## 1. ANALOGY BETWEEN KNOTS AND PRIMES

Knots and primes are the basic objects of study in knot theory and number theory respectively. Surprisingly, these two seemingly unrelated concepts have a deep analogy discovered by Barry Mazur in the 1960s while studying the Alexander polynomial, which initiated the study of what is now known as arithmetic topology. As motivation for this analogy, we first consider the correspondence between commutative rings and spaces in algebraic geometry.

### 1.1. **Commutative rings and spaces.**

**Example 1.1.** Consider the polynomial ring $\mathbb{C}[t]$: it has transcendence degree one over the field $\mathbb{C}$, which we think of as one degree of freedom. We represent it by a complex line, denoted by $\operatorname{Spec}\mathbb{C}[t]$. Hilbert's Nullstellensatz tells us that there is a bijective correspondence between elements $a \in \mathbb{C}$ and maximal ideals $(t-a)$ of functions that vanish at $a$. Since every nonzero prime ideal of $\mathbb{C}[t]$ is a maximal ideal, this justifies us labeling the complex line as $\operatorname{Spec}\mathbb{C}[t]$, the set of prime ideals of the ring $\mathbb{C}[t]$. (The zero ideal corresponds to the generic point, which one should think of as the entire line.) The inclusion of the point representing $(t-a)$ into the complex line corresponds to the quotient map $\mathbb{C}[t] \twoheadrightarrow \mathbb{C}[t]/(t-a) \cong \mathbb{C}$ in the opposite direction and is denoted by a map $\operatorname{Spec}\mathbb{C} \hookrightarrow \operatorname{Spec}\mathbb{C}[t]$.

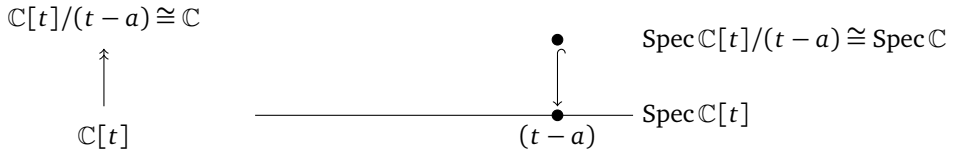



FIGURE 1. Inclusion $\operatorname{Spec}\mathbb{C} \hookrightarrow \operatorname{Spec}\mathbb{C}[t]$

**Example 1.2.** There is a similar story for the ring of integers $\mathbb{Z}$. Above, we used transcendence degree as a measure of dimension; however, we could equally well have used Krull dimension, that is, the supremum of all integers $n$ such that there is a strict chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$, as the Krull dimension of a domain finitely generated over a field is equal to its transcendence degree. Krull dimension turns out to be the "correct" notion of dimension in algebraic geometry, as it is defined for all commutative rings. The Krull dimension of $\mathbb{Z}$ is one, so once again we represent it by a line, denoted by $\operatorname{Spec}\mathbb{Z}$; its points are prime ideals $(p)$ where $p$ is a prime number. As before, the inclusion of the point representing $(p)$ into the complex line corresponds to the quotient map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(p) \cong \mathbb{F}_p$ in the opposite direction and is denoted by a map $\operatorname{Spec}\mathbb{F}_p \hookrightarrow \operatorname{Spec}\mathbb{Z}$.

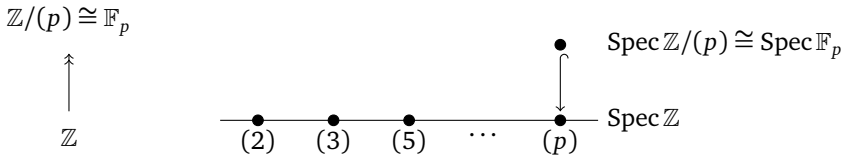



FIGURE 2. Inclusion $\operatorname{Spec}\mathbb{F}_p \hookrightarrow \operatorname{Spec}\mathbb{Z}$

### 1.2. **Knots and primes.**

The key idea behind the analogy between knots and primes is to use a different notion of dimension, namely étale cohomological dimension. The space $\operatorname{Spec}\mathbb{F}_p$ has étale homotopy groups

$$\pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{F}_p) = \operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}, \qquad \pi_i^{\text{ét}}(\operatorname{Spec}\mathbb{F}_p) = 0 \ (i \geq 2)$$

