TÔPÔ SỐ HỌC: SỐ NGUYÊN TỐ GIỐNG NÚT NHƯ THẾ NÀO?

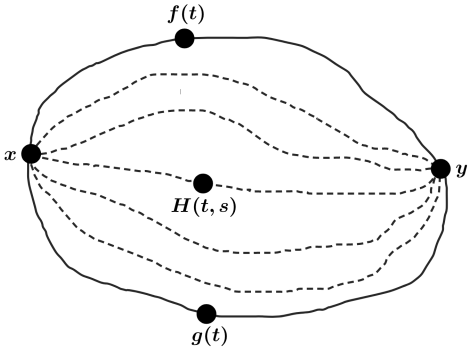
NGUYỄN MẠNH LINH[1]

Tôpô học là lĩnh vực nghiên cứu các không gian trừu tượng, những đối tượng liên tục. Ngược lại, số học là lĩnh vực nghiên cứu các số nguyên, những đối tượng rời rạc. Hai lĩnh vực này dường như nằm ở hai thái cực đối lập của toán học. Đấy là cho đến khoảng vài thập kỷ trở lại đây, khi các nhà toàn học phát hiện ra mối liên hệ giữa hai đối tượng tưởng như chẳng liên quan ở hai bên. Người ta đang xây dựng một cầu nối, một cuốn từ điển cho phép dịch các định lý từ một bên sang bên kia và ngược lại. Lĩnh vực mới toanh này được gọi là **tôpô số học**.

Nhóm cơ bản

Để nói về tôpô số học, tất nhiên ta phải bắt đầu với... tôpô học và số học. Các không gian tôpô là các đối tượng cho phép ta nói về lân cận của các điểm, cũng như các hàm liên tục. Sự "giống nhau" giữa các không gian tôpô được cho bởi các phép đồng phôi, các hàm liên tục $1-1$ mà hàm ngược cũng liên tục. Để đơn giản, ta sẽ chỉ quan tâm đến các không gian **liên thông**: hai điểm bất kỳ luôn nối được bằng một đường. Một **đường** giữa hai điểm x, y trong một không gian tôpô X đơn giản là một hàm liên tục $f : I \to X$ sao cho $f(0) = x$ và $f(1) = y$.

Giả sử ta có một đường khác $g : I \to X$ từ x đến y. Không gì cản chúng ta nói về khái niệm "đường giữa hai đường f và g", mà toán học gọi là **đồng luân**. Đó là một hàm liên tục $H : I \times I \to X$ sao cho $H(t,0) = f(t)$, $H(t,1) = g(t)$, $H(0,s) = x$ và $H(1,s) = y$. Nói cách khác, H là một họ các đường trung gian được tham số hóa bởi s, thể hiện sự biến dạng liên tục từ đường f (khi $s = 0$) đến đường g (khi $s = 1$), đồng thời giữ cố định hai đầu mút x, y.

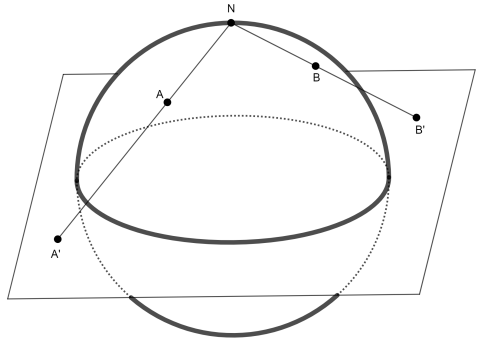


Hình 1: Một phép đồng luân giữa hai đường f và g.

Khi H tồn tại, ta nói hai đường f và g đồng luân, ký hiệu bởi $f \sim g$. Khi hai đường bất kỳ giữa hai điểm cho trước luôn đồng luân, ta nói không gian X **đơn liên**. Ví dụ về không gian đơn liên là không gian Euclid $\mathbb{R}^n$. Thật vậy, cấu trúc cộng và nhân với vô hướng

[1] *Université Paris–Saclay.*

trong $\mathbb{R}^n$ cho phép ta định nghĩa phép đồng luân $H(t,s) = (1-s)\cdot f(t) + s\cdot g(t)$ giữa hai đường f, g tùy ý. Mặt siêu cầu $\mathbb{S}^n$, thu được bằng cách thêm một điểm ở xa vô tận vào $\mathbb{R}^n$, cũng đơn liên với $n > 1$: hãy chọn một điểm P tùy ý trên mặt cầu và hình dung rằng mọi đường đều có thể biến dạng liên tục thành một đường không đi qua P. Mà $\mathbb{R}^n$ bỏ đi P chính là (đồng phôi với) $\mathbb{R}^n$, nên hai đường không đi qua P luôn đồng luân.

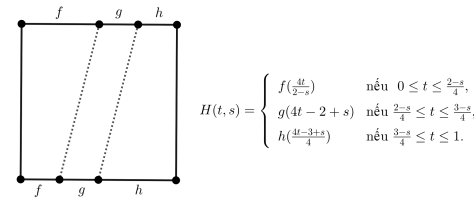


Hình 2: Qua phép chiếu lập thể, mặt cầu $\mathbb{S}^2$ bỏ đi điểm cực bắc N trở thành mặt phẳng $\mathbb{R}^2$. Ta có thể xem N như "điểm ở xa vô tận" của mặt phẳng.

Các đường cho ta bất biến đại số đầu tiên cho phép phân biệt các không gian tôpô (cho biết khi nào chúng không đồng phôi), được gọi là **nhóm cơ bản**, định nghĩa bởi Henri Poincaré năm 1895. Ta hãy cố định một điểm $x \in X$ và xét các đường từ x đến chính nó, được gọi là các **khuyên**. Ta xây dựng một phép toán trên chúng: cho f và g là hai khuyên tại x, ta định nghĩa $g * f : I \to X$ là khuyên thu được bằng cách đi theo f với vận tốc gấp đôi rồi đi theo g với vận tốc gấp đôi. Bằng công thức,

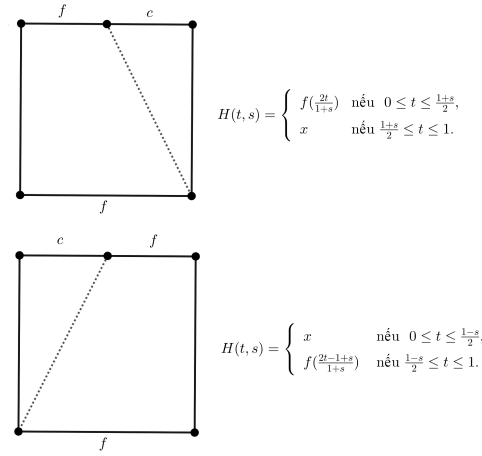
$$(g*f)(t) \begin{cases} = f(2t) & \text{nếu } 0 \le t \le \frac{1}{2} \\ = g(2t-1) & \text{nếu } \frac{1}{2} \le t \le 1. \end{cases}$$

Như một thủ tục, ta cần kiểm tra các tiên đề của nhóm. Đầu tiên là tính kết hợp. Bằng tính toán trực tiếp, ta thấy ngay $h*(g*f) \neq (h*g)*f$. Tuy nhiên, hai đường này đồng luân. Điều này gợi ý rằng ta cần xem hai đường là như nhau nếu chúng đồng luân.



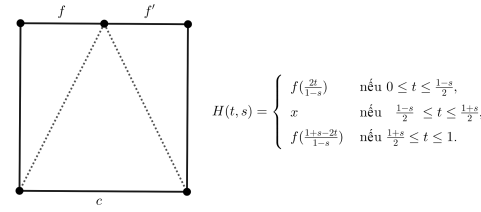
Hình 3: $h*(g*f) \sim (h*g)*f$.

Thứ hai, ta cần chỉ ra phần tử trung lập. Một cách trực giác, ta thấy nó phải là đường hằng c, cho bởi "đứng yên tại x", hay $c(t) = x$.



Hình 4: $f*c \sim f$ và $c*f \sim f$.

