IV Groups

A. Basic Group Theory

a group is a set G together with a binary operation (usually called multiplication)

$$\cdot : G \times G \to G : (a,b) \mapsto a \cdot b$$

satisfying 1) $\exists$ an element $e \in G$ s.t.

$$e \cdot g = g \cdot e = g \quad \forall g \in G$$

e is called the identity element

2) for each $g \in G$ there is an element $g' \in G$ s.t.

$$g \cdot g' = g' \cdot g = e$$

g' is called the inverse of g and denoted g^{-1}

3) for all g_1, g_2, g_3 in G

$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \qquad \text{associativity}$$

examples:

1) $(\mathbb{R},+), (\mathbb{Q},+), (\mathbb{Z},+), (\mathbb{C},+)$ are groups

0 is the identity element

$-a$ is the inverse of a

2) $(\mathbb{N},+)$ is not a group (no identity element)

3) $(\mathbb{N} \cup \{0\}, +)$ is not a group (no inverses)

4) $(\mathbb{Q}-\{0\}, \times), (\mathbb{R}-\{0\}, \times), (\mathbb{C}-\{0\}, \times)$ are groups

1 is the identity element

$1/q$ is the inverse of q

5) let $\mathbb{Z}_p$ = integers modulo p

(that is, call 2 integers equivalent n, m equivalent modulo p if $n-m$ is a multiple of p

$\mathbb{Z}_p$ = set of equivalence classes)

so $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$

our binary operation is $+$

$(\mathbb{Z}_p, +)$ is a group

e.g. $\mathbb{Z}_4$ is

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

symmetric group on n elements

6) let S_n = set of permutations of $\{1, 2, \dots, n\}$

i.e. $\sigma \in S_n$ is a bijection $\sigma : \{1, 2, \dots n\} \to \{1, 2, \dots, n\}$

the binary operation is comosition

exercise: 1) $(S_n, \circ)$ is a group with identity = identity map

2) S_n has $n!$ elements

e.g.: in S_3 let $[i, j, k]$ be the map

$$\begin{aligned} 1 &\mapsto i \\ 2 &\mapsto j \\ 3 &\mapsto k \end{aligned}$$

e.g. $[2, 1, 3]$ is the map

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 3 \end{aligned}$$

S_3 has 6 elements

$[1,2,3]$, $[1,3,2]$, $[2,1,3]$, $[2,3,1]$, $[3,1,2]$, $[3,2,1]$

note: $[2,1,3] \circ [1,3,2] = [2,3,1]$

$[1,3,2] \circ [2,1,3] = [3,1,2]$

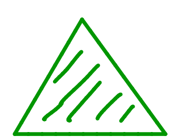
so multiplication is not commutative

a group is called abelian if $a \cdot b = b \cdot a$ for all $a, b \in G$

examples 1), 4), 5) are abelian, 6) is not for $n \geq 3$

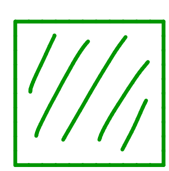
7) let Δ_n be a regular n-gon

$n = 3$



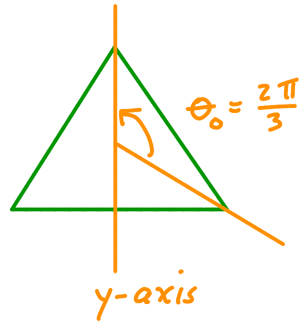
let D_n = symmetries of Δ_n with multiplication being composition

$n = 4$



D_n is called the dihedral group

e.g. $n=3$



let x = rotation by θ_0
y = reflection about y-axis

let e = identity

note: $x \cdot x$ = rotation by $2\theta_0$
$x \cdot x \cdot x$ = rotation by $3\theta_0 = e$
$y \cdot y = e$

similarly for n-gon there is rotation by $\frac{2\pi}{n}$ denoted x
and $x^n = e$

and reflection in y-axis (so $y^2 = e$)

exercise: 1) $x \cdot y \cdot x \cdot y = e$ in D_n (any n)
2) every element in D_n can be written as
$$x^i y^j$$
some i,j
3) D_n has $2n$ elements

8) let X be any topological space
let $\mathrm{Homeo}(X) = \{$all homeomorphisms of $X\}$

exercise: this is a group

let $\mathrm{Mod}(X) = \mathrm{Homeo}(X)/\sim$

called the mapping class group

where $\sim$ is isotopy

exercise: this is a group

lemma 1:

let $(G, \cdot)$ be a group

1) if $e_1, e_2 \in G$ such that $e_1 \cdot g = g \cdot e_1 = g = e_2 \cdot g = g \cdot e_2 \ \forall g \in G$
then $e_1 = e_2$ (identity in G unique)

2) if $g_1, g_2 \in G$ such that $g \cdot g_1 = g_1 \cdot g = e = g_2 \cdot g = g \cdot g_2$, then $g_1 = g_2$
(inverses are unique)

Proof:

2) $g_2 = g_2 \cdot e = g_2 \cdot (g \cdot g_1) = (g_2 \cdot g) \cdot g_1 = e \cdot g_1 = g_1$

1) $e_1 = e_1 \cdot e_2 = e_2$ ∎

If $(G, \cdot)$ and $(H, \times)$ are groups

a homomorphism is a map $f: G \to H$ such that $f(a \cdot b) = f(a) \times f(b)$

an isomorphism is a bijective homomorphism

fundamental equivalence relation for groups
try to understand groups upto isomorphism

Remark:

homomorphisms of groups are like continuous maps of topological spaces (i.e. "preserve" structure)

isomorphisms of groups are like homeomorphisms of topological spaces

lemma 2:

If $f: G \to H$ is an isomorphism, then $f^{-1}: H \to G$ is a homomorphism (and hence an isomorphism)

Proof: given $a, b \in H$

$\exists!\ a', b' \in G$ such that $f(a') = a$, $f(b') = b$

so $f(a' \cdot b') = f(a') \times f(b') = a \times b$

thus $f^{-1}(a \times b) = a' \cdot b' = f^{-1}(a) \cdot f^{-1}(b)$ ∎

examples:

