Alpha 1.1.1

이산수학 개론

이산수학의 기본이 되는 공의, 정의, 정리 개념과 자연수와 정수에 대해서 알아봅시다.

1. 이산수학의 정의

이산수학은 “이산” 과 “수학” 의 개념이 합쳐진 것으로, “이산” 이란 “연속” 과 반대되는 개념으로 서로 구별될 수 있는 부분들로 이루어진 것을 말합니다. “수학” 이란 수학적 대상, 존재하는 것과 존재하지 않는 모든 추상적인 것들의 성질을 연구하는 학문입니다.

이에 따라 “이산수학” 은 이산수학적 대상의 성질들을 연구하는 학문입니다. 이산수학 특성 상 서로의 값들이 연속적이지 않고 떨어져 있기에 이산수학의 가장 기본은 “세는 것” 입니다.

2. 공리, 정의, 그리고 정리

이산수학에서는 증명을 많이 다루게 되는데 이때 필수적으로 알아야 하는 개념들이 바로 “공리” , “정의” , “정리” 입니다. 차례대로 알아보도록 하겠습니다.

공리(Axiom)는 “증명 없이 참으로 받아들이는 명제” 를 의미합니다. 이론 체계의 가장 기초적 근거가 됩니다. 그러나 각각의 공리가 증명이 필요없는 자명한 명제라 하더라도 여러 공리가 함께 있는 공리계에서는 문제가 될 수 있습니다. 완전하고 모순이 존재하지 않는 공리는 없기 때문입니다. (With 괴델의 불완전성 정리)

정의(Definition)는 “용어나 기호의 의미를 명확히 정한 것” 입니다.

정리(Theorem)는 “공리계와 정의를 통하여 명제의 참 또는 거짓을 판별할 때, 참으로 증명된 명제” 를 말합니다. 그리고 어떤 정리의 증명에 필요한 정리를 “보조정리(Lemma)” , 어떤 정리가 증명되면 자연스레 증명되는 정리를 “따름정리(Corollary)” 라고 합니다.

> 이해하기: 공의, 정의, 정리
>
> 공리라는 약속을 통하여 수학의 토대를 만들고, 그 위에 정의라는 약속을 통해 수학 용어를 만들고, 공리와 정의를 통하여 정리가 만들어지는 것입니다.

3. 자연수

자연수는 무엇일까요? 예를 들어 723이라는 수가 있다고 생각해보면 723은 100이 7개, 10이 2개, 1이 3개로 이루어진 수라 할 수 있습니다. 그러나 이렇게 723이라는 수를 정의하기 위해서는 덧셈, 곱셈, 1, 10, 100, 2, 3, 7 이라는 개념을 알아야 합니다. 그 개념을 모르는 상태로는 어떻게 개념을 정의할 수 있을까요?

723을 정의할 때, “722보다 하나 더 큰 수” 라고 정의해봅시다. 그러면 또 질문이 나오게 됩니다. “722는 어떻게 정의할 수 있는가?” 그렇다면 또 “721보다 하나 더 큰 수” 라고 정의할 수 있게 되고, 이 작업을 반복하면 “2는 1보다 하나 더 큰 수” 라고 대답하게 될 것입니다. 그러면 723이라는 수를 1과 덧셈만으로 정의를 한 것입니다.
이 방식은 “자연수에 대한 공리적 접근 방식” 이라고 합니다. 즉, 기본 항과 공리들을 정의하는 것입니다.

페아노 공리계

이탈리아 수학자 "페아노"는 이러한 자연수에 대한 공리들을 제시했습니다. 이를 "페아노 공리계"라고 합니다. 페아노 공리계에서는 기본적으로 "1", "Successor", "자연수" 만을 사용힙니다. 이때 "Successor"는 다음 숫자를 의미하는 용어입니다.

