Thursday, January 31, 2019 9:26 AM

Permutations

$f: S \to S$

f is bijection

we call f a permutation

permutation

$S = \{1,2,3\}$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

[3, 1, 2]

$f: S \to S$

$g: S \to S$

f & g are ~~bij~~

$g \circ f$ $f \circ g$ are also bij.

$G_S = \{f : S \to S \mid f \text{ is a bij}\}$

$G_S \neq \emptyset \because id_S \in G_S$.

if $f, g \in G_S$, then $f \circ g$ & $g \circ f \in G_S$.

G_S is closed under functional composition.

$id_S \circ f = f$ $f \circ id_S = f$

if $f \in G$, then $\exists\, g = f^{-1}$ s.t. $g \circ f = id$

$f \circ g = id$

$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$f \circ f^{-1}$ $f^{-1} \circ f$

$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \end{pmatrix}$ $f^{-1} \circ f$ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

a, b, c

$\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$

$S = \text{range}(10)$

$\begin{pmatrix} 0 & \dots & 9 \\ & (0 \dots 9) \text{ in any} & \end{pmatrix}$

$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 0 & 2 \end{pmatrix}$

$\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array}$

[1, 3, 4, 0, 2]

$f, g, h \in G_S$, then $f \circ (g \circ h) = (f \circ g) \circ h$

Def A group G is a set together with an operation $*: G \times G \to G$ s.t.

1) $\exists\, e \in G$ s.t. $\forall g \in G$ $g * e = e * g = g$ (we call e the identity) Often people write 1
2) $\forall g, h, k \in G$ $(g*h)*k = g*(h*k)$ (Associative)
3) $\forall g \in G$ $\exists\, g^{-1} \in G$ s.t. (such that) $g * g^{-1} = e = g^{-1} * g$

What's missing?

Groups do not ~~have~~ have to have $f*g = g*f$

If G is commutative we call G abelian or commutative

Abel abelian

$\mathbb{R}$ with $*$ is this a group? No, 0^{-1} does not exist

$\mathbb{R} - \{0\}$ with $*$. Group? Yes Abelian? Yes

$\mathbb{N}, *$? Group? No No No, 1000* No

$\mathbb{N}, +$ No

$\mathbb{Z}, +$ Yes $e = 0$, $-n + n = 0$, $n + (-n) = 0$ Assoc

Abelian? Yes

$\mathbb{Q}, *$, No: $0 \in \mathbb{Q}$

$\mathbb{Q} - \{0\}, *$, Yes

$\mathbb{Z}, *$, Not a group: 0

$\mathbb{Z} - \{0\}, *$, No: inverse

$\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

$\mathbb{Z}_7$ has $+, *$

is $\mathbb{Z}_7, +$ a group?

$\mathbb{Z}_7, *$ a group? No

$\mathbb{Z}_7 - \{0\}, *$ a group? $1 = e$, Assoc.

$1^{-1} = 1$

$2^{-1} = 4 \quad 4^{-1} = 2$

$3^{-1} = 5 \quad 5^{-1} = 3$

$6^{-1} = 6$

Abelian? Yes

$\mathbb{Z}_8 - \{0\}, * \quad 2 * 4 = 0$

$\left.\begin{array}{l}\mathbb{Z}_p - \{0\}, \text{ p is prime} \\ \text{is a group}\end{array}\right\}$ Conjecture

$\mathbb{Z}_n - \{0\}, *$ n composite is not a group

$n = a * b$

$a * b = 0 \mod n$

$\mathbb{Z}_8 - \{0\}, \quad \{1, 3, 5, 7\} \quad 1^{-1} = 1 \quad 3^{-1} = 3 \quad 5^{-1} = 5 \quad 7^{-1} = 7$

```
GCD(a,b)
  if a%b == 0:
    return b
  return GCD(b, a%b)
```

$a = q * b + r \qquad r = \underline{\underline{a - q * b}}$

127

$\mathbb{Z}_p - \{0\}$, p a prime

$g = GCD(a,b)$

$\exists\, s,t$ s.t. $g = s*a + t*b$.   Extended GCD

$GCD(63,45) = GCD(45,18) = GCD(18,9) = 9$

$s*63 + t*45 = 9$ (You do this)

a rel prime to p

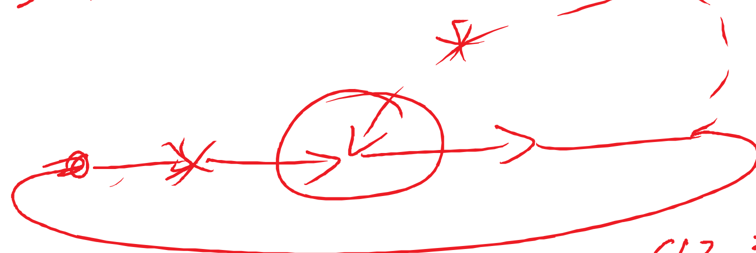
$s*a + \underbrace{t*p}_{\to 0} = 1$

$s*a = 1 \mod p$

$S = \; a \xrightarrow{f} f(a) \xrightarrow{f} ff(a) \xrightarrow{f} fff(a)$

$a \to f(a) \to ff(a) \to fff(a) \to \cdots$

S is finite



$\begin{pmatrix}1&2&3&4&5\\3&5&1&2&4\end{pmatrix} \longrightarrow (13)(254) \longrightarrow \begin{pmatrix}1&2&3&4&5\\3&5&1&2&4\end{pmatrix}$

$(254)(13)$

$(23)(254)$ $\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}$ $\begin{pmatrix}1&2&3&4&5\\1&5&3&2&4\end{pmatrix}$

$1 \to 2$

$\begin{pmatrix}1&2&3&4&5\\1&5&3&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix} = \; ?$ $\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}$

$\begin{pmatrix}1&2&3&4&5\\2&5&1&3&4\end{pmatrix}$

convert to cycle notation.