RECENT DEVELOPMENTS ON ARTIN'S BRAID GROUPS

by

Christian Kassel

Institut de Recherche
Mathématique Avancée
Université Louis Pasteur - CNRS
Strasbourg, France

Definition. *The braid group B_n is the group generated by generators $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ and the relations*

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{if } |i-j| > 1,$$
$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \quad \text{if } |i-j| = 1.$$

The braid group first appeared in work by Hurwitz (1896) on ramified coverings of the projective line.

It was formally introduced by Emil Artin around 1926.

The braid groups appear in many fields: algebra, topology, group theory, algebraic geometry, and recently in cryptography.

Other definitions:

- group of geometric braids
- mapping class group of a disk with n punctures
- fundamental group of the configuration space of n points in the plane

Recent progress on braid groups:

• P. Dehornoy (Caen) in 1991–92: B_n *has an invariant linear ordering*

This originates from an unexpected connection between braid groups and modern set theory (theory of large cardinals) *via* sets with a self-distributive law.

• D. Krammer (Basel), S. Bigelow (Berkeley) in 2000: B_n *has a finite-dimensional faithful linear representation*

Linearity of B_n:

Burau (1935) : $B_n \to GL_n(\mathbf{Z}[t, t^{-1}])$

$$\sigma_i \mapsto \begin{pmatrix} 1 & \dots & & & \dots & \dots & 0 \\ \vdots & \ddots & & & & & \vdots \\ & & 1-t & t & & & \\ & & 1 & 0 & & & \\ \vdots & & & & 1 & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ 0 & \dots & & & & & 1 \end{pmatrix}$$

- $n = 2, 3$: faithful
- $n = 4$: open question
- $n = 5$: not faithful (Bigelow, 1999)
- $n = 6, 7, 8$: not faithful (Long and Paton, 1993)
- $n \geq 9$: not faithful (Moody, 1991)

In 1999 Krammer constructed a representation

$$\rho_n : B_n \to GL_{n(n-1)/2}(\mathbf{Z}[t, t^{-1}, q, q^{-1}])$$

• Krammer (1999): ρ_4 is faithful

• Bigelow (2000): ρ_n is faithful for all n (topological proof)

• Krammer (2000): ρ_n is faithful for all n (algebraic proof)

Reference:

• V. Turaev, *Faithful linear representations of the braid groups*, Séminaire Bourbaki n° 878 (June 2000)

Dehornoy's linear ordering:

DEFINITION. *a) A braid is called σ-positive if it can be represented by a braid word in which the generator with lowest index appears only with positive powers.*

b) β is σ-negative if and only if β^{-1} is σ-positive.

EXAMPLE. $\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2^{-1}\sigma_1\sigma_2$ is σ-positive

THEOREM (Dehornoy, 1991–92). *A braid is either 1, or σ-positive, or σ-negative.*

It is not obvious at all that a σ-positive braid is not trivial or σ-negative, nor that a braid $\neq 1$ is either σ-positive or σ-negative.

Consequences:

• Define $\beta < \beta'$ if $\beta^{-1}\beta'$ is σ-positive. Then $<$ is a linear ordering on B_n, invariant under left multiplication

• B_n is a torsion-free group

• If R is a ring without zero divisors, then the group ring $R[B_n]$ has no zero divisors (Kaplansky conjecture), and any invertible element of $R[B_n]$ is of the form $r\beta$, where $r \in R^*$ and $\beta \in B_n$

• Dehornoy constructed a very efficient algorithm based on this ordering to solve the word problem in B_n

References:

• P. Dehornoy, *Braids and self-distributivity*, Progr. in Math. 195, Birkhäuser, 2000

• C. Kassel, *L'ordre de Dehornoy sur les tresses*, Séminaire Bourbaki n° 865 (November 1999) http://www-irma.u-strasbg.fr/~kassel/

Definition. *A LSD-set is a set equipped with a binary law $S \times S \to S$ satisfying*

$$a * (b * c) = (a * b) * (a * c). \qquad \text{(LSD)}$$

Example. Take $S = \mathbf{Z}[t, t^{-1}]$ and

$$a * b = (1 - t)a + tb.$$

We get the Burau representation

$$B_n \to GL_n(\mathbf{Z}[t, t^{-1}]).$$

This is an example of a LSD-set S in which left multiplications are *bijective*. Such a LSD-set gives rise to an action of the group B_n on the power-set S^n.

Definition. *A LSD-set S is acyclic if*

$$((a * b_1) * b_2) * b_3 \ldots \neq a$$

for all $a, b_1, b_2, b_3, \ldots \in S$.

An acyclic LSD-set in set theory

Axiom. *There exists a rank E with an elementary embedding $j : E \to E$.*

Elementary embedding: a non-bijective injection preserving all properties of E that can be defined using basic set-theoretical properties.

Rank: set considered in set theory with the property that (roughly) any function $E \to E$ can be considered as an element of E.

Take the set S of all elementary embeddings of the rank E: $S \neq \emptyset$.

If $i, j \in S$, define $i * j = i(j) \in S$. This binary laws satisfies Condition (LSD).

Proposition (Laver, 1989). *For any $j \in S$, the sub-LSD-set of S generated by j is an acyclic LSD-set.*

THEOREM (Dehornoy, 1991). *The free LSD-set D_1 on one generator is acyclic.*

Elements of D_1 are equivalence classes of $x,\ x*x,\ x*(x*x),\ (x*x)*x, \ldots$ modulo the (LSD) Relation, or, equivalently, modulo the action of the group G with the following presentation:

Generators: ∇_α where α runs over all finite sequences of 0 and 1

Relations:

$$\nabla_{\alpha 0\beta}\,\nabla_{\alpha 1\gamma} = \nabla_{\alpha 1\gamma}\,\nabla_{\alpha 0\beta}$$
$$\nabla_{\alpha 0\beta}\,\nabla_{\alpha} = \nabla_{\alpha}\,\nabla_{\alpha 10\beta}\,\nabla_{\alpha 00\beta}$$
$$\nabla_{\alpha 10\beta}\,\nabla_{\alpha} = \nabla_{\alpha}\,\nabla_{\alpha 10\beta}$$
$$\nabla_{\alpha 11\beta}\,\nabla_{\alpha} = \nabla_{\alpha}\,\nabla_{\alpha 11\beta}$$
$$\nabla_{\alpha 1}\,\nabla_{\alpha}\,\nabla_{\alpha 1}\,\nabla_{\alpha 0} = \nabla_{\alpha}\,\nabla_{\alpha 1}\,\nabla_{\alpha}$$

There exists a surjective homomorphism of groups $\pi = G \to B_\infty = \cup_n B_n$ defined by

$$\pi(\nabla_\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ contains } 0 \\ \sigma_{i+1} & \text{if } \alpha = 11\ldots1 \ (i \text{ times}) \end{cases}$$