Free Groups

Rather than begin with the definition of a free group, let's begin with some examples. The free group on two generators x and y, denoted $\langle x,y\rangle$, has as its elements all the (finite) words in x and y. By a *word* in x and y, we mean a finite product of powers of x and y. Whenever two powers of x are juxtaposed, we simplify using the rule $x^ix^j=x^{i+j}$ (here $i,j\in\mathbb{Z}$); similarly for powers of y. Furthermore $x^0=y^0=1$ is the identity. No other simplification is possible in a free group. Consider for example the product of $x^2y^{-3}xy^{-2}$ with $y^2x^{-4}y^{-1}$:

$$(x^2y^{-3}xy^{-2})(y^2x^{-4}y^{-1})=x^2y^{-3}xx^{-4}y^{-1}=x^2y^{-3}x^{-3}y^{-1}.$$

The inverse of $x^2y^{-3}xy^{-2}$ is $y^2x^{-1}y^3x^{-2}$. It is not hard to see that $\langle x,y\rangle$ is a group. This group is generated by x and y, which are independent symbols (hence 'free', meaning that there are no relations between x and y).

For any set X (finite or infinite), we similarly construct the free group on X. This group, denoted by $\langle X\rangle$, consists of all words in the elements of X (these being finite products of powers of elements of X). Here is an example of a computation in $\langle x,y,z\rangle$:

$$\begin{aligned}(y^{-1}zy^2x^{-1}y)^2(z^{-1}yx^{-1}y)^{-1}&=(y^{-1}zy^2x^{-1}y)(y^{-1}zy^2x^{-1}y)(y^{-1}xy^{-1}z)\\&=y^{-1}zy^2x^{-1}zyz.\end{aligned}$$

The free group on one generator is infinite cyclic:

$$\langle x\rangle=\{\ldots,x^{-2},x^{-1},1,x,x^2,x^3,\ldots\}.$$

Evidently $\langle X\rangle$ is abelian iff $|X|\leqslant 1$. The case $|X|=0$ gives the trivial group: $\langle\varnothing\rangle=\{1\}$.

As straightforward as this general construction is, it is notable for several reasons:

- It provides an early example of a class of groups constructed not from numbers, matrices, or functions, but in a purely formal manner.
- Some of our earliest examples of fundamental groups may be identified (up to isomorphism) as free groups. Indeed if $X=\mathbb{R}^2\smallsetminus\{P_1,P_2,\ldots,P_n\}$, where $P_1,\ldots,P_n$ are distinct points in the plane, then $\pi_1(X)$ is a free group on n generators.
- It provides the starting point for describing the more general notion of group presentations (specification of groups using generators and relations).

As simple and natural as the construction of free groups appears, already we encounter several interesting features. In particular, it is true (but not obvious) that every subgroup of a free group is free. To prove this or any other substantial facts regarding free groups, the construction we have described above is not very suitable. However we are about to present the actual *definition* of a free group, which is suitable for proving basic facts about free groups.

To understand this point, let me draw an analogy with the system of real numbers. We learn at an early age how to represent real numbers as decimals. But to understand any of the essential features of $\mathbb{R}$ (from the most basic algebraic properties, such as the field axioms, to the more subtle properties used in modern real analysis) one appeals to a definition of $\mathbb{R}$ as a completion of $\mathbb{Q}$, i.e. real numbers are represented using Cauchy sequences of rational numbers*. Imagine how cumbersome it would be to try to prove the distributive law for real numbers, if one were to use decimal representations to actually *define* $\mathbb{R}$!

Let us motivate the definition of a free group by observing that the elements of X play the same role in the free group $F = \langle X \rangle$, as that played by a basis of a vector space: the elements of the subset $X \subset F$ generate F, but there are no nontrivial relations between the elements of this subset. Our definition of a free group will in fact mimic another important property of a basis of a vector space. Let V be a vector space, and $\mathcal{B} \subset V$ a basis. Then every linear transformation $\varphi : V \to W$ is uniquely determined by its values on $\mathcal{B}$. This leads to an equivalent definition of a basis, as follows. (All vector spaces are over the same field F, by assumption.)

Definition. Let B be a subset of a vector space V. We say that B is a *basis of* V if every map φ from B to an arbitrary vector space W, has a unique extension to a linear transformation $\widehat{\varphi} : V \to W$.