(here $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$). Since the circle $S^1$ has homotopy groups

$$\pi_1(S^1) = \operatorname{Gal}(\mathbb{R}/S^1) = \mathbb{Z}, \qquad \pi_i(S^1) = 0 \ (i \geq 2),$$

this suggests that $\operatorname{Spec}\mathbb{F}_p$ should be regarded as an arithmetic analogue of $S^1$. (It is a classical theorem in algebraic topology that a space with only one nonzero homotopy group, called an *Eilenberg-MacLane space*, is unique up to homotopy equivalence.) On the other hand, the space $\operatorname{Spec}\mathbb{Z}$ (or in fact $\operatorname{Spec}\mathcal{O}_k$, where $\mathcal{O}_k$ is the ring of integers of a number field $k$) satisfies Artin-Verdier duality, which one can think of as some sort of Poincaré

duality for 3-manifolds, and $\pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{Z}) = 1$. Hence it makes sense to regard $\operatorname{Spec}\mathbb{Z}$ as an analogue of $\mathbb{R}^3$. (The reader may wonder why we regard $\operatorname{Spec}\mathbb{Z}$ as an analogue of $\mathbb{R}^3$ instead of $S^3$. It turns out that the correct analogue of $S^3$ is $\operatorname{Spec}\mathbb{Z} \cup \{\infty\}$ (the prime at infinity), just as $S^3 = \mathbb{R}^3 \cup \{\infty\}$.) Thus, the embedding

$$\operatorname{Spec}\mathbb{F}_p \hookrightarrow \operatorname{Spec}\mathbb{Z}$$

is viewed as the analogue of an embedding

$$S^1 \hookrightarrow \mathbb{R}^3.$$

This yields an analogy between knots and primes.

This analogy can be extended to many concepts in knot theory and number theory. We list some of these analogies in Table 1.