공리: 페아노 공리계

1. 1은 자연수이다.
2. 각각의 자연수는 오직 하나의 Successor만을 갖는다.
3. 1은 어떠한 자연수의 Successor가 아니다.
4. 만약 $\mathrm{Succ}(x) = \mathrm{Succ}(y)$이면 $x = y$이다.
5. 만약 M이 다음을 만족하는 자연수들의 부분집합이면, M은 모든 자연수들의 집합이다.
   - $1 \in M$
   - $x \in M \Rightarrow \mathrm{Succ}(x) \in M$

자연수의 성질

자연수의 성질에 대해 알아보기 전, "닫힘 성질"에 대해서 알아야 합니다. 닫힘 성질은 다음과 같습니다.

정리: 닫힘 성질

"집합 A가 연산 $*$에 닫혀있다"는 것은 집합 A의 임의의 원소 a, b에 대해 $a * b$ 또한 집합 A의 원소가 된다는 것이다.

자연수는 덧셈과 곱셈에 대해서 닫혀있습니다. 2개의 자연수의 합 또는 곱의 결과 또한 자연수가 된다는 뜻입니다. 그러나 뺄셈과 나눗셈에 대해서는 닫혀있지 않습니다.

닫힘 성질을 만족하는 자연수의 성질에 대해서 더 알아보겠습니다.

정리: 자연수에 대한 성질

a, b, c를 자연수라 하면 다음과 같은 성질을 만족한다.

1. $a + b = b + a$ (덧셈의 교환법칙).
2. $a \times b = b \times a$ (곱셈의 교환법칙)
3. $a + (b + c) = (a + b) + c$ (덧셈의 결합법칙)
4. $a \times (b \times c) = (a \times b) \times c$ (곱셈의 결합법칙).
5. $a \times (b + c) = (a \times b) + (a \times c)$ (분배법칙)

마지막으로 자연수의 성질 중 “항등원” 에 대해서 알아보겠습니다.

정의: 항등원

어떤 연산에 대해 닫혀있는 집합이 존재할 때, 이 집합의 원소와 이항 연산을 했을 때 다시 그 원소를 값으로 갖는 유일한 원소 곱셈 연산자의 항등원: $a \times x = a$인 x는 1이다. 덧셈 연산자의 항등원:

$a + x = a$인 x는 0인데, 0은 자연수가 아니기에 자연수에서 덧셈 연산자의 항등원은 존재하지 않는다.

정렬순서 원리

자연수에 대한 정렬순서 원리에 대해 알아보겠습니다. 그 전에 정렬순서 원리를 이해하기 위해서는 순서 관계를 이해해야 하는데 어떠한 집합이 순서 관계를 가지려면 다음을 만족해야 합니다.

정의: 순서 관계

- 두 원소 x, y가 다르다면 $x > y$ 이거나 $x < y$ 이다.
- 임의의 x에 대해서 $x > x$ 이거나 $x < x$ 는 성립하지 않는다.
- $x > y$ 이고 $y > z$ 이면 $x > z$ 이다.

정리: 정렬순서 원리

어떤 집합에 대해서 공집합이 아닌 임의의 모든 부분집합들은 각각 하나의 최소 원소를 갖는다.

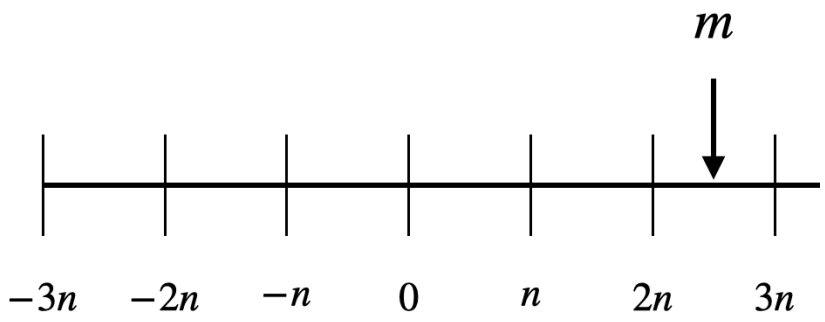
즉, 정렬순서 원리는 집합의 원소들 사이에 순서가 잘 정해져 있어, 그 집합(공집합 제외)의 어떤 부분집합에서 최소 원소가 있을 때, 그 집합은 정렬되었다 라고 합니다. 자연수들의 집합에서 공집합이 아닌 임의의 부분집합을 잡아도 그 부분집합에는 최소 원소가 존재하기에 자연수는 정렬순서 원리를 따릅니다.

