

# What is a Braid Group?

Daniel Glasscock, June 2012

*These notes complement a talk given for the What is ... ? seminar at the Ohio State University.*

## Intro

---

The topic of braid groups fits nicely into this seminar. On the one hand, braids lend themselves immediately to nice and interesting pictures about which we can ask (and sometimes answer without too much difficulty) interesting questions. On the other hand, braids connect to some deep and technical math; indeed, just *defining* the geometric braid groups rigorously requires a good deal of topology.

I hope to convey in this talk a feeling of how braid groups work and why they are important. It is not my intention to give lots of rigorous definitions and proofs, but instead to draw lots of pictures, raise some interesting questions, and give some references in case you want to learn more.

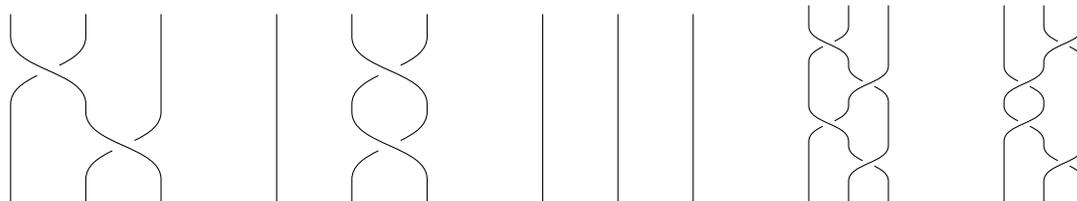
## Braids

---

A *braid\** on  $n$  strings is an object consisting of  $2n$  points ( $n$  above and  $n$  below) and  $n$  strings such that

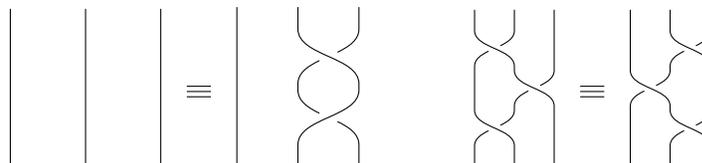
- i.* the beginning/ending points of the strings are (all of) the upper/lower points,
- ii.* the strings do not intersect,
- iii.* no string intersects any horizontal line more than once.

The following are braids on 3 strings:



We think of braids as lying in 3 dimensions; condition *iii.* is then that no string in the projection of the braid onto the page (as we have drawn them) intersects any horizontal line more than once.

Two braids on the same number of strings are *equivalent* ( $\equiv$ ) if the strings of one can be continuously deformed – in the space strictly between the upper and lower points and without crossing – into the strings of the other.



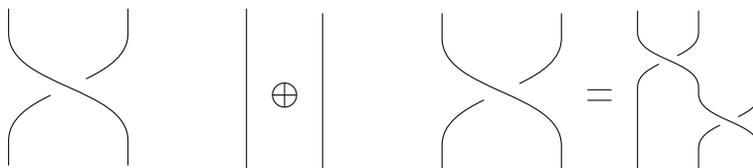
Denote by  $B_n$  be the set of all braids (up to equivalence) on  $n$  strings.

\*These are actually *braid diagrams*. See the definitions at the end of this note for the textbook definition of a geometric braid.

## Braid groups

---

Two braids in  $B_n$  can be “added” ( $\oplus$ ) to yield a new braid by joining the bottom points of the first braid to the top points of the second.



It is now a little exercise to check that  $(B_n, \oplus)$  forms a group. You may want to pause to check the existence of inverses.

Let's consider the first couple braid groups:

**$B_1$**  This group consists of all braids on 1 string. It is the trivial group.

**$B_2$**  The elements in this group are twists of two strings. By giving a twist in one direction the value  $+1$  and a twist in the other direction the value  $-1$ , it follows that  $B_2$  is isomorphic to the group of integers under addition.

**$B_3$**  This group is infinite and non-abelian (check that adding the two braids above in the opposite order yields a different braid). By keeping one string fixed, we see that  $B_3$  contains several copies of  $B_2$ .

To get a better idea about  $B_3$ , we might ask:

1. How does  $B_3$  relate to some groups we already know?
2. Are there braids with finite order? (Is  $B_3$  torsion free?)
3. Are there braids that commute with all other braids? (Does  $B_3$  have trivial center?)
4. Does  $B_3$  arise or act naturally? (What are the representations of  $B_3$ ?)
5. Is  $B_3$  even linear (a subgroup of  $GL_m(\mathbb{C})$  for some  $m$ )?
6. What about homology/cohomology of  $B_3$ ?

