선형대수학 2 숙제 #2

2017-18570 컴퓨터공학부 이성찬

11.3.18 (가) $(\mathbb{Z}, +) = \langle 1 \rangle$ 임은 자명하다. $(\mathbb{Z}, +)$ 에 0 은 당연히 있고, 1 이 있으니 -1 도 있고, 반복해서 더하면 임의의 정수를 만들 수 있으므로 $\cdots\cdots$. 이때, 가능한 generator 는 $1, -1$ 뿐이다. 만약 $a \in \mathbb{Z} - \{0\}$ $(|a| \neq 1)$ 가 generator 였다면, 지수법칙으로부터 $na = 1$ 이 되는 정수 n 이 존재해야만 한다. 하지만 이러한 정수 n 은 존재하지 않으므로 모순.

(다) $-2 + 3 = 1$ 이므로, 양변을 k배 하면 $(-k)2 + (k)3 = k$ 가 되어 임의의 정수를 생성할 수 있다. 마찬가지로 $(-26)4 + (7)15 = 1$ 으로부터 양변을 k배 하여 임의의 정수를 생성할 수 있다. $(k \in \mathbb{Z})$ 그리고 $S = \{6x + 9y \mid x, y \in \mathbb{Z} \text{ and } 6x + 9y > 0\}$ 에는 1 이 없다. 이 집합의 원소들은 전부 $\gcd(6, 9) = 3$의 배수 꼴이다.[1]

$6 \in S$ 이므로 S 는 nonempty 이고, well-ordering principle 에 의해 S 에는 최소의 원소 $d = 6s + 9t$ 가 존재한다. 이제 $d = \gcd(6, 9)$ 임을 보이자. 6 을 d 로 나누면 $6 = dq + r$, $0 \leq r < d$ 이고 $r = 6 - qd = 6 - q(6s + 9t) = 6(1 - qs) - 9qt$ 인데 $r \neq 0$ 이면 d 의 최소성에 모순이므로 $r = 0$. 따라서 $d \mid 6$ 이고 마찬가지로 $d \mid 9$. 이제 c 가 $6, 9$ 의 공약수라고 하자. 그러면 $6 = cu, 9 = cv$ 인 u, v 가 존재한다. 따라서 $d = 6s + 9t = cus + cvt = c(us + vt)$ 이므로 $c \mid d$ 가 되어 $c \leq d$. 따라서 $d = \gcd(6, 9)$.

11.3.20 (가) 우선 $\{id\}$. 그리고 2-cycle 들이 포함된 $\{id, (1, 2)\}, \{id, (2, 3)\}, \{id, (1, 3)\}$. 그리고 3-cycle 들이 포함된 $\{id, (1, 2, 3), (1, 3, 2)\}$, 그리고 마지막으로 S_3.[2]

(나) No. S_3 가 cyclic 이었다면, S_3는 commutative group 이다. 하지만 우리는 S_3 에서 일반적으로 교환법칙이 성립하지 않음을 잘 안다. 당장 서로 다른 두 transposition 을 잡아 계산해봐도 성립하지 않는다.

(다) $\sigma_1 = (1, 2), \sigma_2 = (2, 3)$ 으로 두면, $(1, 3) = \sigma_2 \circ \sigma_1 \circ \sigma_2$, $(1, 3, 2) = \sigma_2 \circ \sigma_1$ 이고 $(1, 2, 3) = (1, 3, 2)^2$ 이며 id 는 이미 포함되어 있으므로 S_3 를 생성했다.

$\sigma = (1, 2), \tau = (1, 2, 3)$ 으로 두면, $(1, 3, 2) = \tau^2$ 이고, $(1, 3) = \tau \circ \sigma$, $(2, 3) = \sigma \circ (1, 3) \circ \sigma$ 이고 id 는 이미 포함되어 있으므로 S_3 를 생성했다.

11.8.15 (가) $\mu_3 \times \mu_3$ 의 모든 원소는 3-제곱 하면 $(1, 1)$ 이 된다. 하지만 μ_9 에는 order 가 9 인 원소가 존재한다. Group 의 구조가 다르므로 not isomorphic.

(나) Let $\mu_2 = \{1, -1\}, \mu_3 = \{1, \zeta_3, \zeta_3^2\}, \mu_6 = \{1, \zeta_6, \ldots, \zeta_6^5\}$. Define $\varphi : \mu_2 \times \mu_3 \to \mu_6$ as

$$\varphi((-1)^r, \zeta_3^s) = \zeta_6^{(3r+2s) \bmod 6}, \qquad \text{where } r = 0, 1,\ s = 0, 1, 2$$

그리고 정의역의 6개의 원소들에 대하여 φ 가 bijective homomorphism 임을 확인할 수 있다. 따라서 $\mu_2 \times \mu_3 \approx \mu_6$.

