제 3 장　해 설

§ 3.1.1　이항정리와 다항정리

§ 3.1.2　환의 Quasi-regular 원소

§ 3.3.1　Boole 환과 Boole 다원환

§ 3.10.1 연속함수환의 극대이데알

§ 3.10.2 국소환

§ 3.10.3 素스펙트럼과 極大스펙트럼

§3.1.1 이항정리와 다항정리

여기서 논한 사항은 [5] 의 §2.3, §2.4 의 정리를 다시 쓴 것이다.

정리 1 양의 정수 n과 $0 \le r \le n$인 정수 r에 대하여 다음이 성립한다.

(1) $\binom{n}{r} = \binom{n}{n-r}$ (2) $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

증 명 정리 2.3.5에 의하여 다음 두 등식이 성립한다.

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{n!}{(n-r)!\,[n-(n-r)]!} = \binom{n}{n-r},$$

$$\begin{aligned}\binom{n}{r-1} + \binom{n}{r} &= \frac{n!}{(r-1)!\,(n-r+1)!} + \frac{n!}{r!\,(n-r)!} \\ &= \frac{n!\,r + n!\,(n-r+1)}{r!\,(n-r+1)!} = \frac{n!\,(n+1)}{r!\,(n-r+1)!} \\ &= \frac{(n+1)!}{r!\,[(n+1)-r]!} = \binom{n+1}{r}\end{aligned}$$

정리 2 (이항정리, Binomial theorem) 양의 정수 n과 서로 다른 두 문자 a, b에 대하여 다음이 성립한다.

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}, \quad (a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$$

증 명 각 정수 r $(0 \le r \le n)$에 대하여 곱

$$(a+b)^n = (a+b)\,(a+b)\,\cdots\,(a+b)$$

의 n개의 인수 $(a+b)$ 중에서 r개의 인수에서는 a를 택하고 나머지 $n-r$개의 인수에서는 b를 택하여 곱하면 $a^r b^{n-r}$를 얻는다. 그런데, 이와 같이 택하는 방법은 $\binom{n}{r}$ 가지이므로 다음 등식이 성립한다,

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

마찬가지 방법으로, 다음 등식이 성립함을 증명할 수 있다.

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$$

양의 정수 n과 $0 \le r \le n$인 정수 r에 대하여

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$$

를 **이항계수**(binomial coefficient)라고 한다.

이항계수의 값은 정리 1을 이용하여 오른쪽 표와 같이 순차적으로 구할 수 있다.

이 표를 Pascal 의 삼각형이라고 한다.

```
                1     1
             1     2     1
          1     3     3     1
       1     4     6     4     1
    1     5    10    10     5     1
 1     6    15    20    15     6     1
```

보기 1 이항정리에 의하여 다음 등식을 얻는다.

$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$
$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

보기 2 이항정리에 의하여 다음 등식이 성립한다.

$$(1+x)^n = \sum_{r=0}^{n} \binom{n}{r} x^r = \binom{n}{0} + \binom{n}{1} x + \cdots + + \binom{n}{n} x^n$$

이 등식의 양변에 $x = 1$과 $x = -1$을 대입하면 다음 결과를 얻는다.

(1) $\displaystyle\sum_{r=0}^{n} \binom{n}{r} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$

(2) $\displaystyle\sum_{r=0}^{n} (-1)^r \binom{n}{r} = \binom{n}{0} - \binom{n}{1} + \cdots + + (-1)^n \binom{n}{n} = 0$

유한집합 U에서 $|U| = n$일 때, 각 정수 r $(0 \le r \le n)$에 대하여 r개의 원소를 가진 U의 부분집합의 개수는 $\binom{n}{r}$이므로 위의 등식 (1) 에 의하여 U의 부분집합 전체의 개수는 $|\mathcal{P}(U)| = \displaystyle\sum_{r=0}^{n} \binom{n}{r} = 2^n$이다.

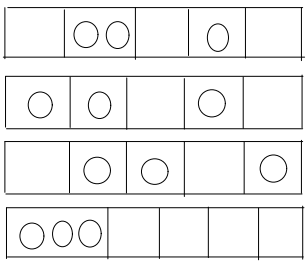
정의 3 서로 다른 n개의 원소 중에서 중복을 허락하여 몇 개의 원소를 택하여 일렬로 늘어놓은 것을 **중복순열**(permutation with repetition)이라 고 한다. 그리고, 서로 다른 n개의 원소 중에서 중복을 허락하여 r개의 원소를 택하여 만든 중복순열 개수를 ${}_n\Pi_r$로 나타낸다.

그리고, 서로 다른 n개의 원소 중에서 중복을 허락하여 몇 개의 원소를 택하여 모아놓은 것을 **중복조합**(combination with repetition)이라고 한다. 그리고, 서로 다른 n개의 원소 중에서 중복을 허락하여 r개의 원소를 택하여 만든 중복조합 전체의 개수를 ${}_n\mathrm{H}_r$로 나타낸다. 여기서 H 는 **동차곱** (homogeneous product)의 머리 글자이다.

곱의 원리에 의하여 다음 정리가 성립한다.

정리 4 서로 다른 n개의 원소 중에서 중복을 허락하여 r개의 원소를 택하여 일렬로 늘어놓은 중복순열의 개수는 ${}_n\Pi_r = n^r$ 이다.

서로 다른 다섯 문자 a_1, a_2, a_3, a_4, a_5 중에서 중복을 허락하여 세 문자를 택하여 만든 중복조합의 개수 ${}_5\mathrm{H}_3$를 구해 보자.



오른쪽 그림에서 연이은 5 개의 빈 네모가 차례로 a_1, a_2, a_3, a_4, a_5 를 나타낼 때, 이 상자에 3 개의 동그라미를 그리되 한 네모에 들어 있는 동그라미는 동일한 것으로 생각하면 ${}_5\mathrm{H}_3$는 이 상자에 3 개의 동그라미를 그려 넣는 방법의 가짓수와 같다. 예를 들면, 첫째 그림은 a_1, a_2, …, a_5 중에서 3 개의 원소를 택하되 a_2는 두 번 택하고 a_4는 한 번 택한 것을 나타낸다. 그런데, 네모의 내부 벽을 막대로 나타내면, 이 그림은 4 개의 막대와 3 개 의 동그라미를 써서

$$\big|\bigcirc\bigcirc\big|\ \ \big|\bigcirc\big|$$

으로 나타낼 수 있다. 여기서 막대는 a_1, a_3, a_5 를 택하지 않았음을 뜻한다.

그런데, 이 상자에는 내부 벽이 4 개 있고 동그라미는 3 개 있으며 이들 7 (= 4+3) 개의 막대와 동그라미의 위치에 따라 어떤 원소를 몇 번 택할 것인지가 결정된다. 따라서 이들 7 개의 막대 또는 동그라미를 모두 서로 다르다고 생각4

하면, 구하는 ${}_5\mathrm{H}_3$ 는 서로 다른 7 개의 원소 중에서 서로 다른 3 개의원소를 택하여 만든 조합의 개수와 같으므로 다음이 성립한다.

$$ {}_5\mathrm{H}_3 = \left(\begin{matrix} 7 \\ 3 \end{matrix} \right) = {}_7\mathrm{C}_3 = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35 $$

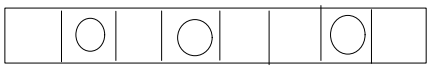
위와 마찬가지 방법으로 다음 정리를 증명할 수 있다.

정리 5 서로 다른 n 개의 원소 $a_1, a_2, \cdots, a_n$ 에서 중복을 허락하여 r 개의 원소를 택하여 만든 중복조합의 개수 ${}_n\mathrm{H}_r$ 는 다음과 같다.

$$ {}_n\mathrm{H}_r = \left(\begin{matrix} n+r-1 \\ r \end{matrix} \right) = {}_{n+r-1}\mathrm{C}_r = \frac{(n+r-1)!}{r!\,(n-1)!} $$

정리 6 원소 n 개 중에서 n_1 개의 원소는 동일한 유형 1 의 원소이고 n_2 개의 원소는 동일한 유형 2 의 원소이며, $\cdots$, n_k 개의 원소는 동일한 유형 k 의 원소이고 $n = n_1 + n_2 + \cdots + n_k$ 일 때, 이들 n 개의 원소를 일렬로 늘어놓는 방법의 가짓수는 $\dfrac{n!}{n_1! \cdot n_2! \cdot \cdots \cdot n_k!}$ 이다.

