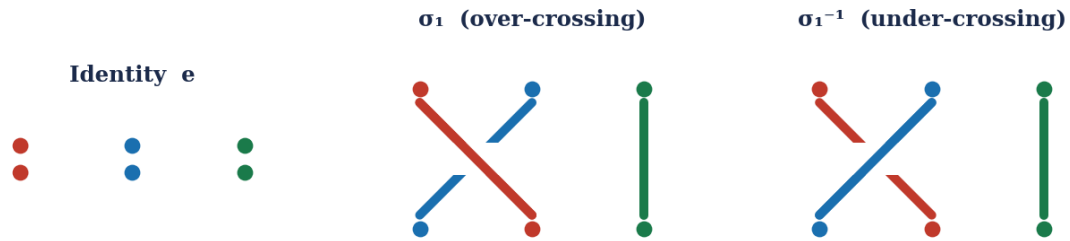
Tangled Up in Groups

The Hidden Algebra of Braids

Tom Rocks Maths Essay Competition 2026

Figure 1 — The generators of B_3



Three fundamental braids in B■ — the generators of an entire algebra.

1 Introduction

Braiding is one of the oldest human technologies. Archaeologists have found braided plant fibres in South African caves dating to 73,000 BCE; a carved statuette from ancient Egypt depicts an intricate braided wig from 3,500 BCE. Every culture on Earth, independently, invented braiding. For most of history, mathematicians paid it no attention at all.

That changed in 1925, when Emil Artin — a German-American algebraist with a taste for the beautiful — sat down and asked: *what exactly is a braid, mathematically?* The answer he found was so rich, so unexpectedly profound, that it now connects differential topology, quantum physics, and cryptography. Today, braid groups are central to the design of **topological quantum computers** — a technology that may define the next century of computing.

This essay takes you on Artin's journey. We begin with the simple act of crossing two strands, and arrive at the frontier of physics. The mathematics is genuine — there are real equations, a real group presentation, a real theorem connecting braids to knots. But the core idea is beautifully visual, and A-level algebra is sufficient to follow every step.

2 What Is a Braid?

A mathematician's braid is a precise version of the everyday object. Fix *n* parallel strings at the top and *n* endpoints at the bottom. The strings descend — always moving downward, never looping back up — and may cross over or under each other. The result, read top to bottom, is a braid.

> **Definition 2.1 (Braid).** A **braid on n strands** is a collection of n paths in the strip ■ × [0, 1], starting at {1, 2, …, n} × {0} and ending at {1, 2, …, n} × {1}, such that each path moves monotonically from top to bottom, and paths may cross but never pass through each other.

Two braids are **isotopic** (i.e., considered the same) if one can be continuously deformed into the other without moving the endpoints. Crucially, we track whether each crossing is an *over*- or *under*-crossing: a strand passing over its neighbour is genuinely different from one passing under. This distinction, as we will see, is where all the richness lives.

Figure 1 shows the three simplest braids in B■. The leftmost braid has no crossings — three strands drop straight down. The middle has strand 1 crossing *over* strand 2 (denoted σ■). The rightmost has strand 1 crossing *under* strand 2 (denoted σ■■¹). These three braids are mathematically distinct objects — and they are the atoms of an infinite algebraic universe.

3 The Braid Group B_n

Here is Artin's key observation: braids can be **multiplied**. Given two braids on *n* strands, stack the second directly below the first, connecting the bottom endpoints of the first to the top endpoints of the second. The result is a new braid on *n* strands. Figure 2 shows this for σ■ and

σ■ in B■.