4. 정수

정수는 양의 정수(자연수)와 0, 음의 정수(자연수에 $-$ 기호를 붙인 수)로 이루어진 수 체계입니다. 정수 또한 자연수와 같이 셀 수 있는 무한집합이며 덧셈, 뺄셈, 곱셈에 대해서 닫혀있습니다.

정수 표현

두 개의 정수 n과 m에 대해서 n이 0이 아닐 때, 직선 위에 n의 정수배들을 점으로 찍어 표현할 수 있고 이때, m을 어디든지 놓을 수 있습니다. 말로만 하면 어렵기에 그림을 통해 이해해보도록 하겠습니다.



이 그림과 같은 경우, 연속적인 점들 사이의 거리는 n의 절댓값인 $|n|$ 입니다. 만일 m이 n의 배수라고 하면 $m = qn + r$이라고 쓸 수 있으며, $r = 0$ 입니다. 만약 m이 n의 배수가 아니면 $m = qn + r$이라고 쓰며, $0 < r < |n|$ 입니다.

정의: 정수 표현 방법

두 정수 m, n에 대해서 모든 경우는 $m = qn + r$ 이며, $0 \leq r \leq |n|$ 으로 표현할 수 있다. (이때 q는 정수이다.)

정수의 성질

정수 표현에 있어서 중요한 배수 표현은 다음과 같습니다. 배수 표현을 통하여 정수의 성질도 도출해낼 수 있습니다.

정의: 배수 표현

두 정수 m과 n에 대하여, m은 n의 배수이면 $n \mid m$ 이라 쓰며 n은 m을 나눈다라고 표현한다.

정리: 정수의 성질

1. 만일 $a \mid b$ 이고, $a \mid c$ 이면 $a \mid (b \pm c)$ 이다.
2. 만일 $a \mid b$ 혹은, $a \mid c$ 이면 $a \mid bc$ 이다.
3. 만일 $a \mid b$ 이고, $b \mid c$ 이면 $a \mid c$ 이다

소수와 합성수

소수는 현대 암호 시스템에서 필수적인 개념입니다. 특히 소수에 관한 내용 중 알아야 하는 것은 "소수 판별법" 입니다. 그러나 현재까지는 어떤 수가 소수인지를 빠르게 계산하는 알고리즘을 찾지 못했습니다.

정의: 소수

약수(나누어떨어지는 수)로 1과 자기 자신만을 갖는 1보다 큰 정수 Ex: $2,\ 3,\ 5,\ 7...$

정의: 합성수

소수가 아닌 1보다 큰 정수 Ex: $4,\ 6,\ 8,\ 9...$

소수에 대한 내용은 추후에 더 깊고 자세하게 다루도록 하겠습니다.

이산수학 개론

행과 열을 수학적으로 표기하는 기법인 행렬 대해서 알아봅시다.

1. 행렬

행렬은 행과 열로 나열하는 것을 말합니다. 기본적으로 연립방정식을 풀기 위하여 만들어진 개념이며, 수, 문자, 함수 등을 괄호 안에 배열한 것입니다. 행렬의 각 성분은 실수여야 하고, 이는 "스칼라(Scalar)" 라고 합니다. 스칼라는 크기만 있고 방향을 가지지 않는 양을 말하며, 벡터와는 반대되는 개념입니다. 수학적으로 정의한 행렬은 다음과 같습니다.

정의: 행렬

행렬 A는 실수들을 사각형의 배열로 표시한 것이다(단, m과 n은 양의 정수). 각각 n쌍으로 된 m개의 수평 성분 $(a_{i1}\ a_{i2}\ a_{i3}\cdots a_{in})$ (단, $1 \le i \le m$)을 A의 행(row)이라고 하고, 각각 m쌍으로 된 n개의 수직 성분 $(a_{1j}\ a_{2j}\ a_{3j}\cdots a_{mj})$(단, $1 \le j \le n$)을 A의 열(column)이라고 한다.

