Noteworthy properties of free groups:

- If $|X| = 1$ then $F(X) \simeq \mathbb{Z}$.
- If $|X| \geq 2$ then $F(X)$ is nonabelian. To see this, note if $x, y \in X$ then $xyx^{-1}y^{-1}$ is a reduced word, so $xyx^{-1}y^{-1} \neq id$ (because reduced words are only equal if they are equal entry-by-entry).
- It can be proved by induction that $g \in F(X), g \neq id$ implies $g^n \neq id$ for all n.
- Famous theorem (hard to prove):
  If $H \subset F(X)$ is some subgroup of $F(X)$, then there exists a set Y such that $H \simeq F(Y)$. (I.e. every subgroup of a free group is a free group).

The universal property of free groups:

Theorem: Let $i : X \longrightarrow F(X)$ be the inclusion map. If G is a group and $f : X \longrightarrow G$ is any map of sets, then there is a unique homomorphism of groups $\bar{f} : F(X) \longrightarrow G$ such that

$$\begin{tikzcd} X \arrow[r, hook, "i"] \arrow[dr, "f"'] & F(X) \arrow[d, dashed, "\bar{f}"] \\ & G \end{tikzcd}$$

commutes, ie $\bar{f} \circ i = f$.

Remark:

This means the free group on a set X is the unique group (up to isomorphism) containing X such that every map of sets $X \xrightarrow{f} G$ can be "extended" to map of groups (homomorphism) $F(X) \xrightarrow{\bar{f}} G$.

Proof: Given $f: X \to G$, we need to define $\bar{f}: F(X) \to G$ that "agrees with f" on the set X. So set $\bar{f}(id) = id$, and given a reduced word $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in F(X)$, set

$$\bar{f}(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} \cdot f(x_2)^{\varepsilon_2} \cdots f(x_n)^{\varepsilon_n}.$$

Since $f(x_i)$ are all elements of the group G and $\varepsilon_i = \pm 1$, the product on the right hand side makes sense as an element of G. It is easy to check cases and verify that $\bar{f}$ is a homomorphism, e.g. if

$x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in F(X)$ and $y_1^{\delta_1} \cdots y_m^{\delta_m} \in F(X)$ with

$$(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})(y_1^{\delta_1} \cdots y_m^{\delta_m}) = x_1^{\varepsilon_1} \cdots x_{n-k}^{\varepsilon_{n-k}} y_{k+1}^{\delta_{k+1}} \cdots y_m^{\delta_m}$$

(so there has been some cancelation)

then

$$\bar{f}((x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})(y_1^{\delta_1} \cdots y_m^{\delta_m})) = \bar{f}(x_1^{\varepsilon_1} \cdots x_{n-k}^{\varepsilon_{n-k}} y_{k+1}^{\delta_{k+1}} \cdots y_m^{\delta_m})$$

$$= f(x_1)^{\varepsilon_1} \cdots f(x_{n-k})^{\varepsilon_{n-k}} f(y_{k+1})^{\delta_{k+1}} \cdots f(y_m)^{\delta_m}$$

while

$$\bar{f}(x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n})\cdot\bar{f}(y_1^{\delta_1}\cdots y_m^{\delta_m}) = f(x_1)^{\varepsilon_1}\cdots\underbrace{f(x_n)^{\varepsilon_n}f(y_1)^{\delta_1}}_{\substack{\text{cancelation in } G\\ \text{will happen here}}}\cdots f(y_m)^{\delta_m}$$

$$= f(x_1)^{\varepsilon_1}\cdots f(x_{n-k})^{\varepsilon_{n-k}} f(y_{k+1})^{\delta_{k+1}}\cdots f(y_m)^{\delta_m}$$

So it works.

Now suppose g is any other homomorphism $g: F(X)\longrightarrow G$ with $g(x) = f\circ i(x)$ for all $x\in X$.

