Lecture 02, Math 447

Marius Junge

University of Illinois at Urbana-Champaign

Axioms for N

$\mathbb{N} = (\mathbb{N}, S, 1)$

b0) $\mathbb{N}$ is infinite.

b1) $\mathrm{Im}(S) = \mathbb{N} \backslash \{1\}$.

b2) S injective.

b3) $A \subset \mathbb{N}$ such that

$$\left.\begin{array}{ll} & 1)\ 1 \in A \\ 2')\ S(A) \subset A & 2)\ n \in A \Rightarrow S(n) \in A \end{array}\right\} \Rightarrow A = \mathbb{N}.$$

Remark: Assuming b1) and b3) then b0) $\iff$ b2). *Prove this!*

Hint: Assuming b1) and b3) we can define

$\min(A) = \text{smallest } \# \text{ in } A$ for every subset $A \subseteq \mathbb{N}$

$\min(\emptyset) = \infty$

Consider $A \subset \mathbb{N}$ of numbers with two predecessors.

Review: Relations

X any set; a **relation** is a subset $R \subset X \times X$.

R is called **reflexive** if $\forall x \quad (x, x) \in R$

symmetric if $\forall x, y \quad (x, y) \in R \iff (y, x) \in R$

transitive if $\forall x, y, z \quad (x, y) \in R$ and $(y, z) \in R$

$$\implies (x, z) \in R$$

R is an **equivalence relation** if R is reflexive, symmetric and transitive.

Let R be an equivalence relation.

Define:

$$[x] = \{y \mid x \sim y\}.$$

$$[\ \ ]\colon X \to 2^x \qquad x \mapsto [x].$$

$$X/\sim \;=\; \mathrm{Im}([\ \ ]) \subset 2^X.$$

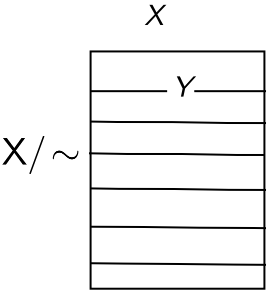
Equivalence Classes

Remark: $X = \bigcup^{\text{disjoint}}_{Y \in X/\sim} Y$

Key: $Y \bigcap Z \neq \emptyset \implies Y = Z$

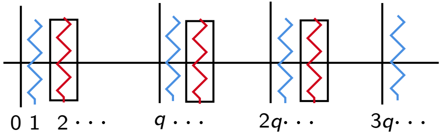
$$\textbf{Let} \quad \left.\begin{array}{l} x_0 \in Y \bigcap Z \\ x_1 \in Y \\ x_2 \in Z \end{array}\right\} \implies \begin{array}{l} x_0 \sim x_1 \\ x_0 \sim x_2 \end{array} \implies x_1 \sim x_2$$

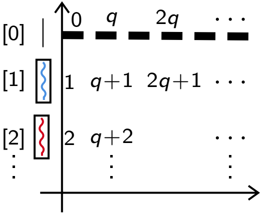
$\implies Y = [x_1] = [x_2] = Z$



Ex: In $\mathbb{Z}$ $\quad a \sim b$ if $\quad q \big| a - b$

(haven't introduced $\mathbb{Z}$ yet, but informally...)





timestamp: 10:47

Cancellation property (for semigroups)

Dfn $(S,+)$ is a **commutative semigroup** if $\quad \forall a,b,c \in S$

$$\begin{aligned} (a+b)+c &= a+(b+c) && \text{(associativity)} \\ a+b &= b+a. && \text{(commutativity)} \end{aligned}$$

$(S,+)$ has **cancellation property** if $\quad \forall a,b,c \in S$

$$a+c = b+c \Rightarrow a=b.$$

Lemma $(\mathbb{N},+)$ has cancellation property.

Proof: $A(m)$: $\quad$ " $\forall (k,\ell \in \mathbb{N}) \quad k+m = \ell+m \implies k=\ell$ ".

To prove (by induction): $\quad A(m)$ holds for all m.

$A(1)$: $\quad \ell+1 = k+1 \iff S(\ell) = S(k) \overset{(S \text{ injective})}{\Longrightarrow} \ell = k.$

Assume $A(m)$. Let $\ell, k \in \mathbb{N}$ satisfy $\ell + (m+1) = k + (m+1)$.

$(\ell+m)+1 = (k+m)+1 \overset{A(1)}{\Longrightarrow} \ell+m = k+m \overset{A(m)}{\Longrightarrow} k=\ell.$

Grothendieck group exists

Prop $(S,+) \neq \emptyset$ commutative semigroup with cancellation.

Then there exists smallest abelian group containing S.

(This is the "Grothendieck group" for S.)

Def $(G, \circ, 1)$ abelian group if

$$\left.\begin{array}{l} \textbf{1)}\ 1 \circ g = g \circ 1 = g \\ \textbf{2)}\ (g \circ h) \circ \ell = g \circ (h \circ \ell) \\ \textbf{3)}\ \forall g\ \exists! h \quad g \circ h = h \circ g = 1 \end{array}\right\} \text{group}$$

4) $g \circ h = h \circ g$ abelian

Proof of proposition

To prove the prop, construct G from S. For $a, b, c, d \in S$,

define: $(a, b) \sim (c, d)$ if $a + d = b + c$

Idea comes from fractions: $(a, b) \sim (c, d)$ $\frac{a}{b} = \frac{c}{d} \iff ad = bc$,
but we're writing additively.

Claim: This is an equivalence relation. *Prove this!*

For transitivity, assume $(a, b) \sim (c, d) \sim (e, f)$.

$$\implies \left.\begin{array}{l} a + d = b + c \\ c + f = d + e \end{array}\right\} \implies a + d + c + f = b + c + d + e$$

$$\overset{\text{cancellation}}{\implies} a + f = b + e \implies (a, b) \sim (e, f).$$

Prove the rest of the properties.

Proof (cont.): construction of G

Define $G = (S \times S)/\sim$ and operation $+$ on G:

$$[(a,b)] + [(c,d)] \stackrel{\text{def}}{=} [(a+c),(b+d)].$$

Need to prove $+$ is well-defined (left as exercise).

Clearly commutative and associative.

Neutral element (**identity**): $[(a,a)] = 0$.

Note $\quad \forall a, b \quad (a,a) \sim (b,b) \quad$ since $\quad a + b = a + b$.

Also $\quad [(a,a)] + [(b,c)] = [(a+b, a+c)] = [(b,c)]$

because $a + b + c = a + c + b$.

Inverses: $[(a,b)] + [(b,a)] = [(a+b, a+b)] = 0$.

Note: Uniqueness should be proved.

If another group contains S it has to contain G. *Prove this!*

timestamp: 36:14

Grothendieck group of $\mathbb{N}$

Model of proof: $(\mathbb{N}, \cdot)$ $\quad \frac{p}{q} = \{\, (pr, qr) \mid r \in \mathbb{N} \,\}.$

Most important example: $(\mathbb{N}, +) \to \mathbb{Z}$

$$(\mathbb{N} \times \mathbb{N})/\sim \quad = \quad \mathbb{N} \times \{+\} \bigcup \mathbb{N} \times \{-\} \bigcup \{0\}.$$

$$(a, b) \sim \begin{cases} \big((b-a), +\big) & \text{if } a < b \\ \big((a-b), -\big) & \text{if } a > b \\ 0 & \text{if } a = b. \end{cases}$$

timestamp: 42:33