算术动力系统——代数数论专题 VI

October 28, 2022

0、前言

所谓动力系统，即研究一个 (满足某些性质的) 空间在某些变换迭代作用下的演化行为. 特别地，研究概率空间上保测变换的迭代则是遍历论的主要课题，它主要反映系统演化的“统计学”性质. 本讲义中，我们主要介绍遍历论与动力系统的基本内容——包括 (多重) 回复性、遍历性、不变 (遍历) 测度、熵、临界点和周期点、Julia 集和 Fatou 集等；然后把它们应用到数论的背景当中——我们将介绍 Van der Waerden 定理、Szemerédi 定理、Borel 正规数定理、Hopf 定理、Weyl 定理等具体例子.

算术动力学是代数数论与动力系统交叉的领域. 例如 Margulis 关于不定二次型的工作，他将整点的逼近问题转化为齐性空间的纯拓扑问题，并用动力系统的思路证明了 Oppenheim 猜想. 而在算术几何领域，我们可以考虑某种与 Adele 群类似的紧群 (Solenoid，笔者将它译为“线圈”) 或其变体上的变换，用该系统演化的熵来解释椭圆曲线的 Néron-Tate 高度，从而引出约化理论的局部动力学解释. 此外，著名的 Collatz 猜想猜测对任何正整数而言，若是奇数则乘 3 加 1，若是偶数则除以 2，不断进行这样的操作最后总会掉入 $\{1,4,2\}$ 循环的“黑洞”(Attractor，吸引子) 中，而最近关于这方面的很多工作都是基于动力学的. 这些内容预示着动力系统和数论有许多更深层次的联系，关于这方面的研究方兴未艾，笔者仅作综述.

本文的综合性很强，阅读本文需要大量分析、代数、几何、拓扑、数论等预备知识，甚至了解一些物理也会对理解本文有一定帮助. 本文各节的内容相对独立，大致上可以分为 4 个专题：遍历论及其应用 (第 1-4 节)、Oppenheim 猜想 (第 5 节)、熵与高度 (第 6-9 节)、模空间动力系统 (第 10-12 节).

本文为首师大 2021 秋季学期动力系统讨论班的讲稿，受到孙善忠、徐飞、唐舜、方江学、范祐维、谢俊逸、刘志远、孟云鹏、邓子房等人的支持，其中邓子房主要负责本文第 9 节的撰写. 笔者在此感谢他们.

参考文献

[1] J.H. Silverman. The Arithmetic of Dynamical Systems(GTM241). Springer.

[2] G.A. Margulis. Indefinite Quadratic Forms and Unipotent Flows on Homogeneous Spaces. Dynamical Systems and Ergodic Theory, 1989.

[3] M. Einsiedler, T. Ward. Ergodic Theory-With a View towards Number Theory(GTM259). Springer.

[4] G.A. Margulis. Lie Groups and Ergodic Theory. Algebra-Some Current Trends, Lecture Notes in Math., Springer, 1988.

[5] G.A. Margulis. Discrete Subgroups and Ergodic Theory. Number Theory, Trace Formulas and Discrete Groups, 1989.

[6] 孙文祥. 遍历论. 北京大学出版社.

[7] M. Einsiedler, G. Everest, T. Ward. Entropy and the Canonical Height. Journal of Number Theory, 2001.

[8] M. Pollicott, M. Yuri. Dynamical Systems and Ergodic Theory. Cambridge University Press.

[9] H. Furstenberg. Poincaré Recurrence and Number Theory. Bull. Amer. Math. Soc., 1981.

[10] 徐飞, 张润林. Counting Integral Points on Indefinite Ternary Quadratic Equations over Number Fields. 2021.

[11] 朱子阳. 椭圆曲线的算术——代数数论专题 II. https://www.cnblogs.com/zhuziyangcnu/.

[12] 朱子阳. Tate 的论文——代数数论专题 III. https://www.cnblogs.com/zhuziyangcnu/.

[13] G. Everest, T. Ward. A Dynamical Interpretation of the Global Canonical Height on an Elliptic Curve. Experiment. Math., 1998.
[14] D.A. Lind, T. Ward. Automorphisms of Solenoids and p-adic Entropy. Ergodic Theory Dynam. Systems, 1988.
[15] P. D'Ambros, G. Everest, R. Miles, T. Ward. Dynamical Systems Arising From Elliptic Curves. Colloq. Math., 2000.
[16] C.T. McMullen. From Dynamics on Surfaces to Rational Points on Curves. 1999.
[17] G. Everest, T. Ward. Heights of Polynomials and Entropy in Algebraic Dynamics. Springer.
[18] A. Borel. Density Properties for Certain Subgroups of Semi-Simple Groups Without Compact Components. Annals of Mathematics, 1960.
[19] A. Borel. Linear Algebraic Groups(GTM126). Springer.
[20] J.H. Silverman. The Arithmetic of Elliptic Curves(GTM106). Springer.
[21] Z. Coelho, W. Parry. Ergodic Decomposition of p-adic Multiplications. Topology, Ergodic Theory, Real Algebraic Geometry, 2001.
[22] T. Tao. Almost all Orbits of the Collatz Map Attain Almost Bounded Values. arXiv:1909.03562v3.
[23] D.J. Bernstein. A Non-Iterative 2-adic Statement of the $3N+1$ Conjecture. Proceedings of the American Mathematical, 2001.
[24] R. Olivier. The $3x+1$ Problem: A Lower Bound Hypothesis. arXiv:1510.01610.
[25] B. Farb, M. Dan. A Primer on Mapping Class Groups. Princeton University Press.
[26] 文兰. 微分动力系统. 高等教育出版社.
[27] A. Hatcher. Algebraic Topology. Cambridge University Press.
[28] 李文威. 模形式初步. 高等教育出版社. https://www.wwli.asia/index.php/zh/.
[29] D.G. Northcott. Periodic Points on An Algebraic Variety. Ann. of Math., 1950.
[30] B. Green. Long Arithmetic Progressions of Primes. Clay Mathematics Proceedings, 2007.
[31] O. Robert. From Schwarz to Pick to Ahlfors and Beyond. Notices of the AMS, 1999.
[32] M. Hindry, J.H. Silverman. The Canonical Height and Integral Points on Elliptic Curves. Invent. Math., 1988.
[33] R. Hartshorne. Algebraic Geometry(GTM52). Springer.
[34] P. Walters. An Introduction to Ergodic Theory(GTM79). Springer.
[35] B. Poonen. Rational Points on Varieties. American Mathematical Society.
[36] 童纪龙. Arithmetic of Etale Fundamental Groups. Seminar at Capital Normal University, 2021.
[37] G.K. Francis. A Topological Picturebook. Springer-Verlag.
[38] Stacks Project Authors. Fundamental Groups of Schemes. THE STACKS PROJECT, 0BQ6.
[39] Y. Imayoshi, H. Shiga. A Finiteness Theorem for Holomorphic Families of Riemann Surfaces. Springer-Verlag.
[40] J.S. Milne. Abelian Varieties. https://www.jmilne.org/math/index.html.
[41] M. Morishita. Knots and Primes-An Introduction to Arithmetic Topology. Springer.
[42] J. Neukirch. Algebraic Number Theory. Springer.
[43] 张寿武. Distributions in Algebraic Dynamics. Surveys in Differential Geometry, 2005.
[44] 张寿武. Equidistribution of Small Points on Abelian Varieties. Ann. of Math., 1998.
[45] 袁新意. Algebraic Dynamics, Canonical Heights and Arakelov Geometry.
[46] 谢俊逸, 袁新意. Geometric Bogomolov Conjecture in Arbitrary Characteristics. Invent. Math., 2022.
[47] D. Roessler. A Note on the Manin-Mumford Conjecture. arXiv:math/0409083v1.

朱子阳[1]，2021 年 6 月于首都师范大学

[1]邮箱 zhuziyang@cnu.edu.cn

1、回复性

定义 1.1(保测变换) 设 $(X,\mathcal{B}_X,\mu_X)$ 和 $(Y,\mathcal{B}_Y,\mu_Y)$ 均是**概率空间**，映射 $\phi:X\to Y$ 在某个零测集之外有定义. 称 ϕ 是**可测**的，如果 Y 中可测集的原像是 X 中的可测集；称 ϕ 是**保测**的，如果 ϕ 可测且对任意 $B\in\mathcal{B}_Y$，$\mu_X(\phi^{-1}B)=\mu_Y(B)$；称保测映射 ϕ 是**可逆保测**的，如果 ϕ^{-1} 在某个零测集之外有定义且可测. 特别地，如果变换 $T:(X,\mathcal{B},\mu)\to(X,\mathcal{B},\mu)$ 保测，则称 μ 是T**-不变测度**，称 $(X,\mathcal{B},\mu,T)$ 是一个**保测系统**，称 T 是一个**保测变换**.

例 1.2 (1) 考虑 $\mathbb{T}:=\mathbb{R}/\mathbb{Z}\cong[0,1)\cong S^1$，其上配备 Lebesgue 测度. 对任意 $\alpha\in\mathbb{R}$，定义逆时针旋转 $R_\alpha:\mathbb{T}\to\mathbb{T},t\mapsto t+\alpha(\mathrm{mod}\ 1)$，则 R_α 保测. 一般地，考虑紧群 X，配备 (左)Haar 测度. 对任意 $g\in X$，定义左平移 $T_g:X\to X,x\mapsto gx$，则 T_g 保测.

(2) 考虑 $\mathbb{T}$ 并配备 Lebesgue 测度，定义映射 $T_2:\mathbb{T}\to\mathbb{T},t\mapsto 2t(\mathrm{mod}\ 1)$，则 T_2 保测 (注意，这给出了一个保测但 $\mu(TA)\neq\mu(A)$ 的例子). 一般地，考虑紧 Abel 群 X 并配备 Haar 测度 m，则任何 X 的满自同态 T 保测$\big($设 $\mu(A):=m(T^{-1}A)$，则由 $\mu(A+x)=m(T^{-1}(A+x))=m(T^{-1}A+y)=m(T^{-1}A)=\mu(A)$ 知 μ 平移不变，又因为 T 满蕴含 $\mu(X)=m(X)$，故根据 Haar 测度的存在唯一性得 $\mu=m\big)$.

(3.**Bernoulli 试验**) 考虑离散集合 $\{1,2,\cdots,n\}$，数字 k 赋予权重 $p_k(1\le k\le n,p_k\ge 0,\sum_{k=1}^n p_k=1)$，定义 $\{1,2,\cdots,n\}$ 上的概率 μ 为加权计数测度. 现考虑 $\boldsymbol{X}:=\prod_{i\in\mathbb{Z}}\{1,2,\cdots,n\}$(即重复无数次独立试验)，其上配备积拓扑并与度量 $d\big((x_i),(y_i)\big):=2^{-\sup(\{n:\forall|i|\le n,x_i=y_i\}\cup\{0\})}$ 相容 (此时 $\boldsymbol{X}$ 是紧致度量空间)，配备乘积测度 $\boldsymbol{\mu}=\prod_{i\in\mathbb{Z}}\mu$. 现定义左平移 $\boldsymbol{T}:\boldsymbol{X}\to\boldsymbol{X},(x_i)\mapsto(y_i),y_i:=x_{i+1}$(这是一个连续映射)，易见 $\boldsymbol{T}$ 保测.

命题 1.3 X 上的测度 μ 是 T-不变的当且仅当对任意 $f\in\mathscr{L}^\infty(X,\mu):=\{f\text{可测}:\|f\|_\infty<\infty\}$，均有 $\int_X f d\mu=\int_X f\circ T d\mu$. 此外，如果 μ 是 T-不变的，则对任何 $f\in L^1(X,\mu):=\mathscr{L}^1(X,\mu)/$几乎处处相等，$\int_X f d\mu=\int_X f\circ T d\mu$.