| KNOTS | PRIMES |
|---|---|
| **Fundamental/Galois groups** | |
| $\pi_1(S^1) = \operatorname{Gal}(\mathbb{R}/S^1)$<br>$= \langle [l] \rangle$<br>$= \mathbb{Z}$<br>Circle $S^1 = K(\mathbb{Z}, 1)$ | $\pi_1(\operatorname{Spec}(\mathbb{F}_q)) = \operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, $q = p^n$<br>$= \langle [\sigma] \rangle$<br>$= \hat{\mathbb{Z}}$<br>Finite field $\operatorname{Spec}(\mathbb{F}_q) = K(\hat{\mathbb{Z}}, 1)$ |
| Loop $l$ | Frobenius automorphism $\sigma$ |
| Universal covering $\mathbb{R}$ | Separable closure $\overline{\mathbb{F}_q}$ |
| Cyclic covering $\mathbb{R}/n\mathbb{Z}$ | Cyclic extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ |
| **Manifolds** | **Spec of a ring** |
| $V \simeq S^1$<br>$V \setminus S^1 \simeq \partial V$<br>($\simeq$ denotes homotopy equivalence) | $\operatorname{Spec}(\mathscr{O}_p) \simeq \operatorname{Spec}(\mathbb{F}_q)$<br>$\operatorname{Spec}(\mathscr{O}_\mathfrak{p}) \setminus \operatorname{Spec}(\mathbb{F}_q) \simeq \operatorname{Spec}(k_\mathfrak{p})$<br>($\simeq$ denotes étale homotopy equivalence; $\mathscr{O}_\mathfrak{p}$ is a $\mathfrak{p}$-adic integer ring whose residue field is $\mathbb{F}_q$ and whose quotient field is $k_\mathfrak{p}$) |
| Tubular neighborhood $V$ | $\mathfrak{p}$-adic integer ring $\operatorname{Spec}(\mathscr{O}_\mathfrak{p})$ |
| Boundary $\partial V$ | $\mathfrak{p}$-adic field $\operatorname{Spec}(k_\mathfrak{p})$ |
| 3-manifold $M$ | Number ring $\operatorname{Spec}(\mathscr{O}_k)$ |
| Knot $S^1 \hookrightarrow \mathbb{R}^3 \cup \{\infty\} = S^3$ | Rational prime $\operatorname{Spec}(\mathbb{F}_p) \hookrightarrow \operatorname{Spec}(\mathbb{Z}) \cup \{\infty\}$ |
| Any connected oriented 3-manifold is a finite covering of $S^3$ branched along a link (Alexander's theorem) | Any number field is a finite extension of $\mathbb{Q}$ ramified over a finite set of primes |
| **Knot group** | **Prime group** |
| $G_K = \pi_1(M \setminus K)$ | $G_{\{\mathfrak{p}\}} = \pi_1^{\text{ét}}(\operatorname{Spec}(\mathscr{O}_k \setminus \{\mathfrak{p}\}))$ |
| $G_K \cong G_L \iff K \sim L$ for prime knots $K$, $L$ | $G_{\{(p)\}} \cong G_{\{(q)\}} \iff p = q$ for primes $p$, $q$ |
| **Linking number** | **Legendre symbol** |
| Linking number $\operatorname{lk}(L, K)$ | Legendre symbol $(\frac{q^*}{p})$, $q^* := (-1)^{\frac{q-1}{2}} q$ |
| Symmetry of linking number $\operatorname{lk}(L, K) = \operatorname{lk}(K, L)$ | Quadratic reciprocity law $(\frac{q}{p}) = (\frac{p}{q})$ $(p, q \equiv 1 \bmod 4)$ |
| **Alexander-Fox theory** | **Iwasawa theory** |
| Infinite cyclic covering $X_\infty \to X_K$<br>$\operatorname{Gal}(X_\infty/X_K) = \langle \tau \rangle \cong \mathbb{Z}$ | Cyclotomic $\mathbb{Z}_p$-extension $k_\infty/k$<br>$\operatorname{Gal}(k_\infty/k) = \langle \gamma \rangle \cong \mathbb{Z}_p$ |
| Knot module $H_1(X_\infty)$ | Iwasawa module $H_\infty$ |
| Alexander polynomial $\det(t \cdot \mathrm{id} \mid H_1(X_\infty) \otimes_\mathbb{Z} \mathbb{Q})$ | Iwasawa polynomial $\det(T \cdot \mathrm{id} - (\gamma - 1) \mid H_\infty \otimes_{\mathbb{Z}_p} Q_p)$ |

TABLE 1. Analogies between knots and primes

## 2. PRELIMINARIES ON KNOT THEORY

**Definition 2.1.** A *knot* is the image of an embedding of $S^1$ into $S^3$ (or more generally, into an orientable connected closed 3-manifold $M$). A *knot type* is the equivalence class of embeddings that can be obtained from a

particular one under ambient isotopy. (However, following common parlance, we shall often refer to a knot type simply as a knot when there is no danger of confusion.)

We shall be concerned only with *tame* knots, that is, knots which possess a tubular neighborhood. A knot is tame if and only if it is ambient isotopic to a piecewise-linear knot, or equivalently, to a smooth knot.

2.1. **Knot diagrams.** Let $K$ be a knot. By removing a point in $S^3$ not contained in $K$ (call it $\infty$), we may assume that $K \subset \mathbb{R}^3$.

**Definition 2.2.** A projection of $K$ onto a plane in $\mathbb{R}^3$ is called *regular* if it has only a finite number of multiple points, all of which are double points.

Clearly, any knot projection can be transformed into a regular projection by a slight perturbation of the knot. All the knot projections we consider will be regular, with the over- and undercrossings marked.

**Definition 2.3.** The *crossing number* of a knot (type) is the least number of crossings in any projection of a knot of that type.

**Definition 2.4.** Given two knots $J$ and $K$, the *connected sum* or *composition* of $J$ and $K$, denoted $J\#K$, is the knot obtained by removing a small arc from each knot projection and connecting the endpoints by two new arcs, as in Figure 3.

