제 8 장 해 설

§8.3 선형점화수열과 선형 Shift Resister

§8.4 직교행렬과 유니테리 행렬

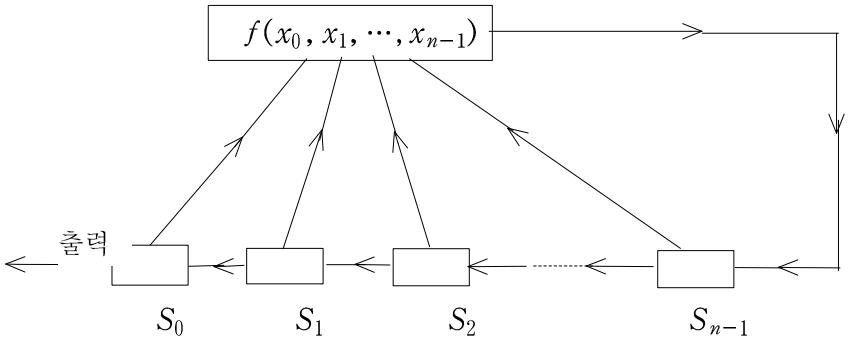
§8.7 군의 행렬 표현

§8.8.1 정사영과 멱등행렬

§8.8.2 멱영행렬

§8.3 선형점화수열과 선형 Shift Resister

다음 그림은 체 F에서의 무한수열 $\{s_t\}$를 생성해내는 장치를 보여준다.



이 장치를 체 F에서의 ***n* 단계 Shift Register**라 하고, 또 함수

$$f : \ F^n \longrightarrow F, \quad y = f(x_0, x_1, \cdots, x_{n-1})$$

이며 f를 이 Shift Register의 **feedback 함수**(feedback function)라고 한다.

이 그림에서 단위 시각 $t = 0, 1, 2, \cdots$ 에 따라 t시각일 때의 각 단계(stage) S_i의 내용을 $s_i(t)$ 라고 하면 다음 두 조건이 성립한다.

(i) $s_i(t+1) = s_{i+1}(t), \qquad (0 \le i \le n-2)$

(ii) $s_{n-1}(t+1) = f(s_0(t), s_1(t), \cdots, s_{n-1}(t))$

따라서 t 시각에서의 $S_0, S_1, \cdots, S_{n-2}, S_{n-1}$ 의 내용은 각각

(1) $\qquad s_0(t), \ s_1(t), \ \cdots, \ s_{n-2}(t), \ s_{n-1}(t)$

이고 $t+1$ 시각에서의 $S_0, S_1, \cdots, S_{n-2}, S_{n-1}$ 의 내용은 각각 다음과 같다.

(2) $\quad s_1(t), \ s_2(t), \ \cdots, \ s_{n-1}(t), \ f(s_0(t), s_1(t), \cdots, s_{n-1}(t))$

여기서 (2) 의 처음 $n-1$ 개의 항은 (1) 의 첫째 항을 제외한 항을 차례로 왼쪽으로 평행이동시킨(shift) 것이고 또 (2) 의 끝항은 (1) 의 n 개의 항과 feedback 함수 f에 의하여 결정된다.

시각 t 에서의 S_0 의 내용 $s_0(t)$ 를 s_t 라고 하면,

$$\begin{aligned} s_t &= s_0(t) \\ s_{t+1} &= s_0(t+1) = s_1(t) \\ &\vdots \\ s_{t+n-1} &= s_0(t+n-1) = \cdots = s_{n-1}(t) \\ s_{t+n} &= s_0(t+n) = \cdots = s_{n-1}(t+1) = f(s_t, s_{t+1}, \cdots, s_{t+n-1}) \end{aligned}$$

이므로 각 시각 t 에서의 $S_0, S_1, \cdots, S_{n-2}, S_{n-1}$ 의 내용은 다음과 같다.

$$\begin{aligned} t=0 \text{ 일 때} &: \ s_0,\ s_1,\ \cdots,\ s_{n-2},\ s_{n-1} \\ t=1 \text{ 일 때} &: \ s_1,\ s_2,\ \cdots,\ s_{n-1},\ s_n \\ t=2 \text{ 일 때} &: \ s_2,\ s_3,\ \cdots,\ s_n,\ s_{n+1} \\ t=3 \text{ 일 때} &: \ s_3,\ s_4,\ \cdots,\ s_{n+1},\ s_{n+2} \\ &\vdots \qquad\qquad\qquad\quad \vdots \end{aligned}$$

그리고 $t = 0, 1, 2, \cdots$ 일 때의 S_0 의 내용으로부터 무한수열

$$\{s_t\} : \ s_0,\ s_1,\ s_3,\ s_4,\ \cdots,\ s_t,\ \cdots$$

를 얻는다. 결국 feedback 함수가 $f : F^n \longrightarrow F$ 인 n 단계 Shift Register 에 의하여 생성된 무한수열 $\{s_t\}$ 는 초기조건 $(s_0, s_1, \cdots, s_{n-1})$ 와 관계식

$$s_{t+n} = f(s_t, s_{t+1}, \cdots, s_{t+n-1}) \qquad (t = 0, 1, 2, \cdots)$$

에 의하여 완전히 결정된다.

예를 들면, 체 $\mathbb{F}_2 = \{0, 1\}$ 에서의 무한수열 $\{s_t\}$ 가 함수

$$f : \mathbb{F}_2{}^3 \longrightarrow \mathbb{F}_2, \ f(x_0, x_1, x_2) = x_0 + x_1 + x_1 x_2$$

를 feedback 함수로 가지는 Shift Register 에 의하여 생성된 수열이면, $\{s_t\}$ 는 (s_0, s_1, s_2) 와 다음 관계식에 의하여 결정된다.

$$s_{t+3} = f(s_t, s_{t+1}, s_{t+2}) = s_t + s_{t+1} + s_{t+1} s_{t+2} \quad (t = 0, 1, 2, \cdots)$$

특히, $(s_0, s_1, s_2) = (0, 0, 1)$ 일 때, $\{s_t\}$ 는 다음과 같이 결정된다.

$$s_3 = 1+0+0+0 = 1,$$
$$s_4 = 1+0+1+1 = 1,$$
$$s_5 = 1+1+1+1 = 0,$$
$$s_6 = 1+1+1+0 = 1,$$
$$s_7 = 1+1+0+0 = 0,$$
$$s_8 = 1+0+1+0 = 0$$

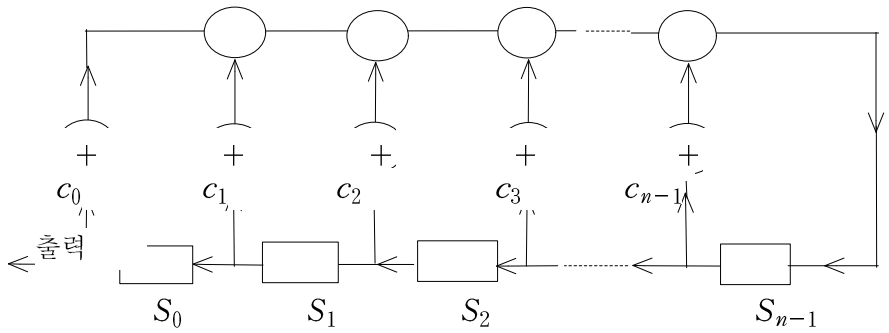
t	s_t	s_{t+1}	s_{t+2}
0	0	0	1
1	0	1	1
2	1	1	1
3	1	1	0
4	1	0	1
5	0	1	0
6	1	0	0

정의 1 체 F에 대하여 다음과 같이 정의된 함수 $f : F^n \longrightarrow F$를 체 F 에서의 **동차 선형함수**(homogeneous linear function)라고 한다.

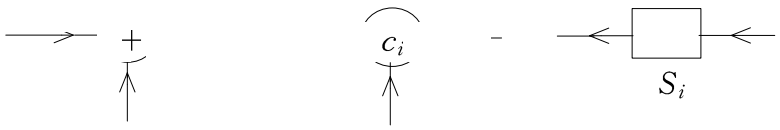
$$f(x_0, x_1, \cdots, x_{n-1}) = c_0x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1}$$
$$(c_0, c_1, \cdots, c_{n-1} \in F)$$

그리고, 체 F에서의 동차 선형함수 $f : F^n \longrightarrow F$를 feedback 함수로 가지는 Shift Register를 ***n*단계 동차 선형 Shift Register** 라고 한다.

다음 그림은 n단계 동차 선형 Shift Register를 나타내는 그림이다.



위의 그림의 n단계 동차 선형 Shift Register 에서



는 각각 더하는 과정, c_i를 곱하는 과정, 지연시키는 과정을 나타낸다.

이 동차 선형 Shift Register 에 의하여 생성된 무한수열 $\{s_t\}$ 는 다음 동차 선형점화식을 만족시키는 n 차의 동차 선형점화수열이다

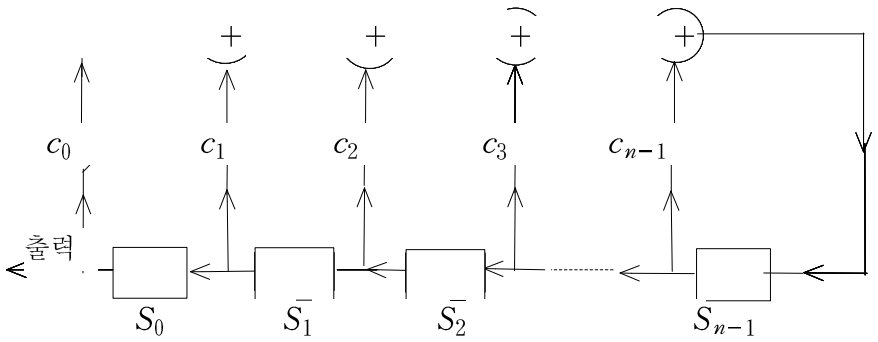
$$s_{t+n} = c_0 s_t + c_1 s_{t+1} + \cdots + c_{n-1} s_{t+n-1} \qquad (t = 0, 1, 2, \cdots)$$

특히, 체 $\mathbb{F}_2 = \{0, 1\}$ 에서의 동차 선형함수

$$f : \mathbb{F}_2{}^n \to \mathbb{F}_2, \ f(x_0, x_1, \cdots, x_{n-1}) = c_0 x_0 + c_1 x_1 + \cdots + c_{n-1} x_{n-1}$$

를 feedback 함수로 가지는 Shift Register 를 ***n* 단계 이진 동차 선형 Shift Register** 라고 한다.