Figure 2 — Composition: stacking braids

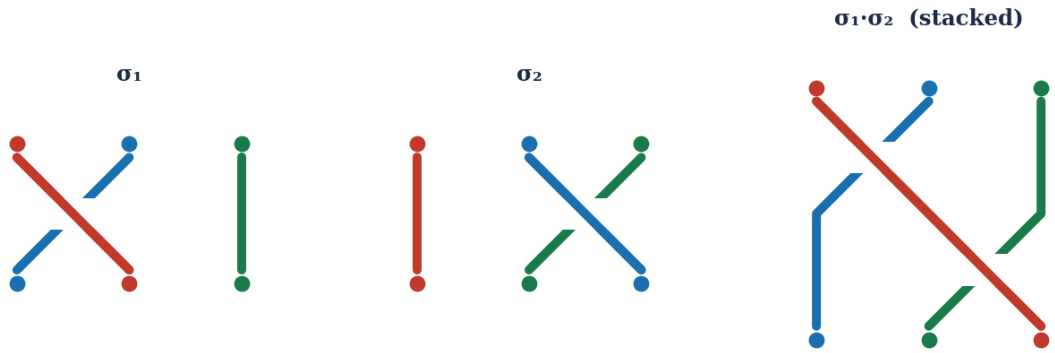


Figure 2 — Stacking braids: the product σ■·σ■ (right) is obtained by placing σ■ on top of σ■. This is how braids are multiplied.

This multiplication makes the set of all n-strand braids into a **group** — one of the foundational structures of abstract algebra. We verify the four group axioms:

Closure. Stacking two n-strand braids gives another n-strand braid. ✓

Associativity. (A then B) then C = A then (B then C), since the top-to-bottom order is unchanged. ✓

Identity. The braid with no crossings (all strands straight down) changes nothing when stacked. ✓

Inverses. Every braid has a mirror image (swap every over-crossing for an under-crossing); stacking a braid with its mirror unwinds all crossings. ✓

> **Definition 3.1.** The **braid group on n strands**, denoted B_n, is the group of all n-strand braids under the operation of stacking.

Artin showed that B_n has an elegant algebraic **presentation**: it is generated by elements σ■, σ■, …, σ_{n-1}, where σ_i is the braid where strand i crosses *over* strand i+1 and all other strands are straight. The inverse σ_i^{-1} has strand i crossing *under* strand i+1. Every braid is a product (a "word") in these generators and their inverses.

4 The Artin Relations

A group presentation is only as useful as our understanding of which words represent the same element. All equalities in B_n follow from just two families of relations, which Artin identified in 1925.

Relation 1 — Far generators commute. If $|i - j| \geq 2$, then:

$$\sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i$$

This is geometrically obvious: if the crossings σ_i and σ_j involve completely separate pairs of strands, they cannot interact and can happen in either order. Figure 5 demonstrates this for σ_1 and σ_3 in B_4.

Figure 5 — Commutation: $\sigma_1\sigma_3 = \sigma_3\sigma_1$ in B_4

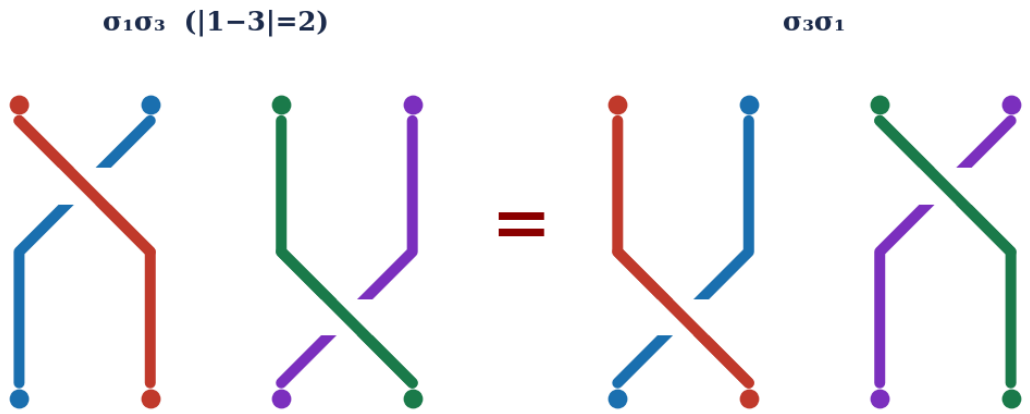


Figure 5 — Non-adjacent crossings commute: $\sigma_1\sigma_3 = \sigma_3\sigma_1$ in B_4, because strands 1–2 and strands 3–4 never meet.