1) $f: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, \cdot) : x \mapsto n \cdot x$ (n a fixed integer)

is a homomorphism since

$f(a+b) = n \cdot (a+b) = n \cdot a + n \cdot b = f(a) + f(b)$

if $n \neq \pm 1$, then f not a bijection, so not an isomorphism

if $n = \pm 1$, then f is an isomorphism

exercise: 1) if G a group, then show

$\mathrm{Iso}(G) = \{\text{isomorphisms of } G\}$

is a group under composition

2) $\mathrm{Iso}(\mathbb{Z}) \cong \mathbb{Z}_2$

2) $f : (\mathbb{Z}, +) \to (\mathbb{Z}_p, +) : x \mapsto [x]$ equivalence class mod p

is a homomorphism since

$$f(a+b) = [a+b] = [a] + [b] = f(a) + f(b)$$

3) the only homomorphis $(\mathbb{Z}_p, +) \to (\mathbb{Z}, +)$ is the trivial map

indeed if $f([1]) = n$, then $n = f([1]) = f(\underbrace{[1] + \ldots + [1]}_{p+1 \text{ times}})$

$$= n + \ldots + n = (p+1)\,n$$

so $pn = 0 \quad \therefore n = 0$

4) by lemma III.2 it is easy to check

$$\mathrm{Mod}(S^1) \cong \mathbb{Z}_2$$

5) note S_3 and $\mathbb{Z}_6$ are not isomorphic even though they both have 6 elements (S_3 not abelian, $\mathbb{Z}_6$ is)

lemma 3:

If $f : G \to H$ a homomorphism, then

1) $f(e_G) = e_H$ (takes identity to identity)

2) $f(g^{-1}) = (f(g))^{-1}$ (takes inverses to inverses)

Proof:

1) $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$

multiply both sides by $f(e_G)^{-1}$ to get

$$e_H = f(e_G) \cdot (f(e_G))^{-1} = f(e_G) \cdot f(e_G) \cdot (f(e_G))^{-1} = f(e_G)$$ ✓

2) $f(g^{-1}) = f(g^{-1} \cdot g \cdot g^{-1}) = f(g^{-1}) \cdot f(g) \cdot f(g^{-1})$

multiply both sides by $(f(g^{-1}))^{-1}$ to get

$$e_H = f(g^{-1})(f(g^{-1}))^{-1} = f(g^{-1}) \cdot f(g) \cdot f(g^{-1}) \cdot (f(g^{-1}))^{-1} = f(g^{-1}) \cdot f(g)$$

multiply both sides by $(f(g))^{-1}$ to get

$$f(g)^{-1} = f(g^{-1})$$ ▦

lemma 4:

$$\boxed{\text{a homomorphism } f: G \to H \text{ is injective} \iff f^{-1}(e_H) = \{e_G\}}$$

Proof: $(\Rightarrow)$ if f is injective we have $f^{-1}(e_H) = \{e_G\}$ since we know $f(e_G) = e_H$

$(\Leftarrow)$ suppose $f(a) = f(b)$

then $f(a^{-1}b) = f(a)^{-1} f(b) = e_H$

so $a^{-1}b \in f^{-1}(e_H) = \{e_G\}$ $\therefore$ $a^{-1}b = e_G$

so $a = b$ and f is one-to-one ▦

let $(G, \cdot)$ be a group

a <u>subgroup</u> of G is a subset $H \subset G$ such that $a, b \in H \Rightarrow a \cdot b \in H$

and $a \in H \Rightarrow a^{-1} \in H$

we denote this by $H < G$

exercise: H is a group (with operation coming from G)

examples:

1) if G is a group and $a \in G$, then let $\langle a \rangle$ = all powers of a

exercise: $\langle a \rangle$ is a subgroup of G

$\langle a \rangle$ is called the <u>cyclic subgroup of G generated by a</u>

if $\exists\, a \in G$ s.t. $G = \langle a \rangle$ then G is called a <u>cyclic group</u>

2) $n \in \mathbb{Z}$, then $\langle n \rangle$ = all integers divisible by n

this is a subgroup of $\mathbb{Z}$

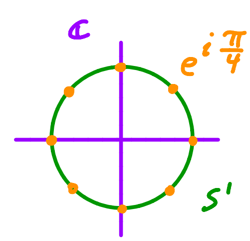
exercise: $\langle n \rangle$ is isomorphic to $\mathbb{Z} \iff n \neq 0$

3) $S^1 \subset \mathbb{C}$ the unit complex numbers

$(S^1, \cdot)$ is a group (where $\cdot$ is multiplication)

let $g = e^{i\frac{2\pi}{n}}$ some $n > 0$ an integer

$\langle g \rangle < S^1$



exercise: $\langle g \rangle$ is isomorphic to $\mathbb{Z}_n$

let $H < G$ be a subgroup

a right coset of H is

$$Hg = \{hg \mid h \in H\} \subset G$$

we say g is a representative of the coset

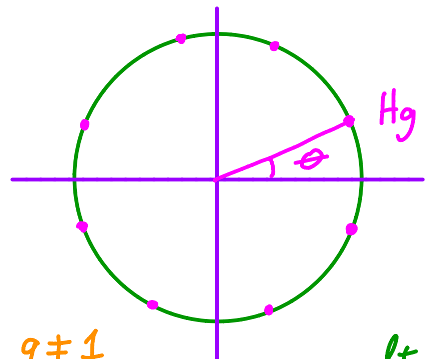
examples:

1) $H = \langle e^{\frac{2\pi i}{n}} \rangle < S^1$

let $g = e^{i\theta}$

then $Hg = \{ e^{i(\frac{2\pi}{n} + \theta)} \}$

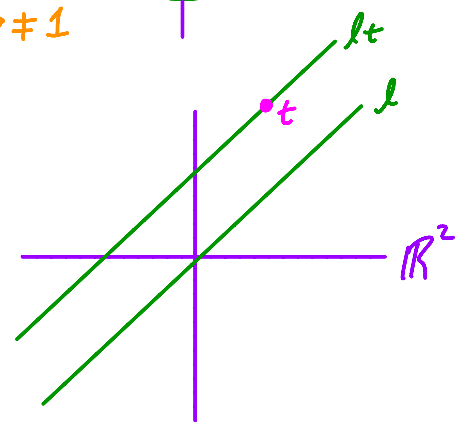
not a subgroup if $g \neq 1$



2) let ℓ be a line in $(\mathbb{R}^2, +)$

$\ell < \mathbb{R}^2$, $t \in \mathbb{R}^2$

ℓ_t = line parallel to ℓ through t



lemma 5:

If $H < G$, then

$$Ht = Hs \Leftrightarrow t \cdot s^{-1} \in H$$

Proof: $(\Rightarrow)$ if $Ht = Hs$, then $t \in Hs$

so $t = h \cdot s$ for some $h \in H$

$\therefore t \cdot s^{-1} = h \in H$ ✓

$(\Leftarrow)$ if $t \cdot s^{-1} = h \in H$ then $t = h \cdot s$

so if $x \in Ht$, then $x = h_x \cdot t$ some $h_x \in H$

$\therefore x = h_x \cdot (h \cdot s) = \underbrace{(h_x \cdot h)}_{\in H} \cdot s$

so $x \in Hs$

can similarly show $Hs < Ht$ $\blacksquare$

lemma 6:

$$\boxed{\text{If } H < G, \text{ then two right cosets are either equal or disjoint}}$$