다음 그림은 이러한 Shift Register를 나타내는 그림이다.



위의 그림에서 각 c_i 의 오른쪽에 있는 기호는 스위치를 나타내며 c_i 의 값이 $0, 1$ 임에 따라 이에 대응하는 스위치는 열리거나 닫히게 된다.

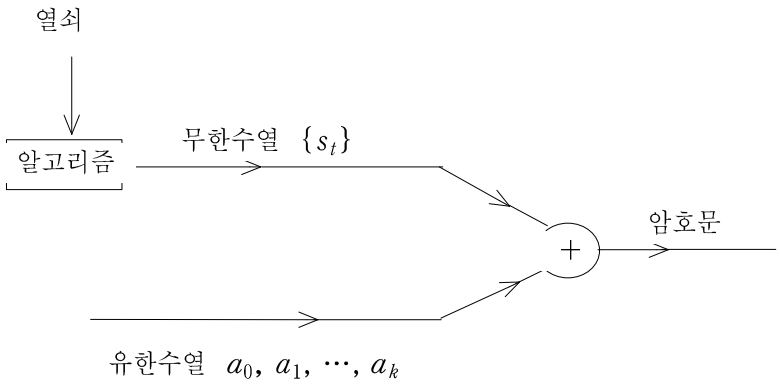
비밀 유지를 요하는 통신문을 **평문**(plaintext)이라 하고, 또 이 평문을 일정한 기호나 수로 전환시켜 놓은 것을 **암호문**(ciphertext)이라고 한다. 특히, 외교용이나 군사용으로 널리 쓰이는 **스트림 암호체계**(stream cipher system) 에서는 여러 대의 이진 선형 Shift Register 를 사용하여 이진수열 $\{s_t\}$ 를 생성해내고 전송할 평문을 유한수열 $a_0, a_1, \cdots, a_k$ 로 나타내어

$$b_i = a_i + s_i \qquad (0 \le i \le k)$$

으로 결정되는 암호문 $b_0, b_1, \cdots, b_k$ 를 전송하며, 전송된 암호문은

$$a_i = b_i - s_i \qquad (0 \le i \le k)$$

으로 결정되는 평문 $a_0, a_1, \cdots, a_k$ 로 복호한다.



이러한 스트림 암호체계는 상업용으로도 사용되고 있고, 또 이동통신 환경에서 구현하기가 용이하고 그 안전성을 수학적으로 엄밀하게 분석할 수 있다는 장점이 있어 무선 데이터를 보호하는 데 적합하다. 스트림 암호체계에서는 다음 조건이 만족되어야 한다.

A.1 열쇠(key)를 선택할 수 있는 방법의 갯수를 충분히 크게 하여 공격자로 하여금 열쇠 전부를 시험해 볼 수 없도록 하여야 한다.

A.2 보안이 유지되기 위해서는 생성되는 무한수열들의 주기를 미리 알 수 있어야 한다.

A.3 암호문은 반드시 任意性(randomness)이 있어야 한다.

그런데, 한 대의 동차 선형 Shift Register를 써서 생성해낸 최대주기수열은 이 수열의 몇 개의 연이은 항을 알면 수열 전체를 알 수 있다는 약점이 있다. 따라서 스트림 암호체계는 다음 조건을 충족시켜야 한다.

A.4 스트림 암호체계는 선형적이 아니어야 한다(nonlinearity).

스트림 암호체계가 선형적이 아니 되도록 하는 데에는 두 개 이상의 선형 Shift Register를 결합하는 방법을 이용하거나 선형함수가 아닌 함수를 feedback 함수로 택하는 방법이 이용된다. 선형함수가 아닌 feedback 함수를 가지는 무한수열로서는 bent 함수 수열, Kasami 수열과 같은 수열이 있으며 이 수열은 좋은 특성을 가지고 있다.

§8.4 직교행렬과 유니테리 행렬

여기서는 직교행렬과 유니테리 행렬에 대하여 논한다([6] 의 §5.3, §6.2).

정의 1 실수체 $\mathbb{R}$ 위의 n 차의 행렬 A 에 대하여

$$A A^T = A^T A = I_n \quad \text{즉} \quad A^{-1} = A^T$$

일 때, A 를 **직교행렬**(orthogonal matrix)이라고 한다.

정리 2 실수체 $\mathbb{R}$ 위의 n 차의 $A = [a_{ij}]_{n\times n}$ 에 대하여

$v_i = (a_{i1}, a_{i2}, \cdots, a_{in}) \quad (1 \le i \le n)$

$w_j = (a_{1j}, a_{2j}, \cdots, a_{nj}) \quad (1 \le j \le n)$

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

이라고 할 때, 다음 세 조건은 서로 동치이다

(1) A 는 직교행렬이다.

(2) $v_i \cdot v_j = \sum_{k=1}^{n} a_{ik} a_{jk} = \delta_{ij} \quad (1 \le i, j \le n)$

즉, $\mathscr{B} = \{v_1, \cdots, v_n\}$ 는 유클리드 공간 $\mathscr{E}^n$ 의 직교정규기저이다.

(3) $w_i \cdot w_j = \sum_{k=1}^{n} a_{ki} a_{kj} = \delta_{ij} \quad (1 \le i, j \le n)$

즉, $\mathscr{C} = \{w_1, \cdots, w_n\}$ 는 유클리드 공간 $\mathscr{E}^n$ 의 직교정규기저이다.

증 명 행렬 A 에 대하여

$$A A^T = A^T A = I_n \iff A A^T = I_n \iff A^T A = I_n$$

이고, 또

$$A A^T = I_n \iff \sum_{k=1}^{n} a_{ik} a_{jk} = \delta_{ij} \quad \text{즉} \quad v_i \cdot v_j = \delta_{ij} \quad (1 \le i, j \le n)$$

$$A^T A = I_n \iff \sum_{k=1}^{n} a_{ki} a_{kj} = \delta_{ij} \quad \text{즉} \quad w_i \cdot w_j = \delta_{ij} \quad (1 \le i, j \le n)$$

이므로 정리가 성립한다.

정리 3 직교행렬에 대하여 다음이 성립한다.

(1) A, B가 n차의 직교행렬이면, AB도 n차의 직교행렬이다.
또, A가 직교행렬이면, A는 정칙행렬이고 A^{-1}도 직교행렬이다.

(2) A가 직교행렬이면, $\det A = \pm 1$이다.

증 명 (1) A, B가 n차의 직교행렬이면, $A^{-1} = A^T$, $B^{-1} = B^T$이므로

$$(AB)^{-1} = B^{-1}A^{-1} = B^T A^T = (AB)^T$$

이고 따라서 AB는 직교행렬이다.

또, A가 직교행렬이면, $A^{-1} = A^T$이므로 A는 정칙행렬이고

$$(A^{-1})^T = (A^T)^T = A = (A^{-1})^{-1}$$

이므로 A^{-1}는 직교행렬이다.

(2) A가 직교행렬이면, $AA^T = I_n$이므로

$$1 = \det(AA^T) = (\det A)(\det A^T) = (\det A)^2$$

이고 따라서 $\det A = \pm 1$이다.

위의 정리 3에 의하여 n차의 직교행렬 전체의 집합

$$O(n) = \{A \in GL_n(\mathbb{R}) \mid A^{-1} = A^T\}$$

는 $GL_n(\mathbb{R})$의 부분군을 이룬다.

군 $O(n)$을 n차의 **直交群**(orthogonal group)이라고 한다.

그리고, 직교군 $O(n)$에서 곱셈군 $U_2 = \{1, -1\}$ 위로의 사상

$$\phi : O(n) \longrightarrow U_2, \quad \phi(A) = \det A$$

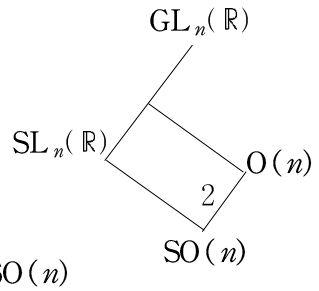
는 군 준형사상이고

$$\operatorname{im}\phi = U_2,$$

$$\ker\phi = \{A \in O(n) \mid \det A = 1\} = SO(n)$$

이므로 $SO(n) \lhd O(n)$이고 다음이 성립한다(정리 3.7.11 의 증명 참조).

$$O(n)/SO(n) \cong U_2, \quad |O(n) : SO(n)| = 2$$



군 $SO(n)$을 n차의 **特殊直交群**(special orthogonal group)이라고 한다.

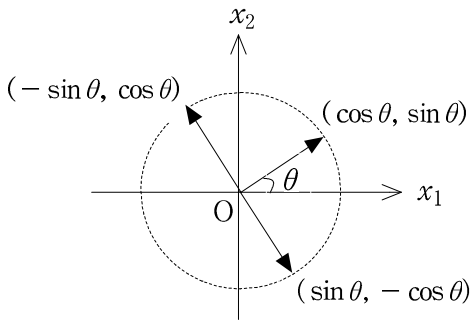
보기 1 2차의 직교행렬 A는 다음과 같은 꼴로 나타내어진다 $(0 \le \theta < 2\pi)$.

(1) $\det A = 1$ 인 경우

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

(2) $\det A = -1$ 인 경우

$$A = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$



따라서 다음이 성립한다.

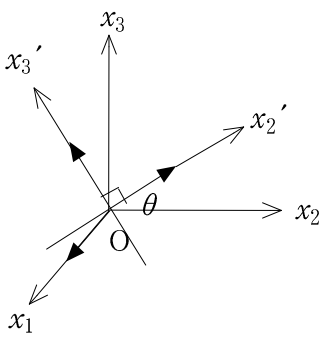
$$SO(2) = \{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mid 0 \le \theta < 2\pi \}$$

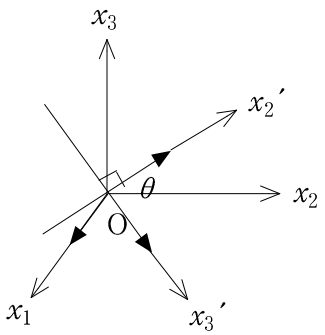
$$O(2) = SO(2) \cup \{ \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \mid 0 \le \theta < 2\pi \}$$

보기 2 다음 행렬은 직교행렬이다$(0 \le \theta < 2\pi)$.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}, \quad \begin{bmatrix} \cos\theta & 0 & -\sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & \cos\theta \end{bmatrix}, \quad \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & \sin\theta & -\cos\theta \end{bmatrix}, \quad \begin{bmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & -\cos\theta \end{bmatrix}, \quad \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ \sin\theta & -\cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$





보기 3 실수체 $\mathbb{R}$ 위의 n차의 행렬 중에서 각 행과 각 열의 단 한 개의 성분만이 1이고 그 밖의 성분은 모두 0인 행렬을 **치환행렬**(permutation matrix)이라고 한다. 분명히, n차의 치환행렬 P의 n개의 행벡터는 유클리드 공간 $\mathscr{E}^n$의 직교정규기저를 이루므로 P는 직교행렬이다.