Relation 2 — The braid relation. For adjacent generators:

$$\sigma_1 \cdot \sigma_2\sigma_1 \cdot \sigma_2 = \sigma_2\sigma_1 \cdot \sigma_2 \cdot \sigma_1\sigma_2$$

This is the deep one. Two different sequences of three adjacent crossings produce the same braid. Figure 3 shows this for B_3: the left side performs crossings 1, 2, 1; the right side performs 2, 1, 2. After a smooth deformation — an isotopy — they are identical.

Figure 3 — The braid relation: σ₁σ₂σ₁ = σ₂σ₁σ₂

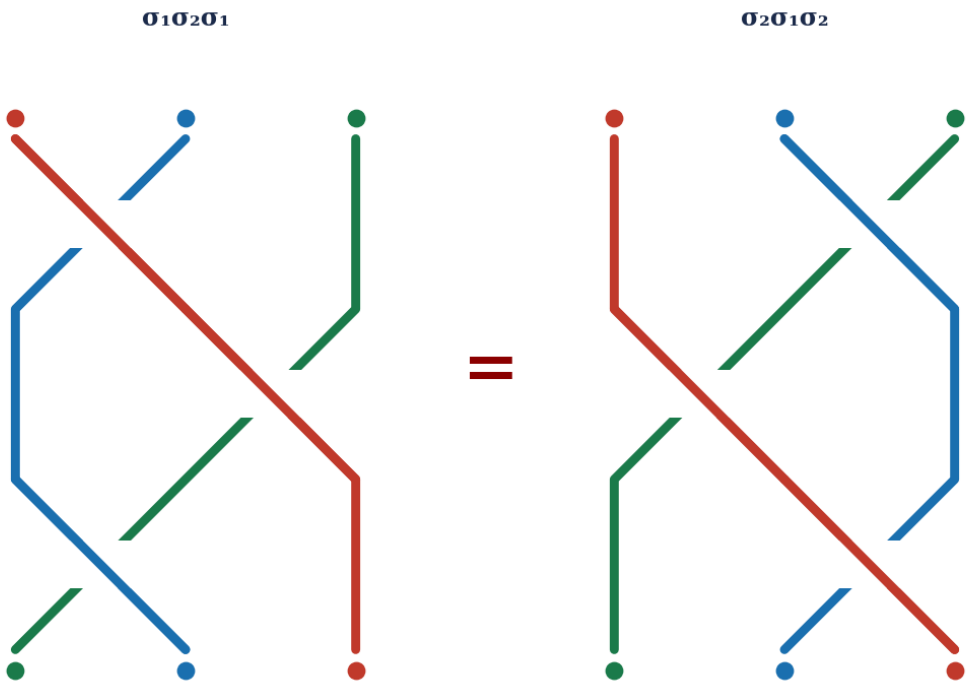


Figure 3 — The braid relation in B■: σ■σ■σ■ = σ■σ■σ■. Both sides are isotopic — continuously deformable into each other. Note how the strands braid through each other in genuinely different orders yet arrive at the same configuration.

Theorem 4.1 (Artin, 1925). The braid group B_n has the group presentation:

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j|\geq 2 \; ; \; \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \rangle$$

This is remarkable. An infinite group — one containing uncountably many braids — is fully described by $n-1$ generators and two short families of relations. The braid relation itself is famous across mathematics and physics: it is the **Yang–Baxter equation**, which independently arises in statistical mechanics, quantum field theory, and the theory of solvable models. Artin discovered it by thinking about hair.

5 Braids and Knots: Alexander's Theorem

In 1923 — two years before Artin published his braid groups — James Waddell Alexander proved a theorem connecting braids to another ancient mathematical structure: **knots**.

A knot, mathematically, is a closed loop in three-dimensional space — imagine a knotted piece of string with its two ends joined. The simplest non-trivial knot is the **trefoil**: three loops interlinked, the shape you see on Celtic jewellery. A central question of knot theory is: when are

two knots the same? That is, when can one be continuously deformed into the other without cutting?