Then

$$g(x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n}) = g(x_1)^{\varepsilon_1}\cdots g(x_n)^{\varepsilon_n} \quad (\text{since } g \text{ is a homomorphism})$$

$$= (f\circ i(x_1))^{\varepsilon_1}\cdots (f\circ i(x_n))^{\varepsilon_n} \quad (\text{since } g = f\circ i).$$

$$= \bar{f}(x_1)^{\varepsilon_1}\cdots\bar{f}(x_n)^{\varepsilon_n}$$

$$= \bar{f}(x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n}), \text{ since } \bar{f} \text{ is a homomorphism}$$

So $\bar{f}$ is unique. (It follows also that $F(X)$ is <u>unique up to isomorphism</u>).

<u>Corollary</u>: Every group G is the image of some free group F under a homomorphism $F \longrightarrow G$.

<u>Proof</u>: Consider the group G as a set, and create the free group $F(G)$. There is an obvious map of sets from the generating set of $F(G)$ to G, it is $\underset{\text{(set element)}}{g} \longmapsto \underset{\text{(group element)}}{g}$.

By the universal property of $F(G)$, there's a homomorphism $\varphi: F(G) \longrightarrow G$ that satisfies $\varphi(g) = g$, so φ is surjective.

<u>Corollary</u>: Every group G is isomorphic to $F(X)/N$, where X is some set and $N \trianglelefteq F(X)$ is some normal subgroup.

<u>Proof</u>: First isomorphism theorem.

Thus, if we are given a group G, we can specify G up to isomorphism by giving a set X and a normal subgroup $N \trianglelefteq F(X)$ such that $G \cong F(X)/N$.

<u>"Review"</u>: Given a group G, <u>the subgroup</u>

generated by a set $S \subset G$ is defined to be:

(i) Intersection of all subgroups of G containing S, ie $\bigcap_{\substack{H \leq G \\ S \subset H}} H$, or equivalently

(ii) It is a subgroup $H \subset G$ such that $S \subset H$ and S is a generating set for H. This means for every $h \in H$, we can write h as a product $h = s_1 s_2 \cdots s_n$ for some choice of $s_i \in S \cup S^{-1}$.

We can also define the normal subgroup of a group G generated by a subset $S \subset G$. It is defined to be:

(i) The intersection of all normal subgroups of G containing S, ie $\bigcap_{\substack{H \trianglelefteq G \\ S \subset H}} H$, or equivalently

(ii) It is a subgroup $H \subset G$ such that $S \subset H$ and every $h \in H$ can be expressed as a product

$$h = g_1 s_1 g_1^{-1} g_2 s_2 g_2^{-1} \cdots g_n s_n g_n^{-1}$$

for some choice of $s_i \in S \cup S^{-1}$ and $g_i \in G$.

So, we can specify normal subgroups of $F(X)$ by giving generators for the normal subgroup. So we make a definition.

Def: Let X be a set and $Y \subset F(X)$ a set of (reduced) words. A group G is said to be the group defined by the generators X and relations Y if $G \cong F(X)/N$, where N is the normal subgroup of $F(X)$ generated by Y. We say

$$\langle X \mid Y \rangle \text{ is a presentation of } G.$$

LaTeX remark: $\langle\ \rangle$ are \langle, \rangle, $\mid$ is \mid.

Example: Suppose $G = \langle a, b \mid a^4 = id,\ a^2b^{-2} = id,\ abab^{-1} = id \rangle$.

(Note: We often write $w = id$ for each $w \in Y$, although some books/sources do simply list the elements of Y with no equalities). Is this a familiar group? What is it isomorphic to?

Useful Theorem: Let X be a set and $Y \subset F(X)$, and $G = \langle X \mid Y \rangle$. If H is any group generated by X and H satisfies all the relations in Y, then there is an onto homomorphism $G \longrightarrow H$.