证明 对任何可测集 A，取 $f=\mathbf{1}_A$ 即可得到必要性. 反过来设 f 非负可积，取 f 的简单函数单调逼近 $\{f_n\}$，则 $\{f_n\circ T\}$ 是 $f\circ T$ 的简单函数单调逼近. 由单调收敛定理知 $\int_X f\circ T d\mu=\lim_{n\to\infty}\int_X f_n\circ T d\mu=\lim_{n\to\infty}\int_X f_n d\mu=\int_X f d\mu$.■

有了保测变换的概念，我们便可给出一些有关动力系统的初步结论，其中最经典的也是最重要的即各种回复 (Recurrence) 定理——它们是鸽巢原理的合理推广，描述了动力系统大时间尺度上的演化规律.

定理 1.4(回复性) 有如下结论：

Poincaré 回复：设 $T:X\to X$ 是保测变换，$E\subseteq X$ 是可测集，则 E 中几乎所有的点在 T 的迭代作用下无限次地回复到 E 中$\big($即存在可测集 $F\subseteq E$ 满足 $\mu(F)=\mu(E)$，且对任意 $x\in F$，存在整数 $0<n_1<n_2<\cdots$ 使得 $T^{n_i}x\in E,i\in\mathbb{Z}_{\ge1}\big)$.

Birkhoff 回复：设 X 是紧致度量空间，$T:X\to X$ 是连续映射，则存在 $x\in X$ 和整数 $0<n_1<n_2<\cdots$ 使得 $T^{n_i}x\to x,i\to\infty$.

多重 Birkhoff 回复：设 X 是紧致度量空间，$T_1,\cdots,T_l$ 是 X 上两两交换的同胚，则存在 $x\in X$ 和整数 $0<n_1<n_2<\cdots$ 使得对任意 $1\le j\le l$ 均有 $T_j^{n_i}x\to x,i\to\infty$.

证明 我们仅证 Poincaré 回复定理，其余证明见 [6]Chapter2.5. 记可测集 $B:=\{x\in E:\forall n\ge1,T^nx\notin E\}$，容易验证 $B,T^{-1}B,T^{-2}B,\cdots$ 两两无交且测度均为 $\mu(B)$，故 $\mu(B)=0$. 此时存在集合 $F_1\subseteq E$ 使得 $\mu(F_1)=\mu(E)$ 且任意 F_1 中的点在 T 的迭代下至少回复 E 一次. 同理，对 $T^2,T^3,\cdots$ 仍进行上述操作将得到 $F_2,F_3,\cdots$，这里 $\mu(F_i)=\mu(E)$ 且任意 F_i 中的点在 T^i 的迭代下至少回复 E 一次. 令 $F=\bigcap_{i\ge1}F_i\subseteq E$，则 $\mu(F)=\mu(E)$ 且任意 F 中的点均回复 E 任意多次.■

哲学上来讲回复定理预示着动力系统通过漫长的演化会无限接近最初的样子. 此处我们更关心它们在数论中的应用：

定理 1.5(Van der Waerden) 设有有限分拆 $\mathbb{Z}=B_1\cup\cdots\cup B_k$(即 $B_i\neq\varnothing,B_i\cap B_j=\varnothing$)，则至少存在某个 $B_r(1\le r\le k)$，在 B_r 中有任意长度的等差数列 (即任意 $N\in\mathbb{Z}_{\ge1}$，存在 $a,b\in\mathbb{Z},b\neq0$ 使得对任意 $j=0,\cdots,N$，均有 $a+jb\in B_r$).

证明 设 $\boldsymbol{X}:=\prod_{i\in\mathbb{Z}}\{1,\cdots,k\}$，定义左平移 $T:\boldsymbol{X}\to\boldsymbol{X},(x_i)\mapsto(x_{i+1})$，定义 $\phi:\mathbb{Z}\to\{1,\cdots,k\},n\mapsto i$，

这里 $n\in B_i$. 此时 $\boldsymbol{x}:=(x_i:=\phi(i))\in\boldsymbol{X}$. 记 $\Omega:=\overline{\{T^n\boldsymbol{x}:n\in\mathbb{Z}\}}\subseteq\boldsymbol{X}$，配备例 1.2(3) 中的度量. 对紧致度量空间 Ω 及其上的同胚 $T,\cdots,T^N$ 使用多重 Birkhoff 回复定理知存在 $\boldsymbol{z}:=(z_i)\in\Omega$ 和 $n_k\to\infty$，使得 $T^{n_k}\boldsymbol{z}\to\boldsymbol{z},\cdots,T^{Nn_k}\boldsymbol{z}\to\boldsymbol{z}(k\to\infty)$. 当 k 充分大时，根据度量的定义立即得到 $z_0=z_{n_k}=\cdots=z_{Nn_k}$. 又因为 $\boldsymbol{z}\in\Omega$，由稠密性知存在 $a\in\mathbb{Z}$ 使得 $d(T^{a+in_k}\boldsymbol{x},T^{in_k}\boldsymbol{z})$ 充分小 $(i=0,\cdots,N)$，从而 $x_a=z_0=z_{n_k}=x_{a+n_k}=\cdots=x_{a+Nn_k}$. 因此 $\{a,a+n_k,\cdots,a+Nn_k\}\subseteq B_{x_a}=B_{\phi(a)}$.■

例 1.6 取 $\mathbb{Z}=P\cup P^c$，其中 P 为所有素数构成的集合. 则在 P^c 中有任意长度的等差数列：若记第 i 个素数为 p_i，则初等数论告诉我们区间 $[p_1\cdots p_k+2,p_1\cdots p_k+(p_{k+1}-1)]$ 中无素数. 但是 P 中是否有任意长度的等差数列则是一个非常困难的问题，Green 和 Tao 于 2007 年就该问题给出了肯定的回答，见 [30].

实际上 Van der Waerden 定理可以推广为“$\mathbb{Z}$ 的正密度子集中含有任意长度的等差数列”. 为此我们需要明确这里“密度”的含义：称一个集合 $A\subseteq\mathbb{Z}_{\geq0}$ 的**密度**为 $\mathrm{den}(A)$，如果极限 $\mathrm{den}(A):=\lim_{N\to\infty}\frac{|A\cap[0,N]|}{N}$ 存在.

定理 1.7(Szemerédi) 设集合 $A\subseteq\mathbb{Z}$ 具有正密度$\big($即 $\limsup_{N\to+\infty}\frac{|\{-N\leq n\leq N:n\in A\}|}{2N+1}>0\big)$，则在 A 中有任意长度的等差数列.

2、遍历论

一类特殊的保测变换即遍历变换，由遍历变换得到的动力系统具有某种极小性——不可能将该系统分解为两个更小的非平凡系统. 依靠这种性质我们可以建立遍历定理，它在数论中也有很多应用. 首先给出基本定义：

定义 2.1(遍历) 设 $(X,\mathcal{B},\mu)$ 是概率空间，一个保测变换 $T:X\to X$ 称为**遍历**的，如果对任意 $B\in\mathcal{B}$，$T^{-1}B=B$ 蕴含 $\mu(B)=0$ 或 $\mu(B)=1$. 此时我们也称 μ 是一个**T-遍历测度**.

注意 2.2 仅对 $\mathcal{B}$ 中的生成元验证定义 2.1 的条件不足以判断一个保测变换是否遍历；但是保测性可以只对生成元检验.

命题 2.3 设 T 是 $(X,\mathcal{B},\mu)$ 上的保测变换，定义由 T 诱导的算子 $U_T:L^2(X,\mu)\to L^2(X,\mu),f\mapsto f\circ T$(由保测性容易验证这是个酉线性算子). 此时下述说法等价：

(1)T 遍历. (2) 对任意 $B\in\mathcal{B}$，$\mu(T^{-1}B\triangle B)=0$ 蕴含 $\mu(B)=0$ 或 $\mu(B)=1$.

(3) 若 $A\in\mathcal{B}$ 满足 $\mu(A)>0$，则 $\mu\big(\bigcup_{n=1}^{\infty}T^{-n}A\big)=1$.

(4) 若 $A,B\in\mathcal{B}$ 满足 $\mu(A)\mu(B)>0$，则存在 $n\in\mathbb{Z}_{\geq1}$ 使得 $\mu(T^{-n}A\cap B)>0$.

(5) 若可测函数 $f:X\to\mathbb{C}$ 满足几乎处处 $f\circ T=f$，则 f 几乎处处为一个常数.

(6)U_T 的特征值 1 的特征子空间中全是常值函数.

证明 **(1 ⇒ 2)** 对任意 $n\geq1$ 均有 $B\triangle T^{-n}B\subseteq\bigcup_{i=0}^{n-1}T^{-i}B\triangle T^{-(i+1)}B$，而 $\mu\big(\bigcup_{i=0}^{n-1}T^{-i}B\triangle T^{-(i+1)}B\big)\leq\sum_{i=0}^{n-1}\mu(T^{-i}(B\triangle T^{-1}B))=0$，故 $\mu(B\triangle T^{-n}B)=0$. 对 $N\geq0$ 令 $C_N:=\bigcup_{n=N}^{\infty}T^{-n}B$，则易见 $C_0\supseteq C_1\supseteq\cdots$ 且 $\mu(C_N\triangle B)\leq\mu\big(\bigcup_{n=N}^{\infty}B\triangle T^{-n}B\big)=0$，故 $\mu\big(C:=\bigcap_{N=0}^{\infty}C_N\big)=\mu(B)$. 此外又不难验证 $T^{-1}C=C$，因此由定义 2.1 得 $\mu(C)=0$ 或 1.

(2 ⇒ 3) 令 $D:=\bigcup_{n=1}^{\infty}T^{-n}A$，则 $T^{-1}D\subseteq D$. 另一方面由 $\mu(T^{-1}D)=\mu(D)$ 得 $\mu(T^{-1}D\triangle D)=0$，所以 $\mu(D)=0$ 或 1. 而又由于 $T^{-1}A\subseteq D$，因此只能有 $\mu(D)=1$.

(3 ⇒ 4) 由条件有 $\mu\big(\bigcup_{n=1}^{\infty}T^{-n}A\big)=1$，故 $0<\mu(B)=\mu\big(\bigcup_{n=1}^{\infty}B\cap T^{-n}A\big)\leq\sum_{n=1}^{\infty}\mu(B\cap T^{-n}A)$，所以必然存在某个 $n\geq1$ 使 $\mu(B\cap T^{-n}A)>0$.

(4 ⇒ 1) 设 A 满足 $T^{-1}A=A$，则任意 $n\geq1$ 有 $0=\mu(A\cap X\backslash A)=\mu(T^{-n}A\cap X\backslash A)$，故 $\mu(A)\mu(X\backslash A)=0$.

(2 ⇒ 5) 不失一般性设 f 是实值函数. 对任意 $k\in\mathbb{Z}$ 以及 $n\geq1$，易见 $T^{-1}\big(f^{-1}[\frac{k}{n},\frac{k+1}{n})\big)\triangle f^{-1}[\frac{k}{n},\frac{k+1}{n})\subseteq\{x\in X:f\circ T(x)\neq f(x)\}$ 是个零测集，故 $\mu\big(f^{-1}[\frac{k}{n},\frac{k+1}{n})\big)=0$ 或 1. 又由于对任意 n，$X=\bigsqcup_{k\in\mathbb{Z}}f^{-1}[\frac{k}{n},\frac{k+1}{n})$，所以必然存在唯一的依赖于 n 的 k_n 使得 $\mu\big(f^{-1}[\frac{k_n}{n},\frac{k_n+1}{n})\big)=1$. 此时 $f|_Y:=\bigcap_{n=1}^{\infty}f^{-1}[\frac{k_n}{n},\frac{k_n+1}{n})$ 是常值函数，且 $\mu(X\setminus Y)=\mu\big(\bigcup_{n=1}^{\infty}(X\cap f^{-1}[\frac{k_n}{n},\frac{k_n+1}{n}))^c\big)\leq\sum_{n=1}^{\infty}\mu\big(X\setminus f^{-1}[\frac{k_n}{n},\frac{k_n+1}{n})\big)=0$.

