다.

그리고 $g(\alpha)=0$를 만족하는 다항식 $g(x)\in E[x], g(x)\neq 0$이 존재한다. 이는 K가 E의 대수적 확대체임을 보여준다. 물론 각각의 E의 원소는 또한 K의 원소이므로 E는 F의 대수적 확대체이다.

(←) 임의의 $\alpha\in K$에 대하여

K는 E의 대수적 확대체이므로 0이 아닌 다항식 $a_0+a_1x+\cdots+a_nx^n\in E[x]$이 존재해서
$a_0+a_1\alpha+\cdots+a_n\alpha^n=0$를 만족한다.
E는 F위에서 대수적이므로 a_i는 F위에서 대수적이다. $(i=1,2,\cdots,n)$
그러므로 $F(a_0,a_1,\cdots,a_n)$는 F위에서 어떤 유한위수 m을 갖는 확대체이다.
α는 E의 차수 $r\le n$를 갖는 대수적 원소이므로 $F(a_0,a_1,\cdots,a_n,\alpha)$는 차수 $\le mr$를 갖는 F의 유한확대체이다. 따라서 유한확대체는 대수적확대체이므로 α는 F위에서 대수적이다.

문 32. E가 체 F의 확대체라면 E에서 F의 대수적 폐포 $\overline{F_E}$에 속하지 않는 모든 $\alpha\in E$는 $\overline{F_E}$위에서 초월적임을 증명하라.

풀 이

결론을 부정하여 α를 $\overline{F_E}$위에서 대수적이라 하자.
그러면 $\overline{F_E}(\alpha)$는 $\overline{F_E}$위에서 대수적이고 정의에 의하여 $\overline{F_E}$는 F위에서 대수적이다.
문제 31에 의하여 $\overline{F_E}(\alpha)$이 F위에서 대수적이고 그래서 α는 F위에서 대수적이다.
하지만 $\alpha\in\overline{F_E}$는 가정에 모순된다. 그러므로 α는 $\overline{F_E}$위에서 초월적이다.

문 33. E가 체 F의 대수적으로 닫혀있는 확대체라면 E에서 F의 대수적 폐포 $\overline{F_E}$는 대수적으로 닫혀 있음을 보여라. (이 문제를 C와 Q에 적용하면 모든 대수적 수들의 체는 대수적으로 닫혀 있는 체임을 알 수 있다.)

풀 이

$f(x)\in\overline{F_E}[x]$라 하자.
$f(x)$가 $\overline{F_E}$에서 영점을 가짐을 보이면 충분하다.
$\overline{F_E}\subseteq E$이므로 $\overline{F_E}[x]\subseteq E[x]$이 성립하여 $f(x)\in E[x]$임을 알 수 있다.
E는 대수적으로 닫혀있는 체이므로 $\exists\,\alpha\in E\ s.t.\ f(\alpha)=0_E$
α는 $\overline{F_E}$위에서 대수적이므로 $\overline{F_E}(\alpha)$는 $\overline{F_E}$의 대수적 확대체이다.
그러면 $F\le\overline{F_E}\le\overline{F_E}(\alpha)$이고 $\overline{F_E}$는 $\overline{F_E}$의 정의에 의하여 F의 대수적확대체임에 자명하다.
$\overline{F_E}(\alpha)$는 문제 31에 의하여 F의 대수적 확대체이다.
그러므로 α는 E에서 F위의 대수적 원소이다. 그러면 $\overline{F_E}$의 정의에 의하여 $\alpha\in\overline{F_E}$이다.
그러면 $f(x)$는 $\overline{F_E}$에서 영점을 갖는다. 따라서 $\overline{F_E}$는 대수적으로 닫혀 있다.

C는 대수적으로 닫혀있는 체이고 $\overline{Q_C}$ 또한 대수적으로 닫혀있는 체이므로 $\overline{Q_C}$ 는 비자명확대체를 갖지 않는다. 하지만 $\overline{Q_C}\subsetneq C$ 이고 $\overline{Q_C}\neq R$ 이다. 그러므로 C와 R은 Q의 대수적 확대체가 아니다.

문 34. E가 체 F 의 대수적 확대체이며 모든 $f(x)\in F[x]$의 $\overline{F}$에 속하는 근들을 포함한다면 E가 대수적으로 닫혀 있는 체임을 보여라.

풀 이

$\alpha\in E$ 이고 $p(x)=irr(\alpha,F)$는 차수 n을 갖는다고 하자.
$p(x)$는 $\overline{F}[x]$에서 $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$으로 인수분해된다.
가정에 의하여 $\overline{F}$에서 $p(x)$는 모든 영점을 가지므로 또한 E에서도 성립한다.
즉, $E[x]$에서 또한 같은 인수분해가 나타난다.

그러므로 $p(\alpha)=(\alpha-\alpha_1)(\alpha-\alpha_2)\cdots(\alpha-\alpha_n)=0$이고 따라서 어떤 i에 대하여 $\alpha=\alpha_i$를 만족한다.

이로부터 $F\leq E\leq \overline{F}$임을 알 수 있다.