증 명 일렬로 늘어놓은 n 개의 자리 중에서 n_1 개의 자리를 택하여



이 자리에 동일한 유형의 n_1 개의 원소를 늘어놓는 방법은 $\left(\begin{matrix} n \\ n_1 \end{matrix} \right)$ 가지이고 또 나머지 $n - n_1$ 개의 자리 중에서 n_2 개의 자리를 택하여 이 자리에 동일한 유형의 n_2 개의 원소를 늘어놓는 방법은 $\left(\begin{matrix} n-n_1 \\ n_2 \end{matrix} \right)$ 가지이며 마지막으로 n_k 개의 자리에 동일한 유형의 n_k 개의 원소를 늘어놓는 방법은 1 가지이다.

따라서 이들 n 개의 원소를 일렬로 늘어놓는 방법의 가짓수는 다음과 같다.

$$ \begin{aligned} & \left(\begin{matrix} n \\ n_1 \end{matrix} \right) \cdot \left(\begin{matrix} n-n_1 \\ n_2 \end{matrix} \right) \cdots \left(\begin{matrix} n-n_1-\cdots-n_{k-1} \\ n_k \end{matrix} \right) \\ = & \frac{n!}{n_1! \cdot (n-n_1)!} \, \frac{(n-n_1)!}{n_2! \cdot (n-n_1-n_2)!} \, \cdots \, \frac{n_k!}{n_k!} \\ = & \frac{n!}{n_1! \cdot n_2! \cdot \cdots \cdot n_k!} \end{aligned} $$

앞의 정리와 마찬가지 방법으로 다음 정리가 성립함을 증명할 수 있다.

정리 7 서로 다른 n 개의 원소를 서로 구별이 되는 k 개의 상자에 각각 n_1 개, n_2 개, …, n_k 개씩 분배하는 방법의 가짓수는 다음과 같다.

$$\frac{n!}{n_1! \cdot n_2! \cdot \cdots \cdot n_k!}$$

위의 정리를 이용하여 다음 정리를 증명할 수 있다.

정리 8 (다항정리, multinomial theorem) 양의 정수 n 과 서로 다른 k 개의 문자 $x_1, x_2, \cdots, x_k$ 에 대하여 다음 등식이 성립한다.

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{0 \le n_1, n_2, \cdots, n_k \le n \\ n_1 + n_2 + \cdots + n_k = n}} \frac{n!}{n_1!\, n_2! \cdots n_k!}\, x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$$

여기서 총합 기호 $\sum$ 는

$$0 \le n_1 \le n,\ 0 \le n_2 \le n,\ \cdots,\ 0 \le n_k \le n,\ \ n_1 + n_2 + \cdots + n_k = n$$

인 정수 $n_1, n_2, \cdots, n_k$ 전체에 대한 합을 나타낸다.

여기서 $\frac{n!}{n_1!\, n_2! \cdots n_k!}$ 를 **다항계수**(multinomial coefficient)라고 한다.

보기 3 다항정리에 의하여 다음 등식이 성립한다.

(1) $(x_1 + x_2 + x_3)^2 = {x_1}^2 + {x_2}^2 + {x_3}^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3,$

(2) $(x_1 + x_2 + x_3)^3 = {x_1}^3 + {x_2}^3 + {x_3}^3 + 3{x_1}^2x_2 + 3{x_1}^2x_3$
$+ 3{x_2}^2x_1 + 3{x_2}^2x_3 + 3{x_3}^2x_1 + 3{x_3}^2x_2 + 6x_1x_2x_3$

(3) $(x_1 + x_2 + x_3)^4 = {x_1}^4 + {x_2}^4 + {x_3}^4 + 4{x_1}^3x_2 + 4{x_1}^3x_3$
$+ 4{x_2}^3x_1 + 4{x_2}^3x_3 + 4x_3^3x_1 + 4{x_3}^3x_2$
$+ 6{x_1}^2{x_2}^2 + 6{x_1}^2{x_3}^2 + 6{x_2}^2{x_3}^2$
$+ 12{x_1}^2x_2x_3 + 12{x_2}^2x_1x_3 + 12{x_3}^2x_1x_2$

보기 4 다항식 $(x_1+x_2+x_3)^3$ 을 전개했을 때 생기는 x_1, x_2, x_3 에 관한 3 차의 동차식은

$$x_1^3,\ x_2^3,\ x_3^3,\ x_1^2x_2,\ x_1^2x_3,\ x_2^2x_1,\ x_2^2x_3,\ x_3^2x_1,\ x_3^2x_2,\ x_1x_2x_3$$

뿐이다. 실제로, 이들 각 곱은 세 문자 x_1, x_2, x_3 에서 중복을 허락하여 3 개를 택하여 곱한 곱이므로 3 차의 동차식의 개수는 ${}_3\mathrm{H}_3 = \left(\begin{matrix}5\\3\end{matrix}\right) = 10$ 이다.

이것은 $(x_1+x_2+x_3)^3$ 을 전개했을 때의 항의 개수와 일치한다.

일반적으로, 서로 다른 n 개의 문자 $x_1, x_2, \cdots, x_n$ 에서 중복을 허락하여 r 개를 택하여 만든 곱인 r 차의 동차식은 $x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ 과 같은 꼴이다. 여기서,

$$0 \le e_1 \le n,\ 0 \le e_2 \le n,\ \cdots,\ 0 \le e_n \le n,$$

$$e_1 + e_2 + \cdots + e_n = r$$

위에서와 마찬가지로, 다음 정리가 성립함을 쉽게 알 수 있다.

정리 9 서로 다른 n 개의 문자 $x_1, x_2, \cdots, x_n$ 에서 중복을 허락하여 r 개를 택하여 만든 r 차의 동차식 전체의 개수는 ${}_n\mathrm{H}_r = \left(\begin{matrix}n+r-1\\r\end{matrix}\right)$ 이다.

보기 5 음이 아닌 정수 r 에 대하여 $x_1, x_2, \cdots, x_n$에 관한 일차방정식

$$x_1 + x_2 + \cdots + x_n = r$$

의 해 중에서 $x_1, x_2, \cdots, x_n$ 의 값이 모두 음이 아닌 정수인 해 전체의 개수 ${}_n\mathrm{H}_r$ 이다. 실제로, 이러한 해

$$x_1 = e_1,\ x_2 = e_2,\ \cdots,\ x_n = e_n$$

에 대하여 서로 다른 n 개의 문자 $y_1, y_2, \cdots, y_n$ 에 관한 r 차의 동차식

$$y_1^{e_1}y_2^{e_2}\cdots y_n^{e_n}$$

이 대응하고, 역으로 $y_1, y_2, \cdots, y_n$ 에 관한 r 차의 동차식 $y_1^{e_1}y_2^{e_2}\cdots y_n^{e_n}$ 에 대하여 조건을 만족시키는 일차방정식의 해가 대응한다.

따라서 정리 9 에 의하여 이와 같은 해 전체의 개수는 ${}_n\mathrm{H}_r$ 이다.

§3.1.2 환의 Quasi-regular 원소

이제 $(R, +, \cdot)$를 단위원 1을 가진 환이라고 하면, 임의의 두 원소 $a, b \in R$에 대하여 다음이 성립한다.

$$(1-a)+(1-b) = 1-(a+b-1),$$
$$(1-a)(1-b) = 1-a-b+ab = 1-(a+b-ab)$$

이 사실을 근거로 하여 집합 R 위에 새로운 덧셈 $\oplus$과 곱셈 $\circ$을

$$a \oplus b = a+b-1, \qquad a \circ b = a+b-ab$$

으로 정의하면, 임의의 원소 $a, b \in R$에 대하여 다음이 성립한다.

$$1-a \oplus b = (1-a)+(1-b),$$
$$1-a \circ b = (1-a)(1-b)$$

그리고, 다음 절차에 따라 $(R, \oplus, \circ)$가 영원 1과 단위원 0을 가진 환임을 증명할 수 있다.

A. R는 연산 $\oplus$에 관하여 덧셈군을 이룬다.

실제로,

$$(a \oplus b) \oplus c = (a+b-1) \oplus c = a+b-1+c-1,$$
$$a \oplus (b \oplus c) = a \oplus (b+c-1) = a+b+c-1-1$$

이므로 $(a \oplus b) \oplus c = a \oplus (b \oplus c)$이고 또

$$a \oplus b = a+b-1 = b+a-1 = b \oplus a$$

이므로 $a \oplus b = b \oplus a$, $a \circ b = b \circ a$ 이다.