---

[1] This is a proof of Bezout's Lemma.

[2] $|S_3| = 6$ 이므로 subgroup 의 원소 수로 가능한 것은 6의 약수인 1, 2, 3, 6 뿐이다.

11.9.12 $A, B \in \mathbf{SL}_n(\mathbb{R})$ 일 때,

$\det(CAC^{-1}) = 1$ 이므로 공역은 $\mathbf{SL}_n(\mathbb{R})$. φ 는 homomorphism 인가? $\varphi(AB) = CABC^{-1} = CAC^{-1}CBC^{-1} = \varphi(A)\varphi(B)$. 모든 B 에 대해 $\varphi(A) = B$ 인 A 가 존재하는가? $A = C^{-1}BC$. $\varphi(A) = \varphi(B)$ 이면 $A = B$ 인가? 양변에서 C^{-1}, C 를 cancel 하면 당연. 따라서 φ 는 $\mathbf{SL}_n(\mathbb{R})$ 의 automorphism.

$\det(A^{\mathbf{t}})^{-1} = 1$ 이므로 공역은 $\mathbf{SL}_n(\mathbb{R})$. ψ 는 homomorphism 인가? $\psi(AB) = ((AB)^{\mathbf{t}})^{-1} = (B^{\mathbf{t}}A^{\mathbf{t}})^{-1} = (A^{\mathbf{t}})^{-1}(B^{\mathbf{t}})^{-1} = \psi(A)\psi(B)$. 모든 B 에 대해 $\psi(A) = B$ 인 A 가 존재하는가? $A = (B^{-1})^{\mathbf{t}}$. $\psi(A) = \psi(B)$ 이면 $A = B$ 인가? 역행렬은 유일하므로 당연. 따라서 ψ 는 $\mathbf{SL}_n(\mathbb{R})$ 의 automorphism.

이제 $C \notin \mathbf{SL}_n(\mathbb{R})$ 인 경우를 살펴보자. (잘 모르겠습니다...)

우선 φ 의 경우 n이 홀수이거나 $\det C > 0$ 이면 inner. C 를 적당히 상수배하여 $\mathbf{SL}_n(\mathbb{R})$ 의 원소가 되게 할 수 있고 이 상수는 C^{-1} 과 곱해지는 과정에서 사라진다. 결국 $C \in \mathbf{SL}_n(\mathbb{R})$ 인 경우와 동일. 반면 n이 짝수이거나 행렬식이 0보다 작은 경우, $n = 2$ 인 경우만 살펴봐도 충분하다. (Block Matrix 를 생각하여 왼쪽 위 block에 2×2 행렬을, 오른쪽 아래 block에 I를, 나머지는 0을 넣는다) 이제 $C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 를 생각하면 φ 가 outer automorphism.

$n = 1$ 인 경우에만 trivial 하게 inner. $n = 2$ 인 경우 모든 $A \in \mathbf{SL}_2(\mathbb{R})$ 에 대해 $(A^{\mathbf{t}})^{-1}X = XA$ 인 X는 0 뿐이다. 이제 $n > 2$ 인 경우에는 $B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$ 에 대해서 생각하고 나머지는 위처럼 block matrix 를 생각해주면 trace 가 달라진다. (Inner automorphism 이면 trace 가 보존되어야 한다) 따라서 outer automorphism 이다.

11.9.21 우선 $S_n \approx S = \{I_\sigma \in \mathfrak{M}_{n,n}(F) \,|\, \sigma \in S_n\}$ 인 것은, 함수 $\varphi : S_n \to S$, $\varphi(\sigma) = I_\sigma$ 로부터 알 수 있다. $\sigma_1, \sigma_2 \in S_n$ 일 때, $\varphi(\sigma_1 \circ \sigma_2) = I_{\sigma_1 \circ \sigma_2} = I_{\sigma_1} I_{\sigma_2} = \varphi(\sigma_1)\varphi(\sigma_2)$. Surjectivity 는 자명. $\varphi(\sigma_1) = \varphi(\sigma_2)$ 이면 $I_{\sigma_1} = I_{\sigma_2}$ 이므로 $\sigma_1 = \sigma_2$. φ 는 group isomorphism.