일반적으로, n차의 치환행렬은 $n!$개 존재하며 3차의 치환행렬은 다음 6개가 존재한다.

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

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

정의 4 복소수체 $\mathbb{C}$ 위의 n차의 행렬 $A=[a_{ij}]_{n\times n}$에 대하여 A의 각 (i,j) 성분 a_{ij}를 $\overline{a_{ij}}$로 바꾸어 놓은 $n\times n$ 행렬을 A의 **켤레행렬**(conjugate matrix)이라 하고 이 행렬을 $\overline{A}$로 나타낸다. 그리고, $\overline{A}$의 전치행렬 $\overline{A}^T$을 A의 **수반행렬**(adjoint) 또는 **켤레 전치행렬**(conjugate transpose)이라 하고 이것을 A^*로 나타낸다.

정리 5 복소수체 $\mathbb{C}$ 위의 n차 행렬 A, B와 복소수 $\alpha\in\mathbb{C}$에 대하여 다음이 성립한다.

(1) $A^*=\overline{A}^T=\overline{A^T}$, $\quad (A^*)^T=\overline{A}=(A^T)^*$

(2) $\overline{(\overline{A})}=A$, $\quad (A^*)^*=A$

(3) $\overline{(A+B)}=\overline{A}+\overline{B}$, $\quad (A+B)^*=A^*+B^*$

(4) $\overline{\alpha A}=\overline{\alpha}\,\overline{A}$, $\quad (\alpha A)^*=\overline{\alpha}A^*$

(5) $\overline{AB}=\overline{A}\,\overline{B}$, $\quad (AB)^*=B^*A^*$

(6) $\overline{I_n}=I_n$, $\quad {I_n}^*=I_n$

(7) A가 정칙행렬이면, $\overline{A}$와 A^*는 정칙행렬이고 또 $\overline{A}^{-1}=\overline{A^{-1}}$, $(A^*)^{-1}=(A^{-1})^*$ 이다.

(8) $\det\overline{A}=\overline{\det A}$, $\quad \det A^*=\overline{\det A}$

정의 6 복소수체 $\mathbb{C}$ 위의 n 차의 행렬 A 가 등식

$$A A^* = A^* A = I_n \quad 즉 \quad A^{-1} = A^*$$

를 만족시킬 때, A 를 **유니테리 행렬**(unitary matrix)이라고 한다.

정리 7 복소수체 $\mathbb{C}$ 위의 n 차의 $A = [a_{ij}]_{n\times n}$ 에 대하여

$$v_i = (a_{i1}, a_{i2}, \cdots, a_{in}) \qquad (1 \le i \le n)$$
$$w_j = (a_{1j}, a_{2j}, \cdots, a_{nj}) \qquad (1 \le j \le n)$$

이라고 할 때, 다음 세 조건은 서로 동치이다.

(1) A 는 유니테리 행렬이다.

(2) 유니테리 공간 $\mathscr{C}^n$ 에서 $\mathscr{B} = \{v_1, \cdots, v_n\}$ 는 직교정규기저이다.

(3) 유니테리 공간 $\mathscr{C}^n$ 에서 $\mathscr{C} = \{w_1, \cdots, w_n\}$ 는 직교정규기저이다.

증 명 행렬 $A = [a_{ij}]_{n\times n}$ 에 대하여

$$A A^* = A^* A = I_n \Leftrightarrow A A^* = I_n \Leftrightarrow A^* A = I_n$$

이므로 정리가 성립한다.

$$A A^* = I_n \Leftrightarrow \sum_{k=1}^{n} a_{ik}\overline{a_{jk}} = \delta_{ij} \quad 즉 \quad v_i \cdot v_j = \delta_{ij} \quad (1 \le i, j \le n)$$

$$A^* A = I_n \Leftrightarrow \sum_{k=1}^{n} \overline{a_{ki}}\, a_{kj} = \delta_{ij} \quad 즉 \quad \sum_{k=1}^{n} a_{ki}\overline{a_{kj}} = \delta_{ij} \quad (1 \le i, j \le n)$$
$$\Leftrightarrow w_i \cdot w_j = \delta_{ij} \quad (1 \le i, j \le n)$$

정리 8 유니테리 행렬에 대하여 다음이 성립한다.

(1) A, B 가 n 차의 유니테리 행렬이면, AB 도 n 차의 유니테리 행렬이다.

(2) 항등행렬 I_n 은 유니테리 행렬이다.

(3) A 가 유니테리 행렬이면, A 는 정칙행렬이고 A^{-1} 도 유니테리 행렬이다.

(4) A 가 유니테리행렬이면, $|\det A| = 1$ 이다.

증 명 (1) A, B 가 유니테리 행렬이면, $A^{-1} = A^*, B^{-1} = B^*$ 이므로

$$(AB)^{-1} = B^{-1}A^{-1} = B^* A^* = (AB)^*$$

이고 따라서 AB는 직교행렬이다.

(2) ${I_n}^{-1} = I_n = {I_n}^*$ 이므로 항등행렬 I_n은 유니테리 행렬이다.

(3) A가 유니테리 행렬이면, $A^{-1} = A^*$ 이므로 A는 정칙행렬이고 또

$$(A^{-1})^* = (A^*)^* = A = (A^{-1})^{-1}$$

이므로 A^{-1}는 유니테리 행렬이다.

(4) A가 유니테리행렬이면, $AA^* = I_n$ 이므로

$$\begin{aligned} 1 &= \det(AA^*) = (\det A)(\det A^*) \\ &= (\det A)(\overline{\det A}) = |\det A|^2 \end{aligned}$$

이고 따라서 $|\det A| = 1$ 이다.

위의 정리 8 에 의하여, n차의 유니테리행렬 전체의 집합

$$\mathrm{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^{-1} = A^*\}$$

는 $\mathrm{GL}_n(\mathbb{C})$ 의 부분군을 이룬다. 군 $\mathrm{U}(n)$을 n차의 **유니테리군**(unitary group)이라고 한다.

또, 유니테리군 $\mathrm{U}(n)$ 에서 곱셈군

$$U = \{e^{i\theta} \mid 0 \le \theta < 2\pi\}$$

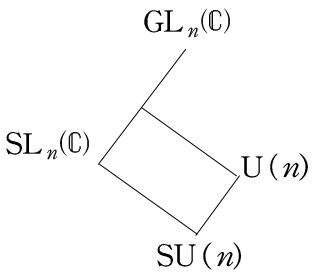
위로의 사상

$$\phi : \mathrm{U}(n) \longrightarrow U, \ \phi(A) = \det A$$

는 군 준형사상이고

$$\begin{aligned} &\mathrm{im}\,\phi = U, \\ &\ker\phi = \{A \in \mathrm{U}(n) \mid \det A = 1\} = \mathrm{SU}(n) \end{aligned}$$

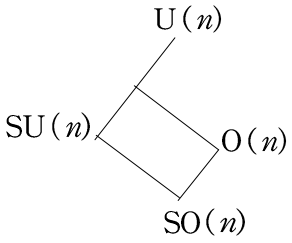
이므로 $\mathrm{SU}(n) \lhd \mathrm{U}(n)$ 이고 $\mathrm{U}(n)/\mathrm{SU}(n) \cong U$이다(정리 3.7.11 의 증명).



군 $\mathrm{SU}(n)$ 을 n차의 **特殊유니테리군**(special unitary group)이라고 한다.

직교행렬 $A \in \mathrm{GL}_n(\mathbb{R})$ 는 유니테리 행렬이기도 하므로 다음이 성립한다.

$$\begin{aligned} &\mathrm{O}(n) \subseteq \mathrm{U}(n), \\ &\mathrm{SO}(n) \subseteq \mathrm{SU}(n) \end{aligned}$$



§8.7 군의 행렬 표현

이 절은 [7] 의 §2.1, §2.2를 그대로 옮겨 놓은 것이다.

정의 1 체 F 위의 n차원 벡터공간 V의 일반선형변환군을 $\mathrm{GL}(V)$로 나타낼 때, 군 G에서 $\mathrm{GL}(V)$로의 준동형사상

$$T : G \longrightarrow \mathrm{GL}(V)$$

를 군 G의 ***F*-表現**(F-representation)이라 하고 또 V를 G의 **표현공간**(表現空間 representation space)이라고 한다. 그리고 $n = \dim_F V$를 표현 T의 **차수**(degree)라 하고 이것을 $\deg T$로 나타낸다.

그리고, 군 G에서 일반선형군 $\mathrm{GL}_n(F)$로의 준동형사상

$$\varphi : G \longrightarrow \mathrm{GL}_n(F)$$

를 군 G의 n차의 ***F*-行列 表現**(F-matrix representation)이라 하고 또 n을 $\deg \varphi$로 나타낸다. 그리고, 군 G의 F-표현 [F-행렬 표현]을 체 ***F* 위에서의 표현** [**行列 表現**]이라고도 한다.

위의 정의에서 T가 G의 표현이라는 말은 다음 조건이 성립함을 뜻한다.

(i) 각 $x \in G$에 대하여 $T(x) \in \mathrm{GL}(V)$ 이다.

즉, 각 $x \in G$에 대하여 $T(x) : V \longrightarrow V$는 V 위의 정칙 선형변환이다.

(ii) 모든 $x, y \in G$에 대하여 $T(xy) = T(x) \circ T(y)$ 이다. 즉,

$$T(xy)(v) = T(x)(T(y)(v)) \qquad (v \in V)$$

이 때, $T(1) = 1_V$, $T(x^{-1}) = T(x)^{-1}$ 이다.