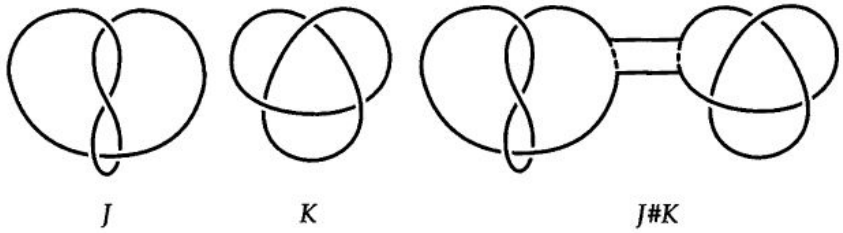
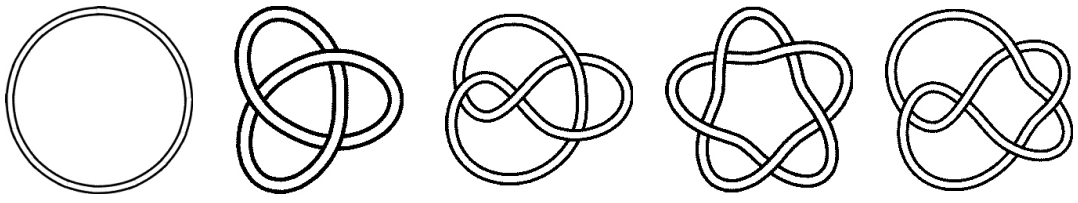



FIGURE 3. Connected sum of two knots

Note that in general, the connected sum of unoriented knots is not well-defined—more than one knot may arise as the connected sum of two unoriented knots. However, the connected sum is well-defined if we put an orientation on each knot and insist that the orientation of the connected sum matches the orientation of each of the factor knots. A knot is called *prime* if it cannot be written as the connected sum of two non-trivial knots, and *composite* otherwise.

**Example 2.5.**



(A) $0_1$ Unknot

(B) $3_1$ $(3,2)$-torus knot Trefoil

(C) $4_1$ Figure eight

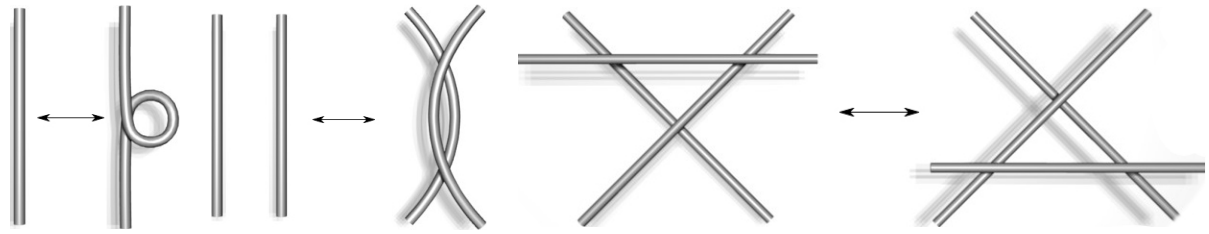
(D) $5_1$ $(5,2)$-torus knot

(E) $5_2$

FIGURE 4. Prime knots (i.e., knots that cannot be expressed as the connected sum of two knots, neither of which is the trivial knot) with crossing number at most 5. The knots are labelled using Alexander-Briggs notation: the regularly-sized number indicates the crossing number, while the subscript indicates the order of that knot among all knots with that crossing number in the Rolfson classification.

**Remark 2.6.** A knot is called *alternating* if it has a projection in which the crossings alternate between over- and undercrossings as one travels along the knot. All prime knots with crossing number less than 8 are alternating (there are three non-alternating knots with crossing number 8); moreover, it is a theorem of Thistlewaite, Kauffman and Murasugi (one of the Tait conjectures) that any minimal crossing projection of an alternating knot is an alternating projection. This provides a useful way to check if one has drawn a projection of a low-crossing knot correctly.

Two knot projections represent the same knot if and only if, up to planar isotopy, one can be obtained from the other via a sequence of *Reidemeister moves*, moves repesenting ambient isotopies that change the relations between the crossings. The Reidemeister moves are shown in Figure 5.



(A) Type I
Twist/untwist

(B) Type II
Move over/under a strand

(C) Type III
Move over/under a crossing

FIGURE 5. Reidemeister moves

2.2. **The knot group.** Let $K$ be a knot. We fix the following notation and terminology.