This is equivalent to the standard definition of a basis. Here, now, is a definition of a free group:

Definition. Let X be a subset of a group F. We say that F is *free on* X if every map φ from X to an arbitrary group G, has a unique extension to a homomorphism $\widehat{\varphi} : F \to G$.

* One must identify Cauchy sequences of rationals having the same limit; so actually a real number is represented as an *equivalence class* of Cauchy sequences of rationals. As an alternative, one can use the easier approach of Dedekind cuts; but this approach relies heavily on the total ordering of $\mathbb{Q}$ and so is not a typical approach to completion of a metric space.

(Note: Although every vector space has a basis, by Zorn's Lemma, not every group is free! The point is that while every group has a set of generators, it is not always possible to find a set of 'independent' generators. The subject of group presentations will resolve this issue.)

While this naturally mimics our definition of a basis, it raises two problems. One is that for a given set X, we need to show that there *exists* a group which is free on X. (This is however not hard; just use the construction given above! Take F to be the set of words constructed from the set of symbols X, and show that F has the required property.) Another is to prove uniqueness (up to isomorphism). But this can be shown without much difficulty; and so one can then speak of *the* free group on X, denoted henceforth by $\langle X \rangle$. All important properties of free groups follow from the defining property, and the construction using words over X takes a secondary place in our minds.

We refer to the defining property of a free group as its *universality*. We dwell on this point because the notion of universality is very useful in defining a wide range of objects (tensor products being a good example), far beyond our immediate goals. The group $F = \langle X \rangle$ is the universal domain for all homomorphisms defined on a set of $|X|$ generators.

There is an even more useful formulation of the definition of a free group, as follows. (This is the definition we will actually use!)

Definition. Let $\iota : X \to F$ be a map from a set X to a group F. We say F is *free on* X if for every map φ from X to an arbitrary group G, there is a unique homomorphism $\widehat{\varphi} : F \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
& X \arrow[ld, "\iota"'] \arrow[rd, "\varphi"] & \\
F \arrow[rr, dashed, "\widehat{\varphi}"'] & & G
\end{tikzcd}$$

The commutativity of the diagram means that $\widehat{\varphi} \circ \iota = \varphi$. It is not hard to see that the uniqueness of $\widehat{\varphi}$ in general, requires that ι be one-to-one; so we may identify X with its image in F. So this definition is equivalent to the previous formulation of freeness.

To prove uniqueness of F, suppose the maps $\iota : X \to F$ and $\widetilde{\iota} : X \to \widetilde{F}$ both satisfy the conditions of the definition. Then there exist maps α and β making the following diagram commute:

$$\begin{tikzcd}
& X \arrow[ld, "\iota"'] \arrow[d, "\widetilde{\iota}"'] \arrow[rd, "\iota"] & \\
F \arrow[r, dashed, "\alpha"'] & \widetilde{F} \arrow[r, dashed, "\beta"'] & F
\end{tikzcd}$$

Now we ask for a map indicated by '?', which makes the following diagram commute:

$$\begin{tikzcd} & X \arrow[dl, "\iota"'] \arrow[dr, "\iota"] & \\ F \arrow[rr, dashed, "?"'] & & F \end{tikzcd}$$

Two candidates are $\beta \circ \alpha$, and the identity map on F. Since F is free on X, this forces $\beta \circ \alpha$ to be the identity on F. A similar argument shows that $\alpha \circ \beta : \widetilde{F} \to \widetilde{F}$ is also the identity. So the homomorphisms α and β are in fact isomorphisms, inverse to each other. In other words, $\widetilde{F} \cong F$ by an isomorphism which identifies the embedded copies of X in these two groups. Our proof of uniqueness is complete.

Observe the advantage of the new formulation of 'free', evident in the latter proof; it allowed us to embed X simultaneously in two different groups. This example (in which the terminology of 'subset' was rephrased in the language of maps) illustrates the modern approach of *topos theory*, or the theory of *topoi* ('topoi' is the plural of 'topos'). In the standard approach, one constructs all of mathematics from sets; for example a function $f : A \to B$ is viewed as a subset of $A \times B$ (so f is a set of ordered pairs). In turn, one constructs ordered pairs of elements $(a, b) \in A \times B$ as sets by defining $(a, b) = \{\{a\}, \{a, b\}\}$. In this way all of mathematics is reduced to set theory (in a somewhat ad hoc manner, but one that seems to work). A perspective of topos theory is to turn things around by making functions the basic notions (not expressible in terms of any simpler notions), and defining notions of 'set', 'subset', 'Cartesian product', etc. in terms of functions. 'Nuff said.

