주의 및 추가

연습문제 0. 표지 그림은 LCG (Linear Congruence Generator) 를 이용하여 만들어졌다. 즉, $x_1 = 1015568748$ 에서 시작하여

$$x_{n+1} \equiv ax_n + b \pmod N$$

을 이용하여 (보기 12.2.8 의 표기법 참조), $x_2, x_2, \ldots$ 를 구한 후 모두 10-digit 의 수로 나타낸 것이다. 따라서, 각 row 에는 각각 5 개의 10-digit 의 수가 있다. 예를 들어, $x_2 = 1586005467$ 이고, $x_{21} = 0927463856$ 이다 (x_{21} 은 실제는 9 자리 수). **이때, 자연수 a, b 와 N 을 구하라**.

주의 1. 이 책에서 [최초의 1] 은 항상 정의 1.2.2 에 있는 의미로 사용된다. 따라서, 정리 4.4.4 의 증명이나 보기 5.4.14 등의 [최초의 1 을 포함하는 column] 의 표현도 정의 1.2.2 에 있는 의미로 받아들여야 한다. 예를 들어, 연습문제 1.2.1 (나) 항의 (4×7)-행렬에서 $(1, 2)$-성분의 1 은 [최초의 1] 이 아니고, 따라서 이 행렬의 second column 은 [최초의 1 을 포함하는 column] 이 아니다.

주의 2. 주의 3.2.5 는 여전히 미묘하다. 이는 $\{a, b\} = \{a, a, b\}$ 이므로 생기는 피할 수 없는 문제이다. 우리가 "집합 S 가 일차종속(일차독립)"이라고 말할 때에는 S 의 한 원소를 두 번 이상 '쓰지' 않는 것으로 이해해야 한다. 만약 이 원칙이 없다면 집합 S 의 일차종속(일차독립) 여부를 판정할 수 없을 것이다. 물론 집합을 원소나열법으로 나타낼 때는 주의 3.2.5 의 원칙을 따른다.

추가 3. 정리 5.3.5 (선형대수학의 기본정리) 에서 함수 $\Phi_{\mathfrak{C}}^{\mathfrak{B}} : \mathfrak{M}_{m,n}(F) \to \mathfrak{L}(V, W)$ 가 well-defined 되어 있는지 설명이 필요. 즉, $A \in \mathfrak{M}_{m,n}(F)$ 일 때, $\Phi_{\mathfrak{C}}^{\mathfrak{B}}(A) \in \mathfrak{L}(V, W)$ 인지 확인하여야 한다.

추가 4. §5.4 에 **Rank Theorem 의 새 증명 추가**: $A \in \mathfrak{M}_{m,n}(F)$ 일 때, $UA = R$ 을 A 의 row-reduced echelon form 이라고 하자 (단, $U \in \mathfrak{M}_{m,m}(F)$ 는 가역). 그러면, A 와 R 의 row rank 는 같다 (따름정리 4.4.7). 한편, L_U 는 isomorphism 이므로, A 와 R 의 column rank 도 같다 (왜 그런가?). 이제 행 간소 사다리꼴의 row rank 와 column rank 는 당연히 같으므로, 증명 끝.

추가 5. 연습문제 5.5.9 에 추가: $[\alpha_{\mathfrak{B}}^{\mathcal{E}} = L_P, \ \alpha_{\mathcal{F}}^{\mathfrak{C}} = L_Q]$.

추가 6. §5.6 에 **row-reduced echelon form 의 uniqueness 새 증명 추가**: Elementary row operation 은 row space 를 변화시키지 않으므로, 아래 보조정리에 의해 당연.

보조정리 $R, S \in \mathfrak{M}_{m,n}(F)$ 가 row-reduced echelon form 이고, R 의 row space 와 S 의 row space 가 같으면, $R = S$.

증명: 우선, row-reduced echelon form 의 일반적인 모습은 다음과 같다:

$$[L_A]_{\mathfrak{C}}^{\mathcal{E}} = \begin{array}{c} \begin{array}{cccccccc} & k_1 & & k_2 & & k_3 & & \\ & \downarrow & & \downarrow & & \downarrow & & \end{array} \\ \begin{pmatrix} \mathbf{0} & 1 & * & 0 & * & 0 & * & \cdots \\ \mathbf{0} & 0 & \mathbf{0} & 1 & * & 0 & * & \cdots \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & 1 & * & \cdots \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & \cdots \end{pmatrix} \end{array}.$$

위 행렬에서, 굵은 $\mathbf{0}$ 이나 $*$ 는 여러 column 을 계속할 수도 있다는(없을 수도 있고) 뜻이고, $*$ 는 무언가(zero 이건 non-zero 이건) 있다는 뜻이다. 물론 $k_1, \ldots, k_r$ 은 [최초의 1]을 갖는 column 의 위치를 나타낸다.

[Step 1] Row space 가 같으면, 그의 dimension(즉, row rank)도 같다. 그리고 row-reduced echelon form 의 row rank 는 당연히 [최초의 1]의 개수와 같다. 이제 R, S 의 (공통의) row rank 를 r 로 표기하자.[1]

[Step 2] R, S 의 첫 번째 row 의 [최초의 1]의 위치(즉, 위 행렬의 k_1)는 같다. 왜냐하면, k_1 은 R, S 의 row space 에 속하는 vector 들의 첫 번째 non-zero 좌표이기 때문이다.