$\overline{F}$의 정의로부터 F와 E의 대수적인 원소를 모두 포함한다.

즉, $E=\overline{F}$이고 그러므로 대수적으로 닫혀있음을 알 수 있다.

문 35. 홀수표수를 갖는 유한체는 대수적으로 닫혀 있지 않음을 보여라.
(실제로 표수 2인 유한체도 대수적으로 닫혀 있지 않다.)
[힌트: 헤아림에 의해서 그런 유한체 F에 대해서 어떤 다항식 x^2-a는 F에서 근을 가질 수 없다. 단 , $a\in F$이다. 29장의 문제32 참조]

풀 이

F를 홀수표수를 갖는 유한체라 하자. 그러면 F위에서 $1\neq -1$이다.

$1^2=(-1)^2=1$이므로 F의 제곱근의 원소는 기껏해야 F상의 $|F|-1$개의 원소이다.

그러면 어떤 $a\in F$가 존재해서 제곱근이 아님을 알 수 있다.

그러므로 다항식 x^2-a는 F위에서 영점을 갖지 않는다.

따라서 F는 대수적으로 닫혀있지 않음을 알수 있다.

[참고]

위의 사실로부터 유한체는 대수적으로 닫혀있지 않음을 알 수 있다.

만약 Z_p의 대수적 확대체 $\overline{Z_p}$라고 하면 $\overline{Z_p}$는 무한체이다.

문 36. 본문에서 설명했듯이 C에서 Q의 대수적 폐포는 Q의 유한확대체가 아님을 증명하라.

풀 이

① 임의의 $n\in N$와 $n\geq 2$에 대하여 x^n-2는 Q위에서 $p=2$일 때, $Eisenstein$ 판정법에 의하여 기약이다. 그러면 임의의 $n\in N$와 $n\geq 2$에 대하여 $\exists F\leq C\ s.t.\ F$는 Q의 유한확대체이다.

② F를 Q의 유한확대체라 하자.

그러면 F는 Q의 대수적 확대체이다.

$\overline{Q_C}$는 Q의 대수적 폐포이므로 $\overline{Q_C}$는 Q의 최대의 대수적확대체이다.

그러면 Q의 모든 대수적확대체는 $\overline{Q_C}$에 포함된다.

따라서 $F\leq \overline{Q_C}$이다.

③ $\overline{Q_C}$가 Q의 유한확대체라 가정하자.

그러면 $\exists m\in N\ s.t.\ \left[\overline{Q_C}:Q\right]=m$

이제 ①에 의하여 임의의 $n>m$에 대하여 $\exists F\leq C\ s.t.\ F$는 $[F:Q]=n$인 Q의 유한확대체이다.

그러면 ②에 의하여 $Q\leq F\leq \overline{Q_C}$가 성립한다.

그러므로 $\left[\overline{Q_C}:Q\right]=\left[\overline{Q_C}:F\right][F:Q]$이 성립해서 $[F:Q]\mid\left[\overline{Q_C}:Q\right]$이므로 $n\mid m$이다.

이는 모순이다.

따라서 $\overline{Q_C}$는 Q의 유한확대체가 아니다.

문 37. R의 모든 유한 확대체는 R 자신이나 C와 동형임을 증명하라.

풀 이

R의 유한확대체를 E라 하면 E는 대수적 확대체이므로 $\exists\,\alpha\in C\,s.t.\ E=R(\alpha)$

그러면 $[C:R]=[C:R(\alpha)][R(\alpha):R]$이 성립한다. ($\because C$는 대수적 폐체이므로 $R(\alpha)$는 C의 부분체이다)

한편, $[C:R]=2$이고 2는 소수이므로 $C=R(\alpha)=E$ or $R=R(\alpha)=E$이다.

따라서 R의 확대체는 R자신이거나 C와 동형이다.

문 38. $Zorn$의 보조정리를 이용하여 단위원을 갖는 환 R의 모든 진부분 아이디얼은 어떤 극대아이디얼에 속함을 증명하라.

풀 이

R를 단위원 1_R를 가진환, N을 R의 진부분 아이디얼이라 하자.

그러면 $N\subseteq M$을 만족하는 어떤 R의 극대아이디얼 M이 존재함을 보인다.

$S=\{M\lhd R \mid M\neq R, N\subseteq M\}$이라 하자. $N\in S$이므로 $S\neq\varnothing$이다.

$M_1, M_2\in S$에 대하여 $M_1\leq M_2$이면 $M_1\subseteq M_2$라 정의하자.

그러면 $(S,\leq)$는 일부분은 순서집합이다.

T를 S에서 연쇄라 하자. 즉, T는 S의 전체적인 순서부분집합이다.

이제 $W=\bigcup_{I\in T} I$ 라 놓자. 앞으로 W가 S에서 T의 상계임을 보이면 충분하다.

$a,b\in W$와 $r\in R$에 대하여 $\exists\,H,K\in T\ s.t.\ a\in H\ \wedge\ b\in K$

T는 S에서 연쇄이므로 $H\subseteq K$ 또는 $K\subseteq H$이다.