Free Subgroups of Linear Groups

A *linear group* is a subgroup of $GL(V)$ for V a vector space. We will take $V = F^n$ where F is a field; thus our linear groups are subgroups of $GL_n(F)$. The *composition factors* of a group G have the form N/K where $N \leqslant G$ and K is a maximal normal subgroup of N. (So all composition factors of G are simple, hence either cyclic or nonabelian simple.) A group is *solvable* if all its composition factors are cyclic. A group is *viritually solvable* if it has a solvable subgroup of finite index. (In particular every finite group is virtually solvable; and so is every solvable group.) A famous theorem of Jacques Tits (1972), is:

Theorem (Tits Alternative). Let G be an arbitrary linear group (so $n \geqslant 1$ and $G \leqslant GL_n(F)$ where F is an arbitrary field). Then either G is virtually solvable, or G has a free subgroup on two generators.

For every cardinality of set $r = |X|$, one has the free group on X, which is a free group F_r of rank r. These groups are not isomorphic for different r. But every subgroup of a free group is free; and F_2 contains free subgroups of every countable rank (finite or infinite countable). So the second conclusion of the Tits Alternative may be replaced by 'a free subgroup of countable rank'.

The Theorem answered an earlier question of Hyman Bass and Jean-Pierre Serre. It is a cornerstone of Geometric Group Theory. Its conclusion is a true alternative: if G is virtually solvable, then it cannot have a free subgroup of rank 2. The proof requires extensive background preparation in several areas, including algebraic geometry. We will not have time to prove it here.

We will however present the result in an easy special case, where $G = SO_3(\mathbb{R})$. In this case (as with most linear groups over $\mathbb{R}$ or $\mathbb{C}$), there are *many* ways to choose $A, B \in G$ which generate a free subgroup of rank 2. Topological methods show that most pairs A, B suffice. This is to be expected: for example if $A_\theta, B_\theta \in SO_3(\mathbb{R})$ are rotations by the same angle θ about the x- and y-axes, respectively, then 'most' choices of θ give generators of a free group of rank 2. There are only countably many words in A_θ and B_θ; and for every such word, we expect that only countably many values of θ will fail to give generators of a free group. Since there are uncountably many choices of angle θ, with only countably many choices failing to give a free group $\langle A_\theta, B_\theta\rangle$, there should exist values of $\theta \in [0, 2\pi)$ that work. Rather than trying to provide such an existence proof, we proceed to construct an explicit pair of generators.

A Free Subgroup of $SO_3(\mathbb{R})$

Our proof follows [W, pp.15–16]. (It seems however thatsome of the details in [W] are incorrect…probably he means to work mod 3 in some places but hasn't explicitly indicated this. In any case, I will rewrite the proof in a way that I find more clear insightful.) Consider the matrices

$$A^{\pm 1} = \frac{1}{3}\begin{bmatrix} 1 & \mp 4 & 0 \\ \pm 2 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}, \quad B^{\pm 1} = \frac{1}{3}\begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & \mp 2 \\ 0 & \pm 4 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note that $\det A = \det B = 1$; moreover the matrices

$$D^{-1}AD = \begin{bmatrix} \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} & 0 \\ \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad D^{-1}BD = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \mp\frac{2\sqrt{2}}{3} \\ 0 & \pm\frac{2\sqrt{2}}{3} & \frac{1}{3} \end{bmatrix}$$

are orthogonal. We will show that they generate a subgroup $\langle D^{-1}AD, D^{-1}BD\rangle < SO_3(\mathbb{R})$ which is free of rank 2. After conjugating by D, it clearly suffices to show that the group $\langle A, B\rangle < GL_3(\mathbb{R})$ is free of rank 2.