(5 ⇒ 2) 考虑可测函数 $\mathbf{1}_B$ 即可. **(5 ⇔ 6)** 显然.■

例 2.4 例 1.2(1) 中的逆时针旋转 R_α 是遍历的当且仅当 α 是无理数；(2) 中的 T_2 是遍历的；(3) 中的 $\boldsymbol{T}$ 是遍历的.

证明 (1) 设 $\alpha\notin\mathbb{Q}$，$f\circ R_\alpha=f\in L^2$，记 $g=f\circ R_\alpha-f$. 考虑 Fourier 反演 $f(t)=\sum_{n\in\mathbb{Z}}c_ne^{2\pi int},g(t)=\sum_{n\in\mathbb{Z}}c_n(e^{2\pi in\alpha}-1)e^{2\pi int}$. 由 $0=\|g\|_2^2=\|\widehat{g}\|_2^2=\sum_{n\in\mathbb{Z}}|c_n(e^{2\pi in\alpha}-1)|^2$ 知对任何 $n\in\mathbb{Z}$，$c_n=c_ne^{2\pi in\alpha}$. 又因为 α 是无理数，故当 $n\neq0$ 时 $c_n=0$，因此 f 几乎处处常值，由命题 2.3(6) 知 R_α 遍历. 另设 $\alpha=\frac{p}{q}\in\mathbb{Q}$，则函数 $h(t)=e^{2\pi iqt}$ 满足 $h\circ R_\alpha=h$，但它显然不会与一个常值函数几乎处处相等.

(2) 设 $f\circ T_2=f\in L^2$，考虑 Fourier 反演 $f(t)=\sum_{n\in\mathbb{Z}}c_ne^{2\pi int}=f(T_2t)=\sum_{n\in\mathbb{Z}}c_ne^{2\pi i2nt}$. 类比 (1) 的论证我们不难得到对任意 $n\in\mathbb{Z}$ 均有 $c_{2n}=c_n$，再注意到 $\|f\|_2^2=\sum_{n\in\mathbb{Z}}|c_n|^2<\infty$，故当 $n\neq0$ 时只能有 $c_n=0$，这意味着 f 几乎处处常值，由命题 2.3(6) 知 T_2 遍历.

(3) 设 $\boldsymbol{T}^{-1}B=B$. 对任意 $\epsilon>0$，存在 $A:=\bigsqcup_{l,n,a_l,\cdots,a_n}^{<\infty}\left\{(x_i)\in\boldsymbol{X}:\forall l\leq i\leq n,x_i=a_i\right\}$ 使得 $\boldsymbol{\mu}(A\triangle B)<\epsilon$. 显然 $|\boldsymbol{\mu}(A)-\boldsymbol{\mu}(B)|<\epsilon$. 现取充分大的 N，使得 $\boldsymbol{T}^{-N}A=\bigsqcup_{t,m,b_t,\cdots,b_m}^{<\infty}\left\{(y_j)\in\boldsymbol{X}:\forall t\leq j\leq m,y_j=b_j\right\}$ 中这些区间 $[t,m]$ 与所有的 $[l,n]$ 完全无交，此时根据乘积测度的性质有 $\boldsymbol{\mu}(A\cap\boldsymbol{T}^{-N}A)=\boldsymbol{\mu}(\boldsymbol{T}^{-N}A)\boldsymbol{\mu}(A)=\boldsymbol{\mu}(A)^2$. 另由保测变换 $\boldsymbol{T}$ 满足 $\boldsymbol{T}^{-N}B=B$ 得 $\boldsymbol{\mu}(B\triangle\boldsymbol{T}^{-N}A)<\epsilon$，并且注意到 $B\triangle(A\cap\boldsymbol{T}^{-N}A)\subseteq(A\triangle B)\cup(B\triangle\boldsymbol{T}^{-N}A)$，所以 $\boldsymbol{\mu}(B\triangle(A\cap\boldsymbol{T}^{-N}A))<2\epsilon$. 因此 $|\boldsymbol{\mu}(B)-\boldsymbol{\mu}(B)^2|\leq|\boldsymbol{\mu}(B)-\boldsymbol{\mu}(A\cap\boldsymbol{T}^{-N}A)|+|\boldsymbol{\mu}(A\cap\boldsymbol{T}^{-N}A)-\boldsymbol{\mu}(B)^2|<2\epsilon+|\boldsymbol{\mu}(A)^2-\boldsymbol{\mu}(B)^2|\leq2\epsilon+\boldsymbol{\mu}(A)|\boldsymbol{\mu}(A)-\boldsymbol{\mu}(B)|+\boldsymbol{\mu}(B)|\boldsymbol{\mu}(A)-\boldsymbol{\mu}(B)|<4\epsilon$，即 $\boldsymbol{\mu}(B)=\boldsymbol{\mu}(B)^2$，这意味着只能有 $\boldsymbol{\mu}(B)=0$ 或 1.■

现在我们来建立遍历定理，它表明一个较好的点在遍历变换的迭代下将均匀稠密地分布于整个空间.

定理 2.5(遍历定理) 有如下结论：

平均遍历定理：设 $(X,\mathcal{B},\mu,T)$ 是保测系统，定义由 P 诱导的正交投射 $P_T:L^2(X,\mu)\twoheadrightarrow\{g\in L^2(X,\mu):U_Tg=g\}$，则对任意 $f\in L^2(X,\mu)$，$\mathsf{A}(N,f):=\frac{1}{N}\sum_{n=0}^{N-1}U_T^nf\to P_Tf$(按 2 范数). 此外，对任意 $f\in L^1(X,\mu)$，极限 $\lim_{N\to\infty}\mathsf{A}(N,f)$ 在 $L^1(X,\mu)$ 中存在 (按 1 范数) 且在 U_T 作用下不变.

极大遍历定理：设 $(X,\mathcal{B},\mu,T)$ 是保测系统，$g\in\mathscr{L}^1(X,\mu)$ 是实值函数. 对任意 $\alpha\in\mathbb{R}$，若记 $E_\alpha:=\{x\in X:\sup_{N\geq1}\mathsf{A}(N,g)(x)>\alpha\}$，则 $\alpha\mu(E_\alpha)\leq\int_{E_\alpha}gd\mu\leq\|g\|_1$. 特别地，当 $T^{-1}A=A$ 时 $\alpha\mu(E_\alpha\cap A)\leq\int_{E_\alpha\cap A}gd\mu$.

Birkhoff 遍历定理：设 $(X,\mathcal{B},\mu,T)$ 是保测系统，$f\in\mathscr{L}^1(X,\mu)$，则函数列 $\left\{\frac{1}{n}\sum_{i=0}^{n-1}f(T^ix)\right\}_{n\geq1}$ 几乎处处收敛于 $f^*\in L^1(X,\mu)$，$f^*\circ T=f^*$，且 $\int_Xf^*d\mu=\int_Xfd\mu$. 特别地，如果 T 遍历，则 f^* 与常数 $\int_Xfd\mu$ 几乎处处相等.

证明 分别见 [3]Chapter2.5，[3]Chapter2.6.2 和 [3]Chapter2.6.5.■

注意 2.6 利用 Birkhoff 遍历定理可以从另一种观点来定义 Riemann 积分：$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}f(T^ix)=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}f(\xi_i)$. 等式左边由一个比较好的点遍历迭代产生 (轨道平均)，右边则由积分区域分割的加细产生 (空间平均). 具体描述见引理 4.8.

Birkhoff 遍历定理通常被用来统计某些事件发生的概率. 我们以 Borel 正规数定理为例给出其动力学证明：

定理 2.7(Borel) 几乎所有的实数其十进制表示的小数部分中各数出现的概率相等 (称这样的数为**正规数**. 当然有不满足这个性质的无理数，例如 $0.1010010001\cdots$ 中数字 1 出现的密度趋于 0. 很容易证明非正规数有不可数无穷多个，但构成的集合零测).

证明 我们证明一个比该定理更广的结论. 考虑映射 $T:[0,1]\to[0,1],x=0.a_1a_2a_3\cdots\mapsto10x(\mathrm{mod}\ 1)=0.a_2a_3a_4\cdots$. 由例 2.4(2) 知 T 关于 Lebesgue 测度 m 遍历，因此应用 Birkhoff 遍历定理知对几乎所有的 x，均有 $\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}\mathbf{1}_{A_{j,k}}(T^ix)=\int_0^1\mathbf{1}_{A_{j,k}}(x)dm(x)=\frac{1}{10^k}$，这里 $A_{j,k}=[\frac{j}{10^k},\frac{j+1}{10^k})$，$j=10^{k-1}j_1+10^{k-2}j_2+\cdots+j_k$. 这意味着对几乎所有的实数 $x\in[0,1]$ 及所有 $k\in\mathbb{Z}_{\geq1}$，其十进制表示 $x=0.\cdots\underline{j_1\cdots j_k}\cdots$ 中字节 $j_1\cdots j_k$ 以渐进 10^{-k} 的密度出现.■

事实上要判断一个数是否正规无比困难，像 $\sqrt{2},\pi,e,\ln2$ 这些数的正规性还未知，只是实验猜测它们可能都是正规的. 关于此 D.H. Bailey 和 R.E. Crandall 猜想所有无理的代数数都是正规的，但迄今仍未能证明其中任何一个数的正规性，也没有找到反例.

3、与算术有关的案例

在第 2 节中我们介绍了遍历定理，它是整个遍历论的核心. 本节我们围绕遍历定理再研究两个具体的例子，

看看遍历论的技术如何在与数论有关的领域中应用. 第一个例子是连分数，首先给出定义：

定义 3.1(连分数) 称形如 $[a_0;a_1,\cdots,a_n]:=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots+\cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}}$ 的表达式为**有限连分数**；形如 $[a_0;a_1,a_2,\cdots]:=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots}}$ 的表达式为**无限连分数**，其中 $a_0\in\mathbb{Z}_{\geq 0},a_{n\geq 1}\in\mathbb{Z}_{\geq 1}$. 一般用字母 $u:=[a_0;a_1,a_2,\cdots]$ 表示无限连分数.

以下是关于连分数的一些简单结论.

命题 3.2 设有序列 $\{a_n\}_{n\geq 0}$ 满足 $a_0\in\mathbb{Z}_{\geq 0},a_{n\geq 1}\in\mathbb{Z}_{\geq 1}$.

(0) 存在递推关系 $[a_0;a_1,\cdots,a_n]=a_0+\frac{1}{[a_1;a_2,\cdots,a_n]}$.

(1) 对任意 $n\geq 1$，约定 $p_{-1}=1,q_{-1}=0,p_0=a_0,q_0=1$ 之后，有理数 $\frac{p_n}{q_n}:=[a_0;a_1,\cdots,a_n],(p_n,q_n)=1,p_n,q_n\geq 1$ 可被递归地计算：$\left(\begin{smallmatrix}p_n & p_{n-1}\\ q_n & q_{n-1}\end{smallmatrix}\right)=\left(\begin{smallmatrix}a_0 & 1\\ 1 & 0\end{smallmatrix}\right)\left(\begin{smallmatrix}a_1 & 1\\ 1 & 0\end{smallmatrix}\right)\cdots\left(\begin{smallmatrix}a_n & 1\\ 1 & 0\end{smallmatrix}\right)$. 利用这个递推可得：

(1.1) 对任意 $n\geq 0$，有 $p_{n+1}=a_{n+1}p_n+q_{n-1},q_{n+1}=a_{n+1}q_n+q_{n-1}$.

(1.2) 由于 $a_{n\geq 1}\geq 1$，因此 $1=q_0\leq q_1<q_2<\cdots$.

(1.3) 对任意 $n\geq 1$，数学归纳法给出 $q_n\geq 2^{\frac{n-2}{2}},p_n\geq 2^{\frac{n-2}{2}}$.

