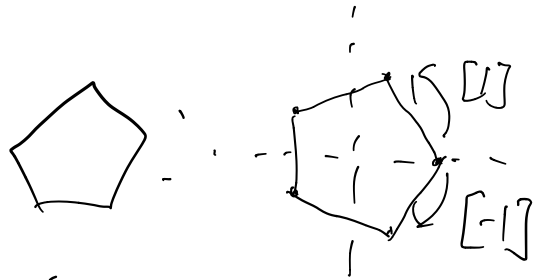
Automorphisms of free groups, understood geometrically

Automorphism groups

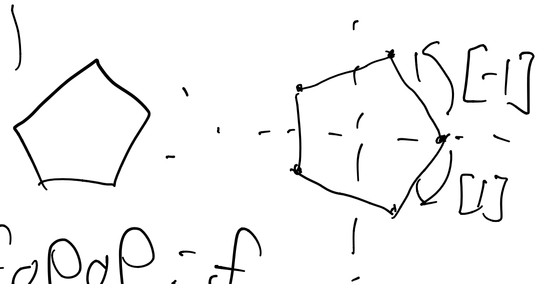
$G \mapsto Aut(G)$?

ex] $\mathbb{Z}/5 \circlearrowleft^{\rho}$



$f: \mathbb{Z}/5 \to \mathbb{Z}/5 : f([x]) = f([-x])$

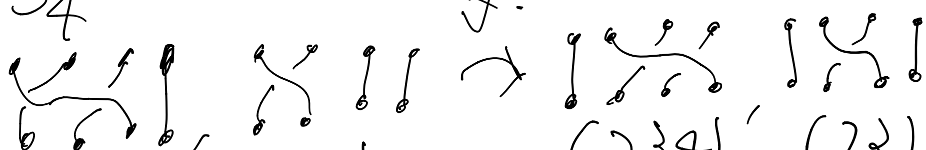
$\mathbb{Z}/5 \circlearrowleft^{(f\circ\rho)}$



$\rho = \rho^{-1}$; $f \circ \rho \circ \rho = f$

ex] $f: S_4 \to S_4$ $\qquad f: S_4 \to S_4$

$S_4 =$



(123), (12) $\mapsto$ (234), (23)

i.e. $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 1$, ...

Inner Automorphisms

$f: G \to Aut(G)$, $f(g): G \to G$, $f(g)(h) = ghg^{-1}$

$\mathrm{Im} f =$ "$\mathrm{Inn}(G)$" $\ker f =$ "$Z(G)$", "the center of G"

$\mathrm{Inn}(G) \trianglelefteq Aut(G)$, "$Aut(G)/\mathrm{Inn}(G)$" = "$\mathrm{Out}(G)$"

ex] $\mathrm{Inn}(\mathbb{Z}/5\mathbb{Z}) = 1$; $[x][y][x]^{-1} = [x+y-x] = [y]$

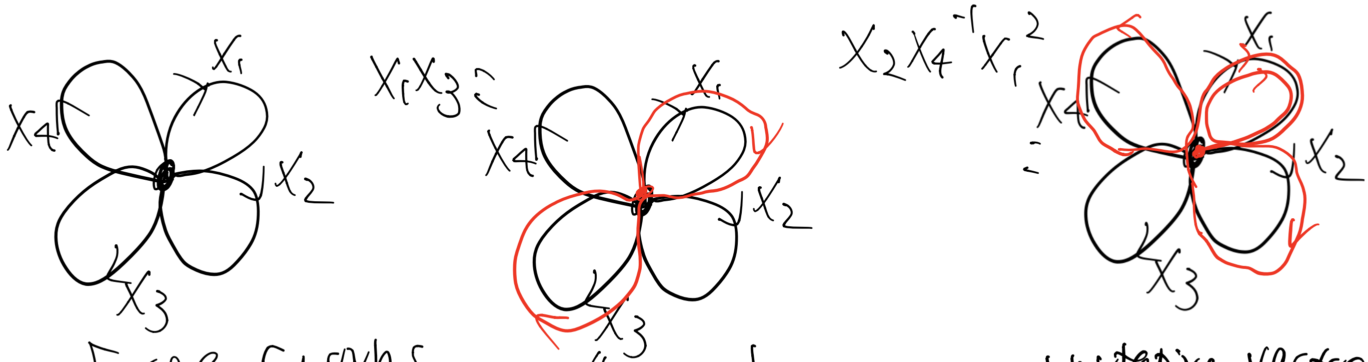
$\mathrm{Inn}(S_4) =$?