We begin with a technical result concerning the nontrivial 2×2 principal submatrices of A and B:

Lemma. *For every positive integer k, the matrices $\left[\begin{smallmatrix} 1 & \mp 4 \\ \pm 2 & 1 \end{smallmatrix}\right]^k$ and $\left[\begin{smallmatrix} 1 & \mp 2 \\ \pm 4 & 1 \end{smallmatrix}\right]^k$ have integer entries which are not divisible by 3.*

Proof. Let $k \geqslant 1$. An easy induction shows that the entries of $\left[\begin{smallmatrix} 1 & 4 \\ -2 & 1 \end{smallmatrix}\right]^k$ and its transpose reduce (mod 3) to $\left[\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$, according as k is even or odd. Similarly, the entries of $\left[\begin{smallmatrix} 1 & -4 \\ 2 & 1 \end{smallmatrix}\right]^k$ and its transpose reduce (mod 3) to $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]$ mod 3, according as k is even or odd. □

In the following, we use the 3-adic norm on $\mathbb{Q}$ defined by

$$\|x\| = \|x\|_3 := \begin{cases} 0, & \text{if } x = 0; \\ 3^{-r}, & \text{if } x = 3^r \frac{a}{b} \text{ where } a, b, r \in \mathbb{Z} \text{ and } ab \not\equiv 0 \bmod 3. \end{cases}$$

Elementary number theory reasoning show that this is an ultrametric, i.e.

(i) $\|x\| \geqslant 0$, where equality holds iff $x = 0$;
(ii) $\|xy\| = \|x\| \cdot \|y\|$;
(iii) $\|x + y\| \leqslant \max\{\|x\|, \|y\|\}$; and
(iv) equality holds in (iii) whenver $\|x\| \neq \|y\|$.

Although we did not mention (iv) in class, it follows easily from (iii). For example, suppose that $\|x\| < \|y\|$. If the inequality in (iii) is strict, then $\|x+y\| < \|y\|$, so $\|y\| = \|(x+y) - x\| \leqslant \max\{\|x+y\|, \|x\|\} < \|y\|$, a contradiction.

Consider the subsets $L_r, R_r \subset \mathbb{Q}^3$ defined by

$$L_r = \big\{(v_1, v_2, v_3)^T \in \mathbb{Q}^3 : \|v_1\| = \|v_2\| = 3^r > \|v_3\|\big\},$$
$$R_r = \big\{(v_1, v_2, v_3)^T \in \mathbb{Q}^3 : \|v_1\| < \|v_2\| = \|v_3\| = 3^r\big\}.$$

Theorem. *For all integers $k \neq 0$ and $r \geqslant 1$, we have*

$$A^k R_r \subseteq L_{|k|+r} \qquad \textit{and} \qquad B^k L_r \subseteq R_{|k|+r}\,.$$

Proof. Let $k \neq 0$, $r \geqslant 1$ and $v \in R_r$; thus $v = (v_1, v_2, v_3)^T$ where $\|v_1\| < \|v_2\| = \|v_3\| = 3^r$. By the Lemma, $A^k v = v' = (v_1', v_2', v_3')^T$ where

$$\left.\begin{aligned} v_1' &= \alpha v_1 + \beta v_2, \\ v_2' &= \gamma v_1 + \delta v_2, \\ v_3' &= v_3 \end{aligned}\right\}, \quad \|\alpha\| = \|\beta\| = \|\gamma\| = \|\delta\| = 3^{|k|}.$$

Since $\|\alpha v_1\| = 3^{|k|}\|v_1\| < 3^{|k|}\|v_2\| = \|\beta v_2\|$, (iv) gives

$$\|v_1'\| = \|\alpha v_1 + \beta v_2\| = \|\beta v_2\| = 3^{|k|+r}.$$

Similarly, $\|v_2'\| = 3^{|k|+r}$. Since $\|v_3'\| = \|v_3\| = 3^r < 3^{|k|+r}$, we obtain $v' \in L_{|k|+r}$. The proof that $B^k L_r \subseteq R_{|k|+r}$ is similar. □

Theorem. *$\langle A, B\rangle$ is a free subgroup of $GL_3(\mathbb{R})$. Thus $\left\langle D^{-1}AD, D^{-1}BD\right\rangle$ is a free subgroup of $SO_3(\mathbb{R})$.*