① $H\subseteq K$일 때,

$a,b\in K$에 대하여 $K\lhd R$이므로 $a\pm b, ab, ra, ar\in K$이다.

그러면 $a\pm b, ab, ra, ar\in\bigcup_{I\in T} I=W$이 성립해서 $W\lhd R$이다.

② $K\subseteq H$일 때,

$a,b\in H$에 대하여 $H\lhd R$이므로 $a\pm b, ab, ra, ar\in H$이다.

그러면 $a\pm b, ab, ra, ar\in\bigcup_{I\in T} I=W$이 성립해서 $W\lhd R$이다.

이제 ①과 ②에 의하여 $W\lhd R$이다. 즉, W는 R의 아이디얼이다.

모든 $I\in T$에 대하여 I는 R의 진부분 아이디얼이므로 모든 $I\in T$에 대하여 I는 R의 진부분집합이다.

그러면 W 또한 R의 진부분집합이다. 그러므로 W 또한 R의 진부분아이디얼이다.

모든 $I\in T$에 대하여 $T\subseteq S, N\subseteq I$ 이므로 $N\subseteq\bigcup_{I\in T} I=W$ 이 성립한다. 따라서 W는 N을 포함하는 R의 진부분 아이디얼이므로 $W\in S$이다.

모든 $I\in T$에 대하여 $W=\bigcup_{I\in T} I,\ I\subseteq W$이므로 모든 $I\in T$에 대하여 $I\leq W$ 이다.

따라서 W는 S에서 T의 상계이다.

그러므로 $Zorn$의 보조정리에 의하여 S에서 극대인 $M\in S$이 존재한다.

$N\subseteq M$임에 명백하다. 이제 M이 R의 극대아이디얼임을 보이자.

$M\lhd K\lhd R$이고 $K\neq R$이라 하자.

$N\subseteq M,\ M\lhd K$이고 $K\neq R$ 이므로 K는 N을 포함하는 R의 진부분 아이디얼이다. 그러므로 $K\in S$이다.

M은 S에서 극대이므로 $K\leq M$이다. 이는 위의 정의에 의하여 $K\subseteq M$이다. 따라서 $K=M$이다.

그러므로 M은 N을 포함하는 R의 극대아이디얼이다.

문 1. Prove the trigonometric identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ from the Euler formula, $e^{i\theta} = \cos\theta + isin\theta$

풀 이

$e^{i\theta} = \cos\theta + isin\theta$로부터

$\cos 3\theta + isin3\theta = e^{i3\theta} = (e^{i\theta})^3 = (\cos\theta + isin\theta)^3 = \cos^3\theta + 3icos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta$

$\leftrightarrow \cos 3\theta + isin3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta + i(3\cos^2\theta\sin\theta - \sin^3\theta)$

실수부는 실수부끼리 허수부는 허수부끼리 동치이므로 다음이 성립한다.

$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta,\ \sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta$

위의 사실로부터 실수부끼리 비교하면 다음과 같다.

$\cos 3\theta = \cos^3\theta - 3\cos\theta(1 - \cos^2\theta) = 4\cos^3\theta - 3\cos\theta$

따라서 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$인 사실을 유도 할 수 있다.

문 2. 참, 거짓을 판정하라.

(a) 자와 콤파스로서 어떤 작도 가능한 크기의 모서리를 갖는 정육면체를 2배하는 것은 불가능하다.

풀 이 T

(b)가 참이므로 특수한 경우의 (a)도 참이다.

(b) 자와 콤파스로서 모든 작도 가능한 크기의 모서리를 갖는 정육면체를 2배하는 것은 불가능하다.

풀 이 T

모든 작도 가능한 크기의 모서리를 갖는 정육면체는 결국 단위 길이인 1에 대해서 작도 가능하기 때문에 단위 길이에 대해서만 성립함을 보이면 충분하다.

주어진 정육면체의 한 모서리의 길이를 1이라고 하면, 이 정육면체의 부피는 1이다. 따라서 그 2배의 부피를 가지는 정육면체의 한 모서리의 길이는 $\sqrt[3]{2}$이다. 한편, $irr(\sqrt[3]{2}, Q) = x^3 - 2$이므로 $[\sqrt[3]{2}: Q] = 3$인데 3은 2의 거듭제곱이 아니므로 [보조정리 32.8]에 의하여 $\sqrt[3]{2}$는 작도불가능이다.

(c) 자와 콤파스작도로서 작도가능한 반경을 갖는 원과 같은 면적을 갖는 정사각형은 작도불가능하다.

풀 이 T

주어진 원의 반지름의 길이를 1이라고 하면 그 원의 넓이는 π이다. 따라서 작도하려면 정사각형의 한 변의 길이는 $\sqrt{\pi}$이다. 만일 $\sqrt{\pi}$가 작도가능하다고 가정하면, [정리 32.6]과 [보조정리 32.8]에 의하여 $\sqrt{\pi}$는 유리수체 Q위에서 대수적이어야 하고, $(\sqrt{\pi})^2$ 도 Q위에서 대수적이어야 한다. 그러나 이것은 π가 Q위에서 초월적이라는 사실에 모순이다. 따라서 작도불가능하다.