Cuối cùng, ta cần tìm nghịch đảo của một đường f cho trước. Đó là đường f' cho bởi "đi ngược với f", hay $f'(t) = f(1-t)$.

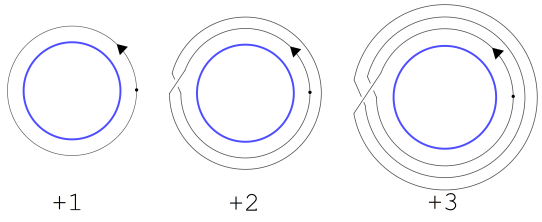


Hình 5: $f*f' \sim c$. Tất nhiên, vì $f'' = f$ nên $f'*f \sim c$.

Vậy các khuyên tại x (sai khác đồng luân) tạo thành một nhóm, nó được gọi là nhóm cơ bản của X, ký hiệu bởi $\pi_1(X)$.

Một không gian là đơn liên khi và chỉ khi nhóm cơ bản của nó tầm thường (mọi khuyên đều biến dạng liên tục được về một điểm). Chẳng hạn $\pi_1(\mathbb{R}^n) = 1$ và $\pi_1(\mathbb{S}^n) = 1$

với $n > 1$. Ví dụ không tầm thường đầu tiên là đường tròn $\mathbb{S}^1$, có thể xem như tập các số phức với môđun bằng 1. Nhóm cơ bản của nó là (đẳng cấu với) $\mathbb{Z}$. Cụ thể, với mỗi số nguyên n, ta xét khuyên f_n cho bởi $f_n(t) = \cos(2n\pi t) + i \cdot \sin(2n\pi t)$, đó là phép cuộn đoạn thẳng thành $|n|$ lần đường tròn (theo chiều dương nếu $n > 0$, theo chiều âm nếu $n < 0$). Một khuyên f tùy ý đồng luân với f_n khi và chỉ khi f quay quanh đường tròn đúng $|n|$ lần với chiều tương ứng với dấu của n.



Hình 6: Nhóm cơ bản của đường tròn.

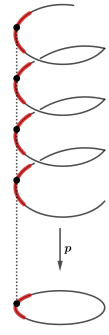
Cuối cùng, $f_n * f_m \sim f_{n+m}$, phép hợp thành của đường tương thích với phép cộng số nguyên, nghĩa là ta có đẳng cấu nhóm $\pi_1(\mathbb{S}^1) = \mathbb{Z}$.

Không gian phủ

Hình 7: Đường tròn là một phủ 4–tờ của chính nó.

Khái niệm gắn liền với nhóm cơ bản là **không gian phủ**. Chẳng hạn, cho số nguyên dương n và xét hàm liên tục $p_n : \mathbb{S}^1 \to \mathbb{S}^1$ cho bởi $p_n(z) = z^n$. Với mỗi điểm $w \in \mathbb{S}^1$, các điểm được p_n biến thành w (các căn bậc n của w) tạo thành **thớ** của p_n tại w. Thớ này gồm n điểm rời rạc. Hơn nữa, nếu ta chọn một lân cận U đủ nhỏ quanh w thì thớ của U gồm n thành phần liên thông rời nhau, mỗi thành phần này là một bản sao của U (cụ thể là p_n cảm sinh một phép đồng phôi từ mỗi thành phần này lên U). Ta gọi một đó là một **phủ n–tờ** hay **phủ bậc n**.

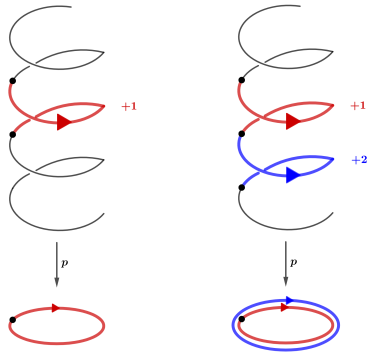
Tổng quát, một phủ của không gian tôpô X được cho bởi một không gian tôpô Y cùng một hàm liên tục $p : Y \to X$ (ta coi X là **không gian nền** nằm dưới, Y là **không gian toàn phần** nằm trên), sao cho mỗi điểm của X đều có một lân cận mà thớ được tạo thành từ một số (có thể vô hạn) bản sao rời rạc. Đây là một điều kiện hoàn toàn địa phương và từ nó không suy ra rằng bản thân Y gồm các bản sao rời rạc của X.



Hình 8: Phủ phổ dụng của đường tròn, cho bởi phép chiếu đường helix trong không gian 3–chiều lên mặt phẳng. Mỗi điểm trên đường tròn đều có một lân cận mà thớ được tạo thành từ các bản sao rời rạc của chính lân cận đó.

Một ví dụ về phủ vô hạn tờ là $p : \mathbb{R} \to \mathbb{S}^1$ cho bởi $p(x) = \cos(2\pi x) + i \cdot \sin(2\pi x)$. Phủ này được gọi là **phủ phổ dụng** của $\mathbb{S}^1$. Tại sao? Vì thông tin của nhóm cơ bản được thể hiện hoàn toàn trên nó. Một tính chất cơ bản của không gian phủ là tính nâng đường: cho một điểm $z \in \mathbb{S}^1$ và một điểm x trên thớ của z, tức là $p(x) = z$. Với một đường bất kỳ $f : I \to \mathbb{S}^1$ xuất phát từ z, ta có thể **nâng** nó thành một đường *duy nhất* $g : I \to \mathbb{R}$ xuất phát từ x, nghĩa là $p(g(t)) = f(t)$ và $g(0) = x$. Chẳng hạn khi f là một khuyên tại z (hay $f(0) = f(1) = z$) thì $g(1)$ cũng nằm trên thớ của z,

điều này tương đương với việc $g(1) - g(0)$ là một số nguyên. Chênh lệch này này hóa ra chính là số vòng quay của khuyên f quanh đường tròn! Đây được gọi là **tác động đơn đạo** của nhóm cơ bản $\pi_1(\mathbb{S}^1)$ lên phủ phổ dụng.



Hình 9: Tác động đơn đạo của nhóm cơ bản: khuyên $f_2(z) = z^2$ trên đường tròn được nâng thành phép tịnh tiến $g(x) = x + 2$ trên phủ phổ dụng.

Như vậy, số vòng quay, vốn là một thông tin bị che mất nếu ta chỉ đơn thuần nhìn vào vết của đường trên không gian nền, đã được phục hồi khi ta nhìn vào không gian phủ.

Định lý cơ bản của lý thuyết không gian phủ nói rằng có một tương ứng $1-1$ giữa các phủ (sai khác tương đương theo một nghĩa nào đó) với các nhóm con của nhóm cơ bản. Trong trường hợp đường tròn, các nhóm con của $\pi_1(\mathbb{S}^1) = \mathbb{Z}$ gồm $n\mathbb{Z}$ với n nguyên dương (nhóm con các số nguyên chia hết cho n), cùng với $\{0\}$. Nhóm $n\mathbb{Z}$ có chỉ số n trong $\mathbb{Z}$ (có n lớp đồng dư modulo $n\mathbb{Z}$), nó ứng với phủ n-tờ $p_n : \mathbb{S}^1 \to \mathbb{S}^1$ cho bởi $p_n(z) = z^n$. Nhóm $\{0\}$ ứng với phủ phổ dụng $p : \mathbb{R} \to \mathbb{S}^1$, một phủ vô hạn tờ (và $\{0\}$ cũng có chỉ số vô hạn trong $\mathbb{Z}$). Và đó là tất cả. Nói riêng, với mỗi n, vì $\mathbb{Z}$ chỉ có đúng một nhóm con với chỉ số n nên $\mathbb{S}^1$ chỉ có đúng một phủ n–tờ (sai khác tương đương).