Proof: The inclusion map $X \longrightarrow H$ yields a surjective homomorphism $F(X) \xrightarrow{\varphi} H$ by the universal property of the free group $F(X)$. Since H satisfies all relations, we know $y \in Y \subset F(X)$ satisfies $\varphi(y) = id \in H$.
Therefore $Y \subset \ker\varphi$, and since $\ker\varphi$ is normal this means $\langle\langle Y \rangle\rangle \subset \ker\varphi$. But then there is a surjective map

$$\begin{array}{ccc} F(X)/\langle\langle Y\rangle\rangle & \longrightarrow & F(X)/\ker\varphi \\ \text{\rotatebox{90}{$\cong$}} & & \text{\rotatebox{90}{$\cong$}} \\ G \text{ since} & & H \text{ by the} \\ G \simeq \langle X \mid Y \rangle & & \text{first isomorphism theorem.} \end{array}$$

So we have a surjective homomorphism $G \longrightarrow H$ as claimed.

Continuing our example, one can check that the group

$$Q_8 = \langle i, j, k, -1 \mid i^2 = j^2 = k^2 = ijk = -1,\ (-1)^2 = id \rangle$$

contains elements a, b that satisfy $a^4 = id$, $a^2b^{-2} = id$ and $abab^{-1} = id$, and serve as generators for Q_8.
Specifically we can take $a = i$, $b = j$ and check:

$$a^4 = i^2 = (-1)^2 = id$$
$$a^2b^{-2} = i^2 j^{-2} = id$$
$$abab^{-1} = ijij^{-1} = kij^{-1} = jj^{-1} = id.$$

So by the previous theorem, there's a homomorphism $\varphi : \langle a, b \mid a^4 = id,\ a^2 b^{-2} = id,\ abab^{-1} = id \rangle \longrightarrow Q_8$ given by $\varphi(a) = i$, $\varphi(b) = j$.

On the other hand, by a similar argument there's a homomorphism $\psi : Q_8 \longrightarrow \langle a, b \mid a^4 = id,\ a^2 b^{-2} = id,\ abab^{-1} = id \rangle$ given by $\psi(i) = a$, $\psi(j) = b$, $\psi(k) = ab$ and $\psi(-1) = a^2$.

Then check that φ and ψ are inverse to one another:

$\psi(\varphi(a)) = \psi(i) = a$

$\psi(\varphi(b)) = \psi(j) = b$, so $\psi \circ \varphi$ is the identity

and

$\varphi(\psi(i)) = \varphi(a) = i$

$\varphi(\psi(j)) = \varphi(b) = j$

$\varphi(\psi(k)) = \varphi(ab) = \underbrace{ij = k}_{\text{by relations in } Q_8}$ so $\varphi \circ \psi$ is the identity.

$\varphi(\psi(-1)) = \varphi(a^2) = i^2 = -1$.

Thus φ and ψ provide isomorphisms

$$\langle a, b \mid a^4 = id,\ a^2 b^{-2} = id\ \ abab^{-1} = id \rangle \cong Q_8.$$

Terminology: If X is finite and $G \simeq \langle X \mid Y \rangle$, we say that G is finitely generated. Given a group G, if there exist finite sets X and Y with $G \simeq \langle X \mid Y \rangle$ then we say G is finitely presented.

Example: Every finite group is finitely presented. To see this, suppose $G = \{g_1, \dots, g_n\}$. Set $S = G$ and observe that the identity

$$\begin{aligned} S &\longrightarrow G \\ g_i &\longmapsto g_i \end{aligned}$$

yields a unique homomorphism $\varphi : F(S) \to G$ with $\varphi(g_i) = g_i$ for all i. The group G is finite and so completely determined by its (finite) multiplication table, ie equations $g_i g_j = g_k$ where $i,j = 1, \dots, n$. Let $R_0 \subset F(S)$ be the set of reduced words

$$\left\{ g_i g_j g_k^{-1} \;\middle|\; \begin{array}{l} i,j = 1, \dots, n \text{ and } g_i g_j = g_k \text{ in } G \\ \text{with } g_i, g_j, g_k \text{ not the identity} \end{array} \right\}$$