마찬가지로, 사상 $\varphi : G \longrightarrow \mathrm{GL}_n(F)$가 군 G의 행렬표현이라는 말은 다음이 성립함을 뜻한다.

(i) 각 $x \in G$에 대하여 $\varphi(x) \in \mathrm{GL}_n(F)$ 이다.

(ii) 모든 $x, y \in G$에 대하여 $\varphi(xy) = \varphi(x)\varphi(y)$ 이다.

특히, $\varphi(1) = I$, $\varphi(x^{-1}) = \varphi(x)^{-1}$ 이다.

군 G의 표현 $T : G \longrightarrow \mathrm{GL}(V)$ 의 핵

$$\ker T = \{x \in G \mid T(x) = 1_V\}$$

는 군 G의 정규부분군이고 또 다음이 성립한다.

$$G/\ker T \cong T(G) = \{T(x) \mid x \in G\} \subseteq \mathrm{GL}(V)$$

마찬가가지로, 군 G의 행렬표현 $\varphi : G \longrightarrow \mathrm{GL}_n(F)$ 의 핵

$$\ker \varphi = \{x \in G \mid \varphi(x) = I\}$$

는 군 G의 정규부분군이고 또 다음이 성립한다.

$$G/\ker \varphi \cong \varphi(G) = \{\varphi(x) \mid x \in G\} \subseteq \mathrm{GL}_n(F)$$

정의 .2 군 G의 표현 $T : G \longrightarrow \mathrm{GL}(V)$ 에 대하여 $\ker T = \{1\}$ 일 때, T를 G의 **충실한**(faithful) **표현**이라고 한다.

마찬가지로, 행렬표현 $\varphi : G \longrightarrow \mathrm{GL}_n(F)$ 에 대하여 $\ker \varphi = \{1\}$ 일 때, φ를 G의 **충실한 행렬표현**이라고 한다.

체 F 위의 벡터공간 V가 1차원 벡터공간이면,

$$V \cong F, \qquad \mathrm{GL}(V) \cong F^* = F - \{0\}$$

이고 또 $\mathrm{GL}_1(F) = F^*$ 이므로, G의 1차의 표현과 1차의 행렬표현은 군 G에서 곱셈군 F^*로의 준동형사상 $G \longrightarrow F^*$라고 생각할 수 있다.

정의 3 군 G의 1차의 표현

$$1_G : G \longrightarrow F^*, \quad 1_G(x) = 1$$

를 G의 **단위 표현**(單位 表現 unit representation) 이라고 한다.

체 F 위의 n차원 벡터공간 V 에서 $\mathscr{B} = \{v_1, \cdots, v_n\}$를 V의 임의의 (순서) 기저라고 하자. 선형변환 $f \in \mathrm{GL}(V)$ 에 대하여

$$f(v_j) = \sum_{i=1}^{n} a_{ij} v_i \qquad (1 \le j \le n)$$

이라고 할 때, f의 기저 $\mathscr{B}$에 관한 행렬은 $[f]_{\mathscr{B}} = [a_{ij}]_{n\times n} \in \mathrm{Mat}_n(F)$ 이다. 이 때, f가 정칙 선형변환이면, $[f]_{\mathscr{B}}$는 정칙행렬이고, 또

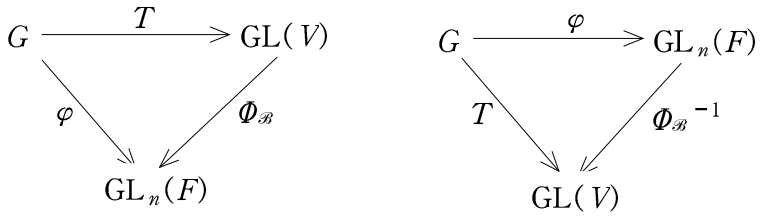
$$\Phi_{\mathscr{B}} \ : \ \mathrm{GL}(V) \longrightarrow \mathrm{GL}_n(F), \quad \Phi_{\mathscr{B}}(f) = [f]_{\mathscr{B}}$$

는 군 동형사상이다. 따라서 사상 $T : G \longrightarrow \mathrm{GL}(V)$가 G의 n차의 F-표현일 때, V의 임의의 기저 $\mathscr{B} = \{v_1, \cdots, v_n\}$에 대하여 다음과 같이 정의된 사상 φ는 G의 n차의 행렬표현이다.

$$\varphi = \Phi_{\mathscr{B}} \circ T : G \longrightarrow \mathrm{GL}_n(F), \quad \varphi(x) = [T(x)]_{\mathscr{B}}$$

$$\varphi(x) = [a_{ij}(x)]_{n\times n} \Leftrightarrow T(x)(v_j) = \sum_{i=1}^{n} a_{ij}(x)\, v_i \quad (1 \le j \le n)$$

이 행렬표현을 표현 T에 의하여 정의된(afforded by T) (기저 $\mathscr{B}$에 관한) 행렬표현이라고 한다. 이 경우에 $\ker T = \ker \varphi$이다.



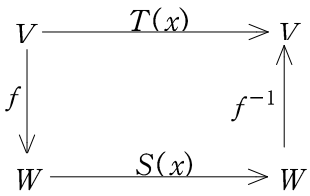
역으로, 군 G의 n차의 F-행렬표현 $\varphi : G \longrightarrow \mathrm{GL}_n(F)$에 대하여, $\mathscr{B} = \{v_1, \cdots, v_n\}$를 기저로 가지는 F-벡터공간 V을 생각하면 사상

$$T = \Phi_{\mathscr{B}}^{-1} \circ \varphi \ : \ G \longrightarrow \mathrm{GL}(V)$$

는 G의 표현이고, 또 T에 의하여 정의된 $\mathscr{B}$에 관한 행렬표현은 본래의 행렬표현 φ와 일치한다.

정의 4 군 G의 F-표현 $T : G \longrightarrow \mathrm{GL}(V)$, $S : G \longrightarrow \mathrm{GL}(W)$에 대하여, $\dim_F V = \dim_F W$ 인 동시에 적당한 F-동형사상 $f : V \longrightarrow W$가 존재하여

$$T(x) = f^{-1} \circ S(x) \circ f \quad (x \in G)$$



일 때 T, S는 **동치**인 표현이라 하고 이 사실을 $T \sim S$로 나타낸다.

그리고, 군 G의 행렬표현

$$\varphi : G \longrightarrow \mathrm{GL}_n(F), \quad \psi : G \longrightarrow \mathrm{GL}_m(F)$$

에 대하여, $n = m$인 동시에 적당한 정칙행렬 $P \in \mathrm{GL}_n(F)$가 존재하여

$$\varphi(x) = P^{-1}\psi(x)P \qquad (x \in G)$$

일 때 φ, ψ는 **동치**인 행렬표현이라 하고 이 사실을 $\varphi \sim \psi$로 나타낸다.

정리 5 군 G에 대하여 사상 $T : G \longrightarrow \mathrm{GL}(V)$가 G의 n차의 F-표현일 때, 벡터공간 V의 기저 $\mathscr{B} = \{v_1, \cdots, v_n\}$, $\mathscr{C} = \{w_1, \cdots, w_n\}$에 대하여 T에 의하여 정의된 행렬표현

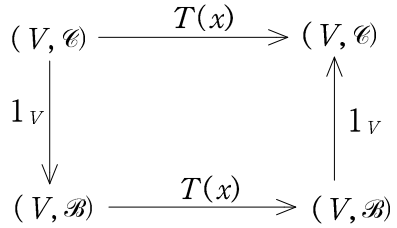
$$\varphi_{\mathscr{B}} : G \longrightarrow \mathrm{GL}_n(F), \quad \varphi_{\mathscr{B}}(x) = [T(x)]_{\mathscr{B}}$$
$$\varphi_{\mathscr{C}} : G \longrightarrow \mathrm{GL}_n(F), \quad \varphi_{\mathscr{C}}(x) = [T(x)]_{\mathscr{C}}$$

는 서로 동치이다.

증명 두 기저 $\mathscr{B}$, $\mathscr{C}$에 대하여

$$w_j = \sum_{i=1}^{n} p_{ij} v_i \quad (1 \le j \le n)$$

이라고 할 때, $P = [p_{ij}]_{n\times n}$는 정칙 행렬이고 다음이 성립한다.



$$\varphi_{\mathscr{C}}(x) = [T(x)]_{\mathscr{C}} = P^{-1}[T(x)]_{\mathscr{B}}P = P^{-1}\varphi_{\mathscr{B}}(x)P \qquad (x \in G)$$

따라서 $\varphi_{\mathscr{B}}$와 $\varphi_{\mathscr{C}}$는 서로 동치이다.

정리 6 군 G의 F-표현 $T : G \longrightarrow \mathrm{GL}(V)$, $S : G \longrightarrow \mathrm{GL}(W)$에 대하여, $\mathscr{B} = \{v_1, \cdots, v_n\}$, $\mathscr{C} = \{w_1, \cdots, w_n\}$를 각각 V, W의 (순서) 기저라 하고 또

$$\varphi_{\mathscr{B}} : G \longrightarrow \mathrm{GL}_n(F), \quad \varphi_{\mathscr{B}}(x) = [T(x)]_{\mathscr{B}}$$
$$\psi_{\mathscr{C}} : G \longrightarrow \mathrm{GL}_n(F), \quad \psi_{\mathscr{C}}(x) = [S(x)]_{\mathscr{C}}$$

를 각각 T, S에 의하여 제공된 행렬표현이라고 하면 다음이 성립한다.

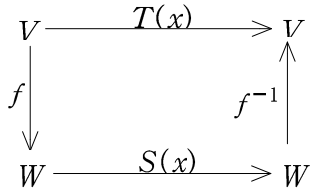
$$T \sim S \iff \varphi_{\mathscr{B}} \sim \psi_{\mathscr{C}}$$

증명 먼저 $T \sim S$ 일 때, F-동형사상

$$f : V \longrightarrow W$$

에 대하여 다음이 성립한다고 하자.

$$T(x) = f^{-1} \circ S(x) \circ f \quad (x \in G)$$



이 때,

$$(*) \qquad f(v_j) = \sum_{i=1}^{n} q_{ij} w_i \qquad (1 \le j \le n)$$

이라 하고 $Q = [q_{ij}]_{n \times n}$ 이라고 하면, $Q \in \mathrm{GL}_n(F)$ 이고 또

$$\varphi_{\mathscr{B}}(x) = [T(x)]_{\mathscr{B}} = Q^{-1}[S(x)]_{\mathscr{C}} Q = Q^{-1} \psi_{\mathscr{C}}(x) Q \quad (x \in G)$$

이므로 $\varphi_{\mathscr{B}} \sim \psi_{\mathscr{C}}$ 이다.