그리고,

$$a \oplus 1 = a+1-1 = a, \quad 1 \oplus a = 1+a-1 = a$$
$$a \oplus (1+1-a) = a+1+1-a-1 = 1$$

이므로 다음이 성립한다.

$$a \oplus 1 = 1 \oplus a = a, \quad a \oplus (1+1-a) = (1+1-a) \oplus a = 1$$

M.1 : $(a \circ b) \circ c = a \circ (b \circ c)$

실제로,

$$\begin{aligned} 1-\{(a\circ b)\circ c\} &= (1-a\circ b)(1-c) \\ &= \{(1-a)(1-b)\}(1-c) \\ &= (1-a)\{(1-b)(1-c)\} \\ &= (1-a)\{1-(b\circ c)\} \\ &= 1-\{a\circ(b\circ c)\} \end{aligned}$$

이므로, $(a\circ b)\circ c = a\circ(b\circ c)$ 이다.

D : $a\circ(b\oplus c) = (a\circ b)\oplus(a\circ c), \quad (a\oplus b)\circ c = (a\circ c)\oplus(b\circ c)$

실제로,

$$\begin{aligned} 1-\{a\circ(b\oplus c)\} &= (1-a)\{1-(b\oplus c)\} \\ &= (1-a)\{(1-b)+(1-c)\} \\ &= \{(1-a)(1-b)\}+\{(1-a)(1-c)\} \\ &= \{1-(a\circ b)\}+\{1-(a\circ c)\} \\ &= 1-\{(a\circ b)\oplus(a\circ c)\}, \end{aligned}$$

$$\begin{aligned} 1-\{(a\oplus b)\circ c)\} &= \{1-(a\oplus b)\}(1-c) \\ &= \{(1-a)+(1-b)\}(1-c) \\ &= \{(1-a)(1-c)\}+\{(1-b)(1-c)\} \\ &= \{1-(a\circ c)\}+\{1-(b\circ c)\} \\ &= 1-\{(a\circ c)\oplus(b\circ c)\} \end{aligned}$$

이므로 다음이 성립한다.

$$a\circ(b\oplus c) = (a\circ b)\oplus(a\circ c), \quad (a\oplus b)\circ c = (a\circ c)\oplus(b\circ c)$$

M.3 : $a\circ 0 = 0\circ a = a$

실제로,

$$a\circ 0 = a+0-a0 = a, \qquad 0\circ a = 0+a-0a = a$$

이므로 $a\oplus 1 = 1\oplus a = a$, $a\circ 0 = 0\circ a = a$ 이다.

따라서 $(R, \oplus, \circ)$ 는 영원 1 과 단위원 0 을 가진 환이다.

특히 $(R, +, \cdot)$ 가 가환환이면, $(R, \oplus, \circ)$ 도 가환환이다.

실제로, 환 $(R, +, \cdot)$ 가 가환환일 때, 임의의 두 원소 $a, b \in R$ 에 대하여

$$\begin{aligned} 1-(a \circ b) &= (1-a)(1-b) \\ &= (1-b)(1-a) \\ &= 1-(b \circ a) \end{aligned}$$

이므로 $a \circ b = b \circ a$ 이고, 따라서 환 $(R, \oplus, \circ)$ 는 가환환이다.

이제 환 $(R, +, \cdot)$ 의 단원군을 $U(R)$ 으로 나타내고 또 환 $(R, \oplus, \circ)$ 의 단원군을 $V(R)$ 로 나타내자. 이 때, 두 원소 $a, b \in R$ 에 대하여

$$\begin{aligned} & a \circ b = 0 = b \circ a = 0 \\ \Leftrightarrow\ & (1-a)(1-b) = (1-b)(1-a) = 1 \end{aligned}$$

이므로 $a \in V(R) \Leftrightarrow 1-a \in U(R)$ 이다.

그리고, $a \in V(R)$ 의 연산 $\circ$ 에 관한 역원을 a' 로 나타내고 또 원소 $1-a \in U(R)$ 의 연산 $\cdot$ 에 관한 역원을 $(1-a)^{-1}$ 으로 나타낼 때,

$$a \circ a' = a' \circ a = 0$$

이므로

$$a + a' - aa' = a + a' - a'a = 0$$

즉 $a'(1-a) = (1-a)a' = -a$ 이고 따라서 $a' = -a(1-a)^{-1}$ 이다.

앞에서 얻은 결과에 의하여 다음이 성립함을 알 수 있다.

(1) 사상

$$\phi : (R, \oplus, \circ) \longrightarrow (R, +, \cdot), \quad \phi(a) = 1-a$$

를 생각하면, 임의의 $a, b \in R$ 에 대하여 다음이 성립한다.

$$\begin{aligned} &\phi(a \oplus b) = 1 - a \oplus b = (1-a) + (1-b) = \phi(a) + \phi(b), \\ &\phi(a \circ b) = 1 - a \circ b = (1-a)(1-b) = \phi(a)\,\phi(b) \end{aligned}$$

그리고, 두 원소 $a, b \in R$ 에 대하여

$$\phi(a) = \phi(b) \Longrightarrow 1-a = 1-b \Longrightarrow a = b$$

이므로 ϕ 는 일대일 사상이고, 또 임의의 $a \in R$ 에 대하여

$$\phi(1-a) = 1-(1-a) = a$$

이므로 $\mathrm{im}\,\phi = \{\phi(x) \mid x \in R\} = R$ 이다. 따라서 ϕ 는 일대일 대응이다..

이 사실은 ϕ 가 환 동형사상임을 뜻한다(정의 3.5.1).

(2) $U(R) = \{1-a \mid a \in V(R)\}$, $V(R) \cong U(R)$

(3) 환 $(R, +, \cdot)$ 가 나눗셈환이면, $U(R) = R - \{0\}$ 이다.

그리고, $V(R) = R - \{1\}$ 이고 따라서 $(R, \oplus, \circ)$ 는 나눗셈환이다.

특히, 환 $(R, +, \cdot)$ 가 체이면, $(R, \oplus, \circ)$ 는 체이다.

단위원 1 을 가진 환 $(R, +, \cdot)$ 에서 원소 $a \in R$ 에 대하여

$$a \circ a' = a' \circ a = 0$$

인 원소 $a' \in R$ 가 존재할 때, 즉 $1-a$ 가 단원일 때 a 를 R 의 **quasi-regular** 원소라 하고 a' 를 a 의 **quasi-regular inverse** 라고 한다.

환 $(R, +, \cdot)$ 의 원소 a 가 적당한 양의 정수 n 에 대하여 $a^n = 0$ 일 때, a 를 멱영원(nilpotent element)이라고 한다. 환 $(R, +, \cdot)$ 의 멱영원은 모두 quasi-regular 이다.

실제로, a 가 멱영원일 때, 적당한 양의 정수 n 에 대하여 $a^n = 0$ 이라고 하면 다음이 성립한다.

$$(1-a)(a + a + a^2 + \cdots + a^{n-1}) = 1 - a^n = 1$$

한편, 나눗셈환 R 에서 $a \in R, a \neq 1$ 는 quasi-regular 이지만 멱영원은 아니다.

이에 관한 상세한 논의는 다음 책의 제 1 장을 참조하기 바란다.

Jacobson, N. Structure of rings, 2nd ed., American Mathematical Society, Providence, R.I., 1964

§3.3.1 Boole 환과 Boole 다원환

한 집합 U 의 부분집합과 이들 부분집합에 대한 연산을 논할 때에는 U를 **전체집합**(universal set)이라고 하며, 전체집합 U 의 모든 부분집합으로 이루어진 집합을 U의 **멱집합**(power set)이라 하고 이것을 $\mathscr{P}(U)$ 로 나타낸다. 임의의 $A, B \in \mathscr{P}(U)$ 에 대하여 $A \cup B$와 $A \cap B$는 $\mathscr{P}(U)$ 에 속하고,
A 의 여집합(complement) $A' = \{x \in U \mid x \notin A\}$ 도 $\mathscr{P}(U)$ 에 속한다.
여기서는, [7] 의 §1.5, §8.3 에서 논한 정의와 정리를 소개하기로 한다.

정리 1 집합 U 의 멱집합 $\mathscr{P}(U)$ 는 $\cup, \cap$ 에 관하여 Boole 다원환을 이룬다. 실제로, 임의의 $A, B, C \in \mathscr{P}(U)$ 에 대하여 다음이 성립한다.