Then $R_0 \subset \ker(\varphi)$, since $\varphi(g_i g_j g_k^{-1}) = g_i g_j g_k^{-1} = id \in G$. Thus there is a surjective homomorphism

$$F(S)/\langle\langle R_0 \rangle\rangle \longrightarrow F(S)/\ker\varphi \simeq G,$$

and we need to show it's injective. To do this, note that if $\langle\langle R_0 \rangle\rangle = N$ then $F(S)/\langle\langle R_0 \rangle\rangle$ is generated by $\{g_1 N, g_2 N, \dots, g_n N\}$ and in fact this set of elements is closed under multiplication, since

$$(g_i N)(g_j N) = g_k N \quad i,j = 1, \dots, n$$

Thus $F(S)/_N = \{g_1 N, \ldots, g_n N\}$. Since this means $|F(S)/_N| = |F(S)/_{\ker\varphi}| = n$, the surjective map

$F(S)/_{\langle\langle R_\circ \rangle\rangle} \longrightarrow F(S)/_{\ker\varphi}$ must also be 1-1, meaning it is an isomorphism. Thus $G \simeq F(S)/_{\langle\langle R_\circ\rangle\rangle}$ so $G \simeq \langle S \mid R_\circ \rangle$ and thus is finitely presented.

Remark: Finding examples of non-finitely presented (yet finitely generated!) groups is extremely hard.
A correction to what I wrote on the board in class is the following example:

First, note that if $G_1 \simeq \langle X_1 \mid Y_1 \rangle$ and $G_2 \simeq \langle X_2 \mid Y_2 \rangle$ then $G_1 \times G_2 \simeq \langle X_1 \cup X_2 \mid Y_1 \cup Y_2 \cup \{aba^{-1}b^{-1} \mid a \in X_1, b \in X_2\}\rangle$.
So $F_2 \times F_2 \simeq \langle a, b, x, y \mid axa^{-1}x^{-1} = aya^{-1}y^{-1} = bxb^{-1}x^{-1} = byb^{-1}y^{-1} = id \rangle$ since $F_2 \simeq \langle a, b \mid \emptyset \rangle$. Thus it is finitely presented.
The kernel of the homomorphism $F_2 \times F_2 \longrightarrow \mathbb{Z}$ sending every generator to 1 is apparently finitely generated but not finitely presented.

A better example (De la Harpe, page 128-129).
Recall that $SL(n, \mathbb{k})$ denotes the group of $n \times n$ matrices with entries in a field $\mathbb{k}$ which have determinant 1. We could also replace $\mathbb{k}$ with any ring (commutative) containing 1.

Let q be any power of some prime number, and $\mathbb{F}_q$ the field of order q. Facts: The notation $\mathbb{F}_q[x]$ means the polynomial ring with coefficients in $\mathbb{F}_q$.

- $SL(2, \mathbb{F}_q[x])$ is not finitely generated
- $SL(n, \mathbb{F}_q[x])$ <u>is</u> finitely generated if $n \geq 3$.

In fact:

- $SL(3, \mathbb{F}_q[x])$ is not finitely presented
- $SL(n, \mathbb{F}_q[x])$ is finitely presented for $n \geq 4$.

So $SL(n, \mathbb{F}_q[x])$ is a concrete example.

<u>Remark</u>: Determining if two presentations yield isomorphic groups is an undecidable problem.