Proof: if $x \in Ht \cap Hs$, then $h_1 \cdot t = x = h_2 \cdot s$ for $h_i \in H$

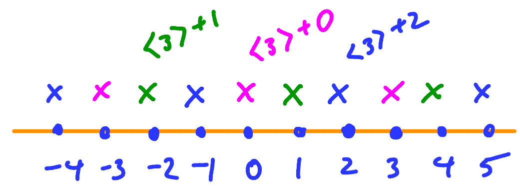
$\therefore\ t \cdot s^{-1} = h_1^{-1} \cdot h_2 \in H$ and so $Ht = Hs$ by lemma 5

lemma 6 says cosets of H decompose G into disjoint sets

If $H < G$, then the index of H in G is the number of right cosets of H in G, and is denoted $[G:H]$

examples:

1) $n \in \mathbb{Z}$, $\langle n \rangle < \mathbb{Z}$



$\langle n \rangle + 0$

$\langle n \rangle + 1$

$\vdots$

$\langle n \rangle + (n-1)$

$\langle n \rangle + n = \langle n \rangle$ so $[\mathbb{Z} : \langle n \rangle] = n$

2) $\langle e^{i \frac{2\pi}{n}} \rangle < S^1$

for $0 \le \theta < \frac{2\pi}{n}$ get disjoint cosets $\langle e^{i\frac{2\pi}{n}} \rangle e^{i\theta}$

so $[S^1 : \langle e^{i\frac{2\pi}{n}} \rangle]$ is infinite

the order of a group G is the number of elements in G

it is denoted $|G|$

lemma 7 (Lagrange):

$$\boxed{\begin{array}{c}G \text{ a finite group and } H < G, \text{ then} \\ |G| = [G:H]\,|H|\end{array}}$$

Proof: there are $[G:H]$ disjoint cosets of H each containing $|H|$ elements examples:

1) $\langle [3] \rangle < \mathbb{Z}_6$

[0]	[1]	[2]	[3]	[4]	[5]
•	•	•	•	•	•
×	×	×	×	×	×

$\langle [3] \rangle$

$\langle [3] \rangle + 1$

$\langle [3] \rangle + 2$

so $[\mathbb{Z}_6 : \langle [3] \rangle] = 3$

$|\langle [3] \rangle| = 2$

$$|\mathbb{Z}_6| = 6 = 3 \cdot 2 = [\mathbb{Z}_6 : \langle [3] \rangle] \cdot |\langle [3] \rangle|$$

2) Fun Th^{m}: if p is prime and $|G| = p$, then G is cyclic (and hence abelian)

Indeed, if G has any element $g \neq e$, then

$\langle g \rangle$ is a subgroup $\neq \{e\}$

$|\langle g \rangle|$ divides $|G|$ so is p or 1

so must be p, $\therefore G = \langle g \rangle$

If $H < G$, then a conjugate of H in G is

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

H is called a normal subgroup of G if

$$gHg^{-1} = H \quad \text{for all } g \in G$$

this is denoted $H \trianglelefteq G$

Th^{m}8:

> If $H \trianglelefteq G$, then the set of right cosets of H form a group

The group is denoted G/H and has order $[G : H]$

Proof: multiplication is just "setwise" multiplication i.e. $S, T \subset G$, then $S \cdot T = \{s \cdot t \mid s \in S, t \in T\}$

since H a subgroup

note: $(Hs)(Ht) = (Hs)((s^{-1}Hs)t) = (Hss^{-1})(Hst) = H(Hst) = Hst$

H normal   check this

so setwise multiplication of cosets is a coset!

easy to see $H = He$ is the identity element,

$H(g^{-1})$ is inverse of Hg, and multiplication is associative

example:

$\langle n \rangle < \mathbb{Z}$

note: $(-m) + \langle n \rangle + (m) = \{-m + nk + m \mid k \in \mathbb{Z}\}$

$= \{nk \mid k \in \mathbb{Z}\} = \langle n \rangle$

so $\langle n \rangle \trianglelefteq \mathbb{Z}$

from above $[\mathbb{Z} : \langle n \rangle] = n$ so $\mathbb{Z}/\langle n \rangle$ has order n

define $\phi: \mathbb{Z}/\langle n \rangle \to \mathbb{Z}_n$

$\langle n \rangle + m \mapsto [m]$

easy to check ϕ is a bijective homomorphism

so $\mathbb{Z}_n \cong \mathbb{Z}/\langle n \rangle$

if $\phi: G_1 \to G_2$ is a homeomorphism, then the kernel of ϕ is

$$\ker \phi = \phi^{-1}(e_2) = \{g \in G_1 : \phi(g) = e_2\}$$

and the image of ϕ is

$$\operatorname{im} \phi = \{\phi(g) : g \in G_1\}$$

here e_i is the identity in G_i

lemma 9:

$\boxed{\phi: G_1 \to G_2 \text{ a homomorphism, then } \ker\phi \trianglelefteq G_1 \text{ and } \operatorname{im}\phi < G_2}$

Proof: $g_1, g_2 \in \ker\phi$, then

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) = e_2 \cdot e_2 = e_2$$

so $g_1 \cdot g_2 \in \ker\phi$

$g \in \ker\phi$, then

$$\phi(g^{-1}) = (\phi(g))^{-1} = (e_2)^{-1} = e_2$$

so $g^{-1} \in \ker\phi$

$\therefore \ker\phi < G_1$

now if $g \in G_1$, we need to see

$$g(\ker\phi)g^{-1} = \ker\phi$$

if $\tilde{g} \in g(\ker\phi)g^{-1}$, then $\tilde{g} = g\bar{g}g^{-1}$ some $\bar{g} \in \ker\phi$

thus $\phi(\tilde{g}) = \phi(g\bar{g}g^{-1}) = \phi(g)\cdot\phi(\bar{g})\cdot\phi(g^{-1}) = \phi(g)\cdot e_2 \cdot (\phi(g))^{-1}$
$= \phi(g)\cdot(\phi(g))^{-1} = e_2$

$\therefore \tilde{g} \in \ker\phi$

similarly, if $\tilde{g} \in \ker\phi$, you can check $\tilde{g} \in g(\ker\phi)g^{-1}$

so $\ker\phi \trianglelefteq G_1$

exercise: show $\operatorname{im}\phi < G_2$

exercise: if $\phi: G_1 \to G_2$ is a homeomorphism, then show

$$G_1/\ker\phi \cong \operatorname{im}\phi$$

isomorphic

(this is the 1st isomorphism theorem)

given two groups A and B, the direct sum of A and B, denoted $A \oplus B$, is the set