(1) $(A \cup B) \cup C = A \cup (B \cup C)$,
$(A \cap B) \cap C = A \cap (B \cap C)$ (결합법칙)

(2) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (교환법칙)

(3) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$ (흡수법칙)

(4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (분배법칙)

(5) $A \cup \emptyset = \emptyset \cup A = A$, $A \cap U = U \cap A = A$
$A \cup U = U \cup A = U$, $A \cap \emptyset = \emptyset \cap A = \emptyset$

(6) $A \cup A' = A' \cup A = U$, $A \cap A' = A' \cap A = \emptyset$

(7) $(A')' = A$, $\emptyset' = U$, $U' = \emptyset$

(8) $A \cup A = A$, $A \cap A = A$

(9) $A \cup (A' \cap B) = A \cup B$, $A \cap (A' \cup B) = A \cap B$

(10) $(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$
(De Morgan 의 법칙)

위의 정리가 성립한다는 의미에서 $\mathscr{P}(U)$ 를 두 이항연산 $\cup, \cap$ 에 관한 **Boole 다원환**(Boolean algebra)이라고 한다.

부울(George Boole, 1815 ~ 1864) 은 영국의 수학자이다.

집합 U 의 부분집합에 관한 명제에서 $\cup$ 와 $\cap$ 를 서로 바꾸어놓고 $\emptyset$ 와 U를 서로 바꾸어 놓은 명제를 본래의 명제의 **쌍대명제**(dual proposition)라고 한다.

앞의 정리 1에서 각 조건의 두 명제는 서로 쌍대명제이므로 멱집합 $\mathscr{P}(U)$ 에 관한 명제가 참인 경우에 이 명제를 증명할 때 이용한 $\cup, \cap, \emptyset, U$ 대신에 각각 $\cap, \cup, U, \emptyset$ 로 바꾸어 놓으면 쌍대명제에 대한 증명을 얻으므로 쌍대명제도 참이다.

이러한 사실을 **쌍대성의 원리**(principle of duality)라고 한다.

앞의 정리 1 과 쌍대성의 원리를 이용하여 다음 정리를 증명할 수 있다.

정리 2 집합 U 의 멱집합 $\mathscr{P}(U)$ 에서 다음 등식이 성립한다.

(11) $(A' \cup B) \cap (A \cup B') = (A \cap B) \cup (A' \cap B')$,
$(A' \cap B) \cup (A \cap B') = (A \cup B) \cap (A' \cup B')$

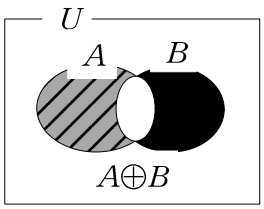
(12) $(A \cup B) \cup (A' \cap C) = A \cup B \cup C$,
$(A \cap B) \cap (A' \cup C) = A \cap B \cap C$

집합 U의 두 부분집합 A, B에 대하여

$$A \oplus B = (A \cap B') \cup (A' \cap B)$$

를 A, B의 **대칭 차집합**이라고 한다.

정리 1을 이용하여 다음 정리를 증명할 수 있다([5] 의 정리 1.5.10).



정리 3 집합 U의 멱집합 $\mathscr{P}(U)$ 위에 두 연산 $\oplus$, $\cdot$ 를

$$A \oplus B = (A \cap B') \cup (A' \cap B), \quad A \cdot B = A \cap B$$

으로 정의하면, $\mathscr{P}(U)$ 는 두 연산 $\oplus$, $\cdot$ 에 관하여 Boole 환을 이룬다.

실제로, 임의의 $A, B, C \in \mathscr{P}(U)$ 에 대하여 다음이 성립한다.

$(A \oplus B) \oplus C = A \oplus (B \oplus C)$, $A \oplus B = B \oplus A$,
$A \oplus \emptyset = \emptyset \oplus A = A$, $A \oplus A = \emptyset$,
$(A \cdot B) \cdot C = A \cdot (B \cdot C)$, $A \cdot B = B \cdot A$,
$A \cdot U = U \cdot A = A$, $A \cdot (B \oplus C) = (A \cdot B) \oplus (A \cdot C)$,
$(A \oplus B) \cdot C = (A \cdot C) \oplus (B \cdot C)$, $A \cdot A = A$

정의 4 집합 B 위에 두 이항연산 $\vee$, $\wedge$ 가 정의되어 있고, 다음이 성립할 때, B를 $\vee$, $\wedge$ 에 관한 **Boole 다원환**(多元環 Boolean algebra)이라고 한다

B.1 : $(a\vee b)\vee c = a\vee(b\vee c)$, $(a\wedge b)\wedge c = a\wedge(b\wedge c)$ (결합법칙)

B.2 : $a\vee b = b\vee a$, $a\wedge b = b\wedge a$ (교환법칙)

B.3 : $a\vee(a\wedge b) = a$, $a\wedge(a\vee b) = a$ (흡수법칙)

B.4 : $a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c)$, $a\vee(b\wedge c) = (a\vee b)\wedge(a\vee c)$ (분배법칙)

B.5 : 특정한 원소 $0, 1 \in B$이 존재하여 모든 원소 $a \in B$에 대하여 다음이 성립한다.

$$a\vee 0 = a,\quad a\wedge 1 = a,\quad a\vee 1 = 1,\quad a\wedge 0 = 0$$

B.6 : 각 $a \in B$에 대하여 $a\vee b = 1$, $a\wedge b = 0$ 인 원소 $b \in B$가 단 하나 존재한다. 원소 b를 a의 **餘원소**(complement)라 하고 이것을 a'으로 나타낸다. 즉, $a\vee a' = 1$, $a\wedge a' = 0$ 이다..

Boole 다원환에 관한 명제에서 $\vee$와 $\wedge$를 서로 바꾸고 놓고 0과 1을 서로 바꾸어 놓은 명제를 본래의 명제의 **쌍대 명제**(雙對命題)라고 한다. 위의 정의의 각 조건의 두 명제는 서로 쌍대명제이다. 따라서 Boole 다원환에 관한 참인 명제의 쌍대명제는 참이다. 이와 같은 사실을 **쌍대성의 원리**(principle of duality)라고 한다. Boole 다원환에 관한 다음 정리를 증명할 수 있다([5] 의 정리 8.3.2).

보기 1 집합 U 의 멱집합 $\mathscr{P}(U)$ 는 두 이항연산 $\cup$, $\cap$ 에 관하여 Boole 다원환을 이룬다. 여기서 최대원소와 최소원소는 각각 $\emptyset$, U이고 임의의 $A \in \mathscr{P}(U)$에 대하여 $A' = U - A$ 이다.

보기 2 집합 $\mathbb{B} = \{0, 1\}$ 는 다음과 같이 정의된 두 이항연산 $\vee$, $\wedge$ 에 관하여 Boole 다원환을 이루고 그 Hasse 다이어그램은 아래 그림과 같다.

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$0' = 1$

$1' = 0$

Boole 다원환의 임의의 원소 a, b, c에 대하여

$$(a \vee b) \vee c = a \vee (b \vee c), \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$$

이므로 이들 원소를 각각

$$a \vee b \vee c, \qquad a \wedge b \wedge c$$

로 나타낸다.

정리 5 Boole 다원환 B에서 다음이 성립한다.

B.7 : $(a')' = a, \quad 0' = 1, \quad 1' = 0$

B.8 : $a \vee a = a, \qquad a \wedge a = a$

B.9 : $a \vee (a' \wedge b) = a \vee b, \quad a \wedge (a' \vee b) = a \wedge b$

B.10 : $(a \vee b)' = a' \wedge b', \quad (a \wedge b)' = a' \vee b'$ (De Morgan의 법칙)

B.11 : $(a' \vee b) \wedge (a \vee b') = (a \wedge b) \vee (a' \wedge b')$,
$(a' \wedge b) \vee (a \wedge b') = (a \vee b) \wedge (a' \vee b')$

B.12 : $(a \vee b) \wedge (a' \vee c) = (a \vee b) \vee c$,
$(a \wedge b) \vee (a' \wedge c) = (a \wedge b) \wedge c$

보기 3 집합 B가 $\vee, \wedge$에 관하여 Boole 다원환을 이룰 때, 임의의 양의 정수 n에 대하여 집합

$$B^n = \{(b_1, \cdots, b_n) \mid b_1, \cdots, b_n \in B\}$$

는 다음과 같이 정의된 두 연산 $\vee, \wedge$에 관하여 Boole 다원환을 이룬다.

$$(a_1, \cdots, a_n) \vee (b_1, \cdots, b_n) = (a_1 \vee b_1, \cdots, a_n \vee b_n)$$
$$(a_1, \cdots, a_n) \wedge (b_1, \cdots, b_n) = (a_1 \wedge b_1, \cdots, a_n \wedge b_n)$$

여기서 $(b_1, \cdots, b_n)' = (b_1', \cdots, b_n')$ 이다.

