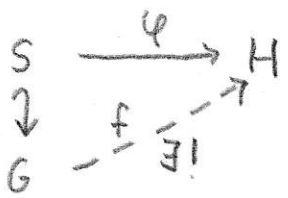
1. Free groups

Definitions and simple facts

1.1 **Definition.** Let G be a group. A basis of G is a subset $S \subset G$ with the following property.

(*) For any group H and any map $\varphi : S \longrightarrow H$ there exists a unique homomorphism $f : G \longrightarrow H$ such that $f(s) = \varphi(s)$ for all $s \in S$.



φ map of sets

f homomorphism of groups

1.2 **Definition.** A group is called free if it possesses a basis. [If G has a basis S we say that G is free with basis S or that G is free over S]

1.3 **Proposition.** For any set T there is a group G and an injective map $\tau : T \longrightarrow G$ such that G is free with basis $\tau(T)$.

Proof. Consider the set $T \times \{-1, 1\}$. For $t \in T$ we write for $(t, 1)$ t or t^1 (i.e. $t = t^1 = (t, 1)$) and for $(t, -1)$ we write t^{-1}; i.e. we write $T \sqcup T^{-1}$ for $T \times \{-1, 1\}$

A word in $T \cup T^{-1}$ is a finite sequence

$$t_1^{\varepsilon_1} \cdot \dots \cdot t_n^{\varepsilon_n}, \quad \varepsilon_i \in \{\pm 1\}, \ t_i \in T,$$

of elements of $T \cup T^{-1}$; the empty word is also a word which we denote by 1. The set of words in $T \cup T^{-1}$ is denoted by $W(T)$. By concatenating words we define a product „$\cdot$" on $W(T)$. The product is associative with 1 as a 2-sided unit.

To introduce inverses we introduce an equivalence relation „$\sim$" on $W(T)$ as follows.

an elementary expansion of a word w is the insertion of $t t^{-1}$ or $t^{-1} t$ somewhere in w, $t \in T$, i.e. $w = w_1 \cdot w_2 \dashrightarrow w' = w_1 t t^{-1} w_2$ or

$$w_1 t^{-1} t \, w_2$$

an elementary reduction of a word is the opposite process, i.e. the removal of a $t^{-1}t$ or $t t^{-1}$ from the word.

Two words are called equivalent if one can pass from one to the other by finitely many expansions and reductions

1.4 Remark: $w_i \sim w_i'$, $i = 1, 2$; then $w_1 w_2 \sim w_1' w_2'$

Proof. by induction on the number of expansions and reductions to pass from w_i to w_i' (Exercise)

consequently, the product on $W(T)$ passes down to a product of $F(T) := W(T)/\sim$ given by

$[w_1][w_2] := [w_1 w_2]$, where $[x]$ means equiv. class of the word x. It is obviously associative with $[1]$ as unit and the inverse of

$$[t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n}] \text{ is } [t_n^{-\varepsilon_n} \cdots t_1^{-\varepsilon_1}]$$

where we set $t^{-(-1)} = t^1 = t$. Thus

$F(T)$ is a group.

Before we show that $F(T)$ is in fact free with basis $\{[t] : t \in T\}$ we solve the so called word problem for the group $F(T)$. We are looking for some algorithm that allows us to answer the following

1.5 Question: Given words $w, w' \in W(T)$. When is $[w] = [w']$ in $F(T)$?

1.6 Definition: A word w is called reduced if it does not contain a subword of the form $t^{\varepsilon} t^{-\varepsilon}$ with $\varepsilon \in \{\pm 1\}$, i.e. if w is not of the form $w_1 t^{\varepsilon} t^{-\varepsilon} w_2$ for some $t \in T$, $w_1, w_2 \in W(T)$.

1.7 Proposition: For every element $[w] \in F(T)$ there is a unique reduced word $\bar{w}$ with $[w] = [\bar{w}]$

Furthermore, if the length $\ell(w)$ of $w = t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n}$ is defined to be n then there is an algorithm which produces in (at most) $\lfloor \frac{n}{2} \rfloor$ steps the unique reduced word equivalent to w.

Proof. Here is an algorithm. Read the word w starting from the left until you hit for the first time a pair of consecutive letters of the form $t^{\varepsilon} t^{-\varepsilon}$, $\varepsilon = \pm 1$. If there is no such pair, we are done. Otherwise, remove this pair and start anew. Since at each step the word length is reduced by 2 we end after $\lfloor \frac{n}{2} \rfloor$ steps either by a 1-letter word or by 1 unless the algorithm stopped before.

To prove 1.7, it remains to show that our algorithm applied to two equivalent words w and w' produces the same reduced word

(This implies in particular: if w and w' are reduced and equivalent then they are identical. For our algorithm leaves a reduced word unchanged)

We do this by induction on the number of expansions and reductions we need to go from w to w'. I.e. it suffices (to show:) if w' is obtained from w by an expansion then our algorithm produces the same reduced word for w' as for w.

1.8: This is an (easy) exercise. □

1.9 Theorem. $\{[t] : t \in T\}$ is a basis of $F(T)$.

Remark: $t \longmapsto [t]$ is injective, since t is reduced.

Proof: Given $\varphi : T \longrightarrow H$, H a group, we need to show that there is a unique homomorphism $f : F(T) \longrightarrow H$ such that $f([t]) = \varphi(t)$, $t \in T$.