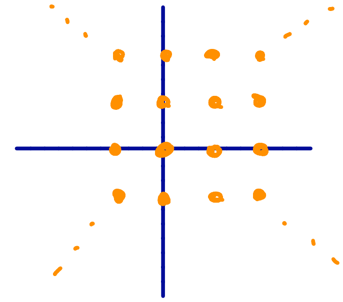
$$A \times B = \{(a,b) : a \in A \text{ and } b \in B\}$$

with multiplication defined component wise

$$(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$$

example: $\mathbb{Z} \oplus \mathbb{Z}$ ordered pairs of integers (n,m)

$$(n,m)\cdot(k,l) = (n+k, m+l)$$



Big Theorem:

any finitely generated abelian group is isomorphic to ← see below

$$\underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n} \oplus \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_2^{n_2}}$$

where p_1 are prime (not nec. distict)

n_2, n are integers

B Group Presentations

We now give a nice way to represent a group

let X be any set

the free group generated by X is the set $F(X)$ of all "reduced words" in the letters $X \cup X^{-1}$

(where X^{-1} is just a copy of X, we denote an element of X^{-1} corresponding to $x \in X$, by x^{-1})

here by reduced word we mean if you see xx^{-1} or $x^{-1}x$, remove it from the word

examples:

1) $X = \{x\}$ then the words are

x			and x^{-1}		
xx	denote	x^2	$x^{-1}x^{-1}$	denote	x^{-2}
xxx		x^3	$x^{-1}x^{-1}x^{-1}$		x^{-3}
$\vdots$		$\vdots$	$\vdots$		$\vdots$

also have the empty word which we denote $e = x^0$

note: we also have xxx^{-1} but not reduced but we can "reduce" it to x

2) $X = \{a, c, d, t, o\}$ so words are like: cat dog $ccta^{-1}o^{-1}\dots$

define multiplication on $F(X)$ by concatenation followed by reduction

examples:

1) $X = \{x\}$

$$x^2 \cdot x^5 = x^7$$

$$x^{-2} \cdot x^5 = x^{-1}x^{-1}xxxxx = xxx = x^3$$

2) $X = \{a, b\}$ then

$$(a^2ba^{-1}b)\cdot(b^{-1}a^3) = a^2ba^2$$

exercise:

1) $F(X)$ with multiplication above is a group

2) note we have a map $i : X \to F(X)$, $x \mapsto x$

Show that given any function $f : X \to G$, where G is some group, there is a unique homomorphism $\tilde{f} : F(X) \to G$ satisfying

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "i"'] & G \\ F(X) \arrow[ur, "\tilde{f}"'] & \end{tikzcd} \qquad \tilde{f} \circ i = f$$

3) if there is a bijection $j : X \to Y$ then $F(X)$ and $F(Y)$ are isomorphic

4) $|X| = 1$, then $F(X) \cong \mathbb{Z}$ (abelian)

but if $|X| > 1$, then $F(X)$ is non-abelian

Hint: map $F(X)$ onto something non-abelian

given a collection R of words in $X \cup X^{-1}$, let $\langle R \rangle$ be the smallest normal subgroup of $F(X)$ containing R

then denote by $\langle X \mid R \rangle$ the group $F(X)/\langle R \rangle$

this is called a group presentation

if G some group and $G \cong \langle X | R \rangle$ then we say $\langle X | R \rangle$ is a presentation of G

if X is finite, say $\{g_1, \ldots g_n\}$, and R is finite, say $\{r_1, \ldots r_m\}$, then we usually write $\langle g_1, \ldots, g_n | r_1, \ldots r_m \rangle$

if G has a presentation where X is finite we say G is <u>finitely generated</u>

if X and R are finite, then we say G is <u>finitely presented</u>

<u>Intuitively</u>: $\langle g_1, \ldots, g_n | r_1, \ldots, r_m \rangle$ is the group of all words in g_1 and g_1^{-1} where if you ever see an r_i you can remove it (you can also insert it anywhere)

<u>examples</u>:

1) $\langle g | g^n \rangle$ this is all words in g, g^{-1}, i.e.

should be writting cosets of $\langle g^n \rangle$, but we just interpret words as their cosets.

$$\ldots, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots, g^{n-1}, g^n, \ldots$$

but $g^n = e$ so $g^{n+1} = g^n \cdot g = g$

$$g^{-1} = g^n g^{-1} = g^{n-1}$$

easy to see every element is of the form g^k, $0 \le k < n$

<u>exercise</u>: $\langle g | g^n \rangle \longrightarrow \mathbb{Z}_n$ is an isomorphism

$$g^k \longmapsto [k]$$

2) a presentation of $\mathbb{Z}$ is $\langle g | \varnothing \rangle$

3) check a presentation of D_n is

$$\langle x, y \,|\, x^n, y^2, xyxy \rangle$$

4) consider $\langle x, y \,|\, xyx^{-1}y^{-1} \rangle$

this is called a <u>commutator</u> of x and y, it is usually denoted $[x, y]$

note, the relation says $xyx^{-1}y^{-1} = e$

i.e. $xy = yx$ (x and y commute)

so any word in the above group can be written $x^n y^m$ for some $n, m \in \mathbb{Z}$

exercise: Show $\mathbb{Z} \oplus \mathbb{Z} \cong \langle x, y \mid xyx^{-1}y^{-1} \rangle$

exercises:

1) Every group G has a presentation

   Hint: let $X = G$

2) let $G = \langle g_1, \dots, g_n \mid r_1, \dots, r_m \rangle$, and H any group

   choose elements $h_1, \dots, h_n \in H$

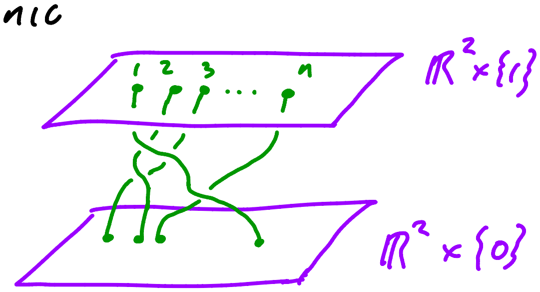
   There is a unique well-defined homomorphism
   $$\phi : G \to H$$
   sending g_i to h_i if "relations respected"

   (i.e. if $r_i = g_{j_1}^{\varepsilon_1} \cdots g_{j_k}^{\varepsilon_k}$, then $h_{j_1}^{\varepsilon_1} \cdots h_{j_k}^{\varepsilon_k} = e_H$)

very important way to construct homomorphisms!