역으로, $\varphi_{\mathscr{B}} \sim \psi_{\mathscr{C}}$ 일 때, 정칙행렬 $Q = [q_{ij}]_{n \times n} \in \mathrm{GL}_n(F)$ 에 대하여 다음이 성립한다고 하자.

$$\varphi_{\mathscr{B}}(x) = Q^{-1} \psi_{\mathscr{C}}(x) Q \qquad (x \in G)$$

즉 $$[T(x)]_{\mathscr{B}} = Q^{-1} [S(x)]_{\mathscr{C}} Q \qquad (x \in G)$$

이 때, 조건 (*) 를 만족시키는 시키는 F-선형사상 $f : V \longrightarrow W$ 가 존재하고 또 P가 정칙행렬이므로 f는 F-동형사상이다. 그리고 위의 조건에 의하여

$$T(x) = f^{-1} \circ S(x) \circ f \qquad (x \in G)$$

이므로 $T \sim S$ 이다.

정리 7 군 G의 F-표현 전체에 대하여 관계 $\sim$ 는 동치관계이다.

다시 말하면, 군 G의 F-표현

$$T : G \longrightarrow \mathrm{GL}(V), \quad S : G \longrightarrow \mathrm{GL}(W), \quad R : G \longrightarrow \mathrm{GL}(U)$$

에 대하여 다음 세 조건이 성립한다.

(i) $T \sim T$

(ii) $T \sim S \Longrightarrow S \sim T$

(iii) $T \sim S, \ S \sim R \Longrightarrow T \sim R$

증명 먼저 모든 원소 $x \in G$ 에 대하여 $T(x) = 1_V \circ S(x) \circ 1_V$ 이므로 $T \sim T$ 이다.

또 모든 $x \in G$ 와 F-동형사상 $f : V \longrightarrow W$ 에 대하여

$$T(x) = f^{-1} \circ S(x) \circ f \implies S(x) = (f^{-1})^{-1} \circ T(x) \circ f^{-1}$$

이므로 $T \sim S \Rightarrow S \sim T$ 이다.

그리고 두 F-동형사상 $f : V \longrightarrow W$, $g : W \longrightarrow U$ 와 모든 $x \in G$ 에 대하여

$$T(x) = f^{-1} \circ S(x) \circ f, \quad S(x) = g^{-1} \circ R(x) \circ g$$
$$\Rightarrow T(x) = (g \circ f)^{-1} \circ R(x) \circ (g \circ f)$$

이므로 $T \sim S$, $S \sim R \Rightarrow T \sim R$ 이다.

위의 정리와 마찬가지로 다음 정리가 성립한다.

정리 8 군 G 의 F-행렬표현 전체에 대하여 관계 $\sim$ 는 동치관계이다. 다시 말하면, 군 G 의 F-행렬

$$\varphi : G \longrightarrow \mathrm{GL}_n(F), \quad \psi : G \longrightarrow \mathrm{GL}_n(F), \quad \theta : G \longrightarrow \mathrm{GL}_n(F)$$

에 대하여 다음이 성립한다.

(i) $\varphi \sim \varphi$

(ii) $\varphi \sim \psi \Rightarrow \psi \sim \varphi$

(iii) $\varphi \sim \psi$, $\psi \sim \theta \Rightarrow \varphi \sim \theta$

이제까지 논한 바에 의하면, 군 G 의 F-표현을 연구하는 문제는 군 G 의 F-행렬표현을 연구하는 문제와 본질적으로 동일하다.

그리고 정리 7 과 정리 8에 의하면, 군 G 의 F-표현 전체는 동치관계 $\sim$ 에 의하여 동치류로 분할되고, 마찬가지로 G 의 F-행렬표현 전체는 동치관계 $\sim$ 에 의하여 동치류로 분할된다.

더욱이, 정리 6 에 의하여 군 G 의 F-표현의 동치류와 G 의 F-행렬표현의 동치류는 일대일로 대응한다.

체 F의 표수가 0일 때 체 F 위에서의 군의 표현을 흔히 **通常 표현** (ordinary representation)이라 하고, 또 체 F의 표수가 소수 p일 때 F 위에서의 군의 표현을 **Brauer 표현** 또는 **Modular 표현**이라고 한다.

보기 1 위수 n인 순환군 C_n의 행렬표현을 생각해 보자. 여기서,

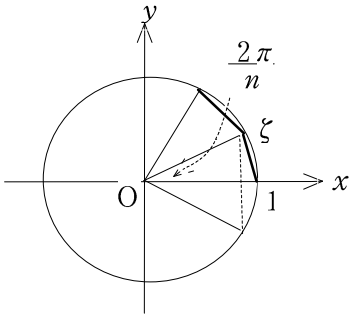
$$C_n = \langle x \mid x^n = 1 \rangle = \{1, x, \cdots, x^{n-1}\}, \quad x^n = 1$$

체 F 위에서의 행렬표현 $\varphi : C_n \longrightarrow \mathrm{GL}_m(F)$는 생성원 x의 상 $\varphi(x)$에 의하여 완전히 결정되고 $\varphi(x)^n = I$이다(I는 m차의 항등행렬).

특히, 사상 $\varphi : C_n \longrightarrow \mathbb{C}^*$가 1차의 표현이면, $\varphi(x)$는 $\mathbb{C}$ 에서의 1의 n제곱근이다. 따라서

$$\varepsilon = e^{\frac{2\pi\sqrt{-1}}{n}} = \cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n}$$

이라고 할 때, 위수 n인 순환군 C_n의 복소수체 $\mathbb{C}$ 위에서의 1차의 표현은 다음과 같이 정의된 n개의 1차의 표현 $\varphi_0, \varphi_1, \cdots, \varphi_{n-1}$ 뿐이다.



$$\varphi_i : C_n \longrightarrow \mathbb{C}^*, \quad \varphi_i(x^k) = (\varepsilon^i)^k = e^{\frac{2\pi\sqrt{-1}}{n}ik}$$
$$(0 \le i, k \le n-1)$$

보기 2 위수 3인 순환군 $C_3 = \{1, x, x^2\}$의 복소수체 $\mathbb{C}$ 위에서의 행렬표현을 생각해 보자.

먼저 1의 한 원시 세제곱근으로서 $\omega = \dfrac{-1+\sqrt{-3}}{2}$ 를 택하면, $\mathbb{C}$ 에서 1의 세제곱근은 $1, \omega, \omega^2$ 뿐이고 ω의 최소다항식은 $p(X) = X^2+X+1$ 이며, 특히 $\omega^2 + \omega + 1 = 0$ 이다.

(1) 순환군 C_3의 1차의 $\mathbb{C}$-표현은 다음과 같이 정의된 표현뿐이다.

$$\varphi_i : C_3 \longrightarrow \mathbb{C}^* \qquad (i = 0, 1, 2)$$

$$\varphi_0(x) = \varphi_0(x^2) = \varphi_0(1) = 1,$$
$$\varphi_1(x) = \omega, \quad \varphi_1(x^2) = \omega^2, \quad \varphi_1(1) = 1,$$
$$\varphi_2(x) = \omega^2, \quad \varphi_2(x^2) = \omega, \quad \varphi_2(1) = 1$$

(2) 다음과 같이 정의된 행렬표현은 2 차의 $\mathbb{C}$-행렬표현이다.

$$\psi_i : C_3 \longrightarrow \mathrm{GL}_2(\mathbb{C}) \qquad (i = 1, 2, 3)$$

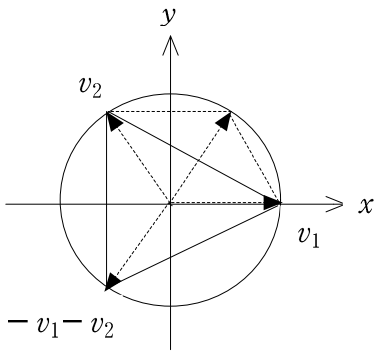
$$\psi_1(x) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \quad \psi_1(x^2) = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \quad \psi_1(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\psi_2(x) = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \quad \psi_2(x^2) = \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega \end{bmatrix}, \quad \psi_2(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\psi_3(x) = \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega \end{bmatrix}, \quad \psi_3(x^2) = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \quad \psi_3(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

한편, 행렬 $\psi_1(x)$ 의 고유다항식은

$$f(X) = \begin{vmatrix} X & 1 \\ -1 & X+1 \end{vmatrix} = X^2 + X + 1$$



이므로 $\psi_1(x)$ 의 고유치는 $\omega, \omega^2 \in \mathbb{C}$ 뿐이다. 그런데, 고유치 ω 에 대응하는 $\psi_1(x)$ 의 고유공간 E_1 은 동차 연립일차방정식

$$\begin{bmatrix} \omega & 1 \\ -1 & \omega+1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

의 해공간이다. 따라서 E_1 은 동차일차방정식 $\omega x_1 + x_2 = 0$ 의 해공간이고 그 일반해는 다음과 같이 나타낼 수 있다.

$$\begin{cases} x_1 = -\omega^2 \alpha \\ x_2 = \alpha \end{cases} (\alpha \in \mathbb{C}) \quad \text{또는} \quad \begin{cases} x_1 = \alpha \\ x_2 = -\omega\alpha \end{cases} (\alpha \in \mathbb{C})$$

그러므로 $\mathrm{E}_1 = \langle(-\omega^2, 1)\rangle = \langle(1, -\omega)\rangle$ 이다.

한편, 고유치 ω^2 에 대응하는 $\psi_1(x)$ 의 고유공간 E_2 는 연립일차방정식

$$\begin{bmatrix} \omega^2 & 1 \\ -1 & \omega^2+1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

의 해공간이고 따라서 E_2 는 동차일차방정식 $\omega^2 x_1 + x_2 = 0$ 의 해공간이다.

그러므로 $\mathrm{E}_2 = \langle(-\omega, 1)\rangle = \langle(1, -\omega^2)\rangle$ 이다.