(d) 어떤 작도 가능한 각도 자와 콤파스로서 삼등분할 수 없다.

풀 이 F

크기가 θ인 각을 작도하는 것은 실수 $\cos\theta$를 작도하는 것과 같다.

$\alpha = \cos\theta, \beta = \cos 3\theta$라 하면

β는 조건에서 작도가능이므로 $\exists k \in N\ s.t.\ [\beta: Q] = 2^k$이고

$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$인 사실로부터 $irr(\alpha, Q(\beta)) = 4x^3 - 3x - \beta$이고 $[\alpha: Q(\beta)] = 3$이다.

그러면 유한확대체의 성질로 부터 $[\alpha:Q]=[\alpha:Q(\beta)][Q(\beta):Q]=3\cdot 2^k$임을 알 수 있고,
따라서 [보조정리 32.8]에 의하여 차수가 2의 거듭제곱이 아니므로 작도불가능하다.

(e) 모든 작도가능한 수는 적당한 $r\geq 0$에 대해서 Q위에서 차수 2^r을 갖는다.

풀 이 T

실수 u가 작도가능하면, [정리 32.6]에 의하여 다음 조건을 만족시키는 양의 실수 $\alpha_1,\cdots,\alpha_n$이 존재한다.

$\alpha_1\in Q=F_0,\ \alpha_i\in Q(\sqrt{\alpha_1},\cdots,\sqrt{\alpha_{i-1}})=F_{i-1}\ (2\leq i\leq n),\qquad u\in Q(\sqrt{\alpha_1},\cdots,\sqrt{\alpha_n})=F_n$

이 때, $[F_n:Q]=[F_n:F_{n-1}][F_{n-1}:F_{n-2}]\cdots[F_2:F_1][F_1:F_0]$이고 각 i에 대하여 $[F_i:F_{i-1}]=1\text{ or }2$이므로 $[F_n:Q]=2^k\ (k\geq 0)$이다. 한편 $u\in F_n$이므로 $Q(u)\subseteq F_n$, $[Q(u):Q]\mid[F_n:Q]$이다.
그런데 $[u:Q]=[Q(u):Q]$이므로 $[u:Q]\mid 2^k$이고 따라서 적당한 정수 $r\geq 0$에 대하여 $[u:Q]=2^r$이다.

(f) 적당한 정수 $r\geq 0$에 대해서 Q위에서 2^r의 차수를 갖는 모든 실수는 작도 가능이다.

풀 이 T

실수 α에 대하여 가정에 의하여 다음이 성립한다고 하자.

$\exists r\in N\ s.t.\ [Q(\alpha):Q]=2^r$

그러면 갈로아 정리에 의하여 $[Gal(Q(\alpha)/Q)]=2^r$이다.
군의 위수가 2^r이면 실로의 정리에 의하여
$0\leq n\leq r$인 모든 $n\in N$에 대하여 위수가 2^n인 부분군이 존재한다.
따라서 다음과 같은 군의 열을 생각할 수 있다.

$$\{e\}<H_1<H_2<\cdots<H_{n-1}<H_n=Gal(Q(\alpha)/Q)$$

H_n의 위수는 2^r 이며 H_{n-1}의 위수는 2^{r-1}이고, … , H_1의 위수는 2이다.
갈루아 정리에 의해 이러한 부분체는 갈루아군의 부분군과 일대일 대응이 되며 다음과 같다.

$$\{e\}<H_1<H_2<\cdots<H_{n-1}<H_n=Gal(Q(\alpha)/Q)$$
$$Q(\alpha)<Fix(H_1)<Fix(H_2)<\cdots<Fix(H_{n-1})<Fix(H_n)=Q$$

그리고 각각의 체의 차수는 모두 2가 된다.
Q로부터 2의 차수를 가진 확대체는 모두 작도 가능 수이므로 이를 유한 번 올라가게 되면 $Q(\alpha)$ 역시 작도가능수의 집합이 된다. 따라서 α 역시 작도 가능하게 된다.

(g) Z가 UFD라는 사실이 정리 32.9과 32.11의 결론을 유도하는데 유용하게 되었다.

풀 이 T

UFD라는 사실은 정리 32.9와 32.11의 Q위에서의 최소 다항식의 기약성을 판단하기 위해 사용되었다.

(h) 헤아림에 의한 증명방법은 아주 중요하게 쓰이는 증명방법이다.

풀 이 T

일례로 정 n각형 등의 작도 가능성을 확인하기 위해서도 헤아림에 의한 증명방법은 중요하다.

(i) 임의의 작도가능한 수는 단위 길이로 주어진 선분에서 시작하여 자와 콤파스를 유한 번 사용하여 얻을 수 있다.

풀 이 T

작도가능한 수의 정의에 의하여 자명하다.

(j) 주어진 단위길이의 선분으로부터 미리 한정된 횟수만큼 자와 콤파스를 사용하여 작도가능한 전체수를 찾을 수 있다.