이제 S 의 행렬들에 대응하는 선형사상을 $\{P_\sigma \in \mathfrak{L}(V, V) \,|\, \sigma \in S_n\}$ 로 정의했고 행렬과 선형사상은 같으므로 두 group 은 isomorphic. Isomorphism 은 equivalence relation 이므로 세 group 은 서로 isomorphic.

11.9.25 **(가)** 정5각형을 그려 꼭짓점에 1, ..., 5 로 numbering 하고, $\sigma = (2, 5)(3, 4)$ 를 생각하면 이는 1번 꼭짓점을 고정하고, 2, 5번 꼭짓점과 3, 4 번 꼭짓점을 서로 바꾸어 주므로 reflection 이다. 그리고 $\tau = (1, 2, 3, 4, 5)$ 는 rotation 으로 생각하면, 5번 회전하면 id 이다. 따라서 G_5는 reflection 과 $2\pi/n$ rotation 으로 생성되었으므로, dihedral group 의 정의와 일치한다. $G_5 \approx D_5$.

(나) 정6각형을 그리고 마찬가지로 numbering 하고, $(2, 6)(3, 5)$ 를 생각하면 이는 1, 4번 꼭짓점을 고정하고, 2, 6번 꼭짓점과 3, 5번 꼭짓점을 서로 바꾸어 주는 reflection 이다. 그리고 $(1, 2, 3, 4, 5, 6)$ 은 6번 회전하면 id 가 되는 rotation 이다. (가)에서와 마찬가지 논리로 $G_6 \approx D_6$.

(다) 정n각형의 꼭짓점을 1, ..., n 으로 numbering 하고, 우선 $\tau = (1, \ldots, n)$ 으로 잡

는다. 그리고 n이 짝수이면 $1, (n/2+1)$번 꼭짓점을 지나는 직선을 대칭축으로 하는 reflection 으로 $\sigma = (2,n)(3,n-1)\cdots(n/2, n/2+2)$ 를 생각한다. n이 홀수이면, 1번 꼭짓점과 $(n+1)/2, (n+1)/2+1$번 꼭짓점의 중점을 지나는 직선을 대칭축으로 하는 reflection 으로 $\sigma = (2,n)(3,n-1)\cdots((n+1)/2, (n+1)/2+1)$ 을 생각한다.

12.2.20 (가) $A \in Z(\mathbf{GL}_n(F))$ 라고 하자. Any elementary matrix X 에 대해서 $AX = XA$ 를 만족해야 한다. X 가 만약 i번째 열 (또는 행 - 왼쪽/오른쪽 중 어디에 곱하느냐에 따라)를 $a(\neq 0)$배 해주는 elementary matrix 라고 해보자. A의 i열에 a배를 해도 $AX = XA$ 가 성립하려면, 그 열의 i행 성분을 제외하고는 전부 0 이어야 한다. 마찬가지 논리를 적용하면 A는 최소한 diagonal matrix 이어야 한다. $A = \mathrm{diag}(a_1, \ldots, a_n)$ 으로 두고, det 가 0이 아니므로 $a_i \neq 0$. 이제 $X = I_\sigma$ ($\sigma = (i,j)$ is any transposition in S_n) 를 잡아 $AX = XA$ 를 계산하면 $a_i = a_j$ 를 얻는다. 이상으로부터 $Z(\mathbf{GL}_n(F)) = \{\lambda I_n \mid \lambda \in F^\times\}$.

(나) $\{\lambda I_n \mid \lambda \in F^\times\}$ 에 포함되지 않은 $Z(\mathbf{SL}_n(F))$ 의 원소가 존재한다면, $\mathbf{SL}_n(F) \subset \mathbf{GL}_n(F)$ 이므로 그 원소는 $Z(\mathbf{GL}_n(F))$ 에 있어야 하므로 모순이다. 따라서 λI 꼴만 고려하면 되며, 이 경우 det 가 1 이므로 $\lambda^n = 1$ 인 경우만 가능하다. 따라서 $Z(\mathbf{SL}_n(F)) = \{\lambda I_n \mid \lambda^n = 1, \lambda \in F^\times\}$.