C. Braid groups and the Jones polynomia

a n-string braid is a disjoint union of arcs in $\mathbb{R}^2 \times [0,1]$ with end points
$$\{(0,i,0)\} \subset \mathbb{R}^2 \times \{0\}$$
$$\{(0,i,1)\} \subset \mathbb{R}^2 \times \{1\}$$
such that the restriction of the projection $\mathbb{R}^2 \times [0,1] \to [0,1]$ to each arc is monotonic

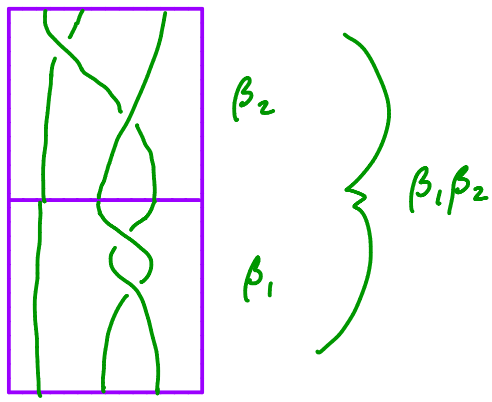


two braids β_0, β_1 are equivalent if $\exists$ 1-parameter family of braids β_t, $0 \le t \le 1$, going from β_0 to β_1

we write $\beta_0 = \beta_1$ if equivalent

Remark: It is a (non-obvious) fact that $\beta_0 = \beta_1 \Leftrightarrow \beta_0$ and β_1 are isotopic in $\mathbb{R}^2 \times [0,1]$, keeping end points fixed

the product of 2 n-strand braids is just concatenation



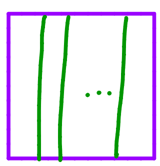
(reparam $[0,2]$ to $[0,1]$)

the n-strand braid group

lemma 10:

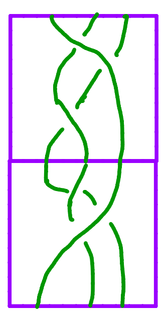
$\boxed{\text{The set } B_n \text{ of n-strand braids is a group with this product}}$

Proof: Identity: is

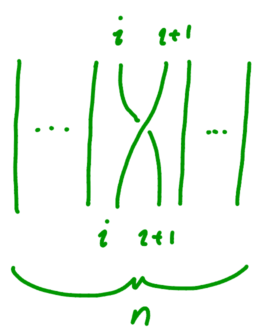


associativity: clear

inverses: β^{-1} = reflection of β in $\mathbb{R}^2 \times \{1\}$

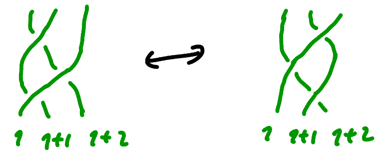


let σ_i in B_n, $1 \leq i \leq n-1$, be the braid



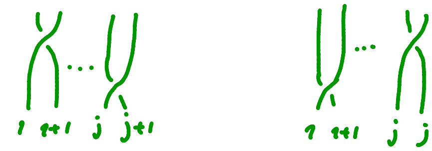
notice that

1) $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$



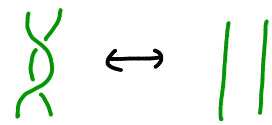
"Reidemeister 3"

2) $\sigma_i \sigma_j = \sigma_j \sigma_i$ if $|i-j|>1$



<u>note</u>: Reidemeister 2 corresponds to group relation

$$\sigma_i \sigma_i^{-1} = e$$

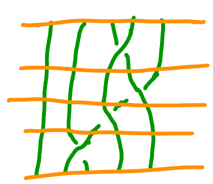


<u>Th$^{\underline{m}}$ 11</u>:

B_n has presentation

$$P = \langle \sigma_1, \ldots \sigma_{i-1} \mid \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1},\ 1 \le i \le n-2,\ \sigma_i \sigma_j = \sigma_j \sigma_i,\ |i-j|>1 \rangle$$

<u>Proof</u>: given any braid β, can isotop so crossings occure at different levels



σ_3
σ_4^{-1}
σ_3^{-1}
σ_2

so β is a product of $\sigma_1, \ldots, \sigma_{n-1}$

$\therefore \sigma_1, \ldots, \sigma_n$ generate B_n

from what we know about group presentations, since we have relations above, we have a homomorphism

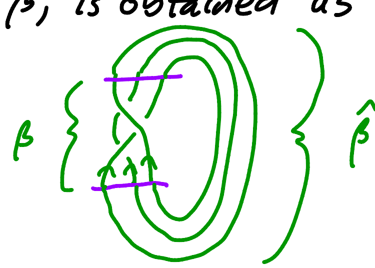
$$P \to B_n$$

and we just saw its surjective

injective is a braid version of Reidemeister's Th$^{\underline{m}}$ (won't do here)

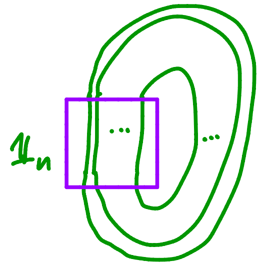
given a braid β orient strands from $\mathbb{R}^2 \times \{0\}$ to $\mathbb{R}^2 \times \{1\}$

the <u>closure</u> of β, denoted $\hat{\beta}$, is obtained as shown



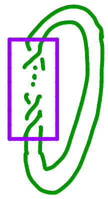
examples:

1) $\mathbb{1}_n \in B_n$



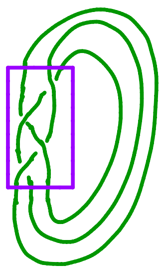
so $\hat{\mathbb{1}}_n = O_n$ ← n component unlink

2) in B_2



$\hat{\sigma}_1^n = (2,n)$ torus link

3) in B_3



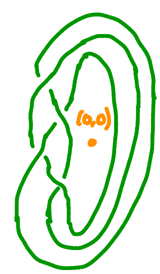
$\widehat{(\sigma_1 \sigma_2^{-1} \sigma_1 \sigma_2^{-1})}$ = figure 8 knot

Th$^{\text{m}}$ 12 (Alexander 1923):

$\boxed{\text{every oriented link is the closure of a braid}}$

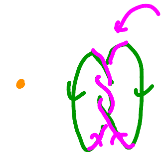
Sketch of proof:

note we can translate $\hat{\beta}$ so it is winding about (0.0) and if K has a diagram such that θ component (in polar coords) always decreasing, then you can isotop all crossings to left hand side and see K as a closed braid

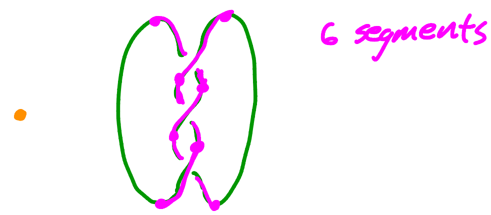


so how can you arrange θ coord condition?

