e의 초월성에 대한 미적분학 레벨의 증명

sos440

2011년 7월 30일

1 준비물

이번 장에서는 증명과정에서 특별히 언급하지 않고 넘어갈 내용들 중 일부 중요한 내용들을 미리 소개하고 증명하도록 하겠습니다. 우선 본 증명에서 가장 기초적으로 사용되는 내용 중 하나는 다음 정리입니다.

> 정리 **1.** k 가 0 이상의 정수이면, 다음 식이 성립한다.
>
> $$k! = \int_0^\infty x^k e^{-x}\, dx \tag{1}$$

증명. 수학적 귀납법으로 원하는 사실을 보여보자. 우선 $k = 0$ 이면

$$\int_0^\infty e^{-x}\, dx = \lim_{R\to\infty} \int_0^R e^{-x}\, dx = \lim_{R\to\infty} \left(1 - e^{-R}\right) = 1$$

이므로 원하는 사실이 성립한다. 이제 식 (1) 이 k 에 대해 성립한다고 가정하자. 그러면

$$\begin{aligned}
\int_0^\infty x^{k+1} e^{-x}\, dx &= \lim_{R\to\infty} \int_0^R x^{k+1} e^{-x}\, dx \\
&= \lim_{R\to\infty} \left(\left[-x^{k+1} e^{-x}\right]_0^R + (k+1) \int_0^R x^k e^{-x}\, dx \right) \\
&= (k+1) \int_0^\infty x^k e^{-x}\, dx \\
&= (k+1) \cdot k! \\
&= (k+1)!
\end{aligned}$$

이고, 수학적 귀납법으로부터 원하는 사실이 증명된다. ■

> 정리 **2.** $f : [a,b] \to \mathbb{R}$ 가 연속함수이면 다음 부등식이 성립한다.
>
> $$\left| \int_a^b f(x)\, dx \right| \le \int_a^b |f(x)|\, dx \tag{2}$$

증명. $\pm f(x) \le |f(x)|$ 가 항상 성립하고, 이 부등호 관계는 양 변을 a 에서 b 까지 적분해도 유지된다. 따라서

$$\pm \int_a^b f(x)\, dx \le \int_a^b |f(x)|\, dx \tag{3}$$

이 성립하고, 좌변은 부호를 적절히 선택해서 $\left| \int_a^b f(x)\, dx \right|$ 로 만들 수 있다. 따라서 증명된다. ■

2 증명

e가 초월수임을 증명하기 위한 전략은 다음과 같습니다. 우선 e가 초월수가 아니라고 가정합니다. 그러면 어떤 자연수 n과 어떤 정수들 $a_0, \cdots, a_n$ (단, $a_n \neq 0$)이 존재하여, e가 다음 방정식

$$a_n e^n + \cdots + a_1 e + a_0 = 0 \tag{4}$$

를 만족할 것입니다. 이때 우리는 각각의 e^k를 특정한 유리수로 근사할 것입니다. 구체적으로, 어떤 정수 $M, M_1, \cdots, M_n$과 어떤 충분히 작은 수들 $\epsilon_1, \cdots, \epsilon_n$ 들을 찾아서

$$e^k = \frac{M_k + \epsilon_k}{M} \quad (k = 1, \cdots, n) \tag{5}$$

이 성립하도록 만들 것입니다. 여기서 ϵ_k 들이 얼마나 작은지는 추후에 결정될 것입니다. 한편 이를 (4)에 대입하여 정리하면

$$(a_0 M + a_1 M_1 + \cdots + a_n M_n) + (a_1 \epsilon_1 + \cdots + a_n \epsilon_n) = 0$$

가 됩니다. 그런데 좌변 중에서 앞쪽의 괄호 안의 식은 전체가 정수가 됩니다. 그리고 우리는 중간 과정에서 M을 적절하게 잡아서 이 앞쪽의 괄호 부분이 0이 되지 않도록 만들 것입니다. 한편, 우리는

$$|a_1 \epsilon_1 + \cdots + a_n \epsilon_n| < \frac{1}{2}$$

가 성립하도록 ϵ_k 들을 결정할 것입니다. 이제 이러한 선택이 가능하다고 가정하면 모순이 발생함을 알 수 있습니다. 왜냐하면

$$|a_0 M + a_1 M_1 + \cdots + a_n M_n| = |a_1 \epsilon_1 + \cdots + a_n \epsilon_n| < \frac{1}{2}$$

에서 좌변은 0이 아닌 정수에 절대값을 취했으므로 1 이상이 되어야 하는데, 이 값이 $\frac{1}{2}$보다 작다는 결론이 나왔기 때문이지요.

이제부터 우리는 위의 모든 조건들을 만족시키는 $M, M_1, \cdots, M_n$과 $\epsilon_1, \cdots, \epsilon_n$을 선택하는 것이 가능하다는 것을 보일 것입니다.