Mở rộng trường

Lý thuyết về không gian phủ có một sự tương tự kỳ lạ với lý thuyết mở rộng trường của Galois. Để thấy phiên bản số học của đường tròn $\mathbb{S}^1$, ta quay lại với thế giới đại số. Một **trường** là một tập hợp số mà ta có thể làm các phép toán cộng, trừ, nhân, chia. Chính xác hơn, ta có hai phép toán $+$ và $\times$ sao cho chúng thỏa mãn các tiên đề kết hợp, giao hoán, phân phối, có phần tử trung lập 0, có phần tử đơn vị 1, mọi "số" đều có số đối, và mọi số khác 0 đều có nghịch đảo. Các ví dụ quen thuộc nhất là $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Trong khi đó, $\mathbb{Z}$ không phải một trường vì ta không thể làm phép chia $1 \div 2$ (sao kết quả vẫn nằm trong $\mathbb{Z}$).

Một thao tác ta có thể làm với các trường là **mở rộng**: ta kết nạp thêm nghiệm của một đa thức vô nghiệm trong trường ban đầu, và xét tất cả biểu thức thu được bằng cách cộng, trừ, nhân chia với phần tử mới này. Chẳng hạn, ta biết rằng đa thức $x^2 - 2$ không có nghiệm trong $\mathbb{Q}$. Khi kết nạp số thực $\sqrt{2}$, ta thu được tập các số $a + b\sqrt{2}$ với $a, b \in \mathbb{Q}$. Giá trị tại $\sqrt{2}$ của mọi đa thức hệ số hữu tỷ đều có thể viết được dưới dạng này: ta chỉ cần làm phép chia Euclid cho đa thức $x^2 - 2$ (dư sẽ có dạng $a + bx$) rồi thay $x = \sqrt{2}$. Để làm phép chia cho một số $a + b\sqrt{2} \neq 0$, ta chỉ đơn giản làm phép nhân liên hợp với $a - b\sqrt{2}$, vì $a + b\sqrt{2} = \frac{a^2 - 2b^2}{a - b\sqrt{2}}$.

Một câu hỏi mà thoạt nhìn có vẻ lẩm cẩm là "số $\sqrt{2}$ lấy từ đâu ra?". Việc xây dựng số thực từ số hữu tỷ là một thao tác phức tạp và nặng tính giải tích (gần như không hề đại số chút nào). Nhưng nếu ta không quan tâm đến tất cả số thực và chỉ muốn "cái gì đó bình phương lên bằng 2" thì sao? Các nhà đại số rất giỏi trong việc này, họ thêm một phần tử mới hoàn toàn hình thức và tuyên bố rằng nó là nghiệm của đa thức $x^2 - 2$, và ký hiệu nó bởi $\sqrt{2}$. Một kiểu "lý sự cùn": tôi chẳng quan tâm $\sqrt{2}$ đến từ đâu, tôi chỉ cần biết nó thỏa mãn $(\sqrt{2})^2 - 2 = 0$ và tôi cộng trừ nhân chia với nó cứ như thể chẳng có gì xảy ra vậy! Nếu để ý, ta sẽ thấy rằng một khi ta đã gọi một nghiệm là $\sqrt{2}$ thì nghiệm còn lại của $x^2 - 2$

là $-\sqrt{2}$ (đa thức bậc 2 nên chỉ có hai nghiệm này). Theo phong cách của các nhà đại số thì hoàn toàn không có cách nào để phân biệt giữa $\sqrt{2}$ và $-\sqrt{2}$ hết. Cứ chỗ nào có $\sqrt{2}$ thì thay bởi $-\sqrt{2}$, các tính toán vẫn không thay đổi. Để phân biệt hai số này, ta cần một thao mới (so với cộng, trừ, nhân, chia) là *so sánh*. Biết rằng có có hai căn bậc hai của 2 trong $\mathbb{R}$, ta sẽ tuyên bố rằng, số nào lớn hơn 0 thì được gọi là $\sqrt{2}$. Tình trạng tương tự xảy ra khi ta kết nạp vào $\mathbb{R}$ số i và tuyên bố rằng $i^2+1=0$, thứ mà ngày nay ta gọi là **số ảo**. Lúc này, để phân biệt i với $-i$, ta không thể so sánh các số phức được nữa, giải pháp duy nhất là chọn một trong hai căn bậc hai của -1 và gọi nó là i.

Tổng quát hơn, nếu f là một đa thức bất khả quy bậc $n>1$ với hệ số trong một trường K nào đó thì f không có nghiệm trong K (nếu nó có nghiệm $\alpha\in K$ thì nó chia hết cho đa thức $x-\alpha$, trái với giả thiết bất khả quy). Ta tuyên bố một cách hình thức rằng α là một "nghiệm nào đó" của f và kết nạp α vào K. Trường mới thu được, ký hiệu bởi $K(\alpha)$, gồm các tổng (hình thức) có dạng $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$, với $a_i\in K$. Ta cộng và trừ chúng một cách hiển nhiên. Khi làm phép nhân, ta chỉ cần chú ý rằng $f(\alpha)=0$, từ đó α^n cũng có dạng $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$, suy rộng ra thì giá trị tại α của mọi đa thức (bậc tùy ý) với hệ số trong K cũng có dạng này. Để làm phép chia cho một phần tử $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}\neq 0$, ta xét đa thức $g(x)a_0+a_1x+\cdots+a_{n-1}x^{n-1}$. Vì $g(x)\neq 0$ nên g không thể chia hết cho f, hay g và f nguyên tố cùng nhau (giả thiết f bất khả quy được dùng ở đây), nên thuật toán Bézout cho ta các đa thức u, v sao cho $fu+gv=1$, suy ra $g(\alpha)v(\alpha)=1$, hay $v(\alpha)$ chính là nghịch đảo cần tìm của $g(\alpha)$. Mở rộng trường $K(\alpha)/K$ được gọi là một **mở rộng bậc** n.

Trường hữu hạn

Nếu ta xét tập hợp $\mathbb{Z}/n\mathbb{Z}$ các lớp đồng dư modulo n với n là số nguyên dương cho trước, ta có thể làm phép cộng và phép nhân trên chúng một cách hiển nhiên. Thế thì $\mathbb{Z}/n\mathbb{Z}$ là một trường khi và chỉ khi $n=p$ là một số nguyên tố. Ta ký hiệu $\mathbb{Z}/p\mathbb{Z}$ bởi $\mathbb{F}_p$, một trường có p phần tử. Các trường hữu hạn tìm thấy những ứng dụng quan trọng trong lý thuyết bảo mật hiện đại.

Tạm gác lại các ứng dụng của $\mathbb{F}_p$ trong tin học, ta hãy xem chúng có liên hệ gì với tôpô. Ta áp dụng phép mở rộng trường cho trường $\mathbb{F}_p$. Một suy luận đếm bằng hàm sinh và công thức nghịch đảo Möbius đảm bảo rằng với mỗi số nguyên dương n, luôn tồn tại một đa thức f với hệ số trong $\mathbb{F}_p$, bậc n, và bất khả quy. Kết nạp một nghiệm hình thức α của f vào $\mathbb{F}_p$, ta thu được trường mới mà mỗi phần tử được viết duy nhất dưới dạng dạng $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$, với $a_i\in\mathbb{F}_p$. Trường mới này vì thế có p^n phần tử.

Chẳng hạn, với $p=n=2$, đa thức bậc 2 bất khả quy duy nhất trên $\mathbb{F}_2$ là x^2+x+1. Ta tuyên bố rằng α là "cái gì đó" sao cho $\alpha^2+\alpha+1=0$ và kết nạp nó vào $\mathbb{F}_2$. Khi đó ta thu được một trường với 4 phần tử là 0, 1, α, $1+\alpha$. Hai phần tử α và $1+\alpha$ là nghịch đảo của nhau vì $\alpha(1+\alpha)=\alpha^2+\alpha=-1=1$ (ta đang xét modulo 2!), từ đó ta có thể dễ dàng cộng, trừ, nhân, chia trên 4 phần tử này.