풀 이 F

한정된 횟수만큼 자와 콤파스를 사용하여 작도 가능한 전체수를 찾을 수 있다고 가정하자.
그러면 Q가 작도가능한 수이므로 한정된 횟수로 표현이 가능하다.
이는 곧 Q가 유한개의 원소를 가짐을 뜻하고 이는 모순이다.
따라서 한정된 횟수로 전체수를 찾을 수 없다.

문 3. 정리 32.11을 이용하여 정9-각형은 작도 불가능함을 보여라.

풀 이

정 9-각형이 작도가능이라고 하자. 그러면 한 내각 40° 도 작도가능이다.
그러면 [정리 32.11]에 의하여 20° 도 작도가능이다.
한편, 정 3-각형은 작도가능이므로 60° 도 작도가능이다.
따라서 60° 의 삼등분각 20° 가 작도가능하게 된다.
이는 [문제 2]-(d)에 모순이다.

문 4. 30° 의 각을 작도할 수 있음을 대수적으로 보여라.

풀 이

크기가 θ인 각을 작도하는 것은 실수 $\cos\theta$를 작도하는 것과 같다.
그러면 $\cos 30^\circ = \frac{\sqrt{3}}{2}$이므로 $irr(\frac{\sqrt{3}}{2}, Q) = 4x^2 - 3$이고 $\left[\frac{\sqrt{3}}{2}; Q\right] = 2$이다.
따라서 [보조정리 32.8]에 차수가 2의 배수이므로 작도가능이다.

[다른풀이]
정 3-각형이 작도 가능함은 자명하므로 60° 는 작도가능이다.
한편 각의 이등분은 가능하다. 즉, 대수적으로 차원이 2이다.
따라서 30° 는 작도가능이다.

문 5. 그림 32.13을 참고하여 정 10각형은 작도가능함을 보여라. (정 8각형도 작도가능하다.)
[힌트: 삼각형 OAP는 삼각형 APQ와 닮은 꼴이다. 대수적으로 r 이 작도가능함을 보여라.]

풀 이

정 5각형이 작도 가능하므로 72° 도가 작도가능하고,
그러면 이 각의 이등분 각인 36° 또한 작도 가능하다.
따라서 정 10각형이 작도가능하다.

※ 위의 풀이에 근거하여 그림과 관련지어 풀면 된다.
그림 첨부하지 못한 관계로 직접적인 풀이는 생략 ㅎㅎ

※ 문제6~9에서의 진술이 참임을 보이기 위해서 필요하다면 문제5의 결과를 사용하여라.

문 6. 정 20-각형은 작도가능하다.

풀 이 T

[문제5]에 의하여 정 10각형이 작도가능하면, 크기가 $\frac{\pi}{5}$인 각이 작도 가능하고

또한 이 각을 이등분하는 작도인 $\frac{\pi}{10}$도 작도가능하다.

그러므로 정20(=$2 \cdot 10$)각형도 작도가능하다.

문 7. 정 30-각형인 작도가능하다.

풀 이 T

정3각형과 정10각형이 작도 가능이고 3과 10은 서로소이므로 정30각형 또한 작도가능이다.

문 8. 각 72°는 삼등분될 수 있다.

풀 이 F

정 5각형이 작도 가능하므로 72°는 작도가능한 각이다.
하지만 [문제 2]-(d) 에 의하여 각 72°는 삼등분될 수 없다.

문 9. 정 15각형은 작도 가능하다.

풀 이 T

정 3각형과 정 5각형은 작도가능하고 3과 5는 서로소이므로 정15각형은 작도가능하다.

※ 문제1~3에서 주어진 원소의 수를 갖는 유한체가 존재하는지 판단하여라.

문 1. 4096

풀 이

존재한다.

($\because$유한체의 위수는 p^n이다. 단, p는 소수이다.

주어진 원소는 $4096 = 2^{12}$이므로 주어진 원소의 수를 갖는 유한체가 존재한다.)

문 2. 3127

풀 이

- 생략함 -

문 3. $68{,}921$

풀 이

- 생략함 -

문 4. $GF(9)$**에 속하는 단위원의 원시 8제곱근의 수를 구하라.**

풀 이

가우스 함수를 이용하면, $\phi(8) = 2^3(1-\frac{1}{2}) = 4$이다.

따라서 단위원의 원시 8제곱근의 수는 4개이다.

문 5. $GF(19)$**에 속하는 단위원의 원시 18제곱근의 수를 구하라.**

풀 이

가우스 함수를 이용하면, $\phi(18) = \phi(3^2)\phi(2) = 3^2(1-\frac{1}{3})2(1-\frac{1}{2}) = 6$이다.

따라서 단위원의 원시 18제곱근의 수는 6개이다.

문 6. $GF(31)$**에 속하는 단위원의 원시 30제곱근의 수를 구하라.**

풀 이

가우스 함수를 이용하면, $\phi(30) = \phi(2)\phi(3)\phi(5) = 2(1-\frac{1}{2})3(1-\frac{1}{3})5(1-\frac{1}{5}) = 8$이다.

따라서 단위원의 원시 30제곱근의 수는 8개이다.

문 7. $GF(23)$**에 속하는 단위원의 원시 10제곱근의 수를 구하라.**

풀 이

$GF(23)^*$는 위수 22인 순환군이다.

