Math 322, lecture 2, 12/9/2017

Today: (1) Division thm
(2) subgps of $\mathbb{Z}$
(3) Multiplicative structure of $\mathbb{Z}$

We're in the middle of proving:

Prop: Given $a, b \in \mathbb{Z}$ with $b > 0$ there exist unique $q, r \in \mathbb{Z}$ with $a = bq + r$, $0 \le r < b$

Pf: Considered $A = \{ n = a - bq \mid q \in \mathbb{Z}, n \ge 0 \}$

saw A is non-empty (take q large and negative)

Let $r = \min A$, then $a = bq + r$ for some q.

$r \ge 0$ since $r \in A$, and $r < b$ because if we had $r \ge b$

then $0 \le r - b = a - bq - b = a - (q+1)b \in A$, a contradiction

For uniqueness, suppose $a = bq + r = bq' + r'$, wlog $r \ge r'$.

Then $r - r' = b(q' - q)$ now $0 \le r - r' < b$

But $r - r'$ is divisible by b so $r - r' = 0$, $q - q' = 0$, ie.

[if $q' \ne q$, $|q' - q| \ge 1$ so $b|q' - q| \ge b > r - r'$] $r = r'$, $q = q'$.

Def: Say $H \subset \mathbb{Z}$ is a subgroup if H is non-empty, whenever $x, y \in H$, $x + y \in H$ and $-y \in H$.

Saw last time: $H = m\mathbb{Z}$ is an example

Prop: Let $H \subset \mathbb{Z}$ be a subgp. Then $H = m\mathbb{Z}$ for some $m \in \mathbb{Z}_{\geq 0}$

Pf: If $H = \{0\}$ then $H = 0\mathbb{Z}$ and we're done.

Otherwise there is some $n \in H$, $n \neq 0$ both $n, -n \in H$ so H contains positive numbers

Let $m = \min(H \cap \mathbb{Z}_{\geq 1})$ (exists by well-ordering since H has positive members)

Since $m \in H$, $m\mathbb{Z} \subseteq H$. (pf by induction: if $nm \in H$ then $(n+1)m = nm + m \in H$)

To see $m\mathbb{Z} = H$ let $a \in H$. By division thm, have $q, r \in \mathbb{Z}$, $0 \leq r < m$ s.t. $a = qm + r$.

Then $r = a - qm \in H$, $r \geq 0$, $r < m$

But m was the least positive member so $r = 0$ and $a = qm \in m\mathbb{Z}$

ideas: (1) "least counter example"

(2) check if $r = r'$ using $r - r'$

(3) check if $m | a$ using division thm

Multiplicative structure

Def: Let $a, b \in \mathbb{Z}$ (not both zero), set $\gcd(a,b)$ = greatest common divisor

Thm (Bezout's thm) there exist $x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a,b)$

Pf: Let $H = \{ax + by \mid x, y \in \mathbb{Z}\}$. This is non-empty, closed under $\pm$:

$(ax+by) \pm (ax'+by') = a(x \pm x') + b(y \pm y') \in H$.

Then $H = m\mathbb{Z}$ for some positive m. ($m \neq 0$ because $a, b \in H$ one of a, b is $\neq 0$)

$a = 1\cdot a + 0\cdot b$, $b = 0a + 1b \in H = m\mathbb{Z}$ so both a, b are multiples of m. (m is a common divisor)
Conversely, if $d \mid a$, $d \mid b$ then $d \mid ax+by$ for any x, y.
In particular, $d \mid m$.

Aside: Read about Euclidean algorithm for computing $\gcd(a,b)$ and x, y s.t. $\gcd(a,b) = ax+by$.

Modular Arithmetic

Motivation: (1) Useful, (2) New groups, (3) quotient constructions

Def: Let $a, b, n \in \mathbb{Z}$, $n \geq 1$. Say a is congruent to b mod n
write $a \equiv b\ (n)$ if $n \mid a-b$

Lemma: This is a equivalence relation:

(1) $a \equiv a\ (n)$
(2) if $a \equiv b(n)$ then $b \equiv a\ (n)$
(3) if $a \equiv b(n)$, $b \equiv c\ (n)$ then $a \equiv c\ (n)$

Pf: $n \mid 0$, if $n \mid a-b$ then $n \mid b-a$,
if $n \mid a-b$, $n \mid b-c$ then $n \mid a-c = (a-b)+(b-c)$

Def: Let $\mathbb{Z}/n\mathbb{Z}$ be the set of equivalence classes mod n

Notation: $[a]_n \stackrel{\text{def}}{=} \{b \mid b \equiv a\ (n)\}$

Examples $\mathbb{Z}/2\mathbb{Z} = \{\{\ldots, -4, -2, 0, 2, 4, \ldots\}, \{\ldots, -5, -3, -1, 1, 3, \ldots\}\}$

By thm on division with remainder,
$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ all distinct.

<u>Def:</u> Let $[a],[b] \in \mathbb{Z}/n\mathbb{Z}$

$$[a]_n \pm [b]_n = [a \pm b]_n$$

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

<u>Lemma:</u> This makes sense.

<u>Pf:</u> Say $a \equiv a' \ (n)$, $b \equiv b' \ (n)$

Need to check: $[a \pm b]_n = [a' \pm b']_n$

$[ab]_n = [a' \cdot b']_n$

unwinding definitions

<u>Equivalently:</u> $n \mid a-a',\ b-b'$

want to show: $n \mid ((a+b)-(a'+b'))$

$n \mid ((a-b)-(a'-b'))$

$n \mid ((ab)-(a'b'))$

But: $(a+b)-(a'+b') = (a-a') + (b-b')$

$(a-b)-(a'-b') = (a-a') - (b-b')$

$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b'$

$\square$

special case: even + odd = ~~even~~ odd

<u>Observation:</u> The laws of arithmetic hold in $\mathbb{Z}/n\mathbb{Z}$

<u>Pf:</u> $([a]_n + [b]_n) + [c]_n \overset{\text{def of }+}{=} [a+b]_n + [c]_n = [(a+b)+c]_n$ arithmetic in $\mathbb{Z}$

$[a]_n + ([b]_n + [c]_n) = [a]_n + [b+c]_n = [a+(b+c)]_n$

Same for other laws: hold for rep's so for classes

* Needed to check operations were well-defined

* Proof relied on map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$$q(a) = [a]_n$$

properties: $q(a \pm b) = q(a) \pm q(b)$

$$q(ab) = q(a)q(b)$$

In particular, get algebraic structure $(\mathbb{Z}/n\mathbb{Z}, +)$

The map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

has $q(a+b) = q(a) + q(b)$

first "map of groups" = "group homomorphism".