A brief discussion of free products:

The free product of groups G_i is another example of a construction that admits a universal property. It is a group constructed as follows:

Given a family of groups $\{G_i \mid i \in I\}$, form the set $X = \bigcup_{i \in I} G_i$ and add one element denoted by id to form $X \cup \{id\}$. A word on X is a sequence $(a_1, a_2, \ldots)$ such that $a_i \in X \cup \{id\}$ and $\exists n$ s.t. $\forall k \geq n$ $a_k = id$. A word is <u>reduced</u> if:

(i) No a_i is the identity element in any G_j

(ii) a_i and a_{i+1} are never from the same group G_j

(iii) $a_n = id$ implies $a_k = id$ $\forall k \geq n$.

As before, the empty word $id = (id, id, \ldots)$ is reduced. Write reduced words as $a_1 \ldots a_n$, as before. Let $\underset{i \in I}{\ast} G_i$ denote the set of all reduced words on X.

The group operation is concatenation, with cancelation if necessary. E.g. if $a_i, b_i \in G_i$ then

$$(a_1 a_2 \cancel{a_3})(\cancel{a_3^{-1}} b_2 b_1 b_3) = a_1 c b_1 b_3 \text{ where } c = a_2 b_2$$

Note that there's an inclusion map

$$i : G_j \longrightarrow \underset{i \in I}{\ast} G_i \text{ by sending } i(g) = g$$

$\leftarrow$ word of length 1

In fact, i is a homomorphism.

<u>Fact</u>: If G_1, G_2 are groups, then $G_1 * G_2$ satisfies a universal property: For every pair of homomorphisms $\varphi_1 : G_1 \longrightarrow H$ and $\varphi_2 : G_2 \longrightarrow H$ there is a <u>unique</u> map $\varphi : G_1 * G_2 \longrightarrow H$ with $\varphi \circ i_j = \varphi_j$. In other words

$$\begin{tikzcd}
H & G_1 \arrow[l, "\varphi_1"'] \arrow[d, "i_1"] \\
G_2 \arrow[u, "\varphi_2"] \arrow[r, "i_2"] & G * G_2 \arrow[ul, dashed, "\exists ! \varphi"']
\end{tikzcd}$$

commutes.

<u>Example</u>: Suppose we have two copies of $\mathbb{Z}$, say $\mathbb{Z} = \langle s \rangle$ and $\mathbb{Z} = \langle t \rangle$. Given any group G, and any elements $g, h \in G$, the assignments $\varphi_1(s) = g$ and $\varphi_2(t) = h$ determine homomorphisms $\varphi_1 : \langle s \rangle \longrightarrow G$, and $\varphi_2 : \langle t \rangle \longrightarrow G$. Then the universal property of $\langle s \rangle * \langle t \rangle = \mathbb{Z} * \mathbb{Z}$ says that there exists unique $\varphi : \mathbb{Z} * \mathbb{Z} \longrightarrow G$ such that $\varphi \circ i_j = \varphi_j$. But this means the set $\{s, t\} \subset \mathbb{Z} * \mathbb{Z}$ has the property that for any choices of $\varphi(s) = g$ and $\varphi(t) = h$, there's a homomorphism $\overline{\varphi} : \mathbb{Z} * \mathbb{Z} \longrightarrow G$ with $\overline{\varphi}(s) = g$ and $\overline{\varphi}(t) = h$.

In other words one can check that

$\mathbb{Z} * \mathbb{Z} \simeq F(\{s,t\})$, the free group on the set $\{s,t\}$.

<u>Conclusion</u>: With a bit of work, one can show that every free group $F(X)$ is just a special case of free products. Specifically, if we let $\{\mathbb{Z}_x \mid x \in X\}$ denote a family of copies of the integers, one for each $x \in X$, then

$$F(X) \simeq \mathop{\ast}_{x \in X} \mathbb{Z}_x .$$

<u>Example</u>

<u>A presentation of</u> $\mathop{\ast}_{i \in I} G_i$ <u>can be obtained as follows</u>:

Suppose $G_i \simeq \langle X_i \mid Y_i \rangle$ for each $i \in I$. Then

$\mathop{\ast}_{i \in I} G_i \simeq \langle \bigcup_{i \in I} X_i \mid \bigcup_{i \in I} Y_i \rangle$. To check this is a presentation of the claimed group, we need to check that $\langle \bigcup_{i \in I} X_i \mid \bigcup_{i \in I} Y_i \rangle = F(\bigcup_{i \in I} X_i) \big/ \langle\langle \bigcup_{i \in I} Y_i \rangle\rangle$

satisfies the required universal property. <u>Exercise</u>: It works.