그런데

$$w_1 = (1, -\omega), \qquad w_2 = (-\omega, 1)$$

또는 $$w_1 = (-\omega^2, 1), \qquad w_2 = (-\omega, 1)$$

이라고 하면 $\mathscr{C} = \{w_1, w_2\}$ 는 벡터공간 $\mathbb{C}^2$ 의 기저이다. 그러므로

$$P = \begin{bmatrix} 1 & -\omega \\ -\omega & 1 \end{bmatrix} \quad \text{또는} \quad P = \begin{bmatrix} -\omega^2 & -\omega \\ 1 & 1 \end{bmatrix}$$

이라고 하면, $P \in \mathrm{GL}_2(\mathbb{C})$ 이고 또 $\psi_2(x) = P^{-1}\psi_1(x)\,P$ 이고, 따라서

$$\psi_2(x^j) = P^{-1}\psi_1(x^j)P \qquad (j = 0, 1, 2)$$

이므로 $\psi_1 \sim \psi_2$ 이다. 한편,

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

이라고 하면, $Q \in \mathrm{GL}_2(\mathbb{C})$ 이고 또 $\psi_3(x) = Q^{-1}\psi_2(x)\,Q$ 이고, 따라서

$$\psi_3(x^j) = Q^{-1}\psi_2(x^j)Q \qquad (j = 0, 1, 2)$$

이므로 $\psi_2 \sim \psi_3$ 이다. 그러므로 ψ_1, ψ_2, ψ_3 는 서로 동치인 표현이다.

(3) 다음과 같이 정의된 $\mathbb{C}$-행렬표현은 모두 3 차의 $\mathbb{C}$-행렬표현이다.

$$\varphi : C_3 \longrightarrow \mathrm{GL}_3(\mathbb{C}), \qquad \psi : C_3 \longrightarrow \mathrm{GL}_3(\mathbb{C})$$

$$\varphi(x) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \psi(x) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$$

$$\varphi(x^j) = \varphi(x)^j, \quad \psi(x^j) = \psi(x)^j \qquad (j = 0, 1, 2)$$

한편, 복소수체 $\mathbb{C}$ 위에서 행렬 $\varphi(x)$ 의 고유다항식은

$$f(X) = \begin{vmatrix} X & 0 & -1 \\ -1 & X & 0 \\ 0 & -1 & X \end{vmatrix} = X^3 - 1$$

이므로 $\varphi(x)$ 의 고유치는 $1, \omega, \omega^2$ 뿐이다.

먼저, 고유치 1 에 대응하는 $\varphi(x)$ 의 고유공간 E_1 은 동차연립일차방정식

$$\begin{bmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

즉 $$\begin{cases} x_1 - x_3 = 0 \\ x_2 - x_3 = 0 \end{cases}$$

의 해공간이므로 $\mathrm{E}_1 = \langle (1,1,1) \rangle$ 이다.

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

마찬가지로, 고유치 $1, \omega, \omega^2$ 에 대응하는 $\varphi(x)$ 의 고유공간 $\mathrm{E}_1, \mathrm{E}_2, \mathrm{E}_3$ 는 각각 다음과 같다.

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

$$\mathrm{E}_1 = \langle w_1 \rangle, \quad w_1 = (1,1,1),$$

$$\mathrm{E}_2 = \langle w_2 \rangle, \quad w_2 = (\omega^2, \omega, 1),$$

$$\mathrm{E}_3 = \langle w_3 \rangle, \quad w_3 = (\omega, \omega^2, 1)$$

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

그런데, $\mathscr{C} = \{w_1, w_2, w_3\}$ 는 벡터공간 $\mathbb{C}^3$ 의 기저이므로

$$P = \begin{bmatrix} 1 & 1 & 1 \\ \omega^2 & \omega & 1 \\ \omega & \omega^2 & 1 \end{bmatrix}$$

이라고 하면, $P \in \mathrm{GL}_3(\mathbb{C})$ 이고 $\psi(x) = P^{-1}\varphi(x)P$ 이다.

따라서

$$\psi(x^j) = P^{-1}\varphi(x^j)P \qquad (j = 0,1,2)$$

이므로 $\varphi \sim \psi$ 이다.

이제까지 논한 (1), (2), (3) 의 결과는 복소수체 $\mathbb{C}$ 위에서 뿐 만아니라

$$\mathbb{Q}(\omega) = \{a + b\omega \mid a, b \in \mathbb{Q}\}$$

위에서도 성립한다.

보기 3 위수 4인 군은 순환군 $C_4 = \langle x \mid x^3 = 1 \rangle$ 와 동형이거나 또는 Klein 의 四元群 V와 동형이다. 여기서,

$$V = \langle a, b \mid a^2 = 1, b^2 = 1, ab = ba \rangle \cong C_2 \times C_2$$

(1) 순환군 $G = \langle x \mid x^4 = 1 \rangle$ 의 복소수체 $\mathbb{C}$ 위에서의 1차의 표현은 다음과 같이 정의된 4개의 표현 $\varphi_0, \varphi_1, \varphi_2, \varphi_3$ 뿐이다.

$$\varphi_i : C_4 \longrightarrow \mathbb{C}^*, \quad \varphi_i(x^j) = (\sqrt{-1})^j \qquad (i = 0, 1, 2, 3)$$

여기서, $\sqrt{-1} \in \mathbb{C}$ 는 1의 원시 네제곱근이다.

(2) $G = \langle a, b \mid a^2 = 1, b^2 = 1, ab = ba \rangle \cong C_2 \times C_2$

사상 $\varphi : G \longrightarrow F^*$ 를 체 F 위에서의 G의 1차의 표현이라고 하면, 군 G에서 $a^2 = 1$, $b^2 = 1$ 이므로 다음 두 등식이 성립한다.

$$\varphi(a)^2 = \varphi(b)^2 = 1$$

먼저 체 F의 표수가 0 또는 素數 $p(\neq 2)$라고 하자(정의 1.6.6). 이 때, F 에서의 1의 제곱근은 $1, -1$ 뿐이므로 체 F 위에서의 군 G의 1차의 표현은 다음과 같이 정의된 4개의 표현뿐이다.

$$\varphi_i : G \longrightarrow F^* \qquad (i = 1, 2, 3, 4)$$

$$\varphi_1(a) = \varphi_1(b) = 1$$
$$\varphi_2(a) = 1, \qquad \varphi_2(b) = -1$$
$$\varphi_3(a) = -1, \quad \varphi_3(b) = 1$$
$$\varphi_2(a) = \varphi_2(b) = -1$$

한편, 체 F의 표수가 2인 경우에 $-1 = 1$ 이므로 체 F 위에서의 군 G의 1차의 표현은 단위표현 $1_G : G \longrightarrow F^*$ 뿐이다.

보기 4 위수 6인 Abel 군은 순환군 $C_6 = \langle x \mid x^6 = 1 \rangle$ 와 동형이고, 위수 6인 非 Abel 군은 위수 6의 정이면체군과 동형이다. 여기서

$$D_3 = \langle x, y \mid x^3 = 1, y^2 = 1, x^y = x^{-1} \rangle$$
$$\cong \{1, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)\} = S_3,$$

위수 6인 정이면체군 $G = D_3$의 임의의 체 F 위에서의 2차의 행렬 표현을 생각해 보자. 여기서, $y^{-1} = y$이므로 다음이 성립한다.

$$x^y = x^{-1} \Leftrightarrow y^{-1}xy = x^{-1} \Leftrightarrow (xy)^2 = 1$$

따라서 군 G의 F-행렬표현

$$\varphi : G \longrightarrow \mathrm{GL}_m(F)$$

는 다음 등식을 만족 시키는 $\varphi(x), \varphi(y) \in \mathrm{GL}_m(F)$에 의하여 결정된다.

$$\varphi(x)^3 = I, \quad \varphi(y)^2 = I, \quad (\varphi(x)\varphi(y))^2 = I$$

(1) 사상 $\varphi : G \longrightarrow \mathbb{Q}^*$가 G의 유리수체 $\mathbb{Q}$ 위에서의 1차의 표현이면,

$$\varphi(x) = 1, \quad \varphi(y) = \pm 1$$

이어야 하므로, G의 1차의 $\mathbb{Q}$-표현은 다음과 같은 2개의 표현뿐이다.

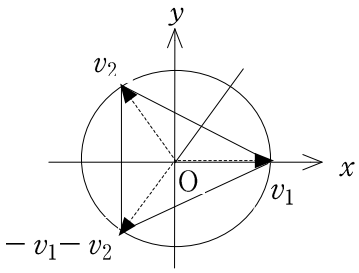
$$\varphi_1 : G \longrightarrow \mathbb{Q}^*, \quad \varphi_1(x) = \varphi_1(y) = 1,$$

$$\varphi_2 : G \longrightarrow \mathbb{Q}^*, \quad \varphi_2(x) = 1, \quad \varphi_2(y) = -1$$

(2) 다음과 같이 정의된 사상 $\varphi : G \longrightarrow \mathrm{GL}_2(\mathbb{Q})$는 군 G의 유리수체 $\mathbb{Q}$ 위에서의 2차의 행렬표현이다.

$$\varphi(x) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix},$$

$$\varphi(y) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



(3) 다음과 같이 정의된 사상은 G의 복소수체 $\mathbb{C}$ 위에서의 2차의 행렬 표현이다.

$$\varphi : G \longrightarrow \mathrm{GL}_2(\mathbb{C}), \quad \psi : G \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

$$\varphi(x) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \quad \varphi(y) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\psi(x) = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \quad \psi(y) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \left(\omega = \frac{-1+\sqrt{-3}}{2}\right)$$

한편, $\varphi(x)$ 의 고유치는 ω, ω^2 뿐이고 이들 고유치에 대응하는 고유공간 E_1, E_2 는 각각 다음과 같다(보기 2.2.2 의 (2) 참조).

$$E_1 = \langle (1, -\omega) \rangle, \qquad E_2 = \langle (-\omega, 1) \rangle$$

그런데 $\mathscr{C} = \{(1, -\omega), (-\omega, 1)\}$ 는 벡터공간 $\mathbb{C}^2$ 의 기저이므로, 행렬

$$P = \begin{bmatrix} 1 & -\omega \\ -\omega & 1 \end{bmatrix}$$

는 정칙행렬이고 또

$$\psi(x) = P^{-1}\varphi(x)P, \quad \psi(y) = P^{-1}\varphi(y)P$$

이므로 $\varphi \sim \psi$ 이다.