특히, 집합 $\mathbb{B} = \{0, 1\}$는 보기 2 에서와 같이 정의된 두 연산 $\vee, \wedge$에 관하여 Boole 다원환을 이루므로

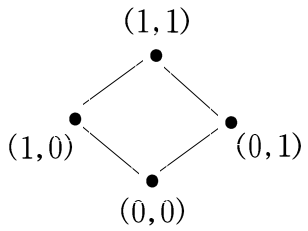
$$\mathbb{B}^n = \{(b_1, \cdots, b_n) \mid b_1, \cdots, b_n \in \mathbb{B}\}$$

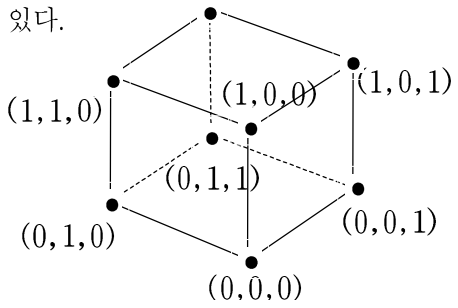
는 위와 같이 정의된 두 연산 $\vee, \wedge$에 관하여 Boole 다원환이다.

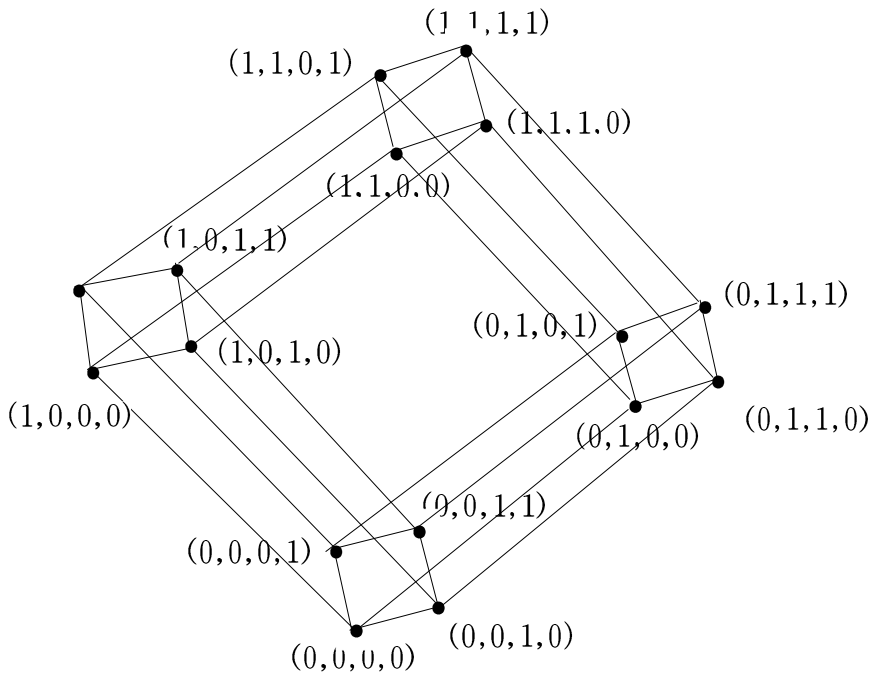
예를 들어, Boole 다원환

$$\mathbb{B}^2 = \{(0,0), (0,1), (1,0), (1,1)\}$$
$$\mathbb{B}^3 = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1),$$
$$(1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$$
$$\mathbb{B}^4 = \{(b_1, \cdots, b_n) \mid b_1, \cdots, b_n \in \mathbb{B}\}$$

를 다음과 같은 그림으로 나타낸다.. 이 그림ᄋ (1,1,1) 소는 그 성분 중에서 단 하나가 다를 때에만 선으로 이어져 있다.







앞 정리 3 과 마찬가지로, Boole 다원환 B의 경우에도 B.1 ~ B.12를 이용하여 다음 정리가 성립함을 증명할 수 있다.

정리 7 Boole 다원환 B에서 임의의 두 원소 a, b에 대하여

$$a \oplus b = (a \wedge b') \vee (a' \wedge b), \quad a \cdot b = a \wedge b$$

이라고 정의하면, B는 두 연산 $\oplus$, $\cdot$ 에 관하여 Boole 환을 이룬다.

실제로, 임의의 $a, b, c \in B$에 대하여 다음이 성립한다.,.

$(a \oplus b) \oplus c = a \oplus (b \oplus c)$, $\quad a \oplus b = b \oplus a$,

$a \oplus 0 = 0 \oplus a = a$, $\quad a \oplus a = 0$,

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\quad a \cdot b = b \cdot a$,

$a \cdot 1 = 1 \cdot a = a$,, $\quad a \cdot a = a$,

$a \cdot (b \oplus c) = (a \cdot b) \oplus (a \cdot c)$, $\quad (a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c)$

보기 4 Boole 환 $\mathbb{B} = \{0, 1\}$의 두 연산 $\oplus$, $\cdot$ 에 관한 연산표와 $\mathbb{Z}_2 = \{0, 1\}$의 두 연산 $+$, $\cdot$ 에 관한 연산표는 본질적으로 동일하다.

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

정의 8 두 Boole 다원환 B, B'에 대하여 사상 $\phi : B \longrightarrow B'$가 다음 조건을 만족시킬 때, ϕ를 **Boole 다원환 준동형사상**이라고 한다.

$$\phi(a \vee b) = \phi(a) \vee \phi(b),$$
$$\phi(a \wedge b) = \phi(a) \wedge \phi(b)$$

그리고, Boole 다원환 준동형사상 $\phi : B \longrightarrow B'$가 일대일 대응일 때, ϕ를 **Boole 다원환 동형사상**이라고 한다.

또, B에서 B' 위로의 Boole 다원동형사상이 존재할 때, B와 B는 **동형**(同型)이라 하고 이 사실을 $B \simeq B'$으로 나타낸다.

정리 9 유한집합 $U=\{x_1, \cdots, x_n\}$, $|U| = n$ 의 멱집합 $\mathscr{P}(U)$ 의 각 원소 A 에 대하여 $\phi(A) = (a_1, \cdots, a_n)$ 을 다음과 같이 정하자.

$$a_i = \begin{cases} 1 & (x_i \in A \text{ 일 때}) \\ 0 & (x_i \notin A \text{ 일 때}) \end{cases}$$

이 때, $\phi : (\mathscr{P}(U), \cup, \cap) \longrightarrow (\mathbb{B}^n, \vee, \wedge)$ 는 Boole 다원환 동형사상이고 $\phi : (\mathscr{P}(U), \oplus, \cdot) \longrightarrow (\mathbb{Z}_2{}^n, +, \cdot)$ 는 환 동형사상이다.

실제로, ϕ 는 일대일 대응이고 임의의 $A, B \in \mathscr{P}(U)$ 에 대하여 다음이 성립한다.

$$\phi(A \cup B) = \phi(A) \vee \phi(B),\ \phi(A \cap B) = \phi(A) \wedge \phi(B)$$

$$\phi(A \oplus B) = \phi(A) + \phi(B),\quad \phi(A \cdot B) = \phi(A) \cdot \phi(B)$$

특히, $|\mathscr{P}(U)| = |\mathbb{Z}_2{}^n| = 2^n$ 이다.

일반적으로, B 가 유한 Boole 다원환이면, 적당한 양의 정수 n 에 대하여 Boole 다원환으로서 $B \cong \mathbb{B}_2{}^n$ 이고 $|B| = 2^n$ 이다.

마찬가지로, R 가 유한 Boole 환이면, 적당한 양의 정수 n 에 대하여 환으로서 $R \cong \mathbb{Z}_2{}^n$ 이고 $|R| = 2^n$ 이다.

정의 9 Boole 다원환 $\mathbb{B} = \{0, 1\}$ 에 대하여 함수

$$F : \mathbb{B}^n \longrightarrow \mathbb{B},\quad y = F(x_1, x_2, \cdots, x_n)$$

를 n 개의 변수를 가진 **Boole 함수**(Boolean function), 또는 **스위칭 함수** (switching function) 또는 **출력함수**(output function)라고 한다.

Boole 함수 $F : \mathbb{B}^n \longrightarrow \mathbb{B}$ 에서 n 개의 변수 $x_1, x_2, \cdots, x_n$ 는 $\mathbb{B}$ 의 원소 0 을 또는 1 을 택하면서 변하고 그 함수값도 $\mathbb{B}$ 의 원소 0 또는 1 이다.

Boole 함수 $F : \mathbb{B}^n \longrightarrow \mathbb{B}$ 전체의 개수는 2^{2^n} 이다(정리 2.1.10). 특히, $n = 1, 2, 3, 4, 5$ 일 때의 2^{2^n} 의 값은 4, 16, 256, 65536, 4294967296 이다.