Trở lại với trường với p^n phần tử, ta đã thấy rằng nó tồn tại. Ta muốn nó "duy nhất" theo nghĩa: hai trường có p^n phần tử thì **đẳng cấu** với nhau; một đẳng cấu trường là một tương ứng $1-1$ tương thích với các cấu trúc của trường (các phép toán cộng, trừ, nhân, chia, số 0, số 1). Trước hết, bằng một suy luận đại số tuyến tính đơn giản, mỗi trường hữu hạn $\mathbb{F}$ đều phải có số phần tử q là lũy thừa của một số nguyên tố, $q=p^n$ chẳng hạn. Lúc này, $\mathbb{F}$ luôn "chứa" trường $\mathbb{F}_p$, theo nghĩa các phần tử $0,1,2\ldots p-1$ trong $\mathbb{F}$ tạo thành một bản sao đẳng cấu với $\mathbb{F}_p$; ta cộng, trừ, nhân, chia chúng theo modulo p. Khi bỏ đi số 0 khỏi $\mathbb{F}$, ta thu được một nhóm đối với

phép nhân, một nhóm với $q-1$ phần tử. Định lý Lagrange trong lý thuyết nhóm đảm bảo rằng $a^{q-1}=1$ với mọi $a\neq 0$, hay $a^q=a$ với mọi $a\in\mathbb{F}$. Đây là một tổng quát hóa của định lý nhỏ Fermat trong $\mathbb{F}_p$ (vì thực ra cách chứng minh cũng y hệt). Vậy, mọi phần tử của $\mathbb{F}$ đều là nghiệm của đa thức x^q-x, hay $\mathbb{F}$ thu được bằng cách kết nạp tất cả nghiệm của đa thức này vào $\mathbb{F}_p$. Lý thuyết mở rộng trường gọi $\mathbb{F}$ là (một) **trường phân rã** của đa thức x^q-x, và nó đảm bảo rằng trường phân rã là duy nhất sai khác đẳng cấu. Như vậy, với mọi lũy thừa nguyên tố p^n, có duy nhất một trường với p^n phần tử, một mở rộng bậc n của $\mathbb{F}_p$.

Tổng quát hơn, nếu $\mathbb{F}$ là một trường hữu hạn thì với mọi số nguyên dương n, tồn tại duy nhất (sai khác đẳng cấu) một mở rộng bậc n của $\mathbb{F}$. Ta đã từng nói rằng lý thuyết không gian phủ có sự tương tự với lý thuyết mở rộng trường. Hãy nghĩ về các phủ n-tờ như các mở rộng bậc n. Vậy chẳng phải trường hữu hạn $\mathbb{F}$ rất giống đường tròn $\mathbb{S}^1$ ư? Dù trông nó như một sự tình cờ, ta hãy miễn cưỡng lấy quan sát này làm mở đầu cho sự liên hệ giữa tôpô và số học ở phần dưới. Sớm thôi, ta sẽ thấy rằng nó cũng không ngẫu nhiên lắm đâu.

Lược đồ

Bây giờ, hãy dạo qua thế giới hình học đại số một chút. Với ý tưởng tiên phong của Descartes là nghiên cứu các đối tượng hình học bằng các hệ tọa độ và phương trình đa thức, người ta đã dần dần phát triển hình học đại số. Khác với những người bạn bên tôpô học, các nhà hình học đại số nghiên cứu các đối tượng cứng nhắc hơn: tập nghiệm của các hệ phương trình đa thức. Sau một thời gian, giới toán học nhận ra rằng các trực giác hình học thường mang đến các chứng minh không chặt chẽ và đặc biệt là không giúp gì được ở số chiều cao hơn. Họ đã chuyển sang dùng đại số giao hoán làm công cụ chính để nghiên cứu hình học. Grothendieck, nhà toán học được công nhận rộng rãi là có ảnh hưởng nhất thế kỷ XX, đã cách mạng hóa hình học đại số một lần nữa bằng định nghĩa **lược đồ**.

Ta quay lại với khái niệm trường. Nếu bỏ qua việc luôn làm được phép chia, ta thu được khái niệm **vành**. Chẳng hạn, $\mathbb{Z}$ và $\mathbb{Z}/n\mathbb{Z}$ là các vành (phép cộng và phép nhân được hiểu theo nghĩa hiển nhiên). Chú ý rằng ta vẫn yêu cầu làm được phép trừ, nên $\mathbb{N}$ không phải là một vành. Với mỗi vành R, ta xây dựng được một không gian tôpô $\mathrm{Spec}(R)$, được gọi là **phổ** của R. Nếu chỉ nhìn $\mathrm{Spec}(R)$ như một không gian thì ta mất rất nhiều thông tin. Chẳng hạn, phổ của một trường luôn là một điểm. Vì thế, người ta đã làm giàu $\mathrm{Spec}(R)$ một cấu trúc gọi là **bó**, chúng làm cho $\mathrm{Spec}(R)$ trở thành một lược đồ.

Cũng như việc người ta quan tâm đến các hàm liên tục giữa các không gian tôpô, trong hình học đại số người ta quan tâm đến các **cấu xạ** giữa các lược đồ. Một cấu xạ $\mathrm{Spec}(R)\to\mathrm{Spec}(S)$ đơn giản được cho bởi một **đồng cấu vành** theo chiều ngược lại $f:S\to R$, đồng cấu ở đây nghĩa là $f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$ và $f(1)=1$. Chẳng hạn, $\mathbb{Z}$ là một vành con của $\mathbb{Q}$, và phép bao hàm $\mathbb{Z}\to\mathbb{Q}$ cho ta một cấu xạ $\mathrm{Spec}(\mathbb{Q})\to\mathrm{Spec}(\mathbb{Z})$. Về mặt tôpô thì $\mathrm{Spec}(\mathbb{Q})$ chỉ có một điểm, nên ảnh của cấu xạ này là một điểm của $\mathrm{Spec}(\mathbb{Z})$, được gọi là **điểm tổng quát**. Với mỗi số nguyên tố p, phép lấy dư modulo $p:\mathbb{Z}\to\mathbb{F}_p$ cho ta một cấu xạ $\mathrm{Spec}(\mathbb{F}_p)\to\mathrm{Spec}(\mathbb{Z})$, đó là một **điểm đóng**. Các điểm đóng này và điểm tổng quát tạo nên không gian $\mathrm{Spec}(\mathbb{Z})$. Khác với các không gian Euclid, tôpô trên lược đồ $\mathrm{Spec}(\mathbb{Z})$ rất thô: điểm tổng quát là một điểm nhưng lại trù mật trong cả không gian (người ta hay nói "điểm tổng quát là điểm nằm ở mọi nơi, nhưng không nằm cụ thể ở đâu cả").

Quay lại với lý thuyết không gian phủ. Khi áp dụng nó cho lược đồ, ta không thể chỉ xét khía cạnh tôpô ngây thơ được. Ta muốn

$\mathrm{Spec}(\mathbb{F}_p)$ giống với đường tròn $\mathbb{S}^1$, nhưng $\mathrm{Spec}(\mathbb{F}_p)$ lại chỉ có một điểm. Vấn đề với không gian tôpô $\mathrm{Spec}(R)$ là nó có quá ít lân cận, mỗi lân cận đều quá lớn. Cách khắc phục là sáng tạo ra một khái niệm tôpô mới dùng được cho các lược đồ (thứ mà ngày nay gọi là tôpô Grothendieck), với các "lân cận" mới. Một trong những loại tôpô đủ mạnh để phân biệt các "không gian 1 điểm" $\mathrm{Spec}(K)$ (với K là các trường) là **tôpô étale**. Từ "étale" được lấy từ văn học Pháp, mang nghĩa nôm na là trạng thái dịu dàng của biển. Với công cụ mới này, người ta định nghĩa được khái niệm nhóm cơ bản étale của lược đồ. Chẳng hạn, nhóm cơ bản étale của $\mathrm{Spec}(\mathbb{F}_p)$ là một nhóm có cùng họ hàng với $\mathbb{Z}$, gọi là "$\mathbb{Z}$ mũ". Điều này giải thích vì sao việc coi $\mathrm{Spec}(\mathbb{F}_p)$ như đường tròn $\mathbb{S}^1$ là hợp lý. Tương tự, khái niệm phủ trong thế giới lược đồ phải được hiểu là phủ étale. Đối với các trường, một phủ étale của $\mathrm{Spec}(K)$ đơn giản là $\mathrm{Spec}(L)$, với L/K là một mở rộng bậc hữu hạn. Như vậy, dù $\mathrm{Spec}(K)$ về mặt tôpô chỉ một 1 điểm, nó lại có nhóm cơ bản étale không tầm thường, hay có rất nhiều phủ.