보기 5 체 F 의 표수가 素數 p 일 때, 체 F 위의 행렬

$$X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(F)$$

에 대하여 다음이 성립한다.

$$X^i = \begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix} \quad (1 \le i \le p-1), \qquad X^p = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

따라서, 순환군 $C_p = \langle x \mid x^p = 1 \rangle$ 에 대하여 사상

$$\varphi : C_p \longrightarrow \mathrm{GL}_2(F), \quad \phi(x^i) = X^i$$

는 순환군 C_p 의 2 차의 F-행렬표현이다.

정리 9 군 G 와 체 F 에 대하여 다음과 같은 꼴의 형식적 유한합(formal finite sum) 을 생각하자.

$$\sum_{x \in G} a_x x \qquad\qquad (a_x \in F)$$

(유한 개를 제외하고서는 모든 $x \in G$ 에 대하여 $a_x = 0$)

또, 이와 같은 형식적 유한합 전체의 집합을 $F[G]$ 로 나타내고, 집합 $F[G]$ 에서의 相等관계, 덧셈, 곱셈, 스칼라 곱셈을 다음과 같이 정의하자.

$$\sum_{x\in G} a_x x = \sum_{x\in G} b_x x \iff a_x = b_x \quad (x\in G)$$

$$\sum_{x\in G} a_x x + \sum_{x\in G} b_x x = \sum_{x\in G} (a_x + b_x) x$$

$$(\sum_{x\in G} a_x x)(\sum_{x\in G} b_x x) = \sum_{x,y\in G} (a_x b_y) xy = \sum_{z\in G} c_z z$$

여기서 $c_z = \sum_{xy=z} a_x b_y$

$$a(\sum_{x\in G} a_x x) = \sum_{x\in G} a a_x x$$

이 때, $F[G]$ 는 체 F 위의 다원환이다(정의 1.3.11). 즉, $F[G]$ 는 위에서 정의한 연산에 관하여 환인 동시에 체 F 위의 벡터공간이다.

이러한 의미에서 $F[G]$ 를 체 F 위의 군 G 의 **군다원환**(群多元環 group algebra) 또는 **군환**(群環 group ring)이라고 한다.

위에서, 각 원소 $x\in G$ 에 대하여 x 와 $F[G]$ 의 원소

$$1\cdot x + \sum_{y\in G, y\neq x} 0\, y$$

을 同一視하여 $G\subset F[G]$ 라고 생각하기로 한다.

특히, G 가 위수 n 인 유한군일 때,

$$G = \{x_1, x_2, \cdots, x_n\}, \quad x_1 = 1$$

이라고 하면 G 의 군다원환 $F[G]$ 의 각 원소는 단 한 가지 방법으로

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \qquad (a_1, a_2, \cdots, a_n\in F)$$

의 꼴로 나타내어지므로 $F[G]$ 는 집합 $\mathscr{B} = G$ 를 기저로 가지는 n 차원 F-다원환이다.

보기 6 위수 n 인 유한군

$$G = \{x_1, x_2, \cdots, x_n\}, \quad x_1 = 1$$

와 체 F 에 대하여 $V = F[G]$ 라고 할 때, 각 $x\in G$ 에 대하여 다음과 같이 정의된 사상은 벡터공간 V 위의 F-선형변환이다.

$$R(x) : V \longrightarrow V, \quad R(x)(x_j) = xx_j \qquad (1\le j\le n)$$

이 때, V의 기저 $\mathscr{B} = G = \{x_1, x_2, \cdots, x_n\}$에 대하여

$$R(x)(\mathscr{B}) = \{xx_1, xx_2, \cdots, xx_n\} = \mathscr{B}$$

이므로 $R(x)$는 V 위의 정칙 선형변환이고 따라서 $R(x) \in \mathrm{GL}(V)$이다. 그리고 임의의 원소 $x, y \in G$에 대하여

$$\begin{aligned} R(xy)(x_j) &= xyx_j = x(yx_j) \\ &= R(x)(R(y)(x_j)) \\ &= (R(x) \circ R(y))(x_j) \qquad (1 \le j \le n) \end{aligned}$$

이므로 $R(xy) = R(x) \circ R(y)$이다. 따라서 사상

$$R : G \longrightarrow \mathrm{GL}(V), \quad x \longmapsto R(x)$$

는 군 G의 n차의 F-표현이다. 또한,

$$\begin{aligned} R(x) = 1_V &\Leftrightarrow R(x)(x_j) = x_j \qquad (1 \le j \le n) \\ &\Leftrightarrow xx_j = x_j \qquad (1 \le j \le n) \\ &\Leftrightarrow x = 1 \end{aligned}$$

이므로 $\ker R = \{1\}$이다. 즉, R는 G의 충실한 n차의 F-표현이다.

이와 같이 정의된 F-표현 $R : G \longrightarrow \mathrm{GL}(V)$를 G의 **(左) 정칙표현**(正則表現, left regular representation)이라고 한다.

한편, 각 원소 $x \in G$에 대하여

$$R(x)(x_j) = x_i \quad \text{즉} \quad xx_j = x_i \qquad (1 \le j \le n)$$

이라고 할 때, 행렬 $\varphi(x) = [R(x)]_{\mathscr{B}}$의 제 j열 성분은 (i, j) 성분만이 1이고 나머지 성분은 모두 0이다.

즉, $\varphi(x)$는 각 행과 각 열의 한 성분만이 1이고 나머지 성분은 모두 0인 **치환행렬**(permutation matrix)이다.

$$\begin{array}{c} \\ 1 \\ \vdots \\ x \\ \vdots \\ x_i \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \cdots & x_j & \cdots \end{array} \\ \left[\begin{array}{cccc} 0 & \cdots & 0 & \cdots \\ \vdots & & \vdots & \\ 1 & \cdots & 0 & \cdots \\ \vdots & & \vdots & \\ 0 & \cdots & 1 & \cdots \\ \vdots & & \vdots & \end{array}\right] \end{array} = \varphi(x)$$

이와 같이 F-표현 R에 의하여 정의된 기저 $\mathscr{B}$에 관한 행렬표현

$$\varphi : G \longrightarrow \mathrm{GL}_n(F), \quad \varphi(x) = [R(x)]_{\mathscr{B}}$$

를 G의 **(左) 正則行列表現**(left regular matrix representation)이라고 한다.

여기서 φ는 G의 충실한 n차의 F-행렬표현이다.

예를 들어, 위수 3인 순환군 $G = \{1, x, x^2\}$와 임의의 체 F에 대하여 다음이 성립한다.

$$R(x)(1) = x = 0\,1 + 1\,x + 0\,x^2$$
$$R(x)(x) = x^2 = 0\,1 + 0\,x + 1\,x^2$$
$$R(x)(x^2) = 1 = 1\cdot 1 + 0\,x + 0\,x^2$$

따라서 체 F 위에서의 G의 정칙 행렬표현 $\varphi : G \longrightarrow \mathrm{GL}_3(F)$는 다음과 같이 정의된 3차의 행렬표현이다(보기 2.2.2 의 (3) 참조).

$$\varphi(x) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \varphi(x^2) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \varphi(1) = I$$

보기 7 임의의 체 F 위에서의 대칭군 S_n의 표현을 생각해 보자.

이제 $\mathscr{B} = \{v_1, \cdots, v_n\}$를 기저로 가지는 n차원 F-벡터공간 V를 생각하고, 각 치환 $\sigma \in S_n$에 대하여 사상 $P(\sigma) : V \longrightarrow V$를 다음과 같이 정의된 F-선형변환이라고 하자.

$$P(\sigma)(v_j) = v_{\sigma(j)} \qquad (1 \le j \le n)$$

이 때,

$$\{\sigma(1), \cdots, \sigma(n)\} = \{1, \cdots, n\}$$

이므로 $P(\sigma)$는 정칙선형변환이고 따라서 $P(\sigma) \in \mathrm{GL}(V)$이다.

그리고 $\sigma, \tau \in S_n$라고 할 때, 각 j $(1 \le j \le n)$에 대하여

$$\begin{aligned} P(\sigma\circ\tau)(v_j) &= v_{(\sigma\circ\tau)(j)} = v_{\sigma(\tau(j))} \\ &= P(\sigma)(v_{\tau(j)}) = P(\sigma)(P(\tau)(v_j)) \\ &= (P(\sigma)\circ P(\tau))(v_j) \end{aligned}$$

이므로 $P(\sigma\circ\tau) = P(\sigma)\circ P(\tau)$이다.

따라서 사상

$$P : S_n \longrightarrow \mathrm{GL}(V), \quad \sigma \longmapsto P(\sigma)$$

는 대칭군 S_n의 n차의 F-표현이다. 또한,

$$\begin{aligned} P(\sigma) = 1_V &\Leftrightarrow P(\sigma)(v_j) = v_j \quad (1 \le j \le n) \\ &\Leftrightarrow \sigma(j) = j \quad (1 \le j \le n) \\ &\Leftrightarrow \sigma = 1 \end{aligned}$$

이므로 $\ker P = \{1\}$이다. 즉, P는 S_n의 충실한 n차의 F-표현이다.

대칭군 S_n의 F-표현 P에 의하여 정의된 기저 $\mathscr{B}$에 관한 행렬표현

$$\pi : S_n \longrightarrow \mathrm{GL}_n(F), \quad \pi(\sigma) = [P(\sigma)]_{\mathscr{B}}$$

는 S_n의 충실한 n차의 F-행렬표현이다.

여기서 각 j $(1 \le j \le n)$에 대하여 $P(\sigma)(v_j) = v_{\sigma(j)}$이므로 행렬 $\pi(\sigma)$의 각 제 j열의 성분은 $(\sigma(j), j)$ 성분만이 1이고 그 밖의 성분은 모두 0이다. 그리고 $\{\sigma(1), \cdots, \sigma(n)\} = \{1, \cdots, n\}$이므로 $\pi(\sigma)$의 각 행과 각 열에 대하여 단 한 개의 성분만이 1이고 그 밖의 성분은 모두 0이다. 즉, $\pi(\sigma)$는 치환행렬이다.