12.4.7 (가) $\overline{A} = \overline{B} \in \mathbf{GL}_n(F)/\mathbf{SL}_n(F) \Leftrightarrow B^{-1}A \in \mathbf{SL}_n(F) \Leftrightarrow \det(B^{-1}A) = 1 \Leftrightarrow \det A = \det B$

(나) $\mathbf{GL}_n(F)/\mathbf{SL}_n(F) \approx F^\times$ 이므로 $F^\times$ 에서 적절하게 원소를 뽑아오면 된다.

$$\mathbf{GL}_n(F) = \coprod_{\lambda \in F^\times} \lambda I_n \cdot \mathbf{SL}_n(F)$$

(다) $\mathbf{U}(n)/\mathbf{SU}(n) \approx S^1$ 이므로 S^1 에서 적절하게 원소를 뽑아오면 된다.

$$\mathbf{U}(n) \coprod_{0 \le \theta < 2\pi} e^{\frac{\mathrm{i}\theta}{n}} I_n \cdot \mathbf{SU}(n)$$

12.4.11 (가) For $g, h \in G$, $\mathrm{Int}(gh) = \mathrm{Int}(g) \circ \mathrm{Int}(h)$ 인지 확인하면 된다. 이제 $x \in G$ 에서 evaluate 하면, $\mathrm{Int}(gh)(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g\mathrm{Int}(h)(x)g^{-1} = (\mathrm{Int}(g) \circ \mathrm{Int}(h))(x)$.

(나) $\mathrm{Int}(G) \leq \mathrm{Aut}(G)$.

$g \in G, \varphi \in \mathrm{Aut}(G)$ 일 때, $\varphi \circ \mathrm{Int}(g) \circ \varphi^{-1} \in \mathrm{Int}(G)$ 를 보인다. Evaluate at $x \in G$.

$$(\varphi \circ \mathrm{Int}(g) \circ \varphi^{-1})(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)x\varphi(g^{-1}) = \varphi(g)x\varphi(g)^{-1}$$

그런데 $\varphi(g) \in G$ 이므로 $\varphi \circ \mathrm{Int}(g) \circ \varphi^{-1} \in \mathrm{Int}(G)$. 따라서 $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$.

(다) $\mathrm{Aut}(G)$ 의 항등원은 id (항등사상) 이므로

$$g \in \ker(\mathrm{Int}) \Leftrightarrow \mathrm{Int}(g) = id \Leftrightarrow gxg^{-1} = x, \text{for } x \in G \Leftrightarrow gx = xg \Leftrightarrow g \in Z(G)$$

따라서 $\ker(\mathrm{Int}) = Z(G)$ 이고, First Isomorphism Thm. 에 의하여 $G/Z(G) \approx \mathrm{Int}(G)$.

12.4.12 (가) (나)에서 ψ 가 group homomorphism 인 것을 보일 것이다. 그리고 $ad - bc = 1$ 임을 이용하여 다음을 계산한다.

$$\det \begin{pmatrix} a^2 & -2ac & -c^2 \\ -ab & ad+bc & cd \\ -b^2 & 2bd & d^2 \end{pmatrix} = (ad-bc)^3 = 1$$

그러므로 사실 공역은 $\mathbf{SL}_n(F)$ 이고 group homomorphism 에 대하여 image 가 공역의 subgroup 인 것은 당연하다.

(나) $A, B \in \mathbf{SL}_2(F)$ 라고 하자. 다음과 같이 두고 계산한다.

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, B = \begin{pmatrix} e & g \\ f & h \end{pmatrix}, AB = \begin{pmatrix} ae+cf & ag+ch \\ be+df & bg+dh \end{pmatrix}$$

$$\begin{aligned} \psi(A)\psi(B) &= \begin{pmatrix} a^2 & -2ac & -c^2 \\ -ab & ad+bc & cd \\ -b^2 & 2bd & d^2 \end{pmatrix} \begin{pmatrix} e^2 & -2eg & -g^2 \\ -ef & eh+gf & gh \\ -f^2 & 2fh & h^2 \end{pmatrix} \\ &= \begin{pmatrix} (ae+cf)^2 & -2(ae+cf)(ag+ch) & -(ag+ch)^2 \\ -(ae+cf)(be+df) & (ae+cf)(bg+dh)+(ag+ch)(be+df) & (ag+ch)(bg+dh) \\ -(be+df)^2 & 2(be+df)(bg+dh) & (bg+dh)^2 \end{pmatrix} \\ &= \psi(AB) \end{aligned}$$

따라서 group homomorphism 이고, $\ker\psi$ 의 원소는 ψ 에 의해 I_3 로 map 된다. $a^2 = 1, ad+bc = 1, d^2 = 1, b = c = 0$ 이므로 $a = \pm 1, d = \pm 1$. $\ker\psi = \{\pm I_2\}$. 그리고 이 집합이 $Z(\mathbf{SL}_2(F))$ 와 같은 것은 당연.