(1.4) 对 (1) 取行列式得对任意 $n\geq 1$，有 $p_nq_{n-1}-p_{n-1}q_n=(-1)^{n+1}$. 利用该式可求得通项 $\frac{p_n}{q_n}=a_0+\sum_{i=1}^{n}(-1)^{i+1}\frac{1}{q_{i-1}q_i}$，因此 $u=[a_0;a_1,\cdots]=\lim_{n\to\infty}\frac{p_n}{q_n}=a_0+\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{q_{n-1}q_n}$. 由 (1.3) 可知该级数绝对收敛，而且一定收敛于一个无理数 (换言之，无限连分数一定是无理数).

(1.5) 由 (1.1) 和 (1.2) 可以估计上述 (1.4) 中级数的收敛速度：$|u-\frac{p_n}{q_n}|=|\frac{1}{q_nq_{n+1}}-\frac{1}{q_{n+1}q_{n+2}}+\cdots|<\frac{1}{q_nq_{n+1}}<\frac{1}{a_{n+1}q_n^2}\leq\frac{1}{q_n^2}$.

(1.6) 由于 (1.4) 中的级数是交错的，故 $\frac{p_0}{q_0}<\frac{p_2}{q_2}<\cdots<\frac{p_{2n}}{q_{2n}}<\cdots<u<\cdots<\frac{p_{2m+1}}{q_{2m+1}}<\cdots<\frac{p_3}{q_3}<\frac{p_1}{q_1}$.

(2) 对于无理数 $u:=[a_0;a_1,\cdots]$，(1.4) 中的逼近在某种意义上是最佳有理逼近. 具体来讲，对任意 $n>1$ 以及任意 p,q 满足 $0<q\leq q_n,\frac{p}{q}\neq\frac{p_n}{q_n}$，有 $|\frac{p_n}{q_n}-u|<|\frac{p}{q}-u|$. 此外，定理 3.3(5) 将断言这个逼近对几乎所有实数来说收敛速度是指数级的：$|\frac{p_n}{q_n}-u|\sim\exp(-\frac{n\pi^2}{6\ln 2}),n\to\infty$.

(3) 无理数连分数表示的存在唯一性.

(3.1) 唯一性：映射 $\mathbb{Z}_{\geq 0}\times\prod_{i=1}^{\infty}\mathbb{Z}_{\geq 1}\to\mathbb{R},(a_0,a_1,\cdots)\mapsto[a_0;a_1,\cdots]$ 是单射.

(3.2) 存在性：对任何无理数 $x\in[0,1]\setminus\mathbb{Q}$，总存在依赖于 x 的序列 $\{a_n(x)\}_{n\geq 1}$ 使得 $x=[0;a_1(x),\cdots]$.

证明 (1) 关于 n 作数学归纳法即可；(1.4) 易证有理数连分数表示的递归一定会在有限步终止，而这会与 $q_1<q_2<\cdots$ 矛盾；(2) 的证明见 [3] 命题 3.3；(3.1) 若 $(a_0,a_1,\cdots)\mapsto u$，显然 $u\in(a_0,a_0+1]$，故 $a_0\in\mathbb{Z}\cap[u-1,u)$ 唯一确定，归纳下去即可；(3.2) 定义映射 $T_{\mathrm{G}}:[0,1]\setminus\mathbb{Q}\to[0,1]\setminus\mathbb{Q},x\mapsto\frac{1}{x}-\lfloor\frac{1}{x}\rfloor=\{\frac{1}{x}\}$，定义序列 $a_{n\geq 1}(x):=\lfloor\frac{1}{T^{n-1}(x)}\rfloor\in\mathbb{Z}_{\geq 1}$. 现用数学归纳法证明 $[0;a_1(x),\cdots,a_{2n}(x)]<x<[0;a_1(x),\cdots,a_{2n+1}(x)]$. 假设命题对 n 成立，则当 $n+1$ 时对 $T_{\mathrm{G}}(x)$ 使用归纳假设得到 $[0;a_2(x),\cdots,a_{2n+1}(x)]<T_{\mathrm{G}}(x)=\frac{1}{x}-a_1(x)<[0;a_2(x),\cdots,a_{2n+2}(x)]$，故 $[0;a_1(x),\cdots,a_{2n+2}(x)]=\frac{1}{a_1(x)+[0;a_2(x),\cdots,a_{2n+2}(x)]}<x<\frac{1}{a_1(x)+[0;a_2(x),\cdots,a_{2n+1}(x)]}=[0;a_1(x),\cdots,a_{2n+1}(x)]$. 对上式再作用一次 T_{G} 并使用相同的论证即可完成归纳. 此时由 (1.3)、(1.4) 和 (1.6) 知 $[0;a_1(x),\cdots,a_{2n+1}(x)]-[0;a_1(x),\cdots,a_{2n}(x)]=\frac{p_{2n+1}}{q_{2n+1}}-\frac{p_{2n}}{q_{2n}}=\frac{1}{q_{2n}q_{2n-1}}\leq\frac{1}{2^{2n-2}}\to 0$，故 $x=[0;a_1(x),\cdots]$.■

对于区间 $[0,1]$，定义其上的 **Gauss 测度**为 $\mu_{\mathrm{G}}(A):=\frac{1}{\ln 2}\int_A\frac{1}{1+x}dx$，这里 A 是 Borel 可测集. 在命题 3.2 的证明中，我们称定义的映射 $T_{\mathrm{G}}:[0,1]\setminus\mathbb{Q}\to[0,1]\setminus\mathbb{Q},x\mapsto\frac{1}{x}-\lfloor\frac{1}{x}\rfloor=\{\frac{1}{x}\}$ 为 **Gauss 映射** (实际上它来源于有理数的有限连分数表示). 注意 T_{G} 在 $[0,1]$ 中至多可数多个点处无定义，而这并不影响测度的计算，所以我们可以随意规定 T_{G} 在 $\mathbb{Q}$ 上的取值. 现引入遍历论的技术，我们给出下定理：

定理 3.3 $\left([0,1],\mathcal{B}_{[0,1]},\mu_{\mathrm{G}},T_{\mathrm{G}}\right)$ 是保测系统，并且 T_{G} 遍历. 因此对几乎所有 (Lebesgue 测度下) 的实数 $x=[0;a_1,\cdots]\in(0,1)$，我们有：

(1) 数字 j 出现在连分数 $[0;a_1,\cdots]$ 中的密度为 $\frac{2\ln(1+j)-\ln j-\ln(2+j)}{\ln 2}$.

(2)$\lim_{n\to\infty}(a_1a_2\cdots a_n)^{1/n}=\prod_{n=1}^{\infty}\left(\frac{(n+1)^2}{n(n+2)}\right)^{\frac{\ln n}{\ln 2}}$. (3)$\lim_{n\to\infty}\frac{1}{n}(a_1+a_2+\cdots+a_n)=\infty$.

(4)$\lim_{n\to\infty}\frac{1}{n}\ln q_n(x)=\frac{\pi^2}{12\ln 2}$. (5)$\lim_{n\to\infty}\frac{1}{n}\ln|x-\frac{p_n(x)}{q_n(x)}|\to-\frac{\pi^2}{6\ln 2}$.

证明 **Step1**：$\left([0,1],\mathcal{B}_{[0,1]},\mu_{\mathrm{G}},T_{\mathrm{G}}\right)$ 是保测系统. **证**：对任意 $s>0$，有

$$\mu_{\mathrm{G}}(T_{\mathrm{G}}^{-1}[0,s])=\mu_{\mathrm{G}}\big(\{x\in(0,1]:0\leq T_{\mathrm{G}}(x)\leq s\}\big)=\mu_{\mathrm{G}}\left(\bigsqcup_{n=1}^{\infty}[\frac{1}{s+n},\frac{1}{n}]\right)=\frac{1}{\ln 2}\sum_{n=1}^{\infty}\int_{\frac{1}{s+n}}^{\frac{1}{n}}\frac{1}{1+x}dx$$

$$= \frac{1}{\ln 2}\sum_{n=1}^{\infty}\ln\left(\frac{1+\frac{1}{n}}{1+\frac{1}{s+n}}\right) = \frac{1}{\ln 2}\sum_{n=1}^{\infty}\ln\left(\frac{1+\frac{s}{n}}{1+\frac{s}{1+n}}\right) = \frac{1}{\ln 2}\sum_{n=1}^{\infty}\int_{\frac{s}{1+n}}^{\frac{s}{n}}\frac{1}{1+x}dx = \mu_{\mathrm{G}}([0,s]).$$

Step2：T_{G} 关于 Gauss 测度 μ_{G} 遍历. **证**：给定 $n\geq 1$，定义映射 $I^n:\prod_{i=1}^n\mathbb{Z}_{\geq 1}\to\{(a,b):0<a<b<1\}, \boldsymbol{a}=(a_1,\cdots,a_n)\mapsto I^n(\boldsymbol{a}):=\{[0;x_1,\cdots]:$ 当$1\leq i\leq n$时，$x_i=a_i\}$. 事实上 $I^n(\boldsymbol{a})=[\frac{p_n+p_{n-1}}{q_n+q_{n-1}},\frac{p_n}{q_n}]$ 是个区间，这里 $\frac{p_n}{q_n}=[0;a_1,\cdots,a_n]$，并且 $I^n(\boldsymbol{a})$ 随 $\boldsymbol{a}$ 的变动构成 $[0,1]$ 的一个分拆 (最多遗漏可数多个点). 现将 $[0,1]\setminus\mathbb{Q}$ 中的数作连分数展开，根据命题 3.2(3) 得到双射 $[0,1]\setminus\mathbb{Q}\leftrightarrow\{[0;a_1,\cdots]:a_i\geq 1\}:=Z$. 易见映射 T_{G} 在 $Z=[0,1]\setminus\mathbb{Q}$ 上表现为平移 $[0;a_1,a_2,\cdots]\mapsto[0;a_2,a_3,\cdots]$. 现考虑闭区间 $A=[d,e]$，显然 $T_{\mathrm{G}}^{-n}(A)$ 是若干个区间的并，且归纳法可证 $I^n(\boldsymbol{a})\cap T_{\mathrm{G}}^{-n}(A)=[\frac{p_n+p_{n-1}d}{q_n+q_{n-1}d},\frac{p_n+p_{n-1}e}{q_n+q_{n-1}e}]$ 仍是区间. 直接计算可得 $m(I^n(\boldsymbol{a})\cap T_{\mathrm{G}}^{-n}(A))=m(A)m(I^n(\boldsymbol{a}))\cdot\left|\frac{q_n(q_n+q_{n-1})(p_nq_{n-1}-p_{n-1}q_n)}{(q_n+q_{n-1}d)(q_n+q_{n-1}e)}\right|$，并且注意到对任何 Borel 集 $B\subseteq(0,1)$ 利用 Gauss 测度的定义和 Taylor 展开可得到 $\frac{m(B)}{2\ln 2}\leq\mu_{\mathrm{G}}(B)\leq\frac{m(B)}{\ln 2}$，因此存在与 $\boldsymbol{a},A$ 有关的常数 K_1,K_2 使得 $K_1\mu_{\mathrm{G}}(A)\mu_{\mathrm{G}}(I^n(\boldsymbol{a}))\leq\mu_{\mathrm{G}}(I^n(\boldsymbol{a})\cap T_{\mathrm{G}}^{-n}(A))\leq K_2\mu_{\mathrm{G}}(A)\mu_{\mathrm{G}}(I^n(\boldsymbol{a}))$.

当 $n\to\infty$ 时，由命题 3.2(1.3) 知 $m(I^n(\boldsymbol{a}))\leq\frac{1}{2^{n-2}}\to 0$，即区间 $I^n(\boldsymbol{a})$ 的长度一致收敛于 0，加之 $I^n(\boldsymbol{a})$ 构成 $[0,1]$ 的一个分拆，故 $I^n(\boldsymbol{a})$ 可单调地逼近任意 Borel 集. 现取 Borel 集 C 满足 $T_{\mathrm{G}}^{-1}(C)=C$，注意到有逼近 $C=\bigcup_n[d_n,e_n]$ 和 $[0,1]\setminus C=\bigcup_n I^n(\boldsymbol{a}_n)$，故对上式取极限得 $\mu_{\mathrm{G}}(C)\mu_{\mathrm{G}}([0,1]\setminus C)\leq 0$，即 $\mu_{\mathrm{G}}(C)=0$ 或 1.