Proof. We must show that no nontrivial word $w \in \langle A, B\rangle$ yields the identity. Without loss of generality, $w = A^{k_r}B^{\ell_r}A^{k_{r-1}}B^{\ell_{r-1}}\cdots A^{k_1}B^{\ell_1}A_{k_0}$ for some nonzero integers $k_r, \ell_r, k_{r-1}, \ell_{r-1}, \ldots, k_1, \ell_1, k_0$; otherwise conjugate w by an appropriate power of A to obtain this form. Let $v = (1,0,0)^T$, so that $A^{k_0}v = (\alpha, \gamma, 0)^T \in L_{|k_0|}$. By the previous Theorem, we obtain $B^{\ell_1}A^{k_0}v \in R_{|\ell_1|+|k_0|}$ and $A^{k_1}B^{\ell_1}A^{k_0}v \in L_{|k_1|+|\ell_1|+|k_0|}$. Continuing in this way, we arrive at

$$\begin{aligned} wv = A^{k_r}B^{\ell_r}A^{k_{r-1}}B^{\ell_{r-1}}\cdots A^{k_1}B^{\ell_1}A_{k_0} &\in L_m\,, \\ m = |k_r|+|\ell_r|+|k_{r-1}|+|\ell_{r-1}|+\cdots+|k_1|+|\ell_1|+|k_0| &> 0\,. \end{aligned}$$

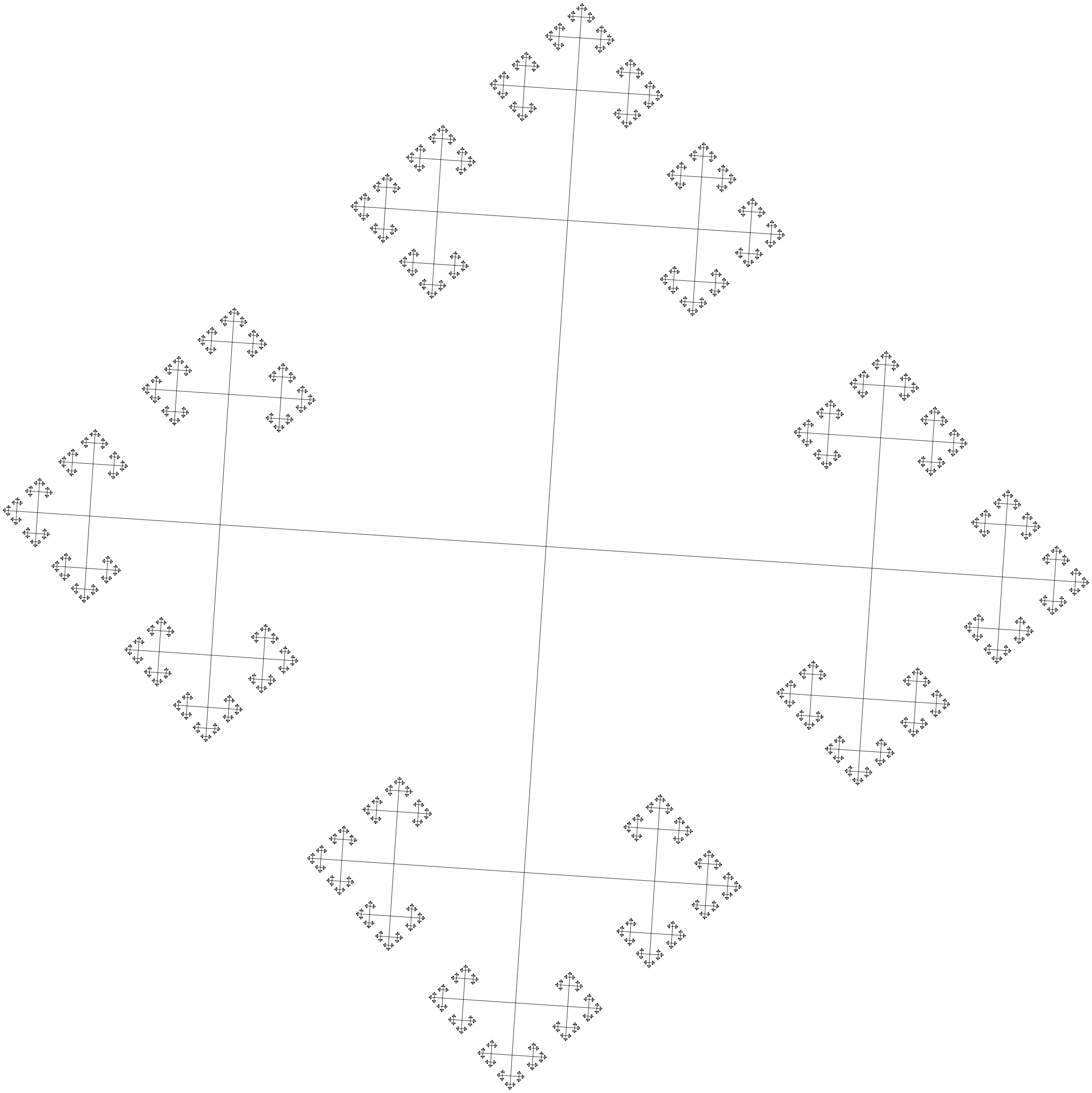
In particular, $wv \neq v$ so $w \neq 1$. □