하지만 22인 순환군에는 위수 10인 부분군이 존재하지 않는다.

따라서 단위원의 원시 10제곱근의 수는 존재하지 않는다.

그러므로 개수는 0이다.

문 8. 참, 거짓을 판정하라.

ⓐ 유한체의 0이 아닌 원소들은 곱셈에 대한 순환군을 이룬다.

풀 이 T

임의의 유한체를 F라 하자.

$F^*(=F-\{0\})$는 곱셈에 관하여 가환군이므로 유한가환생성군의 기본정리에 의하여 다음과 동형이다.

$\langle F^*, \bullet \rangle \simeq \langle Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_n}, + \rangle$ (단, $r_1, r_2, \cdots, r_n$은 소수의 멱이다.)

이제 $Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_n} = \langle (1,1,\cdots,1) \rangle$임을 보이자.

순환군의 정의에 의하여$\langle (1,1,\cdots,1) \rangle \leq Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_n}$임은 자명하다.

$\langle (1,1,1,\cdots,1) \rangle$의 위수를 구하자. 우선 $r_1, r_2, \cdots, r_n$는 서로 서로소이다.

($\because$만약 아니라면 F^*가 영인자를 갖게 되고 이는 F가 체임에 모순이다.)

그러면 다음이 성립한다.

$$|\langle ((1,1,1,\cdots,1) \rangle| = \frac{|Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_n}|}{\gcd(r_1, r_2, \cdots, r_n)} = |Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_n}|$$

따라서 $Z_{r_1} \times Z_{r_2} \times \cdots \times Z_{r_n} = \langle (1,1,\cdots,1) \rangle$이다.

그러므로 F^*는 순환군과 동형이다. 즉, F^*는 곱셈에 관하여 순환군을 이룬다.

ⓑ 유한체의 원소들은 덧셈에 대한 순환군을 이룬다.

풀 이 F

(반례) E를 Z_2의 유한차원 확대체라 하고 그 차수를 2라 하자.

그러면 E는 유한체이고 $E \equiv \{(a_1, a_2) | a_1, a_2 \in Z_2\} = \{(0,0),(0,1),(1,0),(1,1)\}$이다.

각각의 원소에 대하여 덧셈에 관한 순환군는 다음과 같다.

$\langle (0,0) \rangle = \{(0,0)\}$

$\langle (1,0) \rangle = \{(1,0),(0,0)\}$

$\langle (0,1) \rangle = \{(0,1),(0,0)\}$

$\langle (1,1) \rangle = \{(1,1),(0,0)\}$

하지만 이중 어느 것도 E와 동형인 순환군은 존재하지 않는다.

ⓒ C에 속하는 $(x^{28}-1) \in Q[x]$의 근들은 곱셈에 대한 순환군을 이룬다.

풀 이 T

$x^{28}-1 = (x-1)(x^{27}+x^{26}+\cdots+x+1)$이고 이 때, $x^{27}+x^{26}+x^{25}+\cdots+x+1$은 원주등분다항식의 기약성에 의하여 Q위에서 기약이다. 그러므로 E를 $x^{28}-1$의 근들을 첨가하여 얻은 확대체라 할 때, E는 유한체이다. 즉, E는 Q위의 원본확대체이다. 그러므로 E^*는 곱셈에 관하여 순환군을 이룬다. 따라서 주어진 방정식의 근들은 곱셈에 대한 순환군을 이룬다.

ⓓ 60개의 원소를 갖는 유한체가 존재한다.

풀 이 F

60은 소수의 멱이 아니다. 따라서 60개의 원소를 갖는 유한체는 존재하지 않는다.

ⓔ 125개의 원소를 갖는 유한체가 존재한다.

풀 이 T

$125 = 5^3$이므로 즉, 소수의 멱이므로 따라서 125개를 갖는 유한체가 존재한다.

(f) 36개의 원소를 갖는 유한체가 존재한다.

풀 이 F

36은 소수의 멱이 아니다. 따라서 36개의 원소를 갖는 유한체가 존재하지 않는다.

(g) 복소수 i는 단위원의 원시 4제곱근이다.

풀 이 T

$\langle i \rangle = \{1, -1, i, -i\}$이므로 복소수 i는 단위원의 원시 4제곱근이다.

(h) $Z_2[x]$에 속하는 차수 58인 기약 다항식이 존재한다.

풀 이 T

$x^{58} + x^2 + 1 \in Z_2[x]$이 기약임은 자명하다. 그러므로 주어진 명제는 옳다.

(i) Q의 0이 아닌 원소들은 체의 곱셈에 대하여 순환군 Q^*를 이룬다.

풀 이 F

Q^*는 곱셈에 관하여 순환군을 이루지 않는다. 따라서 체의 곱셈에 대하여 순환군이 아니다.

(j) F가 유한체이면 F에서 F의 대수적 폐포 $\overline{F}$의 부분체 위로 대응하는 모든 동형사상은 F의 자기동형사상이다.

풀 이 T

가정에 의하여 단사사상이고 준동형사상임은 만족하므로 $\sigma(F) = F$임을 보이면 충분하다.