Step3：仅以 (1) 为例给出证明，其余证明请参考 [3] 推论 3.8. **证**：注意 $\mu_{\mathrm{G}}(A)=0$ 蕴含 A 的 Lebesgue 测度为 0. 设 $x=[0;a_1,\cdots]$，则数字 j 出现的密度即 $T_{\mathrm{G}}^n(x)\in(\frac{1}{j+1},\frac{1}{j}), n\in\mathbb{Z}_{\geq 1}$ 的密度. 对示性函数 $\mathbf{1}_{(\frac{1}{j+1},\frac{1}{j})}$ 使用 Birkhoff 遍历定理得该密度即 $\lim_{n\to\infty}\frac{1}{n}\sum_{k=0}^{n-1}\mathbf{1}_{(\frac{1}{j+1},\frac{1}{j})}(T_{\mathrm{G}}^k(x))=\int_{[0,1]}\mathbf{1}_{(\frac{1}{j+1},\frac{1}{j})}d\mu_{\mathrm{G}}=\mu_{\mathrm{G}}(\frac{1}{j+1},\frac{1}{j})=\frac{1}{\ln 2}\int_{1/(j+1)}^{1/j}\frac{1}{1+x}dx$，化简即可. 类似地，(2)、(3) 则分别是对 $f_2(x):=\ln a, x\in(\frac{1}{a+1},\frac{1}{a}), a\geq 1$、$f_3(x):=e^{f_2(x)}$ 的简单函数逼近使用 Birkhoff 遍历定理.■

在数论中经常会遇到与某个几何对象自同构群的离散子群有关的动力学问题，例如研究模形式时会需要考虑轨道空间 $\mathrm{PSL}(2,\mathbb{Z})\backslash\mathcal{H}$、微分同胚 $\mathrm{PSO}(2,\mathbb{R})\backslash\mathrm{PSL}(2,\mathbb{R})\cong\mathcal{H}$ 等. 现在我们来介绍另一个例子——上半平面中某个区域上测地流的动力学问题. 首先补充一些 Riemann 几何的背景知识.

考虑 2 维完备 Riemann 流形 $\left(\mathcal{H}:=\{z\in\mathbb{C}:\mathrm{Im}(z)>0\},\frac{|dz|^2}{\mathrm{Im}(z)^2}\right)$，这也是一个 Riemann 曲面. 定义**切丛**$T\mathcal{H}:=\mathcal{H}\times\mathbb{C}=\bigsqcup_{z\in\mathcal{H}}T_z\mathcal{H}$，这里 $T_z\mathcal{H}:=\{z\}\times\mathbb{C}$ 指 $z\in\mathcal{H}$ 处的切空间. 设 $\gamma:[0,1]\to\mathcal{H}$ 是一条可微的曲线，可以定义 γ 在 $t\in[0,1]$ 处的**导数**为 $D\gamma(t):=(\gamma(t),\gamma'(t))\in T_{\gamma(t)}\mathcal{H}$(也就是曲线在 t 处以速度为模长的切向量). 定义 $\mathcal{H}$ 上的距离度量为 $d(z_1,z_2):=\inf\{L(\gamma):[0,1]\xrightarrow{\gamma}\mathcal{H}$连续分段可微$,\gamma(0)=z_1,\gamma(1)=z_2\}$，其中 $L(\gamma):=\int_0^1\|D\gamma(t)\|_{\gamma(t)}dt$(范数 $\|\cdot\|_{\gamma(t)}$ 由 Riemann 度量诱导) 代表曲线 γ 的长度，$\|D\gamma(t)\|_{\gamma(t)}$ 代表曲线 γ 在 t 时刻的速度. 很容易验证 d 确实是 $\mathcal{H}$ 上的一个度量，并且该度量诱导的拓扑与 $\mathcal{H}$ 本来作为拓扑流形所拥有的拓扑是一致的. 我们先列出如下事实 (证明见 [12])：

命题 3.4 若规定 $\mathrm{PSL}(2,\mathbb{R})$ 在 $\mathcal{H}$ 上的作用为 $g=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right):z\mapsto\frac{az+b}{cz+d}$，则：

(1)Riemann 流形 $\mathcal{H}$ 的 (保定向) 等距自同构群、Riemann 曲面 $\mathcal{H}$ 的全纯自同构群均是 $\mathrm{PSL}(2,\mathbb{R})$. 也就是说，对任意 $z_1,z_2\in\mathcal{H},g\in\mathrm{PSL}(2,\mathbb{R})$，$d(gz_1,gz_2)=d(z_1,z_2)$. 此外，若定义 $\mathrm{PSL}(2,\mathbb{R})$ 在 $T\mathcal{H}$ 上的作用为 $g:(z,v\in T_z\mathcal{H})\mapsto(gz,dg_zv)$，记作 Dg，则 Dg 保持 Riemann 度量，这里 $d\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)_z:T_z\mathcal{H}\to T_{gz}\mathcal{H}, v\mapsto\frac{v}{(cz+d)^2}$ 指切映射.

(2)$\mathrm{PSL}(2,\mathbb{R})$ 在 $\mathcal{H}$ 上的作用是可迁的，但不是单可迁 (对任意 $z_1,z_2\in\mathcal{H}$ 只有唯一的 g 使得 $gz_1=z_2$). 但若考虑 (1) 中 $\mathrm{PSL}(2,\mathbb{R})$ 在子集 $T^1\mathcal{H}:=\{(z,v)\in T\mathcal{H}:\|v\|_z=1\}$ 上的作用 (这是合理的，因为 Dg 保持 Riemann 度量从而保持切向量的模长)，则该作用是单可迁的. 因此 $\mathrm{PSL}(2,\mathbb{R})\cong T^1\mathcal{H}, g\mapsto Dg(i,i)=(gi,\frac{i}{(ci+d)^2})$.

(3) 由 $\mathcal{H}$ 上 Riemann 度量 $\frac{|dz|^2}{\mathrm{Im}(z)^2}$ 诱导的体积形式 $dA=\frac{dxdy}{y^2}$，及其诱导的在 $T^1\mathcal{H}\cong\mathrm{PSL}(2,\mathbb{R})$ 上的体积形式 $d\sigma:=\frac{dxdyd\theta}{y^2}$(这里 θ 指 $z=x+iy$ 处切向量的倾斜角) 均在 $\mathrm{PSL}(2,\mathbb{R})$ 的作用下保持不变.

(4) 集合 $\mathscr{E}:=\{z\in\mathcal{H}:-\frac{1}{2}\leq\mathrm{Re}(z)\leq\frac{1}{2},|z|\geq 1\}$ 是子群 $\mathrm{PSL}(2,\mathbb{Z})$ 在 $\mathcal{H}$ 上作用的基本区域；集合 $\mathscr{F}:=\{g\in\mathrm{PSL}(2,\mathbb{R}):g(i)\in\mathscr{E}\}$ 是 $\mathrm{PSL}(2,\mathbb{Z})$ 在 $\mathrm{PSL}(2,\mathbb{R})\cong T^1\mathcal{H}$ 上作用的基本区域.

(5) 在 i 处的稳定子群 $\mathrm{Stab}_{\mathrm{PSL}(2,\mathbb{R})}(i)=\mathrm{PSO}(2,\mathbb{R})$，因此 $\mathrm{PSO}(2,\mathbb{R})\backslash\mathrm{PSL}(2,\mathbb{R})\cong\mathcal{H},\mathrm{PSO}(2,\mathbb{R})g\mapsto g(i)$.

(6) 设 $z_1,z_2\in\mathcal{H}$，则存在唯一连接 z_1,z_2 的曲线 $\gamma:[0,d(z_1,z_2)]\to\mathcal{H}$ 使得 $\gamma(0)=z_1,\gamma(d(z_1,z_2))=z_2$ 且该曲线在任何时刻的速度都是常数 1(即测地线). 若指定标准路径 $\phi:[0,d(z_1,z_2)]\to\{yi:y\geq 1\}\subseteq\mathcal{H}, t\mapsto e^ti$，则存在唯一等距同构 $g\in\mathrm{PSL}(2,\mathbb{R})$ 使得 $\gamma(t)=g(e^ti)$. 也就是说，从任一点发出的任意测地线都可以用 $g(e^ti)$

作参数化.

有了命题 3.4 我们给出如下定义：

定义 3.5(测地流) 设 $t\in\mathbb{R}_{>0}$. 称映射 $g_t:T^1\mathcal{H}\to T^1\mathcal{H},(z,v)\mapsto(z',v')$ 为**测地流** (Geodesic Flow)，其中 z' 为 z 沿切方向 v 的测地线以恒定速度 1 走 t 时刻后到达的点，v' 为 v 走到 z' 处时对应的切向量. 例如，$g_t(i,i)=(e^ti,e^ti)=D\begin{pmatrix}e^{t/2}&0\\0&e^{-t/2}\end{pmatrix}(i,i)$. 又由命题 3.4(2) 知任何 $(z,v)\in T^1\mathcal{H}$ 总形如 $Dg(i,i),g\in\mathrm{PSL}(2,\mathbb{R})$，所以 $g_t(z,v)=Dg(g_t(i,i))=D\left(g\begin{pmatrix}e^{t/2}&0\\0&e^{-t/2}\end{pmatrix}\right)(i,i)$. 此后为了方便约定矩阵 $\hbar_t:=\begin{pmatrix}e^{t/2}&0\\0&e^{-t/2}\end{pmatrix}\in\mathrm{PSL}(2,\mathbb{R})$.

定义 3.6(Fuchs 群) 称 $\mathrm{PSL}(2,\mathbb{R})$ 的离散子群为 **Fuchs 群**；称 Fuchs 群 Γ 为 $\mathrm{PSL}(2,\mathbb{R})$ 中的**格**，如果 $\Gamma\backslash\mathrm{PSL}(2,\mathbb{R})$ 的基本区域在命题 3.4(3) 中的体积测度 $d\sigma$ 下测度有限；称 $\mathrm{PSL}(2,\mathbb{R})$ 中的格 Γ 是**一致**的，如果 $\Gamma\backslash\mathrm{PSL}(2,\mathbb{R})$ 是紧群. 例如命题 3.4(4) 告诉我们 $\mathrm{PSL}(2,\mathbb{Z})$ 是 $\mathrm{PSL}(2,\mathbb{R})$ 中的格.

利用命题 3.4 将线性群 $\mathrm{PSL}(2,\mathbb{R})$ 与具体的几何对象 $T^1\mathcal{H}$ 等同，这样研究 $\mathrm{PSL}(2,\mathbb{R})$ 中特殊矩阵 $\hbar_t$ 的迭代相当于研究 $\mathcal{H}$ 中测地线的几何. 具体来讲，下面的图表交换. 我们断言 $\mathrm{PSL}(2,\mathbb{R})$ 中格的对应基本区域中，测地流 g_t 的迭代是遍历的.

$$\begin{array}{ccc}\mathrm{PSL}(2,\mathbb{R}) & \xrightarrow{\sim} & T^1\mathcal{H}\\ {\scriptstyle\cdot\hbar_t}\downarrow & & \downarrow{\scriptstyle g_t}\\ \mathrm{PSL}(2,\mathbb{R}) & \xrightarrow{\sim} & T^1\mathcal{H}\end{array}$$

定理 3.7(Hopf) 设 Γ 是 $\mathrm{PSL}(2,\mathbb{R})$ 中的格，考虑由测地流 $g_t:\mathrm{PSL}(2,\mathbb{R})\to\mathrm{PSL}(2,\mathbb{R}),g\mapsto gh_t$ 诱导的定义在商空间 $X:=\Gamma\backslash\mathrm{PSL}(2,\mathbb{R})$ 上的变换 $\widetilde{g_t}:X\to X,\Gamma g\mapsto\Gamma g\hbar_t$，则任意 $t>0$，$\widetilde{g_t}$ 关于测度 $d\sigma$(或记作 μ_σ，如果 $\mu_\sigma(X)\neq1$ 则用 $\frac{\mu_\sigma}{\mu_\sigma(X)}$ 替代 μ_σ)遍历. 注意，一般矩阵的右乘迭代不一定是遍历的.