Proof. Let $x \in F(T)$, and $w \in W(T)$ a word representing x, i.e. $x = [w]$. If $w = t_1^{\varepsilon_1} \cdot \ldots \cdot t_n^{\varepsilon_n}$ then $[w] = [t_1]^{\varepsilon_1} \cdot \ldots \cdot [t_n]^{\varepsilon_n}$. Therefore, if f is a homomorphism of groups, we must define

$$f([w]) = \varphi(t_1)^{\varepsilon_1} \cdot \ldots \cdot \varphi(t_n)^{\varepsilon_n}.$$

If f is well-defined then clearly f is a homom. of groups and the only one extending φ.

But if w and w' differ by inserting $t\,t^{-1}$ or $t^{-1}t$ into one of them, say $w' = w_1 w_2$, $w = w_1 t t^{-1} w_2$, then $f[w'] = f[w]$, since $\varphi[t] \cdot \varphi[t]^{-1} = 1$ in H. □

To classify free groups we have

1.10 Let F_i be a free group with basis T_i, $i = 1, 2$. Then $F_1 \cong F_2$ if and only if T_1 and T_2 have the same cardinality.

„⇐" is straightforward using the defining property of a basis.

„⇒" We need to show that the free group F determines the cardinality of any of its bases. So let $T \subset F$ be a basis. Consider the subgroup $G \subset F$ generated by all squares of elements. G is obviously a normal subgroup since $x y^2 x^{-1} = (xyx^{-1})^2$. Furthermore, F/G is abelian since

$$xyx^{-1}y^{-1} = (xy)^2 y^{-1} x^{-2} y\, y^{-2}$$
$$= (xy)^2 (y^{-1}x^{-1}y)^2 y^{-2} \in G$$

Also, for any $x \in F$ we have $(x \cdot G)^2 = x^2 \cdot G = G$ so that F/G is a vector space over $\mathbb{F}_2$, the field with two elements. We claim that $\{[t]\cdot G : t \in T\}$ is a basis of F/G.

Obviously, $\{[t]\cdot G : t \in T\}$ generate F/G. To show that they are linearly independent we need to show that for distinct elements $t_1, \dots, t_n \in T$

$[t_1 \cdot \dots \cdot t_n] \notin G$. Now, every element

$[w_1]^2 \cdot \dots \cdot [w_k]^2$ of G has a representative

$w = w_1 \cdot w_1 \cdot \dots \cdot w_k w_k$ such that for any $t \in T$ the number of times that t or t^{-1} occur is even. This property is preserved under equivalence of words. Thus, if T is finite then $\dim_{\mathbb{F}_2} |F/G|$ is $2^{|T|}$, where $|T|$ is the cardinality of T, and if T is infinite, we have $|T| = |F/G|$. In particular, the isomorphism type of F determines $|F/G|$ and thus $|T|$. □

1.11 Remark: A consequence of 1.10 and 1.9 is that a free group G with basis $T \subset G$ is isomorphic to $F(T)$.

Furthermore, a subset $T \subset G$ of a group G is a basis of G if and only if

(i) T generates G and

(ii) If $w \in W(T)$ is a reduced word and $w_G = 1$, where w_G is the product $t_1^{\varepsilon_1} \cdot \ldots \cdot t_n^{\varepsilon_n}$ in G for the word $w = t_1^{\varepsilon_1} \cdot \ldots \cdot t_n^{\varepsilon_n}$ in $W(T)$, then $w = \emptyset$.

1.12 Notation: The cardinality of a basis of a free group F is called the rank of F. The free group of rank $n \in \mathbb{N}$ will be denoted by F_n

Remarks on presentations of groups.

Let G be a group. Then there exists a free group F and an epimorphism ($=$ surj. homomorphism) $f : F \longrightarrow G$

(Take for example the free group $F = F(G)$, G considered as a set, and use G for S in 1.1 and $\varphi : G \to G$ the identity (Here we identify (the set) G with $\{[g] \in F(G) : g \in G\}$)).

Let $\overline{R} \subset \ker f$ be a subset s.t. $\ker f$ is the smallest normal subgroup of F containing $\overline{R}$. Let T be a basis and choose for every $\overline{r} \in \overline{R}$ a word $r \in W(T)$ such that $[r] = \overline{r}$, and let $R = \{r \in W(T) : \overline{r} \in \overline{R}\}$.

So we have a set T and set R of words in $T \sqcup T^{-1}$.

$\langle \overline{R} \rangle_N$: smallest normal subgp. generated by $\overline{R}$ in $F(T)$.

These two data define the group $F(T)/\langle\langle \overline{R} \rangle\rangle_N$ which is isomorphic to G via $x \cdot \ker f \longmapsto f(x)$, $x \in F(T)$. So the data $\langle T \mid R \rangle$ describe the group G up to isomorphism. The pair $\langle T \mid R \rangle$ is called a presentation for G. Unfortunately every group has many presentations, and there is no algorithm to decide whether two presentations define isomorphic groups, even if for both presentions T and R are finite sets (then G is called finitely presentable.) Anyhow, given a fixed free group F and two sets $S_1, S_2 \subset F$, it is important to know whether there is an algorithm which decides whether there is an automorphism $\Sigma : F \to F$ with $\Sigma(S_1) = S_2$. If time

permits we will look at questions of this type.

Graphs have proved very useful in the study of these questions. That is what we turn to now.