§3.10.1 연속함수환의 극대이데알

각 실수 $c \in [a, b]$ 에 대하여

$$M_c = \{f \in C[a, b] \mid f(c) = 0\}$$

이라고 하자. 그리고, 모든 실수 $c \in [a, b]$ 에 대하여 $M \neq M_c$ 이라고 가정하고, 다음 단계에 따라 모순이 생김을 증명하기로 한다.

(1) 먼저 $c \in [a, b]$ 일 때, 모든 $f \in M$ 에 대하여 $f(c) = 0$ 이면, $M \subseteq M_c$ 이고 M 은 $C[a, b]$ 의 극대이데알이므로 $M = M_c$ 로 되어 가정에 모순된다.

따라서 각 실수 $c \in [a, b]$ 에 대하여 $f_c(c) \neq 0$ 인 $f_c \in M$ 가 존재한다.

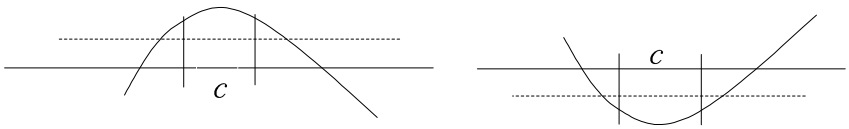
그런데, 이러한 f_c 는 연속함수이므로

$$|x - c| < \delta \implies |f_c(x) - f_c(c)| < \frac{|f_c(c)|}{2}$$

인 양의 실수 $\delta > 0$ 가 존재하고 이때

$$a_c = c - \delta, \quad b_c = c + \delta$$

라고 놓으면 다음이 성립한다.



(i) $c \in (a_c, b_c)$

(ii) 모든 $x \in [a, b] \cap (a_c, b_c)$ 에 대하여 $f_c(x) \neq 0$

각 $c \in [a, b]$ 에 대하여 개구간 (a_c, b_c) 가 정해지므로

$$[a, b] = \cup_{c \in [a, b]} (a_c, b_c)$$

이고 또 폐구간 $[a, b]$ 는 compact 하므로

$$[a, b] \subseteq (a_{c_1}, b_{c_1}) \cup (a_{c_2}, b_{c_2}) \cdots \cup (a_{c_m}, b_{c_m})$$

인 유한 개의 실수 $c_1, c_2, \cdots, c_m \in [a, b]$ 이 존재한다.

이제 연속함수 $f : [0,1] \longrightarrow \mathbb{R}$ 를

$$f = {f_{c_1}}^2 + {f_{c_2}}^2 + \cdots + {f_{c_m}}^2$$

으로 정의하자. 이 때, $f_{c_1}, f_{c_2}, \cdots, f_{c_m} \in M$ 이므로 $f \in M$ 이다.

또, $x \in [a, b]$ 라고 하면, 앞의 결과에 의하여 x 는 개구간

$$(a_{c_1}, b_{c_1}), (a_{c_2}, b_{c_2}), \cdots, (a_{c_m}, b_{c_m})$$

중의 어느 한 개구간에 속하고 따라서

$${f_{c_1}}^2(x), \ {f_{c_2}}^2(x), \ \cdots, \ {f_{c_m}}^2(x)$$

중에서 적어도 하나는 양의 실수이므로 $f(x) > 0$ 이다. 그러므로 함수

$$g : [0,1] \longrightarrow \mathbb{R}, \quad g(x) = \frac{1}{f(x)}$$

는 연속함수이고 모든 $x \in [a, b]$ 에 대하여 $f(x)\, g(x) = 1$ 이므로 $f \cdot g = 1$ 이다.

따라서 f 는 $C[0,1]$ 의 단원이므로 $M = C[a, b]$ 으로 되어 모순이 생긴다

그러므로 적당한 $c \in [0,1]$ 에 대하여 $M = M_c$ 이다.

§3.10.2 국소환

환 R가 단위원 1을 가진 가환환일 때, 임의의 이데알 $I\,(\neq R)$에 대하여 I를 포함하는 극대이데알이 존재하고 특히 R에는 적어도 한 개의 극대이데알이 존재한다. 이 사실은 이른바 Zorn 의 보조정리를 이용하여 증명한다.

단위원 1을 가진 가환환 R가 단 하나의 극대이데알을 가질 때, R를 **국소환**(局所環 local ring)이라고 한다. 예를 들면, F가 체일 때, F의 극대이데알은 $\{0\}$ 뿐이므로 체 F는 국소환이다. 그리고, p가 素數일 때, 임의의 양의 정수 n에 대하여 가환환 $\mathbb{Z}_{p^n}$의 극대에데알은 (p) 뿐이므로 $\mathbb{Z}_{p^n}$는 국소환이다.

정리 2 단위원 1을 가진 가환환 R가 국소환일 때, R의 유일한 극대이데알을 M이라고 하면 다음이 성립한다.

(1) 임의의 원소 $a\in R-M$는 R의 단원이다.

(2) R의 멱등원은 $0, 1$ 뿐이다.

증명 (1) 원소 a에 의하여 생성된 단항이데알 $(a)=\{ax\mid x\in R\}$가 R와 다르다면, (a)는 한 극대이데알에 포함되므로 가정에 의하여 $(a)\subseteq M$이어야 하나 $a\notin M$이므로 $(a)\not\subseteq M$이다.

그러므로 $(a)=R$이므로 적당한 $x\in R$에 대하여 $ax=xa=1$이고, 따라서 a는 R의 단원이다.

(2) 원소 a가 R의 멱등원이라고 하자.

먼저 $a\in M$이면, $1-a\notin M$이므로 (1) 에 의하여 $1-a$는 단원이고 또

$$a(1-a)=a-a^2=a-a=0$$

이므로 $a=0$이다.

다음에 $a\notin M$이면, (1) 에 의하여 a는 단원이므로 a의 곱셈에 관한 역원 a^{-1}가 존재하고 다음이 성립한다.

$$a=a1=a(a\,a^{-1})=a^2\,a^{-1}=a\,a^{-1}=1$$

따라서 R의 멱등원은 $0, 1$ 뿐이다.

정리 3 단위원 1을 가진 가환환 R에서 다음이 성립한다.

(1) $M\ (\neq R)$은 R의 이데알이고 또 모든 원소 $a \in R-M$가 R의 단원이면, R는 국소환이고 M은 R의 유일한 극대이데알이다.

(2) M이 R의 극대이데알이고 또 모든 원소 $m \in M$에 대하여 $1-m$이 R의 단원이면, R는 국소환이고 M은 R의 유일한 극대이데알이다.

증명 (1) 이제 $I\ (\neq R)$를 R의 이데알이라고 하자. 이 때, 정리 3.9.2 에 의하여 I에 속하는 원소는 모두 R의 단원이 아니므로 가정에 의하여 $I \subseteq M$이다. 따라서 R는 국소환이고 M은 R의 유일한 극대이데알이다.

(2) 이제 $a \in R-M$이라고 하자. 이 때, 이데알

$$(a)+M=\{ax+m \mid x \in M\}$$

는 R의 이데알이고 또 $a \notin M$이므로 $(a)+M=R$이다. 따라서 적당한 원소 $x \in R$와 $m \in M$에 대하여

$$ax+m=1$$

이고, 이때 $ax=1-m$이므로 가정에 의하여 ax는 단원이고, 따라서 a도 R의 단원이다.

그러므로 (1) 에 의하여 R는 국소환이고 M은 R의 유일한 극대이데알이다.

보기 素數 p에 대하여 $S=\mathbb{Z}-p\mathbb{Z}$이라 하고

$$\mathbb{Q}_p=\{\frac{a}{s} \in \mathbb{Q} \mid a \in \mathbb{Z}, s \in S\},$$

$$M=\{\frac{b}{s} \in \mathbb{Q} \mid b \in p\mathbb{Z},\ s \in S\}$$

이라고 할 때, $\mathbb{Q}_p$는 극소환이고 그 극대이데알은 M이다(문제 3.10.6).

§3.10.3 素스펙트럼과 極大스펙트럼

환 R가 단위원 1을 가진 가환환일 때, R의 소이데알 전체의 집합과 극대 이데알 전체의 집합에 대하여 생각해 보기로 한다.

환 R의 이데알 A, B에 대하여 AB는 다음과 같은 이데알이다.

$$AB = \{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A,\ b_i \in B,\ n = 1,2,3 \}$$

정리 1 환 R가 단위원 1을 가진 가환환일 때, R의 이데알 $P\ (\neq R)$에 대하여 다음 환 R가 단위원 1을 가진 가환환일 때, R의 이데알 $P\ (\neq R)$에 대하여 다음 두 조건은 서로 동치이다.