证明 由命题 3.4(3) 知 $\widetilde{g_t}$ 保测. 设 $f:X\to\mathbb{R}$ 是一个可测函数且满足 $f\circ\widetilde{g_t}=f$. 对任意 $\epsilon>0$ 用 Lusin 定理取紧集 $K\subseteq X$ 满足 $\mu_\sigma(K)>1-\epsilon$ 使得 $f|_K$ 连续. 考虑集合 $B:=\left\{x\in X:\lim_{n\to\infty}\frac1n\sum_{i=0}^{n-1}\mathbf{1}_K(\widetilde{g_t}^ix)>\frac12\right\}$.

Step1： $\mu_\sigma(B)\geq1-2\epsilon$. **证：** 由 Birkhoff 遍历定理知函数列 $\left\{\frac1n\sum_{i=0}^{n-1}\mathbf{1}_K(\widetilde{g_t}^ix)\right\}$ 几乎处处收敛于 $\mathbf{1}_K^*$ 且 $\int_X\mathbf{1}_K^*d\mu_\sigma=\mu_\sigma(K)\geq1-\epsilon$. 因此 $1-\epsilon\leq\int_B\mathbf{1}_K^*d\mu_\sigma+\int_{X\setminus B}\mathbf{1}_K^*d\mu_\sigma\leq\mu_\sigma(B)+\frac12\mu_\sigma(X\setminus B)=\frac12\mu_\sigma(B)+\frac12$，证毕.

Step2： 记 $\omega_s:=\left(\begin{smallmatrix}1&s\\0&1\end{smallmatrix}\right)$. 对上述 $B\subseteq X$，$f(x)=f(x\omega_s)$ 对任意 $x,x\omega_s\in B$ 成立. **证：** 任取 $x,y:=x\omega_s\in B,s\in\mathbb{R}$，则对任意 $j\geq1$ 有 $f(x)=f(\widetilde{g_t}^jx),f(y)=f(\widetilde{g_t}^jy)$. 当 $j\to\infty$ 时，由线性群上 Riemann 度量的局部左平移不变性(见 [3] 推论 9.11. 当线性群 G 不连通时若记单位元所在连通分支 $G^\odot$ 上的度量为 d，则规定整个群上的度量为 $d_G(g_1,g_2):=\begin{cases}\frac{d(g_1,g_2)}{1+d(g_1,g_2)},g_1G^\odot=g_2G^\odot\\1,\text{其它}\end{cases}$)得 $d(\widetilde{g_t}^jx,\widetilde{g_t}^jy)\leq d(I,\hbar_t^{-j}\omega_s\hbar_t^j)=d(I,\omega_{e^{-jt}s})=d_{T^1\mathcal{H}}\big((i,i),(i+e^{-jt}s,i)\big)\to0$($\hbar_t^{-1}$ 不是测地流！)，并且注意到 $x,y\in B$，因此存在 $j_n\to\infty$ 使得 $\widetilde{g_t}^{j_n}x,\widetilde{g_t}^{j_n}y\in K$. 由于 f 在 K 上一致连续，故有 $f(\widetilde{g_t}^{j_n}x)-f(\widetilde{g_t}^{j_n}y)\to0(n\to\infty)$，这意味着当 $x,y\in B$ 时 $f(x)=f(y)$.

Step2′： 记 $\tau_s:=\left(\begin{smallmatrix}1&0\\s&1\end{smallmatrix}\right)$. 与 Step2 同理知存在 $B'\subseteq X$，$\mu_\sigma(B')\geq1-2\epsilon$ 使得 $f(x)=f(x\tau_s)$ 对任意 $x,x\tau_s\in B'$ 成立. 令 $\epsilon\to0$ 则可设 $\mu_\sigma(B)=\mu_\sigma(B')=1$.

Step3： 若记 $P_\triangle:=\left\{\left(\begin{smallmatrix}1&0\\s&1\end{smallmatrix}\right):s\in\mathbb{R}\right\},P^\triangle:=\left\{\left(\begin{smallmatrix}1&s\\0&1\end{smallmatrix}\right):s\in\mathbb{R}\right\}$，则 $\mathrm{SL}(2,\mathbb{R})=\langle P_\triangle,P^\triangle\rangle$. **证：** 事实上，任意 $g\in\mathrm{SL}(2,\mathbb{R})$ 都可以写成 $g=\tau_{s_4}\omega_{s_3}\tau_{s_2}\omega_{s_1}$.

Step4： 任意 $g\in\mathrm{PSL}(2,\mathbb{R})$，总存在 X_g 使得 $\mu_\sigma(X_g)=1$ 且任意 $x\in X_g$ 总有 $f(x)=f(xg)$. **证：** 根据 Step2 和 Step2′ 取 $C:=B\cap B'$，则 $\mu_\sigma(C)=1$. 由 Step3 设 $g=\tau_{s_4}\omega_{s_3}\tau_{s_2}\omega_{s_1}\in\mathrm{PSL}(2,\mathbb{R})$，考虑测度为 1 的集合 $X_g:=C\cap C\tau_{s_4}^{-1}\cap C(\tau_{s_4}\omega_{s_3})^{-1}\cap C(\tau_{s_4}\omega_{s_3}\tau_{s_2})^{-1}\cap Cg^{-1}$，则对任意 $x\in X_g$ 有 $f(x)=f(xg)$.

Step5： 若 $f\in L^1(X,\mu_\sigma)$ 非常值，则针对某个 $g\in X$ 可构造 $a\in X_g$ 使 $f(a)\neq f(ag)$，与 Step4 矛盾. **证：** 存在 $I_1,I_2\subseteq\mathbb{R}$ 使得 $T_j:=\{x\in X:f(x)\in I_j\},j=1,2$ 既不全是零测集也不全补集零测. 由 [3] 命题 8.6 知存在 $g\in X$ 使得 $\mu_\sigma(T_1\cap T_2g^{-1})>0$. 但由于 X_g^c 零测，故存在 $a\in T_1\cap T_2g^{-1}\cap X_g$，这与 $f(x)=f(xg)$ 矛盾.■

4、遍历分解

一类很自然的问题是：给定拓扑空间 X 及其上的连续变换 $T:X\to X$，我们希望找出那些 T- 不变的测

度 μ(如果存在的话，见命题 4.2)，使得 $(X,\mathcal{B}_X,\mu,T)$ 是一个保测系统. 当然我们还要问这些 T-不变的测度中哪些是遍历的？这个问题当 X 是紧致度量空间时答案是明确的：遍历测度在某种意义下是极端的不变测度 (见定理 4.3). 在具体给出这个断言的证明这之前我们先做一些准备工作.

设 T 是紧致度量空间 (X,d) 上的连续变换，记 $\mathcal{M}(X)$ 为 X 上所有概率测度作成的集合. 关于 $\mathcal{M}(X)$，[3] 定理 B.11 有如下描述：

命题 4.1 (1) 设 $\mu_1,\mu_2\in\mathcal{M}(X)$，则 $\mu_1=\mu_2$ 当且仅当对任意 $f\in C(X)$，$\int_X f d\mu_1=\int_X f d\mu_2$.

(2) 称 $\mathcal{M}(X)$ 上使所有映射 $\mu\mapsto\int_X f d\mu, f\in C(X)$ 连续的最粗的拓扑为**弱 *-拓扑** (Weak *-Topology)，则该拓扑使 $\mathcal{M}(X)$ 成为一个紧致度量空间.

(3)$\mathcal{M}(X)$ 是凸集；若记所有 T-不变测度作成的集合为 $\mathcal{M}^T(X)$，则 $\mathcal{M}^T(X)$ 是 $\mathcal{M}(X)$ 的闭凸紧子集.

(4) 在弱 *-拓扑下 $\mu_n\to\mu$ 当且仅当：对任意 $f\in C(X)$ 有 $\int_X f d\mu_n\to\int_X f d\mu$，且对任意闭集 $C\subseteq X$ 有 $\limsup_{n\to\infty}\mu_n(C)\le\mu(C)$，且对任意开集 $O\subseteq X$ 有 $\liminf_{n\to\infty}\mu_n(O)\ge\mu(O)$，且对任意满足 $\mu(\partial(B))=0$ 的 Borel 集 B 有 $\mu_n(B)\to\mu(B)$.

命题 4.2(Kryloff-Bogoliouboff) 设 (X,d) 是紧致度量空间，$T:X\to X$ 是连续映射，$\{\eta_n\}\subseteq\mathcal{M}(X)$. 则序列 $\left\{\mu_n:=\frac{1}{n}\sum_{i=0}^{n-1}\eta_n\circ T^i\right\}$ 的任意聚点 (在弱 *-拓扑下) 均属于 $\mathcal{M}^T(X)$. 因此根据紧致性知 $\mathcal{M}^T(X)$ 非空.

证明 不失一般性设 $\mu_n\to\mu$. 取定 $f\in C(X)$，则 f 和 $f\circ T^i$ 有界. 当 $n\to\infty$ 时有

$$\left|\int_X f\circ T d\mu_n-\int_X f d\mu_n\right|=\frac{1}{n}\left|\int_X\sum_{i=0}^{n-1}(f\circ T^{i+1}-f\circ T^i)d\eta_n\right|=\frac{1}{n}\left|\int_X(f\circ T^{n+1}-f)d\eta_n\right|\le\frac{2}{n}\sup|f|\to 0,$$

即 $\int_X f\circ T d\mu=\int_X f d\mu$，因此由命题 1.3 知 μ 是 T-不变测度.■

定理 4.3 设 (X,d) 是紧致度量空间，$T:X\to X$ 是可测映射，则 $\mathcal{M}^T(X)$ 中的测度遍历当且仅当它是 $\mathcal{M}^T(X)$ 中的极端点 (即它不能表成其它两个不变测度的非平凡凸线性组合). 特别地，若还假设 T 连续，则由命题 4.2 可知一定存在 T-遍历测度.

证明 充分性. 反证法，设 $\mu\in\mathcal{M}^T(X)$ 非遍历，则存在可测集 B 满足 $T^{-1}B=B$ 但 $\mu(B)\in(0,1)$. 考虑 $\frac{1}{\mu(B)}\mu|_B,\frac{1}{\mu(X\setminus B)}\mu|_{X\setminus B}\in\mathcal{M}^T(X)$，则 $\mu=\mu(B)(\frac{1}{\mu(B)}\mu|_B)+\mu(X\setminus B)(\frac{1}{\mu(X\setminus B)}\mu|_{X\setminus B})$，矛盾.