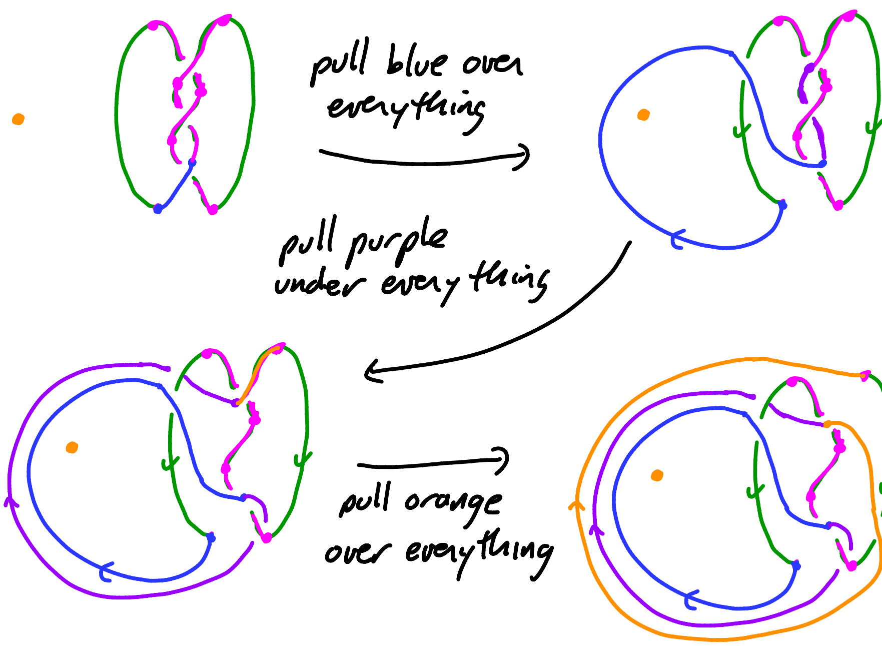
1$^{\text{st}}$ mark strands going "wrong way"



2nd break strands up so they only go over or under other strands



3rd fix strands one by one

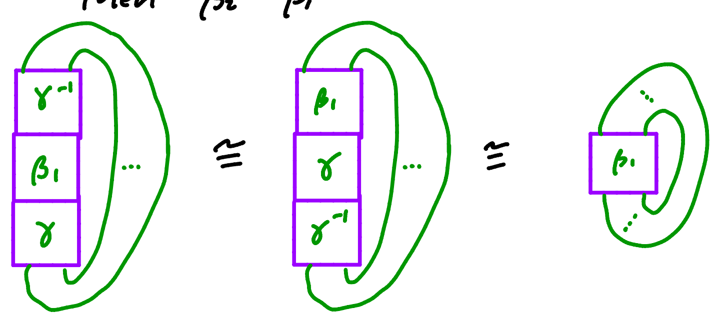


continue till done

So when is $\hat{\beta}_1 = \hat{\beta}_2$?

1) <u>conjugation</u>: if $\beta_1, \beta_2 \in B_n$ and $\exists\, \gamma \in B_n$ s.t. $\beta_2 = \gamma \beta_1 \gamma^{-1}$

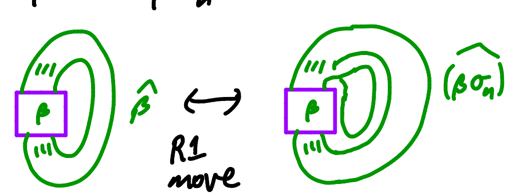
then $\hat{\beta}_2 = \hat{\beta}_1$



2) <u>stabilization</u>: we have a map $s^{\pm} : B_n \to B_{n+1}$

$\beta \longmapsto \beta \sigma_n^{\pm 1}$

clearly $\widehat{(\beta \sigma_n^{\pm 1})} = \hat{\beta}$



the equivalence relation on the set $\coprod_{n=1}^{\infty} B_n$ generated by

1) conjugation in B_n and
2) stabilization

is called Markov equivalence and denoted $\overset{m}{\sim}$

Th^m 13 (Markov 1936)

$$\boxed{\hat{\beta}_1 = \hat{\beta}_2 \Leftrightarrow \beta_1 \overset{m}{\sim} \beta_2}$$

from above we have proven ($\Leftarrow$), the other implication is another Reidemeister type th^m (wont do here)

Remark: We have now turned studying knots into studying group (and an equivalence relation)!

so to get an invariant of links we can look for a Markov trace.

a Markov trace $\mu = \{\mu_n\}$ is a set of functions

$$\mu_n : B_n \to R$$

(where R is some algebraic thing, like a group)

such that

1) $\mu_n(\alpha\beta) = \mu_n(\beta\alpha)$ $\quad (\Leftrightarrow \mu(\gamma\beta\gamma^{-1}) = \mu(\beta))$

2) $\exists$ element $a \in R$ such that

$$\mu_{n+1}(\beta\sigma_n^{\pm 1}) = a^{\pm 1}\mu_n(\beta) \quad \forall \beta \in B_n$$

define the writhe of a braid by

$$\omega : B_n \to \mathbb{Z}$$

by $\omega(\sigma_i) = 1$ and $\omega(\sigma_i^{-1}) = -1$ and extend to a word by adding, i.e. $\omega(\beta) =$ "exponent sum"

e.g. $\omega(\sigma_1\sigma_2\sigma_1^{-1}) = 1$

exercise: 1) this is well-defined

2) if D is a diagram for $\hat{\beta}$ then $\omega(\beta) = \omega(D)$ ← writhe of diagram we defined earlier

$\underline{Th^{m}\ 14:}$

> If $\mu = \{\mu_n\}$ is a Markov trace, then for a link L with $L = \hat{\beta}$ for some braid $\beta \in B_n$ the formula
> $$I_\mu(L) = a^{-\omega(\beta)} \mu_n(\beta)$$
> is a well-defined invariant of oriented links

Proof:

by Th^{m} 12, any L is $\hat{\beta}$ for some $\hat{\beta}$

if $L = \hat{\beta}_1$ and $\hat{\beta}_2$ then by Th^{m} 13 $\beta_1 \overset{M}{\sim} \beta_2$

so they are related by conjugation and stabilization

<u>conjugation:</u> $\mu_n(\gamma\beta\gamma^{-1}) = \mu_n(\beta)$ (by 1)) and $\omega(\gamma\beta\gamma^{-1}) = \omega(\beta)$

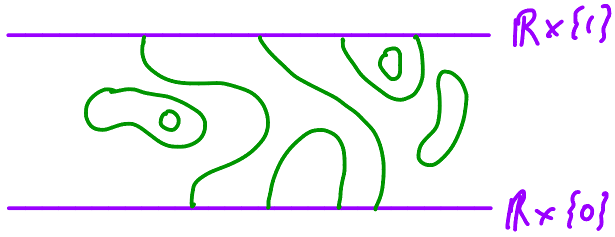
$$\therefore\ a^{-\omega(\gamma\beta\gamma^{-1})}\mu_n(\gamma\beta\gamma^{-1}) = a^{-\omega(\beta)}\mu_n(\beta)$$

