Lecture 19

Recall that the free product $*_\alpha G_\alpha$ of a collection of groups $\{G_\alpha\}_\alpha$ is the set of *reduced* words $g = g_1 \cdot g_m$, with $g_i \in G_{\alpha_i}$, $g_i \neq e_{\alpha_i}$, and $\alpha_i \neq \alpha_{i+1}$ for $i \in \{1, \dots, m-1\}$. We define an operation $\bullet$ on $*_\alpha G_\alpha$ by defining $g \bullet \epsilon = \epsilon \bullet g = g$ (where ϵ is the empty word) and then recursively, for $g = g_1 \cdots g_m$ and $h = h_1 \cdots h_n$,

$$g \bullet h = \begin{cases} g * h & \text{if } g_m, h_1 \text{ not in same group,} \\ g_1 \cdots g_{m-1}(g_m \cdot h_1)h_2 \cdots h_n & \text{if } g_m, h_1 \in G_\alpha \text{ and } g_m \cdot h_1 \neq e_\alpha \\ g_1 \cdots g_{m-1} \bullet h_2 \cdots h_n & \text{if } g_m \cdot h_1 = e_\alpha. \end{cases}$$

where $*$ is the concatenation of words.

Theorem 19.1. *The pair $(*_\alpha G_\alpha, \bullet)$ is a group. The unit element is the empty word and the inverse of a word $g_1 \cdots g_m$ is $g_m^{-1} \cdots g_1^{-1}$.*

Proof. The verification that $g \bullet h$ is again a reduced word follows from the definition: if the concatenation $g * h$ is not reduced, then it is replaced by a shorter word. As words have finite length, this process has to terminate in a reduced word. That the empty word is the unit element follows from the definition of the product $\bullet$. That the inverse element has the given form is obvious, but can be shown formally by induction: if $m = 1$, then $g_1 \bullet g_1^{-1} = \epsilon$ (by the definition of the product) and assuming the statement holds for $m-1$, then

$$g_1 \cdots g_{m-1} g_m \bullet g_m^{-1} g_{m-1}^{-1} \cdots g_1^{-1} = g_1 \cdots g_{m-1} g_{m-1}^{-1} \cdots g_1 = \epsilon.$$

To have a group structure, what remains is to show associativity, namely that for reduced words g, h, k we have

$$(g \bullet h) \bullet k = g \bullet (h \bullet k).$$

To proof this, set $W = *_\alpha G_\alpha$ for the set of reduced words, and consider the group of bijections $\mathrm{Sym}(W)$. We will "embed" W into $\mathrm{Sym}(W)$ via an injective map L that is compatible with multiplication, i.e., $L(g \bullet h) = L(g) \circ L(h)$, and from this the associativity in $\mathrm{Sym}(W)$ will naturally lead to the associativity of the product $\bullet$ in W.

To start with, for every element $g \in G_\alpha$ we have a map L_g, the *left multiplication*, such that $L_g(h) = g \bullet h$ for a word $h \in W$. If $g_1, g_2 \in G_\alpha$ and $h = h_1 \dots h_m$, then one easily verifies that

$$L_{g_1} \circ L_{g_2} = L_{g_1 g_2}, \tag{19.1}$$

and hence that $L_{g^{-1}} = L_g^{-1}$, so that $L_g \in \mathcal{S}(W)$. For any word $g = g_1 \cdots g_m$, the map

$$\begin{aligned} L\colon W &\mapsto \mathrm{Sym}(W) \\ g &\mapsto L_{g_1} \circ \cdots \circ L_{g_m} =: L_{g_1 \cdots g_m} \end{aligned}$$

is injective, since for any $g \in W$, $L_\epsilon(g) = g$.

Note that, by (19.1), the composition $L_g \circ L_h$ obeys the same rules as the product $\bullet$: if $g = g_1 \cdots g_m$ and $h = h_1 \cdots h_n$ are reduced words, then

$$L_g \circ L_h = \begin{cases} L_{g*h} & \text{if } g_1, h_m \text{ not in same group,} \\ L_{g_1} \circ \cdots \circ L_{g_{m-1}} \circ L_{g_m h_1} \circ L_2 \circ \cdots \circ L_n & \text{if } g_m, h_1 \in G_\alpha \text{ and } g_m h_1 \neq e_\alpha \\ L_{g_1} \circ \cdots \circ L_{g_{m-1}} \circ L_{h_2} \circ \cdots \circ L_n & \text{if } g_m \cdot h_1 = e_\alpha. \end{cases}$$

From this it follows that $L_{g \bullet h} = L_g \circ L_h$.

The associativity now follows from

$$\begin{aligned} L_{(g \bullet h) \bullet k} &= L_{g \bullet h} \circ L_k \\ &= (L_g \circ L_h) \circ L_k \\ &= L_g \circ (L_h \circ L_k) \\ &= L_g \circ L_{h \bullet k} \\ &= L_{g \bullet (h \bullet k)}. \end{aligned}$$

By the injectivity of L, $(g \bullet h) \bullet k = g \bullet (h \bullet k)$. □

A consequence of the associativity is that the order in which a reduction is performed does not affect the end result: every word reduces to a unique reduced form.

Example 19.2. Consider two copies of the group $\mathbb{Z}_2 = \mathbb{Z}/(2\mathbb{Z})$, with generators a and b, respectively. Since $a^2 = e$ and $b^2 = e$, all the reduced words consist of alternating sequences of a and b, for example $ababab$ or $babab$. The inverse of ab is ba, and therefore the set of words of even length forms a cyclic subgroup $G \cong \mathbb{Z}$ generated by ab. If $H \cong \mathbb{Z}_2$ is the subgroup generated by a, then $\mathbb{Z}_2 * \mathbb{Z}_2 = GH$; that is, $\mathbb{Z}_2 * \mathbb{Z}_2 \cong \mathbb{Z} \rtimes \mathbb{Z}_2$, the semi-direct product of these two subgroups.