Friday Sept 12, 2014

We've proven basic theorems.

Now let's get some examples.

Last time: $\forall\, g \in G$, we produced $\langle g \rangle \subset G$, grp generated by g.

<u>Exer</u> $\langle g \rangle = \text{image}\begin{pmatrix} \mathbb{Z} \longrightarrow G \\ n \longmapsto g^n \end{pmatrix}$.

We're about to generalize $\mathbb{Z}$: For any map of sets

$$S \longrightarrow G,$$

we'll produce a grp homomorphism

$$F(S) \longrightarrow G,$$

$\uparrow$ free grp on the set S.

$$\left(\begin{array}{c} * \xrightarrow{g} G \\ \updownarrow \\ \mathbb{Z} \longrightarrow G \end{array} \quad \text{analogous statement for } \mathbb{Z} \right)$$

Defn Let X be a set.

A word in X is

a finite, ordered collection of elements in X. Given a word w, we call an element of w a letter of w.

Equivalently, a word is:

- an element of

$$X^n$$

for some $n \geq 0$

- a sequence

$$x_1 x_2 \cdots x_{n-1} x_n$$

where each $x_i \in X$, and $n \geq 0$.

Rmk The empty word is a word w/ no letters.

We let $\mathrm{Word}(X)$ denote the set of all words on X.

Ex If $X = \{a\}$

$$\mathrm{Word}(X) = \{\phi, a, aa, aaa, \cdots\}$$

If $X = \{a, b\}$,

$$\mathrm{Word}(X) = \{\phi, a, b, ab, ba, aa, bb, \cdots\}.$$

Given two words in X,

we can concatenate them to produce a new word:

$$\mathrm{Word}(X) \times \mathrm{Word}(X) \longrightarrow \mathrm{Word}(X)$$
$$(w_1, w_2) \longmapsto w_1 w_2$$

Ex

$$(ba, ab) \longmapsto baab$$

$$(ab, ba) \longmapsto abba.$$

This is clearly associative, and the empty word looks like an identity element.

But no inverses! Let's fix that.

Given a set

$$S = \{a, b, c, \cdots\}$$

let S' be the set of symbols

$$S' = \{a^{-1}, b^{-1}, c^{-1}, \cdots\}.$$

(So S, S' are in bijection.)

We let

$$\underline{S} = S \cup S'$$

$$= \{a, a^{-1}, b, b^{-1}, \cdots\}.$$

<u>Ex</u> A word in $\underline{S}$ can look like

$$w = babb^{-1}a^{-1}c^{-1}ca.$$

<u>Defn</u> A word in $\underline{S}$ is called <u>unreduced</u> if for some $a \in S$, the sequence

$$aa^{-1} \quad \text{or} \quad a^{-1}a$$

appears in the word. A word is called <u>reduced</u> if it is not unreduced.

<u>Ex</u> $aaab^{-1}a^{-1}b$ is reduced.

$$\left.\begin{array}{l} acbcb^{-1}bc^{-1}, \\ acbcbb^{-1}c^{-1} \end{array}\right\} \text{both unreduced.}$$

Defn A word w' obtained from w by removing (aka cancelling) an appearance of aa^{-1} or $a^{-1}a$ is said to be obtained from w by cancellation. We'll write $w \rightsquigarrow w'$.

Ex • The empty word is obtained from $b^{-1}b$ (and from bb^{-1}) by cancellation.

• ab is obtained from

$abb^{-1}ba$ (can remove $a\underbrace{bb^{-1}}ba$ or $ab\underbrace{b^{-1}b}a$.)

$c^{-1}cab$

$acc^{-1}b$

by cancellation.

Defn

A word w' is called a reduction of w if w' is obtained from w by cancellations,

$$w \rightsquigarrow \cdots \rightsquigarrow w'$$

and if w' is reduced.

Prop'n If w' and w'' are reductions of w, then

$$w' = w''!$$

Pf Induction on length w of a word. (Note $w \rightsquigarrow u \Rightarrow \text{length}(u) < \text{length}(w)$).

$l = 0$: empty word is reduced

$l = 1$: No a, a^{-1} can occur adjacently since there's only one element in the word. So $l = 1 \Rightarrow$ word is reduced.

Suppose we've shown every word of length $l-1$ has unique reduction. Prove the same for l.

