Math 322, lecture 1 7/5/17

(1) Concrete Groups

§1. $\mathbb{Z}$

Fact: (a) Integers can be multiplied, added, compared.
(1) $<$ is a linear order + laws of arithmetic
and respects $+$, $\cdot$ by positive numbers
(2) (Well-ordering) If $A \subset \mathbb{Z}$ is non-empty, bound below then A has a least element.

↑ formulation of induction

Example: 1 is the least positive integer.

Example: Every positive integer can be written as
$1+1+1+\cdots+1$ (sum of 1s)

Hint: Let A be the set of positive integers which are not a sum of 1s. Suppose A is non-empty, and let $n \in A$ be its least element.
Think about $n-1$, ..

Lemma: Well-ordering is equivalent to the principle of induction
(if $A \subset \mathbb{Z}$ has: $0 \in A$, if $n \in A$ then $n+1 \in A$
then every positive integer is in A)

Pf: ($\Rightarrow$) Let $A \subset \mathbb{Z}$ satisfy $0 \in A$, $(n \in A \Rightarrow n+1 \in A)$
Let $B = \{n \in \mathbb{Z} \mid n \geq 0, n \notin A\}$. B is bounded below. Suppose it were non-empty. Then it would have a least element, m.
Consider $m \neq 0$ ($0 \in A$). So $m > 0$, $m \geq 1$, $m-1 \geq 0$

$m-1 < m = \min B$ so $m-1 \notin B$ so $m-1 \in A$.

By hypothesis, $m = (m-1)+1 \in A$ also $\not\in$ contradicts $m \in B$.

So $B = \emptyset$, $A \supseteq \{0, 1, 2, \ldots\} = \mathbb{N}$.

($\Leftarrow$) Ex. Let $P(n)$ = "if A is a set of natural numbers and there is $m \in A$, $m \leq n$, then A has a least element".

Show $P(0)$, and $P(n) \Rightarrow P(n+1)$.

The group $(\mathbb{Z}, +)$

Note some properties of $+$: for all $x, y, z \in \mathbb{Z}$:

(1) Associativity: $(x+y)+z = x+(y+z)$

(2) Zero: $0 + x = x$

(3) Inverse: there is $(-x) \in \mathbb{Z}$ s.t. $x + (-x) = 0$

(4) Commutativity: $x + y = y + x$

Problem: Which subsets of $\mathbb{Z}$ are non-empty, closed under $+$ and inverses?

Example: $\{0\}$, $\mathbb{Z}$, $2\mathbb{Z}$ = even integers, $m\mathbb{Z}$, $m \in \mathbb{Z}_{\geq 0}$

Lemma: (Division with remainder): Let $a, b \in \mathbb{Z}$, $b > 0$. Then there are unique $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, $0 \leq r < b$

Pf: Let $A = \{n \geq 0 \mid n = a - bq, q \in \mathbb{Z}\}$. Then A is bounded below, non-empty: if $q = -(|a|+1)$ then $a - bq = a + b\cdot(|a|+1) \geq a + |a| + 1 \geq 1$

so $a - qb \in A$.

Let $r \in A$ be the least element.

Then $\exists q$: $r = a - bq$., i.e. $a = bq + r$.

Also, $0 \le r$ ($r \in A$), and $r < b$:

if we had $r \ge b$ then $r - b \ge 0$ and

then $r - b = a - bq - b = a - b(q+1) \in A$.