Free Groups

$\langle a,b\rangle$ = "reduced words of a's & b's"

i.e. ab, $aba^{-1}b^{-1}a \in \langle a,b\rangle$; $abb^{-1}=a$

$F_n = \langle x_1, x_2, \dots x_n\rangle$; we have the picture

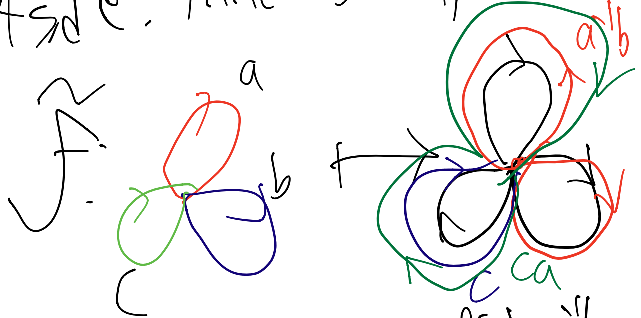


Free groups are "like discrete, noncommutative vector spaces"; like vector spaces, we have a "standard basis": x_1, x_2, x_3, x_4

But there are other bases: for example, $x_1, x_1x_2x_1^{-1}, x_1x_3x_1^{-1}, x_1x_4x_1^{-1}$

The map $f: F_4 \mapsto F_4$, $f(x_1)=x_1$, $f(x_2)=x_1x_2x_1^{-1}$, $f(x_3)=\dots$ is in fact an automorphism of F_4; in general, $f: G \to G$ is an automorphism iff for a (minimal) basis $B \subseteq G$, $f(B)$ is a basis for G.

(Aside: $\mathrm{Inn}(F_n) = F_n$, $\mathrm{Aut}(F_n)$ is interesting but not unexplored)



$f: F_3 \mapsto F_3$ $f(a)=a^{-1}b$, $f(b)=c$, $f(c)=ca$

To find the inverse, we just do $g: F_3 \mapsto F_3$:

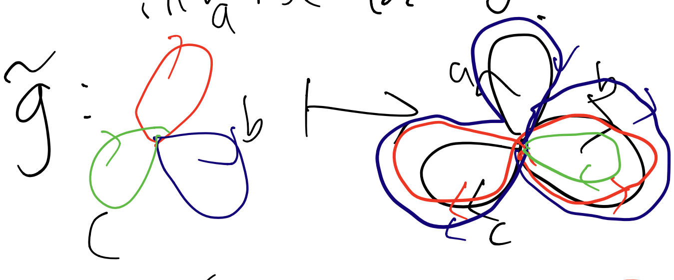
$g(a^{-1}b)=a$ $\quad g(a)=b^{-1}c$

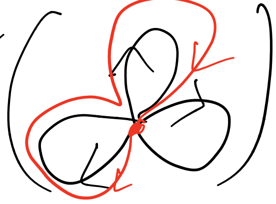
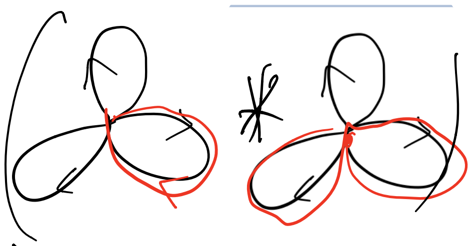
$g(c)=b \Rightarrow g(b)=b^{-1}ca$

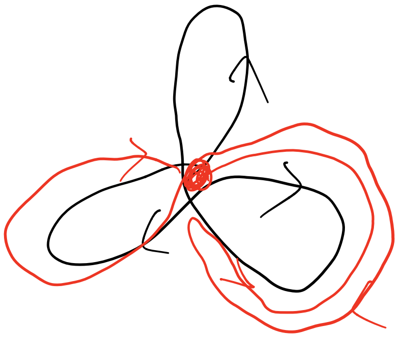
$g(ca)=c$ $\quad g(c)=b$

This is an algebraic inverse, so is $\tilde{g}$ a top. inverse for f?