<u>stabilization:</u>
$$\left.\begin{array}{l} \mu_{n+1}(\beta\sigma_n^{\pm 1}) = a^{\pm 1}\omega_n(\beta) \\ \omega(\beta\sigma_n^{\pm 1}) = \omega(\beta) \pm 1 \end{array}\right\} \Rightarrow \alpha^{-\omega(\beta\sigma_n^{\pm 1})}\mu_{n+1}(\beta\sigma_n^{\pm 1}) = \alpha^{-\omega(\beta)}\mu_n(\beta)$$

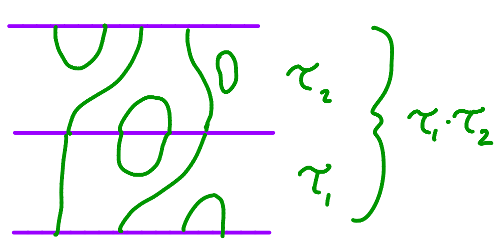
∎

Let's find a Markov trace

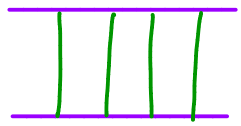
A <u>planar n-tangle</u> is a disjoint union of n arcs and some simple closed curves in $\mathbb{R}\times[0,1]$ with n arc end points in $\{(i,0)\}_{i=1}^{n}$ and n " " in $\{(i,1)\}_{i=1}^{n}$ upto isotopy (fixing $\mathbb{R}\times\{0,1\}$)



$\exists$ a product defined by concatenation

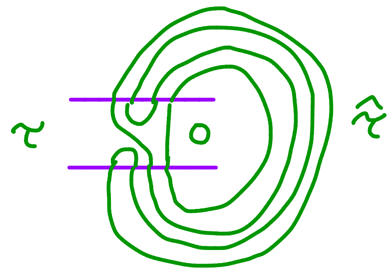


there is an identity



the set PT_n of planar n-tangles is a monoid (i.e. "group without inverses")

for $\tau \in PT_n$ we can form the closure $\hat{\tau} = \amalg$ close curves in $\mathbb{R}^2$



The Temperley-Lieb algebra TL_n is the set of formal sums

$$\sum_{i=1}^{k} p_i \tau_i$$

where $p_i \in \mathbb{Z}[A, A^{-1}]$, A a formal variable

and $\tau_i \in PL_n$

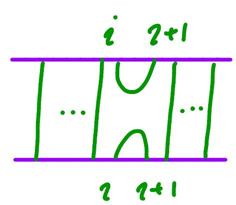
but identify anything of the form

$$\tau \amalg \bigcirc \quad \text{with} \quad (-A^2 - A^{-2})\tau$$

close circle

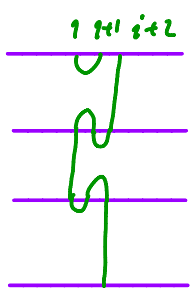
note: we can add and multiply elements of TL_n

in PT_n define elements h_i "hooks"



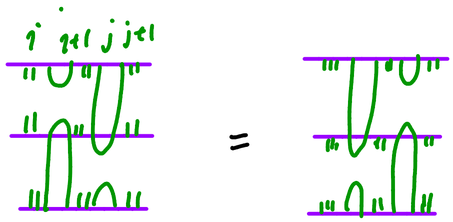
$1 \leq i \leq n-1$

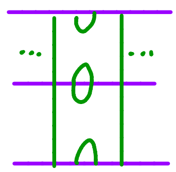
note: 1)



$h_i h_{i+1} h_i = h_i$

(and $h_i h_{i-1} h_i = h_i$)

2)  $h_i h_j = h_j h_i$ if $|i-j|>1$

3)  $h_i^2 = (-A^2 - A^{-2})\, h_i$

Th$^{\underline{m}}$ 15: TL_n is formal sums $\sum p_k w_k$, where $p_k \in \mathbb{Z}[A, A^{-1}]$ and w_k are words in the h_i, subject to the relations 1), 2), 3) above

Motivation: recall Kauffman bracket
$\langle \times \rangle = A \langle)(\rangle + A^{-1} \langle \asymp \rangle$

exercise: Try to prove this!

let $\rho : B_n \to TL_n$ be defined by

$$\rho(\sigma_i) = A + A^{-1} h_i$$
$$\rho(\sigma_i^{-1}) = A^{-1} + A h_i$$

and extend multiplicitively

to see ρ is well-defined we need to see

1) $\rho(\sigma_i)\rho(\sigma_i^{-1}) = 1$

2) $\rho(\sigma_i)\rho(\sigma_j) = \rho(\sigma_j)\rho(\sigma_i) \quad |i-j|>1$

3) $\rho(\sigma_i)\rho(\sigma_{i+1})\rho(\sigma_i) = \rho(\sigma_{i+1})\rho(\sigma_i)\rho(\sigma_{i+1})$

for 1) we have $\rho(\sigma_i)\rho(\sigma_i^{-1}) = (A + A^{-1}h_i)(A^{-1} + A h_i) = 1 + (A^2 + A^{-2}) h_i + h_i^2$
$= 1 + (A^2 + A^{-2}) h_i + (-A^2 - A^{-2}) h_i = 1$

for 2) we have $\rho(\sigma_i)\rho(\sigma_j) = (A + A^{-1}h_i)(A + A^{-1}h_j)$
$= A^2 + h_i + h_j + A^{-2} h_i h_j$
$= A^2 + h_j + h_i + A^{-2} h_j h_i = (A + A^{-1}h_j)(A + A^{-1}h_i)$
$= \rho(\sigma_j)\rho(\sigma_i)$

for 3) we have

$$\rho(\sigma_i)\rho(\sigma_{i+1})\rho(\sigma_i) = (A + A^{-1}h_i)(A + A^{-1}h_{i+1})(A + A^{-1}h_i)$$
$$= (A^2 + h_i + h_{i+1} + A^{-2}h_i h_{i+1})(A + A^{-1}h_i)$$
$$= A^3 + \cancel{A h_i} + A h_{i+1} + A^{-1}h_i h_{i+1} + A h_i + \underbrace{A^{-1}h_i^2}_{A^{-1}(-A^2 - A^{-2})h_i \,=\, (-\cancel{A} - \cancel{A^{-3}})h_i} + A^{-1}h_{i+1}h_i + \cancel{A^{-3}\underbrace{h_i h_{i+1} h_i}_{h_i}}$$
$$= A^3 + A^{-1}(h_i h_{i+1} + h_{i+1}h_i) + A(h_{i+1} + h_i)$$

this is symmetric in i and $i+1$

so $= \rho(\sigma_{i+1})\rho(\sigma_i)\rho(\sigma_{i+1})$ (if not clear to you then work it out)

now define $tr_n : TL_n \to \mathbb{Z}[A, A^{-1}]$

by $tr_n(\tau) = (-A^2 - A^{-2})^{|\hat{\tau}|-1}$ for $\tau \in PL_n$

and extend linearly

finally define $\mu_n : B_n \to \mathbb{Z}[A, A^{-1}]$ by $\mu_n = tr_n \circ \rho$