We remark that a similar strategy is used in proving the Tits Alternative over $\mathbb{R}$ or $\mathbb{C}$ using the metric: one shows $w \neq 1$ by finding $v \in V$ such that wv is metrically very far away from v.

Reference

[W] S. Wagon, *The Banach-Tarski Paradox*, Camb. Univ. Press, 1985.

```
%!PS-Adobe-2.0
%% tree.ps
%% Generates 8th approximation to a tree of degree 4
%% (the parameter "8" which appears below can be changed).
%% G. Eric Moorhouse, University of Wyoming
0.001 setlinewidth
% Stack contains level, initial point and final point
/shrink 0.4 def
/c0 306 def
/c1 396 def
/d0 10 def
/d1 150 def
/twig {13 dict begin
  /y1 exch def
  /x1 exch def
  /y0 exch def
  /x0 exch def
  1 sub /lev exch def
  /v0 x1 x0 sub def
  /v1 y1 y0 sub def
  /x2 x1 v1 shrink mul sub def
  /y2 v0 shrink mul y1 add def
  /x3 v0 shrink mul x1 add def
  /y3 v1 shrink mul y1 add def
  /x4 v1 shrink mul x1 add def
  /y4 y1 v0 shrink mul sub def
  x2 y2 moveto
  x1 y1 lineto
  x3 y3 lineto
  x1 y1 moveto
  x4 y4 lineto
  lev 0 gt
    {lev x1 y1 x2 y2 twig
    lev x1 y1 x3 y3 twig
    lev x1 y1 x4 y4 twig}
    if
  end} def
/branch {2 dict begin
  /y1 exch def
  /x1 exch def
  c0 c1 moveto
  x1 y1 lineto
  8 c0 c1 x1 y1 twig
  end} def
newpath
c0 d0 add c1 d1 add branch
c0 d0 sub c1 d1 sub branch
c0 d1 add c1 d0 sub branch
c0 d1 sub c1 d0 add branch
stroke
showpage
```



```
%!PS-Adobe-2.0
%% tree2.ps
%% Generates 8th approximation to a tree of degree 4
%% (the parameter "8" which appears below can be changed).
%% G. Eric Moorhouse, University of Wyoming
0.001 setlinewidth
/shrink 0.45 def
/c0 306 def
/c1 396 def
/d0 40 def
/d1 150 def
/twig {15 dict begin
  /y1 exch def
  /x1 exch def
  /y0 exch def
  /x0 exch def
  1 sub /lev exch def
  /u0 x1 x0 sub def
  /u1 y1 y0 sub def
  /v0 0.92 u0 mul 0.28 u1 mul add def
  /v1 -0.28 u0 mul 0.92 u1 mul add def
  /x2 x1 v1 shrink mul sub def
  /y2 v0 shrink mul y1 add def
  /x3 v0 shrink mul x1 add def
  /y3 v1 shrink mul y1 add def
  /x4 v1 shrink mul x1 add def
  /y4 y1 v0 shrink mul sub def
  x2 y2 moveto
  x1 y1 lineto
  x3 y3 lineto
  x1 y1 moveto
  x4 y4 lineto
  lev 0 gt
    {lev x1 y1 x2 y2 twig
    lev x1 y1 x3 y3 twig
    lev x1 y1 x4 y4 twig}
    if
  end} def
/branch {2 dict begin
  /y1 exch def
  /x1 exch def
  c0 c1 moveto
  x1 y1 lineto
  8 c0 c1 x1 y1 twig
  end} def
newpath
c0 d0 add c1 d1 add branch
c0 d0 sub c1 d1 sub branch
c0 d1 add c1 d0 sub branch
c0 d1 sub c1 d0 add branch
stroke
showpage
```