Unfortunately... not quite.



ex $\tilde{g}\circ\tilde{f}(c) = \tilde{g}\Big($  $\Big) = \Big($  $\Big) =$



This shrinks (is "homotopy equivalent") to c itself maps are "homotopy inverses"

Stretching

How much does a given automorphism change the length of a given loop? Esp. when applied repeatedly?

Suppose we give each basis loop a length. Then its clear that, say, $L(f(a)) = L(a)+L(b)$.
If $L(a)=\alpha$, $L(b)=\beta$, $L(c)=\gamma$, then our length scaling is the system

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

We'd really like an eigenvector and eigenvalue.
Then, we'd have $L(f^k(a)) = \lambda^k\alpha$, $L(f^k(b)) = \lambda^k\beta$, ...
This is an "irreducible" integer matrix, which is a purely algebraic property, which entails the unique existence of a positive eigenvector with eigenvalue >1. This is certainly something we'd like: positive vector because these are "lengths", and large eigenvector since we're scaling up.
In our case, the correct eigenvalue is about 1.75. Here's the problem: If you perform f twice on c, you'll get a length less than $\lambda^2\gamma$ precisely because of the required

cancellation. The trick is to first do a change of basis, to remove the problematic cancellations. In particular, our new basis is $x = ca$, $y = b$, $z = c$, so $f(x) = zy$, $f(y) = z$, $f(z) = x$. Our new matrix is then

$$\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

which has a new unique eigenvalue satisfying our required properties.

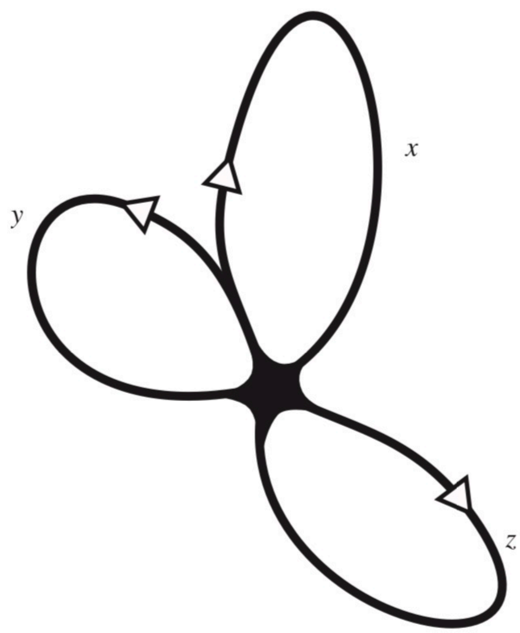
The claim is that this one works, i.e. for our new λ, $L(f^k(x)) = \lambda^k \alpha$, $L(f^k(y)) = \lambda^k \beta$ and $L(f^k(z)) = \lambda^k \gamma$. The reason is that this shall always work so long as we never run into the situation of cancellation. Cancellation occurs precisely when we have two letters next to each other such that $f(x)$ ends with the inverse of $f(y)$. Specifically we care about "turns": the transition of mapping one letter to the next. An example of a bad turn is going from x^{-1} to y; we can check that $f(x^{-1}y) = y^{-1}z^{-1}z$, which cancels. We denote this turn by $\{x, y\}$, with the understanding that cancellation occurs when the first is inverted.

The reason for this is that in this notation, $\{a,b\}$ is good $\iff$ $\{b,a\}$ is good.

There are therefore $\binom{6}{2} - 3$ turns (pick 2 gens, but distinct ones), and it's easy to see that only $\{x,y\}$ is problematic. Therefore, so long as repeatedly stretching our generators never yields $x^{-1}y$ or $y^{-1}x$, we shall be good.

Call the other 11 turns "legal"; our goal axioms are that

- Legal turns map to legal turns under f
- If a (starting) generator maps to a turn, it's legal.



$x \mapsto zy$
$y \mapsto z$
$z \mapsto x$