정리 **3.** *e는 초월수다. 즉, e는 어떠한 정수계수 방정식의 근도 되지 않는다.*

증명. e가 초월수가 아니라고 합시다. 그러면 어떤 자연수 n과 어떤 정수들 $a_0, \cdots, a_n$ (단, $a_n \neq 0$)이 존재하여, e가 식 (4)가 성립합니다. 이제 $p > n$이 소수라고 합시다. 그리고 이때 $M, M_1, \cdots, M_n$과 $\epsilon_1, \cdots, \epsilon_n$

을 다음과 같이 정의합시다.

$$
\begin{aligned}
M &= \int_0^\infty \frac{x^{p-1}\left\{(x-1)\cdots(x-n)\right\}^p e^{-x}}{(p-1)!}\,dx,\\
M_k &= e^k\int_k^\infty \frac{x^{p-1}\left\{(x-1)\cdots(x-n)\right\}^p e^{-x}}{(p-1)!}\,dx,\\
\epsilon_k &= e^k\int_0^k \frac{x^{p-1}\left\{(x-1)\cdots(x-n)\right\}^p e^{-x}}{(p-1)!}\,dx.
\end{aligned}
$$

여기서 다시 한 번 각 변수들의 설정을 체크해보자면, n 과 $a_0, \cdots, a_n$ 은 귀류법 가정으로부터 튀어나온 변수들이며, 증명과정 내내 고정되어 있습니다. 한편 M, M_k, ϵ_k 은 소수 p 의 선택과 (M_k, ϵ_k 의 경우) $k = 1, \cdots, n$ 에 의존하는 양입니다. 우리는 여기서 M, M_k, ϵ_k 들의 성질을 살펴본 후, p 를 적당히 선택해서 원하는 결론을 이끌어내도록 하겠습니다.

1 단계) 우선 M 을 살펴보도록 합시다. M 을 정의하는 적분식 내부에는

$$(x-1)\cdots(x-n)$$

라는 식이 등장합니다. 이 식은 전개를 해 보면

$$x^n + \cdots \pm n!$$

이 됩니다. (중간의 항들은 별로 중요하지도 않고, 사실 관심도 없습니다. 단지 계수가 정수라는 사실이 중요합니다.) 그리고 이 식을 다시 p 제곱하면

$$\left\{(x-1)\cdots(x-n)\right\}^p = x^{pn} + \cdots + (n!)^p$$

가 성립합니다. 그러므로

$$M = \sum_{j=0}^{np} \frac{1}{(p-1)!}\, c_j \int_0^\infty x^{p-1+j} e^{-x}\,dx$$

가 성립합니다. 단, c_j 는 다항식 $\left\{(x-1)\cdots(x-n)\right\}^p$ 을 전개하면서 튀어나온 j 차항의 계수로써 정수이며, 특별히 $c_0 = \pm(n!)^p$ 가 성립합니다. 따라서 정리 1 로부터

$$M = \sum_{j=0}^{np} c_j \frac{(p-1+j)!}{(p-1)!}$$

이 성립합니다. 이제 이 식을 조금 더 자세하게 살펴봅시다. 위 합에서 $j = 0$ 일 때의 항은

$$c_0 \frac{(p-1)!}{(p-1)!} = \pm(n!)^p$$

가 되는데, 우리는 $p > n$ 이고 p 가 소수이므로, $n!$ 은 p 를 인수로 갖지 않음을 압니다. 이 말은, 위 식이 p

로 나눠떨어지지 않음을 뜻합니다. 한편 $j \geq 1$ 인 경우

$$c_j \frac{(p-1+j)!}{(p-1)!} = c_j p(p+1)\cdots(p-1+j)$$

가 성립하고, 따라서 이 식은 p 로 나눠떨어집니다. 그러므로 M 은 p 로 나눠떨어지지 않습니다.

2단계) 이제 M_k 를 살펴봅시다.

$$\begin{aligned} M_k &= e^k \int_k^\infty \frac{x^{p-1}\left\{(x-1)\cdots(x-n)\right\}^p e^{-x}}{(p-1)!}\,dx \\ &= \int_k^\infty \frac{x^{p-1}\left\{(x-1)\cdots(x-n)\right\}^p e^{-(x-k)}}{(p-1)!}\,dx \end{aligned}$$

이 성립하고, 치환 $u = x - k$ 를 통하여 다음 식이 성립함을 알 수 있습니다.

$$M_k = \int_0^\infty \frac{(u+k)^{p-1}\left\{(u+k-1)\cdots u \cdots (u+k-n)\right\}^p e^{-u}}{(p-1)!}\,du$$

이 경우도 아까 M 에서와 비슷하지만, 결정적인 차이가 있습니다. 바로 다항식

$$(u+k)^{p-1}\left\{(u+k-1)\cdots u \cdots (u+k-n)\right\}^p$$

이 u^p 를 인수로 갖고 있다는 것이지요. 따라서 이 다항식을 전개해서

$$(u+k)^{p-1}\left\{(u+k-1)\cdots u \cdots (u+k-n)\right\}^p = c_{np+p-1}^{(k)} u^{np+p-1} + \cdots + c_p^{(k)} u^p$$

로 적었을 때, 이 정수계수들 $c_j^{(k)}$ 이 구체적으로 어떻게 주어지는지와는 상관없이,

$$M_k = \sum_{j=0}^{np-1} \frac{1}{(p-1)!} c_{p+j}^{(k)} \int_0^\infty u^{p+j} e^{-u}\,du = \sum_{j=0}^{np-1} c_{p+j}^{(k)} \frac{(p+j)!}{(p-1)!}$$

는 항상 p 의 배수가 됩니다.