Thực ra khái niệm mở rộng trường và mở rộng vành còn cho ta thêm một chút bên phía tôpô, nó ứng với khái niệm **phủ phân nhánh**. Nói nôm na, một phủ phân nhánh bậc n là một hàm liên tục $p : Y \to X$ sao cho nếu bỏ đi một số hữu hạn điểm của X (và các điểm của Y nằm trên chúng) thì ta thu được một phủ n-tờ. Các điểm bỏ đi kia (cùng các điểm nằm trên) gọi là các **điểm rẽ nhánh** của p. Hiện tượng rẽ nhánh là phiên bản hình học của hiện tượng "nghiệm bội" trong đại số. Ta xét ví dụ khi Y là đường cong elliptic cho bởi phương trình $y^2 = x(x-1)(x-2)$ trong $\mathbb{C}^2$ và $X = \mathbb{C}$. Lấy p là phép chiếu lên trục hoành, $p(x,y) = x$. Khi bỏ đi các điểm $0,1,2$ khỏi X (và các điểm $(0,0),(1,0),(2,0)$ khỏi Y), ta thu được một phủ 2–tờ: với mỗi $x \neq 0,1,2$ thì phương trình $y^2 = x(x-1)(x-2)$ có hai nghiệm phức phân biệt. Ở các điểm $0,1,2$ xảy ra hiện tượng rẽ nhánh, phương trình $y^2 = 0$ có nghiệm kép $y = 0$. Ta nói rằng **chỉ số rẽ nhánh** của p tại các điểm $(0,0),(1,0),(2,0)$ bằng 2.

Lý thuyết số đại số

Để tìm hiểu các phủ (étale) phân nhánh của lược đồ $\mathrm{Spec}(\mathbb{Z})$, ta bắt đầu từ điểm tổng quát: Phủ étale của $\mathrm{Spec}(\mathbb{Q})$ thì có dạng $\mathrm{Spec}(K)$, với $K = \mathbb{Q}(\alpha)$, và α là nghiệm của một đa thức bậc n bất khả quy với hệ số hữu tỷ. Số α như vậy được gọi là một **số đại số**, chẳng hạn $\sqrt{2}, \sqrt[3]{2}, \frac{1+\sqrt{-3}}{2}$ là các số đại số. Trường K được gọi là một **trường số**, và mọi phần tử của nó đều là số đại số. Ta muốn thứ gì đó trong K đóng vai trò như các số nguyên đối với số hữu tỷ. Đó là các **số nguyên đại số**. Chúng là những phần tử của K mà là nghiệm của một đa thức với hệ số nguyên và hệ số đầu bằng 1. Chẳng hạn $\sqrt{2}$ là một số đại số vì nó là nghiệm của $x^2 - 2$. $\frac{1+\sqrt{5}}{2}$ cũng là một số nguyên đại số (dù trông không có vẻ vậy) vì nó là nghiệm của $x^2 - x - 1$. Các số nguyên đại số trong K tạo thành một vành $\mathcal{O}$. Việc chuyển từ $\mathbb{Z}$ sang $\mathcal{O}$ là chuyển từ lý thuyết số sơ cấp sang lý thuyết số đại số. Một bài tập đơn giản (bằng cách dùng phân tích duy nhất ra thừa số nguyên tố) là: Các số nguyên đại số trong $\mathbb{Q}$ chính là các số nguyên theo nghĩa cổ điển.

Lý thuyết số đại số xuất phát từ nỗ lực chứng minh định lý lớn Fermat của Cauchy, Lamé... Ý tưởng như sau: với phương trình $x^2 + y^2 = z^2$ chẳng hạn, ta giải bằng cách đưa về $x^2 = z^2 - y^2 = (z-y)(z+y)$, sau đó lập luận (với phân tích duy nhất ra thừa số nguyên tố) rằng $z-y$ và $z+y$ phải là các số chính phương. Bây giờ, xét phương trình $x^p + y^p = z^p$, với p là số nguyên tố lẻ (dễ thấy ta chỉ cần xét trường hợp này). Để phân tích triệt để $z^p - y^p$ thành các nhân tử bậc nhất, ta buộc phải dùng căn bậc p phức của 1. Gọi nó là $\zeta = \cos(\frac{2\pi}{p}) + i \cdot \sin(\frac{2\pi}{p})$. Thế thì ζ là một

số nguyên đại số (nghiệm của phương trình $x^p - 1$). Và như vậy ta đưa về chứng minh rằng phương trình trên không có nghiệm trong vành mới $\mathbb{Z}[\zeta]$, vành các số nguyên đại số của $\mathbb{Q}(\zeta)$. Sơ hở của cách tiếp cận này là lập luận như trong trường hợp $p = 2$ không còn đúng nữa, vì nói chung không có phân tích duy nhất ra thừa số nguyên tố trong $\mathbb{Z}[\zeta]$.

Một ví dụ về sự thiếu sốt của phân tích duy nhất là trường số $K = \mathbb{Q}(\sqrt{-5})$. Vành số nguyên đại số của nó là $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, gồm các số có dạng $a + b\sqrt{-5}$ với $a, b \in \mathbb{Z}$. Số 6 có thể phân tích thành $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (-\sqrt{-5})$. Để thấy rằng hai phân tích này là triệt để và thực sự khác nhau, ta định nghĩa **chuẩn** của một số $a + b\sqrt{-5}$ bởi $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Đây là một số tự nhiên, và ta thấy ngay rằng $N(xy) = N(x)N(y)$. Trong phân tích $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (-\sqrt{-5})$, ta có $N(2) = 4, N(3) = 9, N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, nên các nhân tử xuất hiện ở hai phân tích thực sự khác nhau. Ngoài ra, về cơ bản ta không thể phân tích thêm được nữa, vì không có phần tử nào có chuẩn bằng 2 hoặc 3 (một tính toán số học đơn giản cho thấy rằng phương trình các $a^2 + 5b^2 = 2$ và $a^2 + 5b^2 = 3$ đều không có nghiệm nguyên). Điều này cho thấy sự thiếu sót của phân tích duy nhất ra thừa số nguyên tố trong $\mathbb{Z}[\sqrt{-5}]$.

Sự sụp đổ của phân tích duy nhất trong $\mathcal{O}$ đã chấm dứt hi vọng chứng minh định lý lớn Fermat bằng lý thuyết số đại số cổ điển. Dù vậy, vành $\mathcal{O}$ vẫn giữ được một tính chất của vành $\mathbb{Z}$; nó là một **vành Dedekind**. Thay vì phân tích duy nhất của các số, người ta định nghĩa khái niệm **số lý tưởng** (cái mà ngày nay gọi là **iđêan**). Đại khái nó là thứ gì đó cho phép nói về quan hệ chia hết cũng như làm phép nhân. Việc $\mathcal{O}$ là vành Dedekind có nghĩa là mọi số lý tưởng đều phân tích một cách duy nhất ra các số lý tưởng nguyên tố. Một số nguyên đại số $a \in \mathcal{O}$ định nghĩa một số lý tưởng (a), được gọi là một số lý tưởng chính. Hai số a và b định nghĩa cùng một số lý tưởng nếu chúng **liên kết**, nghĩa là $a|b$ đồng thời $b|a$. Nói riêng, nếu là $u|1$ thì $(u) = (1)$. Nếu tất cả số lý tưởng nguyên tố đều có dạng trên thì $\mathcal{O}$ có phân tích duy nhất của các số (thực sự). Điều này không đúng trong $\mathbb{Z}[\sqrt{-5}]$; cụ thể là khi phân tích $(6) = (2) \cdot (3) = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, ta vẫn phân tích được tiếp: $(2) = \mathfrak{p}_1\mathfrak{p}_2$, $(3) = \mathfrak{p}_3\mathfrak{p}_4$, $(1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$, $(1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4$, trong đó $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ là các số lý tưởng nguyên tố *không chính*. Chuẩn của chúng lần lượt là $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 2$ và $N(\mathfrak{p}_3) = N(\mathfrak{p}_4) = 3$. Như vậy ta có phân tích duy nhất của (6) thành các số lý tưởng.