**Definition 2.7.** Denote by $V_K$ a tubular neighborhood of $K$. The complement $X_K := S^3 \setminus \text{int}(V_K)$ of an open tubular neighborhood $\text{int}(V_K)$ in $S^3$ is called the *knot exterior*. (Note that $X_K$ is a compact 3-manifold with boundary a torus.) A *meridian* of $K$ is a closed (oriented) curve on $\partial X_K$ which is the boundary of a disk $D^2$ in $V_K$. A *longitude* of $K$ is a closed curve on $\partial X_K$ which intersects with a meridian at one point and is null-homologous in $X_K$. (See Figure 6.)

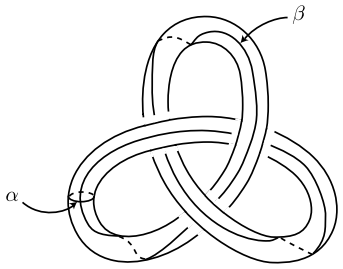



FIGURE 6. Tubular neighborhood of a knot with a meridian $\alpha$ and a longitude $\beta$.

The most obvious invariant of a knot $K$ is the *knot group* $G_K$, which is defined to be the fundamental group of the knot exterior $\pi_1(X_K) = \pi_1(S^3 \setminus K)$. Given a regular presentation of a knot, one can obtain a presentation of the knot group, known as a *Wirtinger presentation*.

**Theorem 2.8.** *Given a regular presentation of a knot $K$, give the knot an orientation and divide it into arcs $c_1$, $c_2$, ..., $c_n$ such that $c_i$ is connected to $c_{i+1}$ at a double point (with the convention that $c_{n+1} = c_1$), as in Figure 7. The knot group $G_K$ has a Wirtinger presentation*

$$G_K = \langle x_1, \ldots, x_n \mid R_1, \ldots, R_n \rangle,$$

*where the relation $R_i$ has the form $x_i x_k x_{i+1}^{-1} x_k^{-1}$ or $x_i x_k^{-1} x_{i+1}^{-1} x_k$ depending on whether the crossing at a double point is a positive or negative crossing, as specified by Figure 8.*

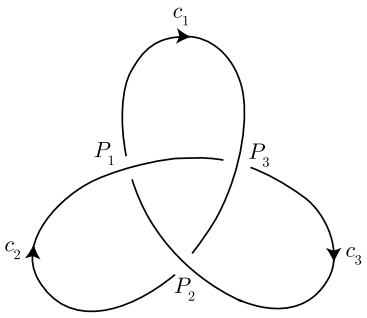
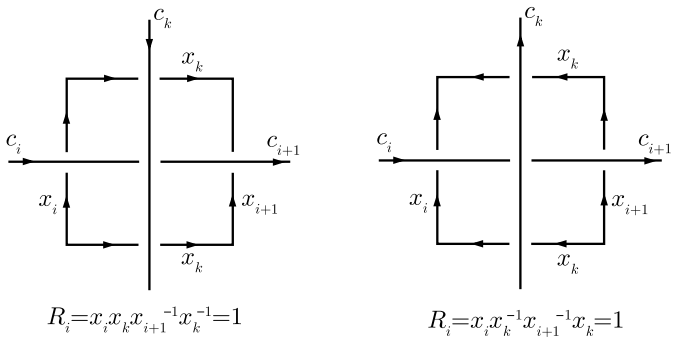



FIGURE 7. Oriented knot $K$, divided into arcs $c_1, c_2, \ldots, c_n$.




(A) Positive crossing (B) Negative crossing

FIGURE 8. Relation in knot group depending on the type of crossing

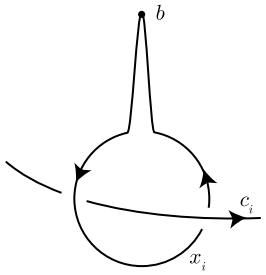



FIGURE 9. Loop $x_i$ passing through the point at infinity and going once under $c_i$ from the right to the left.

*Proof.* For $1 \leq i \leq n$, let $x_i$ be a loop passing through $\infty$ and which goes once under $c_i$ from the right to the left, as shown in Figure 9.