3단계) 이제 ϵ_k 를 살펴봅시다. 구체적으로 ϵ_k 의 크기에 대한 정보를 얻어봅시다. $k = 1, \cdots, n$ 일 때, 정리 2로부터

$$\begin{aligned} |\epsilon_k| &\leq e^k \int_0^k \frac{x^{p-1}\left|(x-1)\cdots(x-n)\right|^p e^{-x}}{(p-1)!}\,dx \\ &\leq e^k \int_0^n \frac{x^{p-1}\left|(x-1)\cdots(x-n)\right|^p e^{-x}}{(p-1)!}\,dx \\ &\leq e^n \int_0^n \frac{n^{p-1}\left|(x-1)\cdots(x-n)\right|^p e^{-x}}{(p-1)!}\,dx \\ &= \frac{e^n n^{p-1}}{(p-1)!} \int_0^n \left|(x-1)\cdots(x-n)\right|^p e^{-x}\,dx \end{aligned}$$

이 성립합니다. 한편 함수 $f(x) = |(x-1)\cdots(x-n)|$ 는 폐구간 $[0,n]$ 위에서 연속이므로, 최대값 A 를 갖습니다. (그리고 당연하게도, 이 최대값은 k 나 p 에 의존하지 않습니다.) 따라서 부등식

$$\begin{aligned} |\epsilon_k| &\leq \frac{e^n n^{p-1}}{(p-1)!}\int_0^n A^p e^{-x}\,dx \\ &\leq \frac{e^n n^{p-1}}{(p-1)!}\int_0^\infty A^p e^{-x}\,dx \\ &= \frac{e^n n^{p-1} A^p}{(p-1)!} \\ &= \frac{e^n}{n}\frac{(nA)^p}{(p-1)!} \end{aligned}$$

이 성립합니다. 그리고 맨 마지막 식이 $p \to \infty$ 일 때 0 으로 수렴하므로, 샌드위치 정리로부터 $p \to \infty$ 일 때 $\epsilon_1, \cdots, \epsilon_n$ 각각 모두 0 으로 수렴합니다.

4단계) 이제 모든 결과들을 종합하고 논리를 정리해서 원하는 모순을 이끌어내봅시다. 우선 M, M_k, ϵ_k 의 정의로부터, 우리는 식 (5) 이 성립함을 쉽게 확인할 수 있습니다. 따라서 이미 살펴봤듯이, 식

$$(a_0 M + a_1 M_1 + \cdots + a_n M_n) + (a_1\epsilon_1 + \cdots + a_n\epsilon_n) = 0 \tag{6}$$

이 성립합니다.

다음으로, 우리는 p 가 n 보다 큰 소수인 한, 그 선택이 자유로우므로, 추가적으로 $p > |a_0|$ 이라고 가정하여도 무방합니다. 그러면 M 과 a_0 모두 p 의 배수가 아니므로, $a_0 M$ 역시 p 의 배수가 아닙니다. 한편 $a_1M_1 + \cdots + a_nM_n$ 는 $M_1, \cdots, M_n$ 들이 모두 p 의 배수이므로 이 전체 식 역시 p 로 나눠떨어집니다. 따라서 (6) 에서 앞쪽 괄호 내의 식

$$a_0 M + a_1 M_1 + \cdots + a_n M_n$$

역시 p 로 나눠떨어지지 않습니다. 특별히, 우리는 이 값이 0 이 아닌 정수라는 사실로부터 부등식

$$|a_0 M + a_1 M_1 + \cdots + a_n M_n| \geq 1$$

을 얻습니다.

한편 (6) 으로부터

$$|a_0 M + a_1 M_1 + \cdots + a_n M_n| = |a_1\epsilon_1 + \cdots + a_n\epsilon_n|$$

이 성립합니다. 그러나 각각의 $\epsilon_1, \cdots, \epsilon_n$ 들은 $p \to \infty$ 일 때 0 으로 수렴하므로, p 를 충분히 크게 잡으면

$$|a_1\epsilon_1 + \cdots + a_n\epsilon_n| \leq \frac{1}{2}$$

가 성립하게 만들 수 있습니다. 그러면 지금까지의 일련의 결과물로부터 $1 \leq \frac{1}{2}$ 라는 모순이 따라나옵니다! 이 모순은 e 가 초월수가 아니라고 가정했기 때문에 발생한 것입니다. 따라서 e 는 초월수입니다. ■