Notes

September 19, 2014

assignment

number of cycles of length n in S_n is $(n-1)!$ because you fix the first entry to eliminate duplicates.

number of cycles of length m of S_n. pick $\binom{n}{m}$ for the first element. $\binom{n}{m}m!/m = \frac{n!}{(n-m)!}\frac{1}{m}$

#12

(ab) is odd, length three cycles are even, two evens multiplied together is even.

3.1 groups

S is a set.

definiton

a binary operation on S is a function $S \times S \to S$, or $(x, y) \to x * y$

interesting binary operations satisfy: associativity, identity($\exists e \in S$ such that $x * e = e * x = x$), inverse ($a * b = b * a = e$). if an element has an inverse, we say that it is invertible.

example

$\mathbb{Z}$ with binary operation is usual addition, $(\mathbb{Z}, +)$, then it is associative, 0 is identity, and all elements are invertible.

$(2\mathbb{Z}, +)$, nothing is different

$(2\mathbb{Z}, \cdot)$. No identity element.o

$(2\mathbb{Z} + 1, +)$, this operation is not closed, it's not a binary operation.

propostion

let $*$ be an associative opertion on S, let $a, b, c \in S$ be invertible elements. then

1. the $*$ operation has at most one identity element
2. if it has an identity elemen, then an element a in S has at most one inverse.

proof

assume that e, e' identity elements, $x \star e = e \star x = x$ and $x \star e' = e' \star x = x$for all $x \in S$.

take $x = e'$ then $e' = e' \star e = e$

now if a has two inverses b, b' then $b = b \star e = b \star (a \star b') = (b \star a) \star b' = e \star b' = b'$

propostion

let $*$ be an associative opertion on S, let $a, b, c \in S$ be invertible elements. then

1. a^{-1} is invertible
   $a \star a^{-1} = a^{-1} \star a = e$
2. $a \star b$ is invertible and $(a \star b)^{-1} = a^{-1} \star b^{-1}$.
   $(a * b) * (b^{-1} * a^{-1}) = a * e * a^{-1} = e$ and similarly $(b^{-1} * a^{-1}) * (a * b) = e$

definition of group

let G be a set and $\star$ be a binary operation on G. we say that $(G, \star)$ is a group if

1. $\star$ is associative
2. $\star$ as an identity element
3. every element of G is invertible.

examples

$(\mathbb{Z}, +)$ is a group, $(\mathbb{Z}, \cdot)$ is not, $(\mathbb{Q}, \cdot)$ is not because zero is not invertible, $(\mathbb{Q}*, \cdot)$ is because the $*$ means throw out zero. $(S_n, \circ)$ where $\circ$ is a permutation, is a group, $(\mathbb{Z}_n, +)$ is a group. $\mathbb{Z}_n^*$ is all the elements of $\mathbb{Z}_n^*$ is all elements of $\mathbb{Z}_n$ that are invertible

proposition

$(G, *)$ is a group, and $a, b, c \in G$ thenn if $ab = ac$ then $b = c$ and if $ba = ca$ then $b = c$
$a^{-1}ab = a^{-1}ac = b = c$

abelian groups (commutative groups)

a group $(G, *)$ is called abelian if $*$ is commutative.
for example $(S_n, \circ)$ is not abelian.
another example is $GL_n(\mathbb{R})$ the invertible $n \times n$ matrices with entries in $\mathbb{R}$. $(GL_n(\mathbb{R}), \cdot)$ is not commutative.