Alexander's insight was to connect knots to braids. Given any braid, form a knot by **closing** it: connect the bottom endpoint of each strand to the top endpoint of the corresponding strand via arcs running outside the braid (Figure 4, dashed arrows). The resulting closed loop is a knot or link.

Figure 4 — Alexander's theorem: closing $(\sigma_1)^3$ yields the trefoil knot

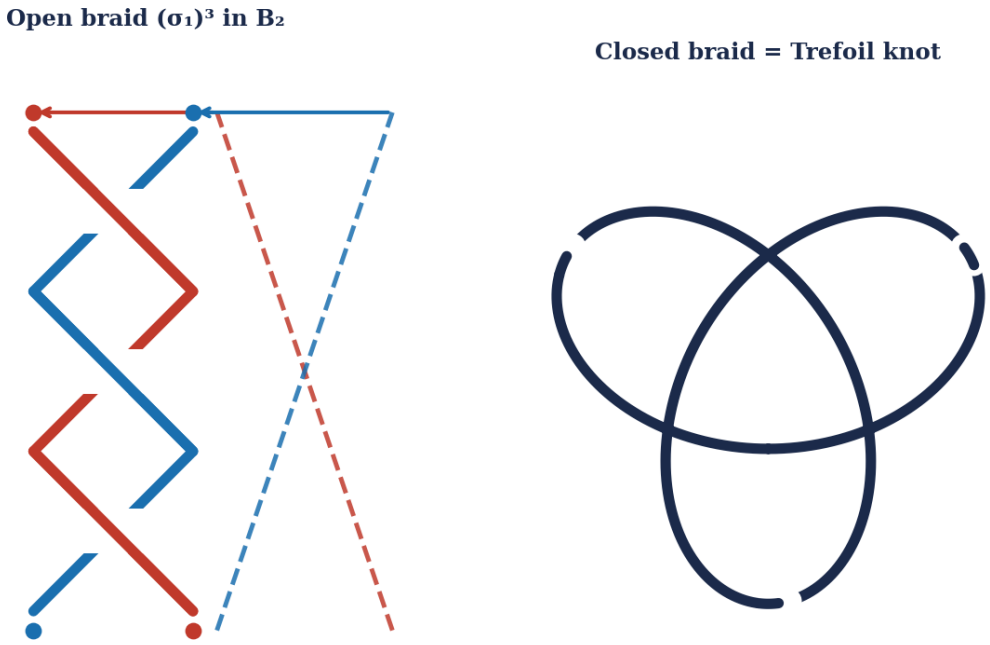


Figure 4 — Alexander's theorem in action: closing the braid $(\sigma_■)^3$ in $B_■$ (left) by connecting endpoints via arcs (dashed) yields the trefoil knot (right). Every knot arises this way from some braid.

> **Theorem 5.1 (Alexander, 1923).** Every knot or link in 3-dimensional space can be represented as the closure of some braid.

The trefoil is the closure of $(\sigma_■)^3$ in $B_■$. The figure-eight knot is the closure of $\sigma_■\sigma_■^{-1}\sigma_■\sigma_■^{-1}$ in $B_■$. Every knot — no matter how tangled — is the closure of some braid word. Alexander's theorem transformed knot theory into a branch of algebra: instead of reasoning geometrically about tangled loops, mathematicians could now compute with words in braid groups.

6 The Word Problem — and Why It's Hard

There is one subtle difficulty: given two words in $\sigma_■, \ldots, \sigma_{n-1}$, how do you decide whether they represent the same braid? This is the **word problem** for B_n, and its difficulty is genuinely

non-trivial.

For instance: is σ■σ■■¹σ■ equal to σ■σ■■¹σ■? (It is — by a variant of the braid relation — but the verification requires a non-trivial calculation.) For a long word in B■■, the answer is far from obvious.