σ를 F에서 F의 대수적 폐포 $\overline{F}$의 부분체 위로 대응하는 임의의 동형사상이라 하자.

F를 어떤 양의 정수 n에 대하여 p^n개의 원소를 갖는 유한체라 하자. 단, p는 소수

그러면 σ는 단사사상이므로 $\sigma(F)$ 또한 p^n개의 원소를 갖는다.

F가 p^n개를 갖는 $\overline{F}$의 부분체이므로 $\overline{F}$에서 p^n개를 갖는 부분체를 존재한다.

이제 F와 K가 각각 p^n개를 갖는 부분체라 하자. 그러면 문제 15번에 의하여 F와 K는 동형이다.

따라서 $\sigma(F) = F$임을 알 수 있다.

그러므로 σ는 F에서 F로의 전단사인 동형사상이므로 자기동형사상이다.

문 9. $\overline{Z_2}$를 Z_2의 대수적 폐포라 하고, $\alpha, \beta \in \overline{Z_2}$를 각각 $x^3 + x^2 + 1, x^3 + x + 1$의 근이라 하자. 이 절의 결과를 사용하여 $Z_2(\alpha) = Z_2(\beta)$임을 보여라.

풀 이

$\alpha, \beta \in \overline{Z_2}$를 각각 $x^3 + x^2 + 1, x^3 + x + 1$의 근이라 하자.

$x^3 + x^2 + 1$과 $x^3 + x + 1$은 모두 Z_2위에서 기약이다. 그러면 각각의 확대체의 차원은 다음과 같다.

$[\alpha : Z_2] = 3, [\beta : Z_2] = 3$

[정리 33.3]에 의하여 $Z_p(\alpha), Z_p(\beta)$는 체 Z_p위에서의 다항식 $x^{2^3} - x \in Z_p[x]$의 분해체이므로

다음과 같은 동형사상 $\sigma : Z_p(\alpha) \to Z_p(\beta)$가 존재한다.

(1) $\sigma(\alpha) = \beta$

(2) 모든 $a \in Z_p$에 대하여 $\sigma(a) = a$

그러므로 $Z_2(\alpha) = Z_2(\beta)$이다.

문 10. $Z_p[x]$에 속하는 모든 기약 다항식은 적당한 n에 대해서 $x^{p^n}-x$의 인수임을 보여라.

풀 이

임의의 $f(x)\in Z_p[x]$가 Z_p위에서 기약이라고 하자.

Z_p의 대수적 폐체를 $\overline{Z_p}$라고 하면, $\exists\alpha\in\overline{Z_p}\ s.t.\ f(\alpha)=0$

그러면 $Z_p(\alpha)$는 유한차원확대체이므로 $\exists n\in N\ s.t.\ [Z_p(\alpha):Z_p]=p^n$

$Z_p(\alpha)^*$는 곱셈에 관하여 순환군이므로 위수의 정의로부터 $\alpha^{p^n-1}=1$이고, $\alpha^{p^n}-\alpha=0$이다.

따라서 $\overline{Z_p}$상에서 $f(x)$의 모든 영점을 갖게 하는 원소에 대하여 $x^{p^n}-x$이 영점을 가지므로

따라서 $f(x)$는 $x^{p^n}-x$의 인수임을 알 수 있다.

문 11. F는 소부분체 Z_p를 포함하고 p^n개의 원소를 갖는 유한체라 하자. $\alpha\in F$가 F의 0이 아닌 원소의 순환군 $\langle F^*,\bullet\rangle$의 생성원이면 $\deg(\alpha,Z_p)=n$임을 보여라.

풀 이

$\alpha\in F$이므로 $Z_p(\alpha)\subseteq F$이다. 하지만 α는 곱셈군 F^*의 생성원이므로 $Z_p(\alpha)=F$ 이다.

여기서 $|F|=p^n$이므로 $\deg(\alpha,Z_p)=n$이다.

문 12. p^n개의 원소를 갖는 유한체는 n의 각 약수 m에 대하여 p^m개의 원소를 갖는 부분체를 단 하나 가짐을 증명하라.

풀 이

① (존재성) p^n개의 원소를 갖는 유한체를 E라 하자. 그리고 $\overline{E}$는 E의 대수적 폐체라 하자.

그러면 E는 Z_p와 동형인 소체를 갖으며 $x^{p^m}-x\in\overline{E}[x]$의 분해체이다.

$m|n$인 m에 대하여 $x^{p^m}-x\in\overline{E}[x]$는 $x^{p^n}-x$의 약수이다.

($\because n=mq$라 할 때, 어떤 s가 존재해서

$x^{p^n-1}-1=(x^{p^m-1}-1)\{(x^{p^m-1})^{s-1}+\cdots+x^{p^m-1}+1\}$이므로 $x^{p^m}-x\mid x^{p^n}-x$)

이제 $x^{p^m}-x\in\overline{E}[x]$의 분해체를 K라 하자.