(1) P는 R의 소이데알이다.

(2) R의 이데알 A, B에 대하여 $AB \subseteq P$이면, $A \subseteq P$ 또는 $B \subseteq P$이다.

증명 먼저 P가 R의 소이데알일 때, R의 이데알 A, B에 대하여 $AB \subseteq P$이고 또 $A \not\subseteq P$이라고 하자. 이 때, $a \in A$, $a \not\in P$인 원소 a를 택하면, 임의의 원소 $b \in B$에 대하여 $ab \in AB \subseteq P$이고 또 P는 소이데알이므로 $b \in P$이고 따라서 $B \subseteq P$이다. 그러므로 (1)이 성립하면, (2)가 성립한다.

다음에 조건 (2)가 성립할 때, 두 원소 $a, b \in R$에 대하여 $ab \in P$이지만 $a \not\in P$, $b \not\in P$ 이라고 가정하자. 이 때,

$$A = (a) + P = \{ax + u \mid x \in R,\ u \in P\},$$
$$B = (b) + P = \{by + v \mid y \in R,\ v \in P\}$$

이라고 하면, $a \not\in P$, $b \not\in P$이므로 $P \subsetneq A$, $P \subsetneq B$이다.

한편, 임의의 $x, y \in R$와 $u, v \in P$에 대하여

$$(ax + u)(by + v) = (ab)(xy) + (ax)v + u(by) + uv$$

이고 $ab, u, v \in P$이므로 $(ax + u)(by + v) \in P$이고, 또 AB의 원소는

$$\sum_{i=1}^{n} (ax_i + u_i)(by_i + v_i) \qquad (x_i, y_i \in R,\ u_i, v_i \in P)$$

와 같은 꼴로 나타내어지므로 $AB \subseteq P$이다. 그러나 이 사실은 조건 (2)에 모순되므로 $a \in P$ 또는 $b \in P$이고, 따라서 P는 R의 소이데알이다.

그러므로 (2)가 성립하면, (1)이 성립한다.

앞의 정리에 근거하여 환 R가 가환환이 아닌 경우에도 R의 이데알 P에 대하여 다음 두 조건이 성립할 때, P를 R의 **素이데알**이라고 한다.

(i) $P \neq R$

(ii) R의 이데알 A, B에 대하여 $AB \subseteq P$이면, $A \subseteq P$ 또는 $B \subseteq P$이다.

정리 2 단위원 1을 가진 가환환 R에서 소이데알 전체의 집합을 $\mathrm{Spec}(R)$로 나타내고 또 R의 임의의 부분집합 E에 대하여

$$V(E) = \{P \in \mathrm{Spec}(R) \mid E \subseteq P\}$$

이라고 하면 다음이 성립한다.

(1) R의 부분집합 E에 대하여 E를 포함하는 가장 작은 이데알을 A라고 하면 $V(E) = V(A)$ 이다.

(2) $V(\{0\}) = \mathrm{Spec}(R), \quad V(R) = \emptyset$

(3) R의 두 부분집합 E_1, E_2에 대하여 $E_1 \subseteq E_2$이면, $V(E_2) \subseteq V(E_1)$이다.

(4) R의 부분집합으로 이루어진 집합족 $\{E_i \mid i \in I\}$에 대하여

$$V(\bigcup\{E_i \mid i \in I\}) = \bigcap\{V(E_i) \mid i \in I\}$$

(5) R의 두 이데알 A, B에 대하여

$$V(A \cap B) = V(AB) = V(A) \cup V(B)$$

증명 (1) R의 부분집합 E에 대하여 E를 포함하는 가장 작은 이데알을 A라고 하면, $P \in \mathrm{Spec}(R)$에 대하여 $A \subseteq P \Leftrightarrow E \subseteq P$이므로 $V(E) = V(A)$ 이다.

(2) 모든 소이데알 $P \in \mathrm{Spec}(R)$에 대하여 $\{0\} \subseteq P$이고 또 $R \not\subseteq P$이므로 $V(\{0\}) = \mathrm{Spec}(R)$, $V(R) = \emptyset$이다.

(3) R의 두 부분집합 E_1, E_2에 대하여 $E_1 \subseteq E_2$일 때, $P \in \mathrm{Spec}(R)$에 대하여 $E_2 \subseteq P$이면 $E_1 \subseteq P$이므로 $V(E_2) \subseteq V(E_1)$이다.

(4) 임의의 $j \in I$에 대하여 $E_j \subseteq \bigcup\{E_i \mid i \in I\})$이므로 위의 (2)에 의하여 $V(\bigcup\{E_i \mid i \in I\}) \subseteq V(E_j)$이고 따라서 다음이 성립한다.

$$V(\bigcup\{E_i \mid i \in I\}) \subseteq \bigcap\{V(E_i) \mid i \in I\}$$

한편, $P \in \bigcap \{V(E_i) \mid i \in I\}$ 이면, 모든 $i \in I$에 대하여 $E_i \subseteq P$ 이므로 $\bigcup \{E_i \mid i \in I\}) \subseteq P$ 이고 따라서 $P \in V(\bigcup \{E_i \mid i \in I\})$ 이다. 그러므로

$$\bigcap \{V(E_i) \mid i \in I\} \subseteq V(\bigcup \{E_i \mid i \in I\})$$

이고, 따라서 $V(\bigcup \{E_i \mid i \in I\}) = \bigcap \{V(E_i) \mid i \in I\}$ 이다.

(5) R의 두 이데알 A, B에 대하여 AB는 R의 이데알이고 $AB \subseteq A \cap B$ 이다(보충문제 3.9.5). 따라서 (2) 에 의하여 $V(A \cap B) \subseteq V(AB)$ 이다.

또, $P \in V(AB)$ 이면, $AB \subseteq P$ 이므로 정리 1 에 의하여 $A \subseteq P$ 또는 $B \subseteq P$ 이고 따라서 $P \in V(A)$ 또는 $P \in V(B)$ 이므로 $P \in V(A) \cup V(B)$ 이고 따라서 $V(AB) \subseteq V(A) \cup V(B)$ 이다.

그리고, $P \in V(A) \cup V(B)$ 이면, $P \in V(A)$ 또는 $P \in V(B)$ 이므로 $A \subseteq P$ 또는 $B \subseteq P$ 이고 따라서 $A \cap B \subseteq P$ 이므로 $P \in V(A \cap B)$ 이다.

그러므로 $V(A) \cup V(B) \subseteq V(A \cap B)$ 이다.

위의 결과에 의하여 $V(A \cap B) = V(AB) = V(A) \cup V(B)$ 이다.

정리 3 단위원 1을 가진 가환환 R의 소이데알 전체로 이루어진 집합 $\mathrm{Spec}(R)$에서 부분집합 $X \subseteq \mathrm{Spec}(R)$가 R의 적당한 부분집합 또는 이데알 A에 대하여 $X = V(A)$ 일 때, X를 $\mathrm{Spec}(R)$에서 **폐집합**이라고 하자.

이 때, 다음이 성립한다.

(1) $\mathrm{Spec}(R)$와 $\emptyset$는 폐집합이다.

(2) 두 집합 $X_1, X_2 \subseteq \mathrm{Spec}(R)$가 폐집합이면, $X_1 \cup X_2$는 폐집합이다.

(3) 폐집합들로 이루어진 집합족 $\{X_i \mid i \in I\}$에 대하여 $\bigcap \{X_i \mid i \in I\}$는 폐집합이다.

(4) 폐집합들로 이루어진 집합족 $\{X_i \mid i \in I\}$에서 임의로 택한 유한 개의 폐집합 $X_{i_1}, \cdots, X_{i_n}$의 교집합 $X_{i_1} \cap \cdots \cap X_{i_n}$이 모두 $\emptyset$이 아니면, $\bigcap \{X_i \mid i \in I\}$도 $\emptyset$이 아니다.

증명 (1) $\{0\}$과 R는 R의 이데알이고 정리 2 에 의하여 $V(\{0\}) = \mathrm{Spec}(R)$, $V(R) = \emptyset$이므로 $\mathrm{Spec}(R)$와 $\emptyset$는 폐집합이다.

(2) 두 집합 $X_1, X_2 \subseteq \mathrm{Spec}(R)$가 폐집합이면, 적당한 이데알 A_1, A_2에 대하여 $X_1 = V(A_1), X_2 = V(A_2)$이고 이때 정리 2 (5) 에 의하여

$$X_1 \cup X_2 = V(A_1) \cup V(A_2) = V(A_1 \cap A_2)$$

이므로 $X_1 \cup X_2$ 는 폐집합이다.