In 1969, Frank Garside solved the word problem for braid groups by introducing a **canonical normal form**: every braid word can be reduced, via finitely many applications of the Artin relations, to a unique standard representative. Two words are equal in B_n if and only if they reduce to the same normal form.

What makes this beautiful — and practically significant — is that the word problem for large braid groups is **computationally hard**. While solvable in theory, the best algorithms have super-polynomial complexity for large *n* and long words. This hardness is the foundation of **braid-based cryptography**.

In 1999, Anshel, Anshel, and Goldfeld proposed the first braid-based public-key cryptosystem. The core difficulty it exploits is the **conjugacy search problem**: given two braids *P* and *Q* in B_n, find a braid *a* such that Q = a·P·a■¹. This is believed to be hard even for quantum computers — unlike RSA and Diffie–Hellman, which Shor's algorithm would break. Braid cryptography is a candidate for the post-quantum world.

7 Braiding the Future: Topological Quantum Computing

The most audacious application of braid groups is not just security — it is the operating principle of a computer.

Ordinary quantum computers store information in **qubits**, which suffer from a fatal flaw: *decoherence*. Any stray vibration, magnetic field, or cosmic ray can destroy the quantum information. Today's quantum computers require ultra-cold temperatures and elaborate error correction simply to function for milliseconds.

In 1997, Alexei Kitaev proposed a radically different approach: **topological quantum computing**. The key ingredient is a hypothetical particle called an **anyon**, which exists only in two-dimensional systems. When two anyons exchange positions — one moving around the other — the quantum state of the system changes in a way that depends only on the *topology* of the path, not its precise shape. This exchange is, mathematically, exactly a **braid**.

Here is why this is revolutionary. Topological information is inherently robust: you cannot accidentally deform a braid from σ■σ■ to σ■σ■ by a small perturbation — these are topologically distinct. A quantum computer built from anyons would be *intrinsically protected* against decoherence. The computation is encoded in the braid type of the anyon paths, which thermal noise cannot alter. In 2023, Microsoft reported experimental evidence of non-Abelian anyons in a superconducting device — a first step toward topological qubits. The mathematical machinery underneath? Artin's braid group presentation, built on $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$.

8 Conclusion

Mathematics has a habit of finding that simple things are secretly profound. A braid — three strands of hair woven by a child in minutes — turns out to generate an infinite non-commutative group with a rich algebraic structure, deep connections to topology, and live applications in cryptography and quantum physics.

Artin's two relations are the punchline of the whole story. The commutation relation $\sigma_i\sigma_j = \sigma_j\sigma_i$ captures the intuition that distant crossings don't interact. The braid relation — $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ — is the surprise: a non-obvious constraint that emerges from pure topology, and turns out to be the same equation appearing in statistical mechanics, in integrable models, and in the physics of anyons.

The arc from grandmother's braiding technique to topological quantum computing passes through a 100-year sequence of mathematical insights, each unlocking the next. That is what makes braid groups irresistible: they are simple enough to draw in a notebook, yet powerful enough to protect data from quantum attacks and encode computation in the geometry of spacetime itself.

And the whole thing started with Artin asking: what is a braid?

References

[1] Artin, E. Theorie der Zöpfe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 4(1):47–72, 1925.

[2] Alexander, J. W. A lemma on systems of knotted curves. *Proceedings of the National Academy of Sciences*, 9(3):93–95, 1923.

[3] Garside, F. A. The braid group and other groups. *The Quarterly Journal of Mathematics*, 20(1):235–254, 1969.

[4] Anshel, I., Anshel, M., & Goldfeld, D. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6(3–4):287–291, 1999.

[5] Kitaev, A. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003.

[6] Birman, J. S. *Braids, Links, and Mapping Class Groups.* Princeton University Press, 1974.

[7] Kassel, C. & Turaev, V. *Braid Groups.* Springer GTM 247, 2008.

[8] Microsoft Azure Quantum Team. Interferometric single-shot parity measurement in InAs–Al hybrid devices. *Nature*, 638, 651–655, 2025.