Thm 16:

$\mu = \{\mu_n\}$ is a Markov trace and the corresponding invariant of oriented links is

$$I_\mu(L) = F_L(A)$$

in particular, get the Jones polynomial with $t = A^{-4}$

Remark: Jones' original definition of $V_L(t)$ used a Markov trace (essentially) as above.

Proof:

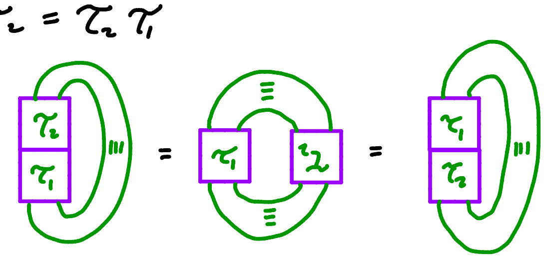
Check: $\mu_n(\alpha\beta) = \mu_n(\beta\alpha)$

note: $\tau_1, \tau_2 \in PL_n$, then $\widehat{\tau_1\tau_2} = \widehat{\tau_2\tau_1}$

$\therefore\ tr_n(\tau_1\tau_2) = tr_n(\tau_2\tau_1)$

$\therefore\ tr_n(ab) = tr_n(ba)\ \ \forall a, b \in TL_n$

$\therefore\ \mu_n(\alpha\beta) = \mu_n(\beta\alpha)\ \ \forall \alpha, \beta \in B_n$

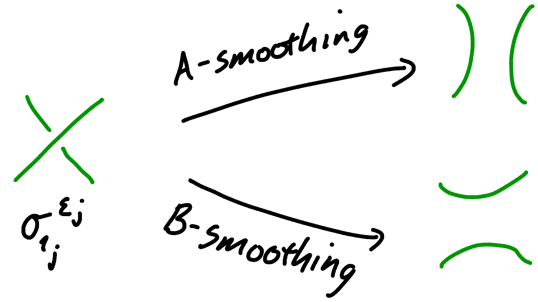


Check: with $a = -A^3$ we have $\mu_{n+1}(\beta\sigma_n^{\pm}) = a^{\pm 1}\mu_n(\beta)$

let $\beta \in B_n$, so $\beta = \prod_{j=1}^{k} \sigma_{i_j}^{\varepsilon_j}$ $\quad \varepsilon_j = \pm 1$

and $\rho(\beta) = \prod_{j=1}^{k} (A^{\varepsilon_j}\cdot 1 + A^{-\varepsilon_j}\cdot h_{i_j})$ when you multiply each term corresp. to a state

recall a state s of β is a choice of A or B-splitting for each σ_{i_j}



set $s_A = \{ j$ s.t. s has an A splitting at $\sigma_{i_j}^{\varepsilon_j}\}$

$s_B = \{ j$ " " B " " $\}$

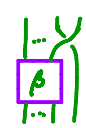
exercise: $\rho(\beta) = \sum_{\text{all states } s} \beta_s \tau_s$ where $\beta_s = A^{\left(\sum_{j\in s_A}\varepsilon_j - \sum_{j \in s_B}\varepsilon_j\right)}$

and $\tau_s \in PL_n$ is $\prod_{j=1}^{k} g_{i_j}$

where $g_{i_j} = \begin{cases} 1 & \text{if } j \in s_A \\ h_{i_j} & \text{if } j \in s_B \end{cases}$

$\therefore \mu_n(\beta) = tr_n(\rho(\beta)) = \sum_s \beta_s d^{|\hat{\tau}_s| - 1}$ $\quad (*)$

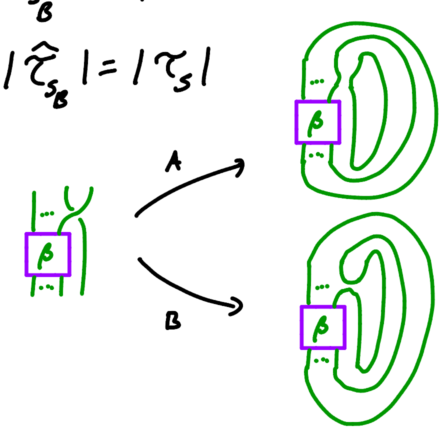
now for $\beta\sigma_n^{\pm 1}$:



for each state s of β we get 2 states s^A, s^B for $\beta\sigma_n^{\pm 1}$ according to splitting at σ_n

note: $(\beta\sigma_n)_{s_A} = A\beta_s$ and $(\beta\sigma_n)_{s_B} = A^{-1}\beta_s$

$|\hat{\tau}_{s_A}| = |\hat{\tau}_s| + 1$ and $|\hat{\tau}_{s_B}| = |\tau_s|$



$$\therefore\ \mu_{n+1}(\beta\sigma_n) = tr_{n+1}(\rho(\beta\sigma_n)) = tr_n\Big(\sum_{\substack{\text{states}\\ s \text{ of } \beta}} (A\beta_s \tau_{s_A} + A^{-1}\beta_s \tau_{s_B})\Big)$$

$$= \sum_s \left(A\beta_s(-A^2-A^{-2})^{|\hat{\tau}_s|+1} + A^{-1}\beta_s(-A^2-A^{-2})^{|\hat{\tau}_s|}\right)$$

$$= (A(-A^2-A^{-2}) + A^{-1})\,\mu_n(\sigma_n)$$

$$= -A^3\mu_n(\sigma_n)$$

similarly $\mu_{n+1}(\beta\sigma_n^{-1}) = -A^{-3}\mu_n(\sigma_n)$ ✓

<u>Check</u>: $I_\mu(L) = F_L(A)$

If $L = \hat{\beta}$ and D is the diagram for L coming from β then one can check that ⊛ shows

$$\mu(\beta) = \langle D \rangle$$ ← Kauffman bracket of D

we also saw $\omega(\beta) = \omega(D)$

so $I_\mu(L) = -A^{-3\omega(D)}\langle D\rangle \underset{\text{by defn}}{=} F_L(A)$ ∎