Notes 2019-09-16

Cole Killian

October 10, 2019

Theorem There are infinitely many primes.

Proof (Argument by contradiction)
Suppose finetly many primes - $P_1, P_2, \ldots, P_n$
let $p = p_1p_2p_3 \ldots p_n + 1$
$p > p_n$ which means that p is not prime
but every composite number has prime factor so $p = p_k r$ for some k
impossible!
$p_k r = p_k(p_1 \ldots p_{k+1} \ldots p_n) + 1$
which would require that $p_k|1$ but this is impossible

Theorem Fundametnal theorem of arithmetic

let $n \in \mathbb{Z}$ with $n > 1$ Then $n = p_1p_2 \ldots p_k$ is a product of primes
This product is unique in a certain sense that:
if $n = q_1q_2 \ldots q_l$, then $k = l$ and sequences are actually the same after reording them
ex. $2 * 2 * 3 * 3 * 3 * 5 * 5$
$5 * 2 * 3 * 2 * 5 * 3 * 3$

Why is this true?

two things going on: exist and unique

proof of existence:

Show by (strong) induction that for $n \geq 2$, $S_n =$ "n is a product of primes"
(base case) n = 2
2 is a product of primes. 2 = 2 ✓
((strong) induction): Either n+1 is prime, or $n + 1 = ab$ where $2 \leq a, b, \leq n$
by (strong) induction, $a = p_1p_2 \ldots p_k, b = q_1q_2 \ldots q_l$ where a and b are a product of primes. Therefore n+1 is a product of primes.

NOTE: STRONG INDUCTION YOU DO NOT HAVE TO HAVE MULTIPLE BASE CASES. SOMETIMES YOU DO. STRONG INDUCTION YOU ALLOW YOURSELF TO DRAW FROM (i don't konw what goes here)

Proof of uniqueness. Note, new discussion, dosen't realte to previous proof

§0.1 Review proof of uniqueness

suppose $p_1 \ldots p_k$ = n = $q_1 \ldots q_l$
assume $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_l$
assume $p_1 \leq q_1$
then $p_1|n$ so $p_1|q_k$ for some k
so $p_1 = q_k$ thus $p_1 \leq q_1 \leq q_k$
so $p_1 = q_1$
now $(p_2 \ldots p_k) = (q_2 \ldots q_l)$ by induction $k = l$ and the sequence are the same. n/p has a unique prime factorization and so

§1 Section 3.2: Definition and example of Groups

a binary operation on a set G is a function $f : G \times G \to G$
math world is built out of binary operation: multiplication, subtraction, addition...
denote $f(a,b)$ by $a \circ b$ or $a \cdot b$ or ab
Def: a group $(G, \circ)$ is a set G with a binary operation $(a,b) \to a \cdot b \in G$
such that
(1) the operation is associative. i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Review: associative, communative...

(2) there exists an identity element $e \in G$ s.t. $e \cdot x = x = x \cdot e$ for all $x \in G$
(3) Each element $x \in G$ has an inverse $y \in G$ s.t. $x \cdot y = e$
x^{-1} Often denotes inverse
We are blessed with a group theorist :)

example

ex. $(\mathbb{Z}, +)$ is a group
(1) $(a+b)+c = a+(b+c)$
(2) $e = 0, a+0 = a = 0+a$
(3) inverse of x denoted by $-x$

idea

$(G, \circ)$ is commutative or abelian if $a \circ b = b \circ a$ for all $a, b \in G$

examples of commutative groups

ex. $(\mathbb{Z}, \cdot)$, $\cdot =$ "times"/multiplication is NOT a group
(1) yes associative $(a * b) * c = a * (b * c)$
(2) has identity element $e = 1$
(3) BUT inverses don't always exist. $2^{-1} =?$. No integer inverse of 2
On the other hand: $(\mathbb{Q}*, \cdot)$ is a commutative group. Note: $\mathbb{Q}* = \mathbb{Q} - \{0\}$
identity (better word for e) is 1

ex. $(\mathbb{Q}, +)$ is a commutative group.

inverse of $\frac{2}{3}$ is $-\frac{2}{3}$

definition: $(G, \circ)$ is a finite group if G is a finite set.

otherwise we call G an infinite group.

What is more important when talking about a group. G or $\circ$? The $\circ$, everything is built into the $\circ$. i.e. $G \times G \to^f G$ and $(a,b) \to a \circ b$.
$|G|$ represents the number of elements in G
Let us now get familiar with Finite cyclic group $\mathbb{Z}_n$
Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
Define binary operation $a + b = c$ where $a + b \equiv_n c$ (called addition modulo n)
Turns out that this is a commutative group. $(\mathbb{Z}_n, +)$ is a commutative group.
ex. in $\mathbb{Z}_n$
$2+2 = 4$, $3+3 = 1$, $4+1 = 0$, $4+4 = 3$

Requirements:
(1) associative ✓
(2) 0 is the identity element
(3) Inverse exists. i.e. inverse of $3 = 2$, inverse of $4 = 1$, inverse of $1 = 4$

Starting discussions on wednesday with Cayley table

I'm not gonna be able to type this lmao

Grid like a multiplication table, but more general. "The Cayley table of a group". Summary of a binary operation.