If w has length l and is reduced, done.

If not, $\exists$ aa^{-1} or $a^{-1}a$ somewhere. Potentially many of them!

<u>Ex</u> $a^{-1}a\,a^{-1}a\,a^{-1}a = w$, length 6.

Pick one of them.

$\cdots \; \underline{a^{-1}a} \cdots .$

A reduction of ω can be achieved by:

(i) cancelling $\underline{a^{-1}a}$ at some stage.

(ii) never cancelling $\underline{a^{-1}a}$.

(ii) only happens if

(*) $\cdots \underline{a^{-1}a}\, a^{-1} \cdots$ appears at some stage, and we take

$$\cdots \underline{a^{-1}} \underbrace{\underline{a}\, a^{-1}}_{\text{cancel}} \cdots \rightsquigarrow \cdots \underline{a^{-1}} \cdots$$

or

(**) $\cdots a\, \underline{a^{-1}a} \cdots$ appears and we take

$$\cdots \underbrace{a \underline{a^{-1}}}_{\text{cancel}}\underline{a} \cdots \rightsquigarrow \cdots \underline{a} \cdots$$

In (*), cancelling $\underline{a^{-1}a}\, a^{-1}$ by $\underbrace{\underline{a^{-1}a}}\, a^{-1}$ or $\underline{a^{-1}}\underbrace{\underline{a}\, a^{-1}}$ produces the same word. Likewise for (**).

So we can assume $\underline{a^{-1}a}$ is reduced at some point.

(Any reduction achieved via (ii) can be achieved via (i).)

So we have a reduction

$$w = \cdots \quad \underline{aa^{-1}} \cdots \underline{b^{-1}b} \cdots c^{-1}c$$

$\wr$ Step one

$$w_1 = \cdots \quad \underline{aa^{-1}} \cdots \cdots \quad \cdots \underline{c^{-1}c}$$

$\wr$

$\vdots$

$\wr$ Step n

w_n reduced.

Well, we get the same reduction if we cancel $\underline{aa^{-1}}$ in step 1, or in some other step. //

<u>Defn</u> Let S be a set. Then the <u>free group</u> $F(S)$ on S is

$$(F(S), m)$$

where

- $F(S)$ is the set of reduced words in $\underline{S} = S \cup S'$.
- $m : F(S) \times F(S) \to F(S)$ sends (w_1, w_2) to the reduction of $w_1 w_2$.

Associativity next week.

Inverses: The inverse to

$$s_1 \cdots s_n \quad \text{is}$$

$$s_n^{-1} \cdots s_1^{-1}$$

since

$$(s_1 \cdots s_n)(s_n^{-1} \cdots s_1^{-1})$$

$$\rightsquigarrow$$

$$s_1 \cdots s_{n-1} s_{n-1}^{-1} \cdots s_1^{-1}$$

$$\rightsquigarrow$$

$$s_1 \cdots s_{n-2} s_{n-2}^{-1} \cdots s_1^{-1}$$

$$\rightsquigarrow$$

$$\vdots$$

$$\rightsquigarrow$$

$$s_1 s_1^{-1}$$

$$\rightsquigarrow$$

$$\phi.$$

Ex $S = \{a\}$, a set w/ one element.

A word in S looks like

$$aaa\,a^{-1}aa^{-1}aa\,a^{-1}a.$$

If a word is <u>reduced</u>, it looks like

$$\underbrace{aaaaa\cdots a}_{n \text{ times}}$$

or

$$\underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}}.$$

So

$$\mathbb{Z} \longrightarrow F(S)$$

$$n \longmapsto \begin{cases} \underbrace{a\cdots a}_{n} & n>0 \\ \underbrace{a^{-1}\cdots a^{-1}}_{n} & n<0 \\ \emptyset & n=0 \end{cases}$$

is a bijection. You can check it's an isomorphism.

Ex $S = \{a, b\}$.

$F(S)$ is free group on two generators.

The elements look like

$\ell = 0 \qquad \emptyset =: 1$

$\ell = 1 \qquad a, \ b, \ a^{-1}, \ b^{-1}$

$\ell = 2 \qquad aa, \ bb, \ ba, \ ab$

$a^{-1}a^{-1}, \ b^{-1}b^{-1}, \ a^{-1}b^{-1}, \ b^{-1}a^{-1}.$