[Step 3] 위 행렬에서 첫 번째 row 를 제거해도 row-reduced echelon form 이 남는다.[2] 뿐만 아니라, R, S 의 첫 번째 row 를 제거한 두 행렬도 여전히 같은 row space 를 갖는다. 이를 증명하려면, $2 \le i \le r$ 일 때, $[R]_i \in \langle [S]_2, \ldots, [S]_r \rangle$ 임을 보이면 된다(왜 그런가?). 그런데

[1] 만약 $r = 0$ 이면, $R = S = 0$ 이므로, $r > 0$ 이라고 가정하자.

[2] 물론 $m > 1$ 일 때.

$$[R]_i = a_1[S]_1 + a_2[S]_2 + \cdots + a_r[S]_r$$

인 $a_1, \ldots, a_r \in F$ 가 존재하고, 이 식 양변의 k_1-좌표를 비교하면, $0 = a_1$ 임을 알 수 있다. 앞 [Step 2]에 의해, $[R]_i$ 의 [최초의 1]의 위치는 k_1 보다 크기 때문이다. (따라서, 이제 r 에 관한(또는 m 에 관한) 귀납법이 가능하다.)

[Step 4] 앞 [Step 3]를 이용하는 귀납법과 [Step 2]에 의해, R, S 의 [최초의 1]의 위치 $k_1, \ldots, k_r$ 은 모두 같다.

[Step 5] $[R]_1 = [S]_1$ 이다. 이를 증명하기 위해

$$[R]_1 = b_1[S]_1 + b_2[S]_2 + \cdots + b_r[S]_r$$

이라고 하자(단, $b_1, \ldots, b_r \in F$). 먼저 이 식 양변의 k_1-좌표를 비교하면 $1 = b_1$ 임을 알 수 있다. 그리고, $1 < i \leq r$ 일 때, 이 식 양변의 k_i-좌표를 비교하면 — [Step 4]에 의해 $[R]_1$ 의 k_i-좌표는 0 이므로 — $0 = b_i$ 인 것도 알 수 있다.

[Step 6] 이제 [Step 3]의 귀납법을 다시 사용하면, [Step 5]에 의해, $R = S$. $\square$

주의 7. 논리적으로는 정리 7.4.3 (minimal polynomial 의 존재와 유일성) 이 관찰 7.4.2 보다 먼저 다루어져야 할 것이다.

추가 8. 연습문제 11.7.7 (마) 항 추가; $|x| = n$ 이면, [$x^a = x^b$ if and only if $a \equiv b \pmod{n}$].

정오표

p. 45, 밑 10 행 ; $(j = 1, \ldots, n) \longrightarrow (i = 1, \ldots, n)$.

p. 101, 밑 12 행 ; 위 (다-ii) 를 (나) 항의 $\longrightarrow$ 위 (나-ii) 를 (가) 항의.

p. 109, 6 행 ; $[(3) \Leftrightarrow (6)] \longrightarrow [(6) \Leftrightarrow (9)]$.

p. 122, 밑 2 행 ; $(n - r) \longrightarrow (m - r)$.

p. 139, 4 행 ; matrx $\longrightarrow$ matrix.

p. 147, 9 행 ; $\widehat{A}_{ik} \longrightarrow \widehat{A}_{ij}$.

p. 147, 12 행 ; $D^i(A) \longrightarrow D_i(A)$.

p. 153, 註 ; $A\mathbf{e}_j = \sum_{i=j}^{n} a_{ij}\mathbf{e}_i \longrightarrow A\mathbf{e}_j = \sum_{i=1}^{j} a_{ij}\mathbf{e}_i$.

p. 165, 관찰 7.2.4 ; $[L]_{\mathfrak{B}}^{\mathfrak{B}}$ 가 diagonalizable $\longrightarrow$ $[L]_{\mathfrak{B}}^{\mathfrak{B}}$ 가 diagonal.

p. 167, 2 행 ; 이 식의 계속 $\longrightarrow$ 이 식에 계속.

p. 173, 밑 1 행 ; $0 \neq a \in F \longrightarrow a \in F$.

p. 180, 4 행 ; $i = 1, \ldots k \longrightarrow i = 1, \ldots, k$.

p. 206, 밑 11 행 ; $p(t)^{r_{ij}} \longrightarrow p_i(t)^{r_{ij}}$.

p. 224, 밑 7 행 ; $L \in \mathfrak{M}_{n,n}(\mathbb{R}) \longrightarrow \mathfrak{L}(\mathbb{R}^n, \mathbb{R}^n)$.

p. 273, 9 행 및 밑 4 행 ; 관찰 $\longrightarrow$ 명제.

p. 326, 1 행 ; patition $\longrightarrow$ partition.

p. 344, 6 행 ; φ 의 역함수 $\longrightarrow$ $\overline{\varphi}$ 의 역함수.

p. 410, ; 15.1.10 (가) $\longrightarrow$ 15.1.10.

p. 417, 밑 2 행 ; 14.9.3 $\longrightarrow$ 14.9.4.

p. 428, 밑 7 행 ; hyphothesis $\longrightarrow$ hypothesis.

p. 429, 8 행 ; $D_n(F) \longrightarrow D_n(\mathbb{C})$.