Cũng như mỗi số nguyên tố p ứng với các điểm đóng $\mathrm{Spec}(\mathbb{F}_p) \to \mathrm{Spec}(\mathbb{Z})$, mỗi số lý tưởng nguyên tố $\mathfrak{p}$ trong trong $\mathcal{O}$ cho ta một trường hữu hạn $\mathbb{F}_\mathfrak{p}$ (gọi là **trường thặng dư** của $\mathfrak{p}$), cùng một điểm đóng $\mathrm{Spec}(\mathbb{F}_\mathfrak{p}) \to \mathrm{Spec}(\mathcal{O})$. Cùng với điểm tổng quát $\mathrm{Spec}(K)$, chúng tạo thành lược đồ $\mathrm{Spec}(\mathcal{O})$. Vì $\mathbb{Z}$ là một vành con của $\mathcal{O}$, ta có một cấu xạ $\mathrm{Spec}(\mathcal{O}) \to \mathrm{Spec}(\mathbb{Z})$, một phủ étale phân nhánh. Mỗi số nguyên tố p trong $\mathbb{Z}$ có thể không còn là số lý tưởng nguyên tố trong $\mathbb{O}$, nó phân rã thành tích của một số hữu hạn số lý tưởng nguyên tố, $(p) = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$. Các số lý tưởng nguyên tố xuất hiện trong phân tích trên chính xác là những điểm của $\mathrm{Spec}(\mathcal{O})$ nằm trên điểm đóng của $\mathrm{Spec}(\mathbb{Z})$ ứng với p. Hiện tượng phân nhánh nhánh xảy ra nếu có một số lý tưởng $\mathfrak{p}_i$ xuất hiện nhiều lần trong phân tích trên, ta gọi đó số lần đó là **chỉ số rẽ nhánh** của $\mathfrak{p}_i$, nó đóng vai trò như chỉ số rẽ nhánh trong tôpô cổ điển.

Một bất đẳng thức trong lý thuyết số đại số, *chặn Minkowski*, cho phép xác định cụ thể phân tích trên. Hơn thế nữa, nó còn cho ta biết chính xác khi nào thì một số nguyên tố p rẽ nhánh trong $\mathcal{O}$. Một hệ quả của nó là với mọi trường số K, luôn có ít nhất một số nguyên tố p rẽ nhánh trong vành $\mathcal{O}$ các

số nguyên đại số trong K, nghĩa là $\mathrm{Spec}(\mathbb{Z})$ không có phủ étale không rẽ nhánh nào ngoài phủ tầm thường (cho bởi ánh xạ đồng nhất $\mathbb{Z} \to \mathbb{Z}$), hay nó là đơn liên.

Nút

Trong thế giới của các không gian tôpô thì có rất nhiều không gian đơn liên, và ta muốn tìm cái nào giống với $\mathrm{Spec}(\mathbb{Z})$. Sự đột phá nằm ở các phát hiện sau đây của Mumford, Manin, và sau này là Mazur. Ở phía tôpô, các khái niệm điểm (0–chiều), đường (1–chiều), mặt (2–chiều) được tổng quát lên thành các đa tạp. Một đa tạp 3–chiều là một không gian tôpô mà nhìn địa phương thì giống như không gian Euclid $\mathbb{R}^3$ (cũng như bề mặt trái đất là một đa tạp 2–chiều, nhìn địa phương thì giống như mặt phẳng).

Bên cạnh nhóm cơ bản, tôpô đại số cổ điển còn cung cấp các bất biến đại số khác cho các không gian tôpô, gọi là các **nhóm đồng điều**. Nhóm đồng điều bậc n của một đa tạp X được xây dựng như sau: Xét các tổ hợp tạo thành từ một số đa tạp con n–chiều (chúng được gọi là các **n-dây chuyền**). Nếu chúng tạo thành một vòng kín, ta gọi nó là một **n–chu trình**. Nếu nó tạo thành biên của một đa tạp con $(n+1)$–chiều, ta gọi nó là một **n–biên**. Một n–biên thì luôn là một n–chu trình. Nhóm $H_n(X)$ được định nghĩa là chênh lệch giữa các nhóm các n–chu trình và nhóm các n–biên: một n–chu trình mà không phải n–biên thì nó bao quanh một "lỗ thủng" $(n+1)$–chiều; như vậy các nhóm đồng điều phát hiện các lỗ thủng trên X. Phiên bản đối ngẫu của đồng điều là **đối đồng điều**, các nhóm $H^n(X)$. Về cơ bản thì chúng cũng phát hiện các lỗ thủng. Về mặt kỹ thuật thì chúng dễ tính toán hơn đồng điều một chút, đồng thời có nhiều cấu trúc hơn. *Đối ngẫu Poincaré* nói rằng nếu X là một đa tạp đóng, khả định hướng, d–chiều, thì ta có một đối ngẫu hoàn hảo giữa hai nhóm $H^{d-i}(X)$ và $H^i(X)$ với mỗi $i = 0, 1, \ldots, d$.

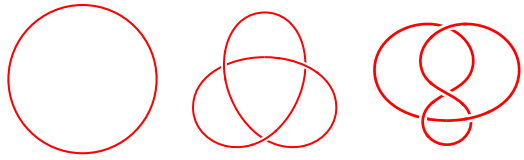
Với các lược đồ, các nhóm đối đồng điều nhìn chung không cho thông tin gì (phần lớn chúng bằng 0) khi ta tính theo tôpô thông thường. Một lần nữa nhờ công của Grothendieck, ta có thể tính đối **đồng điều étale**. Trên một trường, chúng được gọi là đối **đồng điều Galois**, một công cụ đã được dùng từ lâu trước đó trong số học. Với các trường hữu hạn, đối đồng điều Galois của chúng rất đơn giản, chúng khác 0 ngoài bậc 0 và 1, và ta có một đối ngẫu hoàn hảo giữa các nhóm đối đồng điều ở hai bậc này. Điều này tương tự với đối ngẫu Poincaré cho các đa tạp 1–chiều, khẳng định thêm niềm tin rằng phổ của trường hữu hạn là phiên bản đại số của đường tròn.

Đối với các lược đồ $\mathrm{Spec}(\mathscr{O})$, với $\mathscr{O}$ là vành số nguyên đại số của một trường số K nào đó, các nhóm đối đồng điều étale thỏa mãn đối ngẫu giữa bậc 0 và bậc 3 cũng như bậc 1 và bậc 2. Các kết quả này được gọi là *đối ngẫu Artin–Verdier*, được khám phá khi áp dụng đối đồng điều étale cho lý thuyết trường các lớp toàn cục, một phần của lý thuyết số. Điều này gợi cho ta rằng phiên bản tôpô của $\mathrm{Spec}(\mathscr{O})$ "nên" là các đa tạp 3–chiều. Vậy $\mathrm{Spec}(\mathbb{Z})$ ứng với đa đạp đóng 3–chiều nào? Ta thấy ở trên rằng $\mathrm{Spec}(\mathbb{Z})$ đơn liên, và đa tạp đóng 3–chiều đơn liên thì chỉ có thể đồng phôi với mặt (siêu) cầu $\mathbb{S}^3$! Đó là nội dung của *giả thuyết Poincaré*, bài toán duy nhất đã được giải trong 7 bài toán thiên niên kỷ. Tác giả của lời giải, thiên tài lập dị Perelman, đã từ chối cả Huy chương Fields lẫn Giải Breakthrough cho công trình vô song của mình.

