Mathematics 4340
What is a free group?
Ken Brown, Cornell University, February 2009

Intuitively, the free group on two generators a, b is a group $F = F(a, b)$ generated by a and b and satisfying no relations other than those forced by the laws of group theory. Here's one way to construct it rigorously.

Let A be a 4-element set whose elements are denoted $\{a^{\pm 1}, b^{\pm 1}\}$. Let A^* be the set of *words* in the alphabet A; formally, a word is just a finite sequence $(a_1, \dots, a_n)$ $(n \geq 0)$ with $a_i \in A$ for all i, but we will often be less formal and just write $a_1 \cdots a_n$. For example, a, ab, and $aa^{-1}ba$ are all words.

There is an associative product on words, given by juxtaposition. It has an identity (given by the empty word, for which $n = 0$ above). But nothing is invertible except the identity. In order to get inverses, we impose an equivalence relation on A^*: We declare two words w, w' to be *equivalent*, and we write $w \sim w'$, if we can get from one to the other by inserting or deleting zero or more subwords of the form xx^{-1} with $x \in A$. (Here if $x = a^{-1}$, then $x^{-1} := a$, and similarly for b^{-1}.) It is straightforward to check that this equivalence relation is compatible with juxtaposition of words, i.e.,

$$w_1 \sim w_1' \text{ and } w_2 \sim w_2' \implies w_1 w_2 \sim w_1' w_2'.$$

It follows that the set F of equivalence classes inherits a well-defined multiplication operation. This is still associative and still has an identity. Moreover, every element has an inverse; indeed, if f is the equivalence class of a word $(a_1, \dots, a_n)$, then f^{-1} is the equivalence class of the word $(a_n^{-1}, \dots, a_1^{-1})$. Thus F is a group. This is the desired free group on two generators, the generators being the equivalence classes of the words a and b of length 1. Usually we are less formal and simply write a and b for these equivalence classes.

I hope the definition of F seems reasonable to you, based on the intuition expressed in the first sentence of this handout. A more sophisticated way of expressing the same idea is to say that F has the following *universal mapping property*, analogous to the characteristic property of a basis of a vector space:

Theorem. *Given a group G and two elements $\alpha, \beta \in G$, there is a unique homomorphism $\phi\colon F \to G$ such that $\phi(a) = \alpha$ and $\phi(b) = \beta$.*

Sketch of proof. Uniqueness is clear, since a homomorphism is always uniquely determined by its effect on a given set of generators. For existence, first define $\psi\colon A \to G$ in the obvious way [$\psi(a) := \alpha$, $\psi(a^{-1}) := \alpha^{-1}$, and so on]. Now extend ψ to A^* in the equally obvious way [$\psi(a_1, \dots, a_n) := (\psi(a_1), \dots, \psi(a_n))$]. Then ψ preserves products and is compatible with the equivalence relation, i.e.,

$$w \sim w' \implies \psi(w) = \psi(w').$$

It follows that ψ induces a well-defined homomorphism $\phi\colon F \to G$, taking the equivalence class of a word w to $\psi(w)$. By construction, $\phi(a) = \alpha$ and $\phi(b) = \beta$. $\square$

Remark 1. For simplicity, I only treated the free group on two generators. The same method works for any set of generators, finite or infinite.

Remark 2. The simple construction presented here is hardly ever given in group theory books because it's possible to prove a better result, in which the elements of F are represented uniquely as *reduced* words. This requires a more clever approach, but it is not really difficult. We will do it in class. See also Theorem 16 on p. 217 of your text for a *very* concise treatment of this.