그러면 $x^{p^m}-x\in\overline{E}[x]$의 근은 모두 $x^{p^m}-x\in\overline{E}[x]$의 근이므로 K는 p^m개의 원소를 갖는 E의 부분체이다. 따라서 p^m개를 갖는 부분체 K가 존재한다.

② (유일성) 문제 15에 의하여 p^m개의 원소를 갖는 부분체가 존재한다면 그들은 서로 동형이므로 동형에 관계없이 단 하나 존재한다.

문 13. $x^{p^n}-x$는 $Z_p[x]$에 속하며 n을 나누는 차수 d를 갖는 모든 모닉 기약다항식의 곱임을 보여라.

풀 이

$p(x)$를 $GF(p)$위에서의 $x^{p^n}-x$의 기약인수라 하고 그 차수를 d라고 하자.

이 때, $GF(p^n)$는 $x^{p^n}-x$의 근 전체로 이루어진 집합이므로

즉, 분해체이므로 $p(x)$는 $GF(p^n)$내에서 d개의 근을 가진다.

이제 $\alpha\in GF(p^n)$를 $p(x)$의 근이라고 하면,

$GF(p)(\alpha)\subseteq GF(p^n),\ [GF(p)(\alpha):GF(p)]=\deg p(x)=d$

이므로 $GF(p)(\alpha)=GF(p^d)\subseteq GF(p^n)$이다.

따라서 문제 12에 의하여 $d|n$이다.

다음에 n의 양의 약수 d에 대하여 $g(x)$를 $GF(p)$ 위에서의 d차의 기약다항식이라고 하자.

이 때, β를 $GF(p)$ 위에서의 $g(x)$의 분해체 내의 근이라고 하면,
$[GF(p)(\beta) : GF(p)] = d$
이므로 $GF(p)(\beta) = GF(p^d)$이고 따라서 $GF(p)(\beta)$는 $GF(p)$위에서의 $x^{p^d} - x$의 분해체이고, 특히 β는 $x^{p^d} - x$의 근이다. 그런데 $x^{p^d} - x \mid x^{p^n} - x$ 이므로 β는 $x^{p^n} - x$의 근이다.
한편, $g(x) = irr(\beta, GF(p))$이므로 $g(x) \mid (x^{p^n} - x)$이다.

문 14. p를 홀수인 소수라 하자.
(a) $a \not\equiv 0 (\mathrm{mod} p)$인 $a \in Z$에 대하여 합동방정식 $x^2 \equiv a (\mathrm{mod} p)$가 Z에서 근을 가질 필요충분조건은 $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod} p)$임을 보여라.
[힌트: 유한체 Z_p에서 동치인 명제를 만들고 순환군의 이론을 사용하라.]

풀 이

$x^2 \equiv a (\mathrm{mod} p)$가 Z에서 해를 갖는다.
$\Leftrightarrow$ $x^2 = b$가 Z_p에서 해를 갖는다. 단, b는 a를 p로 나눴을 때 나머지이다.
위의 사실에 근거하여 Z_p^*는 $p-1$을 위수로 갖는 순환군이다.
그러면 순환군의 원소 b는 생성원의 짝수인 멱을 갖는 제곱근이므로 $b^{\frac{(p-1)}{2}} = 1$임을 만족한다.
따라서 $a \not\equiv 0 (\mathrm{mod} p)$일 때, $x^2 = a (\mathrm{mod} p)$가 Z에서 해를 갖을 필요충분조건은 $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod} p)$임을 알 수 있다.

(b) (a)를 이용하여 $x^2 - 6$이 $Z_{17}[x]$에서 기약인지 아닌지를 결정하라.

풀 이

$x^2 \equiv 6 (\mathrm{mod} 17) \Leftrightarrow 6^{\frac{17-1}{2}} \equiv 6^8 \equiv (36)^4 \equiv (17 \cdot 2 + 2)^4 \equiv 2^4 \equiv 16 \equiv -1 (\mathrm{mod} 17)$
따라서 $Z_{17}[x]$에서 영점을 갖지 않으므로 기약이다.

문 15. 같은 위수 p^n을 갖는 두 유한체는 동형임을 보여라.
[힌트: $p(x) \in Z_p[x]$가 차수 n인 기약다항식이면 p^n개의 원소를 갖는 모든 체는 $Z_p[x] / < p(x) >$와 동형임을 보여라.]

풀 이

F와 F'를 위수 p^n를 갖는 유한체라 하자.
F와 F'는 Z_p와 동형인 소체 K와 K'를 갖으며 $x^{p^n} - x \in Z_p[x]$의 분해체이다.
또한 F와 F'는 유한체의 유한확대체이므로 단순확대체이다.
그러므로 $F = K(\alpha), F' = K'(\beta)$를 만족시키는 $\alpha \in F, \beta \in F'$가 존재한다.
이제 $\sigma : F \rightarrow F'$를 다음과 같이 정의하자.
① $\sigma(\alpha) = \beta$
② 모든 $a \in F$에 대하여 $\sigma(a) = \tau(a)$
그러면 σ는 동형사상이다. 여기서, K와 K'는 동형사상이므로 $\tau : K \rightarrow K'$인 동형사상이 존재한다.
따라서 F와 F'는 동형이다.