(3) 각 $i \in I$에 대하여 X_i 가 폐집합이면, 적당한 이데알 A_i 에 대하여 $X_i = V(A_i)$ 이고 이때 정리 2 (4) 에 의하여

$$\begin{aligned} \cap \{X_i \mid i \in I\} &= \cap \{V(A_i) \mid i \in I\} \\ &= V(\cup \{A_i \mid i \in I\}) \end{aligned}$$

이므로 $\cap \{X_i \mid i \in I\}$ 는 폐집합이다.

(4) 폐집합들로 이루어진 집합족 $\{X_i \mid i \in I\}$ 에서 임의로 택한 유한 개의 폐집합 $X_{i_1}, \cdots, X_{i_n}$ 의 교집합 $X_{i_1} \cap \cdots \cap X_{i_n}$ 이 모두 $\emptyset$ 이 아니라고 하자.

이 때, $\cap \{X_i \mid i \in I\} = \emptyset$ 이라고 가정하고, 모든 $i \in I$에 대하여 A_i 를 $X_i = V(A_i)$ 인 이데알이라고 하면

$$\begin{aligned} V(\cup \{A_i \mid i \in I\}) &= \cap \{V(A_i) \mid i \in I\} \\ &= \cap \{X_i \mid i \in I\} = \emptyset \end{aligned}$$

이므로 $\cup \{A_i \mid i \in I\}$ 를 포함하는 가장 작은 이데알을 A 이라고 할 때, A 를 포함하는 소이데알은 존재하지 않는다. 그런데, $A \subsetneq R$ 이면, A 를 포함하는 극대이데알이 존재하고 극대이데알은 소이데알이기도 하다. 따라서 $A = R$ 이다.

그러므로 적당한 원소 $a_{i_1} \in A_{i_1}, \cdots, a_{i_n} \in A_{i_n}$ 에 대하여

$$a_{i_1} + \cdots + a_{i_n} = 1$$

이고, 이때 $R \subseteq A_{i_1} + \cdots + A_{i_n} \subseteq R$ 이므로

$$R = A_{i_1} + \cdots + A_{i_n}$$

이고 또 $A_{i_1} \cup \cdots \cup A_{i_n}$ 을 포함하는 가장 작은 이데알은 $A_{i_1} + \cdots + A_{i_n}$ 이므로

$$\begin{aligned} X_{i_1} \cap \cdots \cap X_{i_n} &= V(A_{i_1}) \cap \cdots \cap V(A_{i_n}) \\ &= V(A_{i_1} \cup \cdots \cup A_{i_n}) \\ &= V(A_{i_1} + \cdots + A_{i_n}) \\ &= V(R) = \emptyset \end{aligned}$$

으로 되어 모순이 생긴다.

따라서 $\cap \{X_i \mid i \in I\} \neq \emptyset$ 이다.

단위원 1을 가진 가환환 R의 소이데알 전체로 이루어진 집합 $\mathrm{Spec}(R)$에서, 각 폐집합 X의 여집합 $U = \mathrm{Spec}(R) - X$를 개집합이라고 하면 정리 3 에 의하여 다음이 성립한다.

(1)' $\mathrm{Spec}(R)$와 $\emptyset$는 개집합이다.

(2)' 두 집합 $U_1, U_2 \subseteq \mathrm{Spec}(R)$가 개집합이면, $U_1 \cap U_2$는 개집합이다.

(3)' 개집합들로 이루어진 집합족 $\{U_i \mid i \in I\}$에 대하여 $\bigcup \{U_i \mid i \in I\}$는 개집합이다.

(4)' 개집합들로 이루어진 집합족 $\{U_i \mid i \in I\}$에 대하여

$$\bigcup \{U_i \mid i \in I\} = \mathrm{Spec}(R)$$

이면, $\{U_i \mid i \in I\}$에서 적당히 택한 유한 개의 개집합 $U_{i_1}, \cdots, U_{i_n}$에 대하여 $U_{i_1} \cup \cdots \cup U_{i_n} = \mathrm{Spec}(R)$ 이다.

위의 (1)', (2)', (3)' 은 $\mathrm{Spec}(R)$ 위에 **위상**(位相, topology)이 부여됨을 뜻한다. 이와 같은 위상을 **Zariski 位相**이라 하고, Zariski 위상이 부여된 위상공간(topological space) $\mathrm{Spec}(R)$를 R의 **素스펙트럼**(prime spectrum) 또는 R의 **구조공간**(構造空間, structure space)라고 한다.

앞의 (iv)' 은 위상공간 $\mathrm{Spec}(R)$가 quasi-compact 공간임을 뜻한다.

위상공간 $\mathrm{Spec}(R)$의 서로 다른 두 원소 P_1, P_2에 대하여

$$V(P_1) = \{P \in \mathrm{Spec}(R) \mid P_1 \subseteq P\},$$
$$V(P_2) = \{P \in \mathrm{Spec}(R) \mid P_2 \subseteq P\}$$

을 생각하면, $P_1 \in V(P_1)$, $P_2 \notin V(P_2)$ 이지만 $P_2 \notin V(P_1)$ 또는 $P_1 \notin V(P_2)$ 이므로 $V(P_1) \neq V(P_2)$ 이다. 그리고, $P_2 \notin V(P_1)$ 이면 $\mathrm{Spec}(R) - V(P_1)$는 P_2를 포함하지만 P_1을 포함하지 않는 개집합이고, 한편 $P_1 \notin V(P_2)$ 이면 $\mathrm{Spec}(R) - V(P_2)$는 P_1을 포함하지만 P_2를 포함하지 않는 개집합이다.

이 사실은 $\mathrm{Spec}(R)$가 T_0 공간임을 뜻한다.

가환환 R에서 P가 소이데알일 때, P는 극대이데알이거나 또는 P를 포함하는 극대이데알이 존재하고 또 극대이데알은 소이데알이기도 하다. 따라서 위상공간 $\mathrm{Spec}(R)$에서 한 원소로 이루어진 집합 $\{P\}$가 폐집합이기 위한 필요충분조건은 P가 R의 극대이데알인 것이다.

그러므로 일반적으로 $\mathrm{Spec}(R)$ 는 T_1 공간이 아니고 따라서 T_2 공간이 아니다.

단위원 1 을 가진 가환환 R 의 극대이데알 전체로 이루어진 집합을 $\mathrm{Max}(R)$ 로 나타내면, $\mathrm{Max}(R)$ 는 위상공간 $\mathrm{Spec}(R)$ 의 부분공간을 이룬다. 이 부분공간을 R 의 **극대 스펙트럼**(maximal spectrum)이라고 한다.

보기 1 연속함수환 $C[0,1]$ 에서, 임의의 실수 $c\in[0,1]$ 에 대하여

$$M_c = \{f\in C[0,1] \mid f(c) = 0\}$$

는 $C[0,1]$ 의 극대이데알이고 또 $C[0,1]$ 의 극대이데알은 모두 이와 같은 꼴로 나타내어진다(보기 3.13.5). 따라서 가환환 $C[0,1]$ 의 극대이데알 전체의 집합을 $\mathscr{M}$ 으로 나타내면,

$$\mathscr{M} = \{M_c \mid c\in[0,1]\}$$

이고, 또 두 실수 $x, y\in[0,1]$, $x\neq y$ 에 대하여

$$f(x) = 0,\ f(y)\neq 0$$

인 연속함수 $f\in C[0,1]$ 가 존재하므로 사상

$$\phi : [0,1] \longrightarrow \mathscr{M},\ \phi(c) = M_c$$

는 일대일 대응이다.

한편, 실수 전체의 집합 $\mathbb{R}$는 거리공간이고 $\mathbb{R}$의 부분공간인 폐구간 $[0,1]$은 Hausdorff 인 동시에 **콤팩트 空間**(compact space) 이므로 일대일 대응 ϕ 를 이용하여 $\mathscr{M}$ 위에 위상(topology)을 부여하여 얻은 위상공간은 Hausdoff 공간인 동시에 콤팩트공간이다.

이 사실에 근거하여 단위원 1 을 가진 가환환 R 의 구조공간 $\mathrm{Spec}(R)$ 의 위상을 도입할 수 있다.

이에 관한 자세한 설명은 다음 책의 p.203 - p.205 를 참조하기 바란다.

Jacobson, N., Structure of rings, 2nd ed., American Mathematical Society, Providence, R.I., 1964