Despite the seemingly innocent nature of these questions, most of them are hard to answer, especially in the general case of  $B_n$ . The reader is encouraged to spend a few minutes pondering questions 2 and 3 especially. What does your intuition tell you?

1. To each braid in  $B_3$  we may associate a permutation of  $\{1, 2, 3\}$  by labeling the upper and lower points with 1, 2, 3 and following the strings. For example, the very first braid drawn in these notes corresponds to the permutation  $1 \mapsto 3$ ,  $2 \mapsto 1$ , and  $3 \mapsto 2$ . It is in this way that the braid groups generalize the symmetric groups!

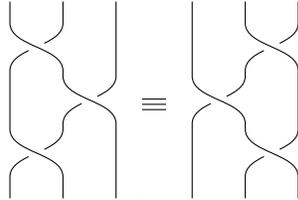
Let  $\varphi : B_3 \rightarrow S_3$  send a braid to its associated permutation. It is an exercise to check that  $\varphi$  is a surjective group (anti-)homomorphism. Thus  $S_3 \cong B_3 / \ker \varphi$ . We recognize  $\ker \varphi$  as the subgroup of braids corresponding to the trivial permutation; these are called the *pure braids*.

2. Your gut may have told you that there are no braids which may be composed with themselves finitely many times to yield the trivial braid. That intuition is correct, but proving such a result is not so

straightforward.

Just as  $S_3$  is generated by the transpositions (12), (23), we see that  $B_3$  is generated by a crossing of strings 1 and 2 and a crossing of strings 2 and 3. More specifically, if  $\sigma_1$  is  and  $\sigma_2$  is , then  $B_3 = \langle \sigma_1, \sigma_2 \rangle$ .

To ask what relations there are between  $\sigma_1$  and  $\sigma_2$  is to ask about the kernel of the homomorphism  $\psi : F_2 \rightarrow B_3$  where  $F_2 = \langle a, b \rangle$  is the free group on two generators and  $\psi(a) = \sigma_1$ ,  $\psi(b) = \sigma_2$ .

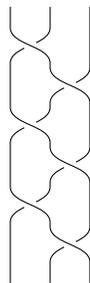


Emil Artin proved in 1925 that  $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$  (shown above) is the fundamental relationship between  $\sigma_1$  and  $\sigma_2$ . In other words,  $B_3 \cong \langle a, b \mid aba = bab \rangle$ .

One can deduce from the presentation  $\langle a, b \mid aba(bab)^{-1} \rangle$  that  $B_3$  has no non-trivial elements of finite order, answering question 2. (See propositions 5.17 and 5.18 in *Combinatorial Group Theory* by R.C. Lyndon and P.E. Schupp.)

The general presentation of  $B_n$  is only slightly more complicated. If  $\sigma_i$  represents the (left over right) crossing of strings  $i$  and  $i+1$ , then  $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$  generate  $B_n$ . Notice that  $\sigma_1$  and  $\sigma_3$  commute; indeed, they involve a disjoint set of strings. One may guess, then, that  $B_n \cong \langle a_1, a_2, \dots, a_{n-1} \mid a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1} \forall 1 \leq i \leq n-2, a_j a_k = a_k a_j \forall |j-k| \geq 2 \rangle$ .

3. Are there any braids which commute with all other braids? The braid  $(\sigma_1\sigma_2)^3$ , drawn below, is one such braid. It can be thought of as a full twist of the strings. The reader is strongly encouraged to give a simple (non-algebraic) reason why this braid commutes with all others.



We may prove that this braid generates the center by utilizing a surprising connection between  $B_3$  and  $PSL_2(\mathbb{Z})$ . We will use two facts without proof:  $PSL_2(\mathbb{Z}) \cong \langle v, w \mid v^2, w^3 \rangle$ , and the center of  $PSL_2(\mathbb{Z})$  is trivial.

The map  $\rho : B_3 \rightarrow PSL_2(\mathbb{Z})$  induced by  $\rho(\sigma_1) = w^{-1}v$  and  $\rho(\sigma_2) = v^{-1}w^2$  is a well defined homomorphism (check that  $\sigma_1\sigma_2\sigma_1(\sigma_2\sigma_1\sigma_2)^{-1}$  maps to the identity). It is an exercise to see that  $\ker \rho = \langle (\sigma_1\sigma_2)^3 \rangle$ . Since  $Z(PSL_2(\mathbb{Z}))$  is trivial and  $PSL_2(\mathbb{Z}) \cong B_3 / \ker \rho$ ,  $Z(B_3) \subseteq \ker \rho$ . Since  $\langle (\sigma_1\sigma_2)^3 \rangle \subseteq Z(B_3)$ , we see that  $Z(B_3) = \langle (\sigma_1\sigma_2)^3 \rangle$ .