Sau khi bỏ ra rất nhiều công sức, ta đã thấy được cầu nối mong manh giữa tôpô, rằng phiên bản số học của $\mathbb{S}^1$ là (phổ của) một trường hữu hạn, và của một đa tạp đóng 3–chiều là vành các số nguyên đại số của một trường số. Bây giờ là lúc chúng ta thu hoạch kết quả, chiêm ngưỡng những sự tương tự đáng ngạc nhiên dựa trên cầu nối này. Một số lý tưởng nguyên tố $\mathfrak{p}$ trong $\mathscr{O}$ cho ta một

phép nhúng $\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathscr{O})$. Về phía tôpô, ta xét các phép nhúng $\mathbb{S}^1 \hookrightarrow M$, với M là một đa tạp (đóng, khả định hướng) 3-chiều. Chúng được gọi là các **nút** trong M. Nói riêng, phiên bản tôpô của mỗi số nguyên tố p (với phép nhúng tương ứng $\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$) là một nút trong $\mathbb{S}^3$ (ta sẽ tập trung vào các nút này). Từ một định lý sâu sắc trong tôpô học, *định lý Borsuk–Ulam*, ta có thể chỉ ra rằng một phép nhúng như thế không thể là toàn ánh, nghĩa là ta có thể xem một nút như một phép nhúng từ $\mathbb{S}^1$ vào $\mathbb{S}^3$ bỏ đi một điểm, nói cách khác chính là không gian Euclid $\mathbb{R}^3$.

Để biểu diễn một nút $K : \mathbb{S}^1 \hookrightarrow \mathbb{R}^3$ ta có thể chiếu nó lên một mặt phẳng sao cho tại mỗi điểm giao nhau chỉ có đúng 2 đường đi qua. Chúng ứng với một **sợi trên** và một **sợi dưới**, ta biểu diễn sợi dưới bằng nét đứt tại giao điểm đó. Đó là một **biểu đồ phẳng** của nút.



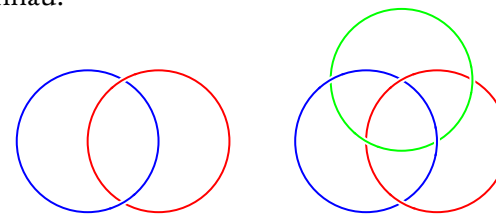
Hình 10: Biểu đồ phẳng của nút tầm thường, nút ba lá, và nút số 8.

Tất nhiên, mọi nút đều đồng phôi với $\mathbb{S}^1$. Ta cần cả thông tin về phép nhúng $\mathbb{S}^1 \to \mathbb{R}^3$ để phân biệt các nút với nhau. Các nhà lý thuyết nút gọi sự giống nhau của các nút là **đẳng luân**. Một cách trực giác, hai nút đẳng luân nếu ta có thể tháo dỡ một nút rồi buộc thành nút còn lại (mà không cắt được cắt nút ra). Hóa ra, hai nút đẳng luân khi và chỉ khi phần bù của chúng trong $\mathbb{S}^3$ đồng phôi với nhau (*định lý Gordon–Luecke*).

Từ điển M^{2}KR

Từ điển Mazur–Morishita–Kapranov–Reznikov (M^{2}KR) là một danh sách những sự tương tự giữa lý thuyết số và hình học của các đa tạp 3–chiều; ở đó các số lý tưởng tưởng ứng với các liên kết, các số lý tưởng nguyên tố ứng với các nút. Sau đây là một số tương ứng giữa tôpô và số học trong từ điển này.

Mỗi số lý tưởng trong $\mathscr{O}$ phân tích thành tích của các số lý tưởng nguyên tố. Phiên bản tôpô của số lý tưởng là **liên kết**: một liên kết trong một đa tạp đóng 3–chiều M là một phép nhúng từ một số hữu hạn bản sao rời rạc của $\mathbb{S}^1$ vào M. Các ví dụ về liên kết trong $\mathbb{S}^3$ là **liên kết Hopf** và **vòng Borromean**, lần lượt được tạo bởi 2 và 3 nút tầm thường lồng nhau.

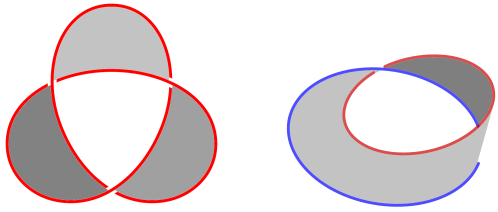


Hình 11: Biểu đồ phẳng của liên kết Hopf và vòng Borromean.

Để thêm phần thuyết phục rằng tại sao M lại tương ứng với (vành số nguyên đại số) một trường số, ta nhắc đến *định lý Alexander*: Mọi đa tạp đóng 3–chiều đều là một phủ phân nhánh của $\mathbb{S}^3$, trong đó các điểm rẽ nhánh trong $\mathbb{S}^3$ tạo thành một liên kết. Tương tự, một mở rộng L/K của trường số có thể được coi như một phủ phân nhánh giữa hai đa tạp đóng 3–chiều.

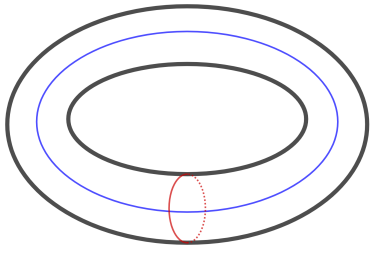
Một số nguyên đại số $a \in \mathscr{O}$ ứng với một mặt compact S (có thể có biên) nhúng trong đa tạp đóng 3–chiều M. Số lý tưởng chính (a) ứng với biên ∂S, đây là một liên kết, và chúng ứng với các 1–đối biên, tức là phần tử 0 trong nhóm đồng điều $H_1(M)$. Các số lý tưởng khác tương ứng với các liên kết, chúng là các 1–chu trình mà không phải biên, đại diện cho các phần tử không tầm thường của $H_1(M)$. Ta biết rằng trong $\mathbb{Z}$ có phân tích duy nhất ra thừa số nguyên tố, hay mọi số lý tưởng nguyên tố đều là số lý tưởng chính. Tương ứng, với $M = \mathbb{S}^3$, ta có $H_1(M) = 0$ (vì $\mathbb{S}^3$ không có lỗ thủng 2–chiều nào), nghĩa là mọi liên kết đều là biên của một mặt nào

đó. Seifert đã đưa ra một thuật toán khá đơn giản để xây dựng một mặt với biên cho trước. Chẳng hạn, **mặt Seifert** của liên kết Hopf chính là *mặt Möbius*.



Hình 12: Mặt Seifert của nút ba lá và của liên kết Hopf (mặt Möbius).

Sự tương tự tiếp theo: với p là một số nguyên tố, ta xét vành $\mathbb{Z}_p$ các số nguyên p–adic cũng như trường $\mathbb{Q}_p$ các số p–adic. So với $\mathrm{Spec}(\mathbb{Z})$, phổ $\mathrm{Spec}(\mathbb{Z}_p)$ chỉ còn 2 điểm là điểm tổng quát $\mathrm{Spec}(\mathbb{Q}_p)$ và điểm đóng $\mathrm{Spec}(\mathbb{F}_p)$, vì thế ta gọi thao tác này **địa phương hóa** (tập trung nhìn vào số nguyên tố p và quên đi các số nguyên tố khác). Thao tác này ứng với việc lấy **lân cận ống** V của nút, kết quả thu được là một hình xuyến đặc. Dù hình xuyến đặc không đồng phôi với đường tròn, chúng **tương đương đồng luân với nhau**, điều này ứng với việc $\mathrm{Spec}(\mathbb{Z}_p)$ và $\mathrm{Spec}(\mathbb{F}_p)$ **tương đương đồng luân étale với nhau**. Khi bỏ nút ban đầu khỏi V, ta thu được một không gian tương đương đồng luân với mặt xuyến (rỗng). Nhóm cơ bản của mặt xuyến là $\mathbb{Z} \times \mathbb{Z}$, một nhóm được sinh bởi hai phần tử là hai khuyên như trong Hình 13.