Nilpotent and Solvable groups

Hungerford § 2.7, 2.8.

The study of solvable groups was historically motivated by the study of solving polynomial equations via radicals. The study of nilpotent groups is then a natural generalization of the study of solvable groups, and we can think of both concepts as a study of groups that are in some sense "almost abelian".

Let G be a group. Denote the centre of G by $C(G) = \{g \in H \mid ghg^{-1}h^{-1} = id \text{ for all } h \in G\}$, and note that $C(G)$ is normal in G. Thus we may consider the quotient $G/C(G)$, and its centre $C(G/C(G))$.

Set
$$C_2(G) = q^{-1}(C(G/C(G))), \text{ where } q : G \to G/C(G)$$
is the quotient map. Then we have a lemma:

Lemma: If $f : G \to H$ is any ~~onto~~ homomorphism of groups and $N \triangleleft H$ is normal then
$$f^{-1}(N) = \{g \in G \mid f(g) \in N\}$$
is a normal subgroup of H.

Proof: Note $f^{-1}(N)$ is nonempty, and suppose $a, b \in f^{-1}(N)$. Then

$f(a), f(b) \in N \Rightarrow f(a)f(b)^{-1} = f(ab^{-1}) \in N \Rightarrow ab^{-1} \in N.$
So N is a subgroup. To see it's normal, let $g \in G$ and $a \in f^{-1}(N)$ be given. Then $f(g)f(a)f(g)^{-1} \in N$ since N is normal, and $f(g)f(a)f(g)^{-1} = f(gag^{-1})$ $\Rightarrow \underline{gag^{-1}} \in N$, so N is normal.

Thus $C_2(G) \trianglelefteq G$. Continue inductively, and make a definition:

Def: Set $C_1(G) = C(G)$ and $C_i(G) = q_i^{-1}\left(C\left(G/C_{i-1}(G)\right)\right)$, where $q_i : G \longrightarrow G/C_{i-1}(G)$ is the quotient map.

The sequence of normal subgroups

$$\{id\} \leq C_1(G) \leq C_2(G) \leq \ldots$$

is called the ascending central series of G.

Definition: A group G is called nilpotent if there exists n such that $C_n(G) = G$. (And so $C_k(G) = G$ for all $k \geq n$).

Example: Every group G with $|G| = p^n$ (p a prime) is nilpotent. (Maybe call this a theorem?).

First recall the class equation:

$$|G| = |C(G)| + \underbrace{\sum |G : C(x)|}_{\substack{\text{Sum over} \\ \text{conjugacy classes w/ more than 1 element}}}$$

Now if $|G| = p^n$, then note that since

$$|G| = |G : C(x)| \cdot |C(x)|,$$

the terms $|G : C(x)|$ must all be divisible by p. So we have; from the class equation:

$$p^n = |C(G)| + \text{divisible by } p$$

$$\Rightarrow |C(G)| \text{ is divisible by } p, \text{ so it's nontrivial.}$$

So now when we take $G/C(G)$, we get another p-group (again its order is p^m for some m). If $m>0$ then its centre is nontrivial again, giving a proper ~~nontrivial~~ $C_2(G) \subset G$. Then $G/C_2(G)$ is also a p-group. if it's trivial, stop, because that means $G = C_2(G)$ is nilpotent. Otherwise $C(G/C_2(G))$ is nontrivial, and we get a proper $C_3(G) \subset G$...

because G is finite, this process must terminate, so eventually $C_k(G) = G$ and G is nilpotent.