예를 들면, 대칭군

$$S_3 = \{1, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)\}$$

와 임의의 체 F에 대하여 S_3의 F-행렬표현

$$\pi : S_3 \longrightarrow \mathrm{GL}_3(F)$$

는 다음과 같이 정의된다.

$$\pi(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \pi((1\ 2\ 3)) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

$$\pi((1\ 3\ 2)) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \qquad \pi((2\ 3)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$\pi((1\ 3)) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \qquad \pi((1\ 2)) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

§8.8.1 정사영과 멱등행렬

여기서는, 특수한 선형변환과 행렬에 대하여 논한다.

정의 1 체 F 위의 벡터공간 V 위에서의 선형변환 $T : V \longrightarrow V$ 가 등식 $T^2 = T$ 를 만족시킬 때, T 를 **정사영**(正射影 projection) 또는 **멱등 선형변환**이라고 한다.

정리 2 체 F 위의 벡터공간 V 에서 부분공간 $W_1, \cdots, W_n$ 에 대하여 $V = W_1 \oplus \cdots \oplus W_n$ 이라고 하면, 각 벡터 $v \in V$ 는 단 한 가지 방법으로

$$v = w_1 + \cdots + w_i + \cdots + w_n \qquad (w_i \in W_i)$$

으로 나타내어진다. 이 때, 사상

$$T_i : V \longrightarrow V, \quad T_i(w_1 + \cdots + w_n) = w_i \qquad (1 \le i \le n)$$

는 정사영이고 다음이 성립한다.

$$\text{im } T_i = W_i, \quad \ker T_i = W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_n$$

증 명 임의의 벡터 $v, u \in V$ 와 $a \in F$ 에 대하여

$$v = w_1 + \cdots + w_n, \quad u = u_1 + \cdots + u_n \qquad (w_i, u_i \in W_i)$$

이라고 하면, 각 i $(1 \le i \le n)$ 에 대하여

$$\begin{aligned} T_i(v+u) &= T_i((w_1+u_1) + \cdots + (w_n+u_n)) \\ &= w_i + u_i = T_i(v) + T_i(u), \\ T_i(a\,v) &= T_i((a\,w_1) + \cdots + (a\,w_n)) = a\,w_i = a\,T_i(v) \end{aligned}$$

이므로 T_i 는 선형변환이다. 또,

$$\begin{aligned} {T_i}^2(v) &= T_i(T_i(v)) = T_i(w_i) \\ &= T_i(0 + \cdots + w_i + \cdots + 0) = w_i = T_i(v) \end{aligned}$$

이므로 ${T_i}^2 = T_i$ 이다. 그리고, 다음이 성립함을 알 수 있다.

$$\text{im } T_i = W_i, \quad \ker T_i = W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_n$$

정리 3 체 F 위의 벡터공간 V 에서 선형변환 $T : V \longrightarrow V$ 가 정사영이면, $V = \text{im } T \oplus \ker T$, $\text{im } T = \{w \in V \mid T(w) = w\}$ 이다.

증명 이제 $W_1 = \text{im } T$, $W_2 = \ker T$ 이라고 하자.

먼저 $w \in W_1$ 이면 $w = T(v)$ 인 $v \in V$ 가 존재하고 이때

$$w = T(v) = T^2(v) = T(T(v)) = T(w)$$

이고, $T(w) = w$ 이면 $w \in W_1$ 이므로 $W_1 = \{w \in V \mid T(w) = w\}$ 이다.

한편, 임의의 벡터 $v \in V$ 에 대하여

$$v = T(v) + (v - T(v))$$

이며, 여기서 $T(v) \in W_1$ 이고 또

$$T(v - T(v)) = T(v) - T(T(v)) = T(v) - T(v) = 0$$

이므로 $v - T(v) \in \ker T = W_2$ 이다. 따라서 $V = W_1 + W_2$ 이다.

그리고, $w \in W_1 \cap W_2$ 이라고 하면 $w \in W_1$ 이므로 $w = T(w)$ 이고 또 $w \in W_2$ 이므로 $w = T(w) = 0$ 이다. 따라서 $W_1 \cap W_2 = \{0\}$ 이다.

그러므로, $V = W_1 \oplus W_2$ 이다.

정의 4 체 F 위의 n 차의 행렬 A 가 등식 $A^2 = A$ 를 만족시킬 때, A 를 **멱등행렬**(idempotent matrix)이라고 한다.

정리 5 체 F 위의 n 차원 벡터공간 V 에서 $T \in \text{End}_F(V)$ 가 정사영(즉 $T^2 = T$) 일 때, $r(T) = r$ 이라고 하면 다음이 성립한다.

(1) $r = 0$ 이면 $T = 0_V$ 이고, 또 $r = n$ 이면 $T = 1_V$ 이다.

(2) $1 \leq r < n$ 일 때, $\mathscr{C}_1$ 과 $\mathscr{C}_2$ 를 각각 $\text{im } T$, $\ker T$ 의 기저라고 하면 $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$ 는 V 의 기저이고 또 기저 $\mathscr{C}$ 에 관한 T 의 행렬 $[T]_{\mathscr{C}}$ 는 다음과 같다,

$$[T]_{\mathscr{C}} = \begin{bmatrix} I_r & O \\ O & O \end{bmatrix}$$

증명 먼저 $r = 0$ 이면, $\text{im } T = \{0\}$, $\ker T = V$ 이므로 $T = 0_V$ 이다. 또, $r = n$ 이면, $\text{im } T = V$, $\ker T = \{0\}$ 이므로 모든 벡터 $v \in V$ 에 대하여 $T(v) = v$ 이고 따라서 $T = 1_V$ 이다(정리 2).

이제 $1 \leq r < n$ 이라고 하자. 이 때, 정리 2에 의하여

$$V = \text{im } T \oplus \ker T, \quad \text{im } T = \{w \in V \mid T(w) = w\},$$
$$\text{im } T \neq \{0\}, \qquad \ker T \neq \{0\}$$

이므로 $\mathscr{C}_1 = \{w_1, \cdots, w_r\}$, $\mathscr{C}_2 = \{u_1, \cdots, u_m\}$ 를 각각 $\text{im } T$, $\ker T$ 의 기저라고 하면 $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$ 는 V의 기저이고 또

$$T(w_i) = w_i,\ T(u_j) = \mathbf{0} \qquad (1 \leq i \leq r,\ 1 \leq j \leq m)$$

이므로 (2) 의 등식이 성립한다.

체 F 위의 n차의 행렬 $A \in \text{Mat}_n(F)$ 에 대하여 다음과 같이 정의된 사상은 선형변환이다.

$$L_A : F^n \longrightarrow F^n, \quad (y_1, \cdots, y_n) = L_A(x_1, \cdots, x_n)$$
$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

그리고, 행렬 A 가 멱등행렬일 때 그리고 이때에만 L_A 는 정사영이다.
따라서 정리 3 에 의하여 다음 정리가 성립한다.

정리 5 체 F 위의 n차의 행렬 A 가 멱등행렬일 때, 즉, $A^2 = A$ 일 때, 다음 중에서 하나가 성립한다.

(1) $A = O_n$

(2) $A = I_n$

(3) 적당한 양의 정수 r $(1 \leq r < n)$ 와 정칙행렬 $P \in \text{Mat}_n(F)$ 에 대하여 $P^{-1}AP = \begin{bmatrix} I_r & O \\ O & O \end{bmatrix}$ 이다.

보기 1 체 F 위의 3 차의 멱등행렬은 다음과 같이 분류된다.
여기서, $P \in \mathrm{Mat}_3(F)$ 는 임의의 정칙행렬이다.

(1) O_3 (2) I_3

(3) $P\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} P^{-1}$ (4) $P\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} P^{-1}$

§8.8.2 멱영행렬

다음 정리의 증명은 [6] 의 §8.6 에서 찾을 수 있다.

정리 1 체 F 위의 n 차의 행렬 $A=[a_{ij}]_{n\times n}$ 가 지수 m 인 멱영행렬일 때, A 의 고유다항식 $f(x)$ 는

$$f(x)=x^n$$

이고 A 의 최소다항식 $p(x)$ 는

$$p(x)=x^m \qquad (1\le m\le n)$$

이며 적당한 정칙행렬 $P\in \mathrm{Mat}_n(F)$ 에 대하여 다음이 성립한다.

$$P^{-1}AP=\mathrm{diag}\{J_1,\cdots,J_t\},$$

$$J_i=\begin{bmatrix}0&0&\cdots&0&0\\1&0&\cdots&0&0\\0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\ddots&0&0\\0&0&\cdots&1&0\end{bmatrix}_{s_i\times s_i}$$

여기서 $m=s_1\ge\cdots\ge s_t\ge 1, \quad s_1+\cdots+s_t=n$

위의 정리에서 행렬 $B=\mathrm{diag}\{J_1,\cdots,J_t\}$ 를 A 의 Jordna 표준형이라고 한다.

보기 2 체 F 위의 4 차의 행렬 A 가 지수 m 인 멱영행렬이라고 하면, A 의 고유다항식과 최소다항식은 각각 다음과 같다

$$f(x)=x^4, \qquad p(x)=x^m \quad (1\le m\le 4)$$

(1) $p(x)=x$ 인 경우에 $A=O_4$ 이다.

(2) $p(x)=x^2$ 인 경우에 $A\neq O_4,\ A^2=O_4$ 이다. 그리고,

$$m=2=s_1,\ s_2=2, \qquad t=2=n(A)$$

또는 $\quad m=2=s_1,\ s_2=1,\ s_3=1,\ \ t=3=n(A)$

이고 이에 따라 A 의 Jordan 표준형은 다음과 같다.

$$B = \left[\begin{array}{cc:cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right] \quad \text{또는} \quad B = \left[\begin{array}{cc:cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

그리고, 적당한 정칙행렬 P에 대하여 $B = P^{-1}AP$이다.

(3) $p(x) = x^3$ 인 경우에

$$m = 3 = s_1, \ s_2 = 1, \ \ t = 2 = n(A)$$

이고 A 의 Jordan 표준형은 다음과 같다.

$$B = \left[\begin{array}{ccc:c} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 \end{array}\right]$$

그리고, 적당한 정칙행렬 P에 대하여 $B = P^{-1}AP$이다.

(4) $p(x) = x^4$ 인 경우에

$$m = 4 = s_1, \ \ s_1 = 4, \quad t = 1 = n(A)$$

이고 A 의 Jordan 표준형은 다음과 같다.

$$B = \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

그리고, 적당한 정칙행렬 P에 대하여 $B = P^{-1}AP$이다.