In general,  $Z(B_n) = \langle (\sigma_1\sigma_2 \cdots \sigma_{n-1})^n \rangle$  is infinite cycle, generated by the full twist.

## Definitions

---

**Group** A *group* is a non-empty set  $G$  with a binary operation  $\oplus : G \times G \rightarrow G$  satisfying the following three properties:

- i. (*associativity*) for all  $g, h, f \in G$ ,  $(g \oplus h) \oplus f = g \oplus (h \oplus f)$ ,
- ii. (*identity*) there exists  $e \in G$  such that for all  $g \in G$ ,  $g \oplus e = e \oplus g = g$ ,
- iii. (*inverses*) for all  $g \in G$ , there exists  $h \in G$  such that  $g \oplus h = h \oplus g = e$ .

**Order** An element  $g \in G$  has *finite order* if there exists  $n \in \{1, 2, \dots\}$  such that  $\underbrace{g \oplus g \oplus \dots \oplus g}_n = e$ .

**Torsion** A group is *torsion free* if the only element with finite order is the identity.

**Center** The *center* of a group  $G$ , denoted  $Z(G)$ , is the set of all elements  $c \in G$  such that for all  $g \in G$ ,  $c \oplus g = g \oplus c$ .

**Braid** Let  $I = [0, 1]$ . A *geometric braid on  $n$  strings* is a set  $B \subseteq \mathbb{R}^2 \times I$  formed by  $n$  disjoint sets, each of which is homeomorphic to  $I$ , such that the projection  $\mathbb{R}^2 \times I \rightarrow I$  maps each set homeomorphically onto  $I$  and  $B \cap (\mathbb{R}^2 \times \{0\}) = \{(1, 0, 0), (2, 0, 0), \dots, (n, 0, 0)\}$ ,  $B \cap (\mathbb{R}^2 \times \{1\}) = \{(1, 0, 1), (2, 0, 1), \dots, (n, 0, 1)\}$ .

$B_n$  The *geometric braid group on  $n$  strings* is the group of braids on  $n$  strings under composition.

$S_n$  The *symmetric group on  $n$  letters* is the group of permutations of  $n$  distinct letters under composition. This may be realized concretely as the group of permutations of  $\{1, 2, \dots, n\}$ .

$GL_n(\mathbb{C})$  The *general linear group of degree  $n$  over  $\mathbb{C}$*  is the group of all invertible  $n \times n$  complex matrices under multiplication.

$PSL_2(\mathbb{Z})$  The *special linear group of degree 2 over  $\mathbb{Z}$* , denoted  $SL_2(\mathbb{Z})$ , is the group of all  $2 \times 2$  integer matrices with determinant 1 under multiplication. The *projective special linear group of degree 2 over  $\mathbb{Z}$*  is the factor group  $SL_2(\mathbb{Z})/\{\pm I\}$  where  $I$  is the  $2 \times 2$  identity matrix.

## References

---

The father of the modern braid group(s) is Emil Artin. See any of the references below for references to his original works. Consult [4–6] as general references. Braids surface in knot theory [2], physics [1], and cryptography [3].

- [1] John Baez. Braids, May 1992. <http://math.ucr.edu/home/baez/braids.html>.
- [2] J. S. Birman and T. E. Brendle. Braids: A Survey. *ArXiv Mathematics e-prints*, September 2004.
- [3] David Garber. Braid group cryptography. In *Braids*, volume 19 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, pages 329–403. World Sci. Publ., Hackensack, NJ, 2010.
- [4] Juan González-Meneses. Basic results on braid groups. *Ann. Math. Blaise Pascal*, 18(1):15–59, 2011.
- [5] Christian Kassel and Vladimir Turaev. *Braid groups*, volume 247 of *Graduate Texts in Mathematics*. Springer, New York, 2008.
- [6] Dale Rolfsen. Tutorial on the braid groups. In *Braids*, volume 19 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, pages 1–30. World Sci. Publ., Hackensack, NJ, 2010.