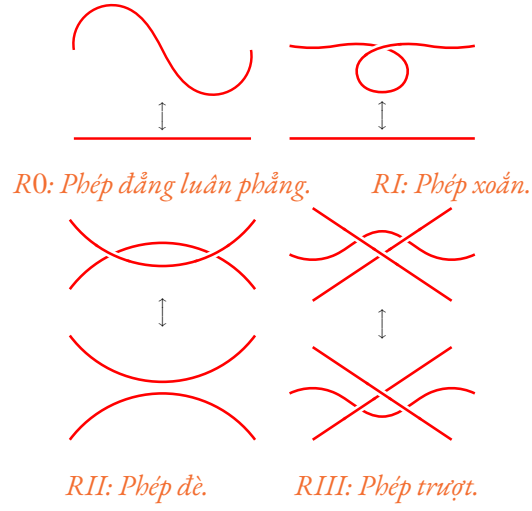


Hình 13: Nhóm cơ bản của mặt xuyến được sinh bởi hai khuyên màu xanh và màu đỏ.

Tương ứng, khi bỏ $\mathrm{Spec}(\mathbb{F}_p)$ khỏi $\mathrm{Spec}(\mathbb{Z}_p)$, ta thu được $\mathrm{Spec}(\mathbb{Q}_p)$, và **nhóm Galois rẽ nhánh yếu** (một phiên bản nhỏ hơn của nhóm cơ bản étale) của $\mathbb{Q}_p$ cũng được mô tả bởi 2 phần tử sinh. Sau cùng, lý thuyết trường các lớp địa phương của Tate cho ta các đối ngẫu hoàn hảo giữa đối đồng điều Galois của $\mathbb{Q}_p$ ở bậc 0 và bậc 2, cũng như ở bậc 1 và chính nó. Tương ứng, ta có đối ngẫu Poincaré cho mặt xuyến, một đa tạp đóng 2–chiều.

Thao tác trên biểu đồ phẳng

Quay lại với sự đẳng luân của các nút. Một câu hỏi rất tự nhiên là làm thế nào để chứng minh hai nút không đẳng luân? Đẳng luân vốn là một điều kiện tôpô quá khó sử dụng. Một khó khăn khi sử dụng các biểu đồ phẳng là hai nút đẳng luôn có thể cho hai biểu đồ phẳng trông rất khác nhau. Vậy vấn đề đầu tiên là ta cần tìm cách phân biệt hai nút qua biểu đồ phẳng của chúng (bài toán nhận biết nút). Điều này có thể được thực hiện một cách tổ hợp. Cụ thể, hai biểu đồ phẳng biểu diễn hai nút đẳng luân khi và chỉ khi tồn tại một chuỗi hữu hạn các thao tác thuộc một trong 4 kiểu, được gọi là các **chuyển động Reidemeister**.



Hình 14: Các chuyển động Reidemeister.

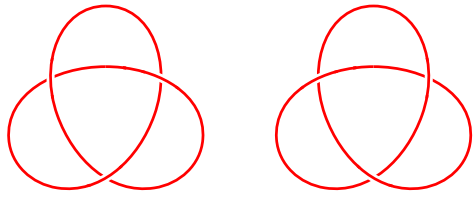
Từ biểu đồ phẳng của nút, ta dùng các đại lượng không đổi qua các biến đổi Reidemeister, các **bất biến nút**. Hai nút có bất biến khác nhau thì phải khác nhau. Một

ví dụ như vậy là **bất biến tô màu**. Ta nói một biểu đồ phẳng của nút là **tô được bằng 3 màu** nếu mỗi sợi (phần đường cong liên tục giữa hai giao điểm liên tiếp của nút) đều có thể tô được bằng một trong 3 màu cho trước, sao cho

- ít nhất hai màu phải được dùng;
- tại mỗi giao điểm, sợi trên cùng 2 sợi dưới hoặc là được tô cùng màu, hoặc là được tô 3 màu khác nhau.

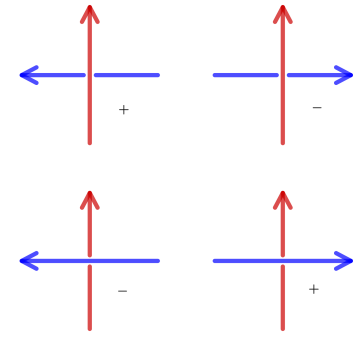
Ví dụ, nút ba lá hiển nhiên tô được bằng 3 màu, nút tầm thường hiển nhiên không tô được bằng 3 màu. Nút số 8 cũng không tô được bằng 3 màu. Vậy ít nhất ta biết rằng nút 3 lá không đẳng luân với nút tầm thường cũng như nút số 8.

Hiển nhiên là bất biến tô màu chỉ cho phép phân loại các nút thành 2 lớp. Ta cần các loại bất biến khác. Ví dụ, xét nút ba lá trái và ảnh gương của nó là nút ba lá phải. Tất nhiên cả hai đều tô được bằng 3 màu. Rất ngạc nhiên, hai nút này không đẳng luân! Hãy thử dùng các biến đổi Reidemeister để gỡ nút này thành nút kia và bạn sẽ sớm bị thuyết phục. Một bất biến cho phép phân biệt hai nút này là **đa thức Alexander**. Đa thức này đến từ *lý thuyết Alexander–Fox*, và người ta phát hiện ra phiên bản số học của nó là *lý thuyết Iwasawa*. Sự song song của chúng cho phép ta dịch các kết quả từ một bên sang bên còn lại.



Hình 15: Nút ba lá trái và nút ba lá phải.

Một kiểu bất biến khác cho liên kết là **số liên kết**. Xét một liên kết được tạo bởi hai nút. Giữa hai nút L và K, ta có thể định nghĩa **số liên kết** qua biểu đồ phẳng của chúng như sau. Chẳng hạn, tô màu đỏ cho L và màu xanh cho K, đồng thời định hướng cho chúng (mỗi nút có thể có 1 trong 2 hướng). Tại các điểm trên biểu đồ phẳng mà có một sợi của nút này nằm trên một sợi của nút kia hoặc ngược lại, ta đánh dấu $+$ hoặc $-$ theo quy tắc ở Hình 16. Sau đó ta lấy số dấu cộng trừ đi số dấu trừ, và lấy kết quả chia đôi. Kết quả cuối cùng thu được được gọi là số liên kết $\mathrm{lk}(L,K)$. Chẳng hạn, số liên kết của hai nút trong liên kết Hopf là 1 hoặc -1, tùy theo cách định hướng hai nút.



Hình 16: Quy tắc tính số liên kết.

Nhiều tính toán cho thấy rằng số liên kết thỏa mãn các tính chất tương tự như **ký hiệu Legendre** $\left(\frac{p}{q}\right)$ giữa hai số nguyên tố p,q trong lý thuyết thặng dư bậc hai. Ta có thể chứng minh rằng $\mathrm{lk}(K,L)=\mathrm{lk}(L,K)$. Tương ứng, ta có luật tương hỗ bậc hai, nói rằng

$$\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right).$$

Bài toán trung tâm của tôpô số học có lẽ là câu hỏi tự nhiên nhất: số nguyên tố nào ứng với nút nào? Đây vẫn là một câu hỏi mở. Nếu một ngày người ta xây dựng được một tương ứng $1-1$ tốt giữa chúng, theo nghĩa mỗi kết quả với số nguyên tố thì ta có kết quả với các nút tương ứng, một số lượng khổng lồ bài toán tôpô học sẽ được giải bằng các kết quả tương tự ở lý thuyết số, và ngược lại. Có thể nói, tôpô số học là một trong những ví dụ điển hình nhất về tư tưởng toán học thống nhất, rằng tất cả những đại số, giải tích, hình học, số học... đều chỉ là một.