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ & & \vdots & & \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

행렬 A를 $A = (a_{ij})$로 표시하는데, 이때, 원소 a_{ij}는 i행의 j번째 열의 원소를 나타냅니다. A를 $m \times n$ 행렬이라고 하며, $m\ by\ n$ 행렬로 읽습니다.

2. 행렬의 연산

기초적인 행렬의 연산을 알아보기 전, "영행렬"과 "행렬의 같음 성질"에 대해서 알아야 합니다. 먼저, 영행렬부터 알아보도록 하겠습니다.

영행렬

만약 각 성분이 0이라면, 이 행렬을 "영행렬" 이라고 하고 0으로 표시합니다.

정의: 영행렬

각 성분이 0인 행렬을 말한다. 영행렬은 0으로 표시한다.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

두 행렬의 같음

두 행렬이 있을 때, 그 두 행렬이 같을 조건은 다음과 같습니다.

정의: 두 행렬의 같음

두 행렬이 $m \times n$ 행렬이고 대응하는 원소가 모두 같으면 $A = (a_{ij})$와 $B = (b_{ij})$는 같다라고 하며, $A = B$ 라고 표현합니다.

지금부터는 본격적인 행렬의 연산 방식에 대해 알아보도록 하겠습니다. 행렬의 기초적인 연산으로는 행렬의 덧셈, 행렬의 실수곱, 행렬곱 등이 있습니다.

행렬의 합

행렬의 합은 다음과 같이 정의합니다.

정의: 행렬의 합

행렬 A와 B가 같은 크기와 행과 열을 가지면, 행렬 A와 B의 행렬의 합은 $A+B$로 표시하고 $A+B=(a_{ij})+(b_{ij})=(a_{ij}+b_{ij})$이다. 즉, 대응하는 성분끼리 합을 구하면 그 값이 $A+B$의 각 성분이 되는 것이다.

행렬의 합을 통하여 알 수 있는 행렬의 덧셈 성질은 다음과 같습니다.

정리: 행렬의 덧셈 성질

1. $A+B=B+A$ (덧셈의 교환법칙)
2. $(A+B)+C=A+(B+C)$ (덧셈의 결합법칙)
3. $A+0=0+A=A$ (덧셈의 항등법칙)

스칼라 곱과 행렬의 곱

스칼라 곱은 행렬에 실수배를 하는 것입니다. 스칼라 곱은 다음과 같이 정의됩니다.

정의: 스칼라 곱

A가 $m\times n$ 행렬이고 c가 실수이면 다음이 성립합니다.

$$c\cdot A=c\cdot(a_{ij})=(c\times a_{ij})$$

두 행렬을 곱하는 행렬의 곱은 다음과 같이 정의됩니다.

정의: 행렬의 곱

$A=(a_{ij})$는 $m\times p$ 행렬이고 $B=(b_{ij})$는 $p\times n$ 행렬일 때, 행렬의 곱 AB는 $m\times n$ 행렬이고 $C=(c_{ij})$가 된다. 이때,

$$C_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}\cdots+a_{ip}b_{pj}\quad (\text{단, } 1\le i\le m,\ 1\le j\le n)$$

입니다. 즉, 행렬의 곱 AB는 다음과 같이 구할 수 있습니다.

$$AB=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ & & \vdots & \\ a_{i1} & a_{i2} & \cdots & a_{ip} \\ & & \vdots & \\ a_{m1} & a_{m2} & \cdots & a_{mp} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} & \cdots b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots b_{1j} & \cdots & b_{2n} \\ & & \vdots & & \\ & & \vdots & & \\ & & \vdots & & \\ b_{p1} & b_{p2} & \cdots b_{1j} & \cdots & b_{pn} \end{pmatrix}=\begin{pmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \cdots & c_{2n} \\ & & \vdots & & \\ & \cdots & c_{ij} & \cdots & \\ & & \vdots & & \\ c_{m1} & c_{m2} & c_{m3} & \cdots & c_{mn} \end{pmatrix}$$