必要性. 设 $\mu=s\eta_1+(1-s)\eta_2$ 是遍历测度，由 Riesz 表示定理知存在 $f\in L^1(X,\mu)$ 使得 $\eta_1(B)=\int_B f d\mu$. 考虑可测集 $E:=\{x\in X:f(x)<1\}$，不妨设 $\mu(E)>0$，下证 $\mu(E\setminus T^{-1}E)=0$. 反证法，若 $\mu(E\setminus T^{-1}E)>0$. 注意到 $f(x)<1$ 对所有 $x\in E\setminus T^{-1}E$ 成立，故存在 $\epsilon>0$ 使得 $\mu|_{E\setminus T^{-1}E}(\{x:f(x)<1-\epsilon\})>0$. 若记 $M:=(E\setminus T^{-1}E)\cap\{x:f(x)<1-\epsilon\},N:=(E\setminus T^{-1}E)\cap\{x:f(x)\ge1-\epsilon\}$，则 $\int_{E\setminus T^{-1}E}f d\mu\le(1-\epsilon)\mu(M)+\mu(N)<\mu(E\setminus T^{-1}E)$ 且 $\int_{(T^{-1}E)\setminus E}f d\mu\ge\mu(T^{-1}E\setminus E)=\mu(E\setminus T^{-1}E)$. 又由于 $\int_{E\cap T^{-1}E}f d\mu+\int_{E\setminus T^{-1}E}f d\mu=\eta_1(E)=\eta_1(T^{-1}E)=\int_{E\cap T^{-1}E}f d\mu+\int_{(T^{-1}E)\setminus E}f d\mu$，而这与上面两个不等式矛盾，因此 $\mu(E\setminus T^{-1}E)=\mu(T^{-1}E\setminus E)=0$，即 $\mu((T^{-1}E)\triangle E)=0$. 由于 μ 遍历，故 $\mu(E)=1$，而这又导致 $\eta_1(X)=\int_E f d\mu<1$，与概率测度的定义矛盾，因此 $\mu(E)=0$. 类似地，$\mu(\{x\in X:f(x)>1\})=0$，故几乎处处 $f=1$，所以 $\eta_1=\mu$.■

虽然遍历测度在所有不变测度当中的地位比较极端，但不变测度的性质却由遍历测度很大程度地反映 (换句话说，可以用遍历测度表示不变测度). 例如研究函数关于某个不变测度的积分时可以转化为研究它关于所有遍历测度的积分$\left($类比复变函数中的 Cauchy 积分公式 $f(z)=\frac{1}{2\pi i}\oint\frac{f(\zeta)}{z-\zeta}d\zeta\right)$，这就是遍历分解定理的想法：

定理 4.4(遍历分解) 设 (X,d) 是紧致度量空间，$T:X\to X$ 是连续映射，则对任意 $\mu\in\mathcal{M}^T(X)$，总存在唯一定义在紧致度量空间 $\mathcal{M}^T(X)$ 上的概率测度 ρ，满足：(1) 若记 $\mathcal{M}^T(X)$ 中所有 T-遍历测度作成的集合为 $\mathcal{E}^T(X)$，则 $\rho(\mathcal{E}^T(X))=1$；(2) 对任意 $f\in C(X)$，$\int_X f d\mu=\int_{\mathcal{E}^T(X)}\left(\int_X f d\eta\right)d\rho(\eta)$.

特别地，当 $\mathcal{M}^T(X)$ 中只有一个元素时那么它一定是遍历的；如果 $\mathcal{M}^T(X)$ 中有多于一个元素时那么一定有无穷多个元素. 我们更关心前面那种情况，因为这时的动力系统有很多有用的性质.

命题 4.5 设 (X,d) 是紧致度量空间，$T:X\to X$ 是连续映射，则下述说法等价：

(1)$|\mathcal{M}^T(X)|=1$. (2)$|\mathcal{E}^T(X)|=1$. (3) 对任意 $f\in C(X)\left($或 $C(X)\hookrightarrow\mathcal{M}(X),f\mapsto(\mu_f:B\mapsto\int_B f d\mu_f)\right.$ 的一个稠密子集$\left.\right)$，$\mathsf{A}(N,f)$ 趋于某个与 x 无关的常数$\left($事实上若 $\mu\in\mathcal{M}^T(X)$，则这个常数为 $\int_X f d\mu\right)$.

称满足上述任何一个条件的 T 是**唯一遍历**的 (Uniquely Ergodic).

证明 $(1\Leftrightarrow 2)$ 定理 4.3 和定理 4.4；$(3\Rightarrow 1)$Lebesgue 控制收敛定理；$(1\Rightarrow 3)$ 命题 4.1 和命题 4.2.■

例 4.6 考虑例 1.2(1) 中的系统 $(\mathbb{T},\mathcal{B}_{\mathbb{T}},m,R_\alpha)$，我们知道 R_α 遍历当且仅当 α 是无理数，此时仅当 $k=0$ 时有 $e^{2\pi ik\alpha}=1$. 考虑正交基 $\{f_k(t):=e^{2\pi ikt}\}_{k\in\mathbb{Z}}$，注意到 $\mathsf{A}(N,f_k)=\frac{1}{N}\sum_{n=0}^{N-1}e^{2\pi ik(t+n\alpha)}\to\left\{\begin{smallmatrix}1,k=0\\0,k\neq 0\end{smallmatrix}\right.=\int_{\mathbb{T}}f_k dm$，因此对任意 $f\in C(\mathbb{T})$ 均满足命题 4.5(3) 的条件，故 R_α 唯一遍历. 而当 α 是有理数时 Lebesgue 测度是非遍历的不变测度，故此时应该有其它使 R_α 遍历的不变测度.

现在给出唯一遍历性的应用——证明 Weyl 定理. 首先根据注意 2.6 的理由抽象 Birkhoff 遍历定理，我们引出均匀分布的概念：

定义 4.7(均匀分布) 设 (X,d) 是紧致度量空间，μ 是 X 上的概率测度. 称序列 $\{x_n\}\subseteq X$ 关于 μ **均匀分布**，如果对任意 $f\in C(X)$，$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^n f(x_i)=\int_X f d\mu$. 由 Riesz 表示定理，这等价于 $\frac{1}{n}\sum_{i=1}^n\delta_{x_i}\to\mu$(在弱 *-拓扑下)，其中 $\delta_{x_i}:A\mapsto\left\{\begin{smallmatrix}1,x_i\in A\\0,x_i\notin A\end{smallmatrix}\right.$. 应该强调，由于 $\mathcal{M}(X)$ 是度量空间，故该极限唯一 (也就是说关于 μ 均匀分布的序列一定不会关于其它测度均匀分布).

对连续映射 $T:X\to X$ 的遍历测度直接应用 Birkhoff 遍历定理和命题 4.5(3) 立得：

引理 4.8 设 (X,d) 是紧致度量空间，$T:X\to X$ 是连续映射，$\mu\in\mathcal{E}^T(X)$，则在测度 μ 下对几乎所有的 $x\in X$，其轨道集 $\{T^nx\}$ 关于 μ 均匀分布. 特别地，若 T 还是唯一遍历的，则对任意 $x\in X$，轨道集 $\{T^nx\}$ 关于这个唯一的 μ 均匀分布. 例如，例 4.6 中当 α 是无理数时，对任意 $x\in\mathbb{T}$，$\{R_\alpha^nx\}\subseteq\mathbb{T}$ 关于 Lebesgue 测度均匀分布 (该结论的推广见定理 4.9).

定理 4.9(Weyl) 设 $p(n)=a_kn^k+\cdots+a_0\in\mathbb{R}[n]$ 且至少有某个 $a_i(1\leq i\leq k)$ 是无理数，则序列 $\{p(n)(\mathrm{mod}\ 1)\}_{n\in\mathbb{Z}_{\geq 0}}$ 在区间 $[0,1]$ 中关于 Lebesgue 测度均匀分布.

证明 **Step1：(Furstenberg)**设紧致度量空间上的同胚 $T:X\to X$ 唯一遍历，记此时的 T-遍历测度为 μ. 设 G 是紧 Abel 群并带有 Haar 测度 m_G，设 $c:X\to G$ 是连续映射，定义 $\Theta:X\times G\to X\times G,(x,g)\mapsto(T(x),c(x)g)$. 若 Θ 在乘积测度 $\mu\times m_G$ 下遍历，则它是唯一遍历的. **证：**Θ 保测由 T 和左平移的保测性得到：由 Fubini 定理知对任意 $f\in C(X\times G)$，$\int_{X\times G}f\circ\Theta d(\mu\times m_G)=\int_X\int_G f(x,g)dm_Gd\mu=\int_{X\times G}fd(\mu\times m_G)$. 现设 Θ 遍历，记 $E:=\big\{(x,g):\{\Theta^n(x,g)\}\text{关于}\mu\times m_G\text{均匀分布}\big\}$，由引理 4.8 知 $(\mu\times m_G)(E)=1$. 任取 $h\in G$，则 $(x,g)\in E$ 意味着 $(x,gh)\in E$ 且对任意 $f\in C(X\times G)$ 均有 $\frac{1}{N}\sum_{n=0}^{N-1}f(\Theta^n(x,gh))\to\int_{X\times G}fd(\mu\times m_G)$. 因此存在 $E_1\subseteq X,\mu(E_1)=1$ 使得 $E=E_1\times G$. 另设 η 是一个 Θ-遍历测度，定义投射 $\pi:X\times G\to X,(x,g)\mapsto x$. 不难验证 $\Theta^{-1}\pi^{-1}A=\pi^{-1}T^{-1}A$，因此由 η 的不变性知 $\eta\circ\pi^{-1}$ 是一个 T- 不变测度，由遍历唯一性知 $\eta\circ\pi^{-1}=\mu$. 特别地，我们有 $\eta(E)=\eta(E_1\times G)=\mu(E_1)=1$，故由引理 4.8 知必然存在 $(x,g)\in E$ 使得 $\{\Theta^n(x,g)\}$ 关于 η 均匀分布. 由 E 的定义和定义 4.7 可知 $\eta=\mu\times m_G$.

Step2：设 α 是无理数，则映射 $\phi:\mathbb{T}^k\to\mathbb{T}^k,(x_1,\cdots,x_k)\mapsto(x_1+\alpha,x_2+x_1,\cdots,x_k+x_{k-1})$ 唯一遍历. **证：**由 Step1 和例 4.6 知只需证 ϕ 关于 $\mathbb{T}^k$ 上的 Lebesgue 测度遍历. 设 $f\in L^2$ 满足 $f\circ\phi=f$，考虑 Fourier 反演 $f(\boldsymbol{x})=\sum_{\boldsymbol{n}\in\mathbb{Z}^k}c_{\boldsymbol{n}}e^{2\pi i\boldsymbol{n}\boldsymbol{x}}=f(\phi\boldsymbol{x})=\sum_{\boldsymbol{n}\in\mathbb{Z}^k}c_{\boldsymbol{n}}e^{2\pi i\boldsymbol{n}\phi(\boldsymbol{x})}=\sum_{\boldsymbol{n}\in\mathbb{Z}^k}c_{\boldsymbol{n}}e^{2\pi in_1\alpha}e^{2\pi i\phi'(\boldsymbol{n})\boldsymbol{x}}$，这里 $\phi':\mathbb{Z}^k\to\mathbb{Z}^k,(n_1,\cdots,n_k)\mapsto(n_1+n_2,n_2+n_3,\cdots,n_{k-1}+n_k,n_k)$ 是自同构，$\sum_{\boldsymbol{n}\in\mathbb{Z}^k}|c_{\boldsymbol{n}}|^2<\infty$. 由 Fourier 系数的唯一性得 $c_{\phi'(\boldsymbol{n})}=e^{2\pi i\alpha n_1}c_{\boldsymbol{n}}$，故对任意 $\boldsymbol{n}\in\mathbb{Z}^k$ 都有 $|c_{\phi'(\boldsymbol{n})}|=|c_{\boldsymbol{n}}|$. 因此要么 $\boldsymbol{n},\phi'(\boldsymbol{n}),\cdots,\phi'^2(\boldsymbol{n}),\cdots$ 两两不同 (此时 $c_{\boldsymbol{n}}=0$)，要么存在 $p>q$ 使得 $\phi'^p(\boldsymbol{n})=\phi'^q(\boldsymbol{n})$(此时对 k 向下归纳得 $n_2=n_3=\cdots=n_k=0$). 对于后者问题只剩下 $\boldsymbol{n}=(n_1,0,\cdots,0)$，而由 $c_{\boldsymbol{n}}=e^{2\pi in_1\alpha}c_{\boldsymbol{n}}$ 得 $n_1=0$ 或 $c_{\boldsymbol{n}}=0$. 所以 f 只能几乎处处为常数，由命题 2.3(6) 知 ϕ 遍历.