It is clear that the loops $x_i$ generate the group $G_K$. Suppose that the arcs $c_i$ and $c_{i+1}$ are separated by $c_k$ at the $i$-th crossing. If the crossing is positive (respectively negative), one can concatenate the loops $x_i$, $x_k$, $x_{i+1}^{-1}$, $x_k^{-1}$ (respectively $x_i$, $x_k^{-1}$, $x_{i+1}^{-1}$, $x_k$) to obtain a null-homologous loop. Hence the relations $R_i$, $1 \leq i \leq n$, hold in $G_K$. (Note that the relation $R_i$ implies any cyclic permutation of it by conjugation.) Moreover, the generators $x_i$ and relations $R_i$ form a presentation for $G_K$: by considering the projection of a loop $\ell$ in $X_K$ onto the plane of the knot projection, one can write $\ell$ in terms of the $x_i$'s. When a homotopy is performed on $\ell$, the word representing $\ell$ changes only when the projection of $\ell$ passes through the crossings of $K$. □

**Fact 2.9.** One of the relations among the $R_i$ is redundant, that is, we can derive any one of the relations $R_i$ from the others.

**Corollary 2.10.** *$G_K$ has a presentation with deficiency 1, that is, a presentation where the number of relations is one fewer than the number of generators.*

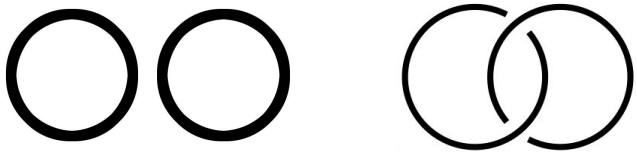
**Definition 2.11.** A $r$-component *link* $L$ is the image of an embedding of a disjoint union of $r$ copies of $S^1$ into $S^3$ (or more generally, into an orientable connected closed 3-manifold $M$). Thus one may write $L = K_1 \cup \cdots \cup K_r$ where the $K_i$ are mutually disjoint knots. (As before, we shall often refer to an equivalence class of links under ambient isotopy simply as a link.)

The *link group* $G_L$ is defined to be $\pi_1(S^3 \setminus L)$. Similarly to the case of knots, $G_L$ has a Wirtinger presentation of deficiency 1. In general, for a knot $K$ or link $L$ in an orientable connected closed 3-manifold $M$, the knot group $G_K(M) := \pi_1(M \setminus K)$ or link group $G_L(M) := \pi_1(M \setminus L)$ also has deficiency 1, but may not have a Wirtinger presentation.

**Example 2.12** (Knot group of trefoil)**.** Consider the trefoil knot from Figure 7. Its knot group has a Wirtinger presentation $\langle x_1, x_2, x_3 \mid x_2 x_1 x_3^{-1} x_1^{-1}, x_3 x_2 x_1^{-1} x_2^{-1}, x_1 x_3 x_2^{-1} x_3^{-1} \rangle$. The product of the three relations in reverse order is 1, hence any one of the relations is redundant. From the second relation, we obtain $x_3 = x_2 x_1 x_2^{-1}$, and substituting this into the first relation, we see that the knot group of the trefoil is the braid group $B_3 = \langle x_1, x_2 | x_1 x_2 x_1 = x_2 x_1 x_2 \rangle$.

**Exercise 2.13.** Show that the above knot group is isomorphic to the group $\langle a, b \mid a^3 = b^2 \rangle$. (In general, a $(p, q)$-torus knot has fundamental group $\langle a, b \mid a^p = b^q \rangle$, but this is harder to show.)

**Exercise 2.14.** Show that two unlinked circles (Figure 10a) and the Hopf link (Figure 10b) are not equivalent.



(A) Two unlinked circles (B) Hopf link

FIGURE 10. Two non-equivalent links

**Remark 2.15.** A knot is said to be *chiral* if it is not equivalent to its mirror image, and *achiral* or *amphichiral* otherwise. Clearly, the knot group cannot detect whether a knot is chiral. The other knot invariant that we shall introduce in this tutorial, the Alexander polynomial, is also unable to detect chirality since it is defined in terms of a homology group. However, other knot invariants such as the Jones polynomial are able to detect the chirality of some knots.