Step3：定理 4.9 的证明. **证：**如果 a_k 是无理数，考虑 $\{\alpha\}\times\mathbb{T}^k\cong\mathbb{T}^k$ 与 Step2 中的 ϕ，我们定义 $\widetilde{\phi}(\alpha,\boldsymbol{x}):=(\mathrm{id},\phi)(\alpha,\boldsymbol{x})=(\alpha,x_1,x_2,\cdots,x_k)\begin{pmatrix}1&1&0&\cdots&0\\0&1&1&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&1\end{pmatrix}=(\alpha,x_1+\alpha,x_2+x_1,\cdots,x_k+x_{k-1})$. 迭代得到 $\widetilde{\phi}^n(\alpha,\boldsymbol{x})=(\alpha,\boldsymbol{x})\begin{pmatrix}1&1&0&\cdots&0\\0&1&1&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&1\end{pmatrix}^n=(\alpha,\boldsymbol{x})\begin{pmatrix}1&n&\binom{n}{2}&\cdots&\binom{n}{k}\\0&1&n&\cdots&\binom{n}{k-1}\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&1\end{pmatrix}=\big(\alpha,n\alpha+x_1,\cdots,\binom{n}{k}\alpha+\binom{n}{k-1}x_1+\cdots+x_k\big)$. 现令上文中的无理数 $\alpha:=k!a_k$，则由待定系数法可取 $\boldsymbol{x}=(x_1,\cdots,x_k)\in\mathbb{T}^k$ 使得 $p(n)\equiv\binom{n}{k}\alpha+\binom{n}{k-1}x_1+\cdots+x_k(\mathrm{mod}\ 1),n\geq k$. 根据 Step2 和引理 4.8 得 $\{\widetilde{\phi}^n(\alpha,\boldsymbol{x})\}\subseteq\{\alpha\}\times\mathbb{T}^k$ 关于 Lebesgue 测度均匀分布，这意味着最后一个分量 $\{p(n)(\mathrm{mod}\ 1)\}\subseteq\mathbb{T}$ 关于 Lebesgue 测度均匀分布. 如果 a_k 是有理数，那么 $qa_k\in\mathbb{Z}$ 从而 mod 1 之后 k 次项消失，使用归纳法即可.■

5、不定二次型

二次型分为确定二次型 (正定、负定、半正定、半负定) 和不定二次型，本节主要讨论不定二次型在保定向变换——即 $\mathrm{SL}(3,\mathbb{R})$ 中矩阵作用下的性质 (因为反转定向会改变二次型的不定性).

Oppenheim 在 1929 年猜测任何未定元个数大于 2 且不与有理二次型成比例的不定二次型将整点映为 $\mathbb{R}$ 的稠密子集，而 Margulis 在 1986 年证明了该猜想的更强版本：可以做到使这样的二次型任意逼近 0，但不为 0. 我们不去证明这个更强的版本 (见 [5]Chapter4)，因为证明办法与解决 Oppenheim 猜想的想法无异. 本节只介绍最简单版本的 Margulis 定理的证明思路，首先给出主要结论：

定理 5.1(Margulis) 设 $n\geq 3$，B 是一个不与有理系数二次型成比例的不定二次型 (例如 $x^2+y^2-\sqrt{2}z^2$)，则对任意 $\epsilon>0$，总存在 $\mathbf{0}\neq(x_1,\cdots,x_n)\in\mathbb{Z}^n$ 使得 $|B(x_1,\cdots,x_n)|<\epsilon$.

定理 5.1 可视作例 1.2(1) 的推广. 事实上，当 α 是无理数时，对任何 $t\in\mathbb{T}$ 序列 $\{R_\alpha^n(t)\}$ 均在 $\mathbb{T}$ 中稠密，这也相当于是说一次型 $L(t,n):=t+n\alpha$ 的像 $L(\mathbb{Z}^2)$ 在 $\mathbb{R}$ 中稠密.

注意 5.2 定理 5.1 中的约束条件都是必要的：(1) 如果 B 是正定的或负定的，则使 $B=0$ 的整点只有 $\mathbf{0}$；(2) 如果 B 是某个有理二次型的倍数，则 $B(\mathbb{Z}^n)$ 一定会落在 $\mathbb{R}$ 的某个离散子群中；(3) 当 $n=2$ 时，Diophantine 逼近([3] 命题 3.10：连分数 $u=[a_0;a_1,\cdots]$ 若满足 $\{a_n\}$ 有界，则存在 $\epsilon>0$ 使得对任何 $\frac{p}{q}\in\mathbb{Q}$ 均有 $|u-\frac{p}{q}|\geq\frac{\epsilon}{q^2}$，且 Lagrange 定理指出任何二次无理数的连分数展开都满足这个条件)告诉我们二次型 $\sqrt{2}x^2-y^2$ 就不满足要求.

若要证明定理 5.1，则只需要考虑 $n=3$ 的情况，这会涉及到一些 3 维的线性群. 为此首先约定一些记号：

定义 5.3 记 $G:=\mathrm{SL}(3,\mathbb{R})$，$\Gamma:=\mathrm{SL}(3,\mathbb{Z})$，$\Omega:=\{\mathbb{R}^3\text{中体积为1的格}\}$，$N_G(F):=\{x\in G:xF=Fx\}$，$d(t):=\begin{pmatrix}t&0&0\\0&1&0\\0&0&t^{-1}\end{pmatrix}$，$v_1(t):=\begin{pmatrix}1&t&\frac{t^2}{2}\\0&1&t\\0&0&1\end{pmatrix}=\exp t\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}$，$v_2(t):=\begin{pmatrix}1&0&t\\0&1&0\\0&0&1\end{pmatrix}=\exp t\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}$，$D:=\{d(t):t>0\}$，$V_1:=\{v_1(t):t\in\mathbb{R}\}$，$V_2:=\{v_2(t):t\in\mathbb{R}\}$，$V_2^+:=\{v_2(t):t>0\}$，$V_2^-:=\{v_2(t):t<0\}$，$V:=V_1\cdot V_2:=\left\{\begin{pmatrix}1&t&s\\0&1&t\\0&0&1\end{pmatrix}:t,s\in\mathbb{R}\right\}$，$W:=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}:a,b,c\in\mathbb{R}\right\}$.

事实上可以把定理 5.1 化归为一个连续 (齐性) 动力系统问题 (这里的动力系统与我们之前介绍的那些迭代动力系统本质上是不一样的)：

定理 5.4(Margulis) 记 G 中保持二次型 $2x_1x_3-x_2^2$ 不变的矩阵构成子群 H. 在一一对应 $G/\Gamma\overset{\sim}{\to}\Omega,g\Gamma\mapsto g\,\mathbb{Z}^3$ 下 (这解释了为何线性群的离散子群被称为格)，若 $z\in\Omega=G/\Gamma$ 满足 $\overline{Hz}$ 在 Ω 中紧，则商群 $H/(H\cap\mathrm{Stab}_G(z))$ 是紧群.

应特别强调这里的 H 相当复杂，一般是很难算出来的. 倘若先承认定理 5.4，则可给出 Oppenheim 猜想的证明：

定理 5.1 的证明 记保持不定二次型 B 不变的矩阵构成 (无限) 子群 $H_B\subseteq G$，通过非退化线性替换可以将 B 约化为 $\lambda(2x_1x_3-x_2^2),\lambda=\pm1$ 的形式，这意味着存在 $g_B\in G$ 使得 $H=g_BH_Bg_B^{-1}$. 反证法，若存在 $\epsilon>0$ 使得对任意 $\mathbf{0}\neq\boldsymbol{x}\in\mathbb{Z}^3$ 均有 $|B(\boldsymbol{x})|>\epsilon$，则任意 $h\in H_B$，$|B(\boldsymbol{x})|>\epsilon$ 对 $\mathbf{0}\neq\boldsymbol{x}\in h\,\mathbb{Z}^3$ 恒成立. 根据 Mahler 定理$\Big($子集 $S\subseteq\Omega$ 的闭包 $\overline{S}$ 在 Ω 中紧当且仅当 $|\det(S)|$ 有界且存在邻域 $\mathbf{0}\in N\subseteq\mathbb{R}^3$ 满足对任意 $\Lambda\in S$ 均有 $\Lambda\cap N=\{\mathbf{0}\}$. 此处取 $N:=\{\boldsymbol{x}\in\mathbb{R}^3:|B(\boldsymbol{x})|\leq\epsilon\}\Big)$和平移不变性知 $\overline{H_B\,\mathbb{Z}^3}$ 在 Ω 中紧，故由定理 5.4 得 $H/(H\cap\mathrm{Stab}_G(g_B\,\mathbb{Z}^3))$ 是紧群. 注意到 $\mathrm{Stab}_G(g_B\,\mathbb{Z}^3)=g_B\Gamma g_B^{-1}$，所以 $H_B/(H_B\cap\Gamma)$ 紧. 由 [18] 的结果可知在 Zariski 拓扑下 $H_B\cap\Gamma$ 在 H_B 中稠密，而代数群理论([19]Chapter AG：若仿射簇上的 $\mathbb{Q}$-点在 Zariski 拓扑下稠密，则该簇定义在 $\mathbb{Q}$ 上)告诉我们 H_B 中的元素皆是有理矩阵，故对任意 $\sigma\in\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ 均有 $H_B=H_{\sigma B}$. 任取 $\sigma\in\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$，由于 $\frac{\sigma B(g\boldsymbol{x})}{B(g\boldsymbol{x})}$ 对任意 $g\in H_B$ 取值不变，因而 σB 和 B 成比例 (比值可以是复数). 根据 σ 的任意性易得 B 与某个有理二次型成比例，矛盾.■

剩下的工作便是处理定理 5.4，它的证明来自于代数群论和“遍历论”(严格来说不是遍历论，而是动力系统的拓扑理论. 笔者也不知道为什么 Margulis 要将自己的工作称为“遍历论”). 介绍这些内容需要很多有关拓扑群的准备，故在此我们不打算一一证明这些结论 (详见 [5]Chapter2)，因为它们虽不涉及高深的技巧但却很麻烦，我们只需要解释这些引理出现的动机即可.

引理 5.5 (1) 设 G 是有可数拓扑基的局部紧群，Ω 是一个拓扑空间，G 在 Ω 上连续且可迁地作用.

(1.1) 设 $F\subseteq P, F\subseteq P'$ 均是 G 的闭子群，$Y,Y'\subseteq\Omega$ 是闭子集且 Y 是紧的极小 F-不变子集 (所谓极小 F-不变是指：$FY=Y$ 且任意 $y\in Y$，Fy 在 Y 中稠密)，M 是 G 的子集. 如果 $PY=Y, P'Y'=Y'$，且对任意 $m\in M$ 均有 $mY\cap Y\neq\varnothing$，则任意 $h\in N_G(F)\cap\overline{P'MP}$(只视作集合，下同)，均有 $hY\subseteq Y'$.

(1.1′) 设 $F\subseteq P$ 均是 G 的闭子群，$Y\subseteq\Omega$ 是闭且紧的极小 F-不变子集，M 是 G 的子集. 如果 $PY=Y$，且对任意 $m\in M$ 均有 $mY\cap Y\neq\varnothing$，则任意 $h\in N_G(F)\cap\overline{PMP}$，均有 $hY=Y$.

(1.2) 设 F 是 G 的闭子群，$y\in\Omega$. 若商群 $F/(F\cap\mathrm{Stab}_G(y))$ 非紧且 Fy 是紧的极小 F-不变子集，则 $\mathrm{id}\in\overline{\{g\in G\setminus F: gy\in Fy\}}$.

(2) 若采用定义 5.3 和定理 5.4 的记号，则：

(2.0)$D\subseteq H$，$V_1=H\cap W$.

(2.1) 如果子集 $M\subseteq G\setminus H$ 且 $\mathrm{id}\in\overline{M}$，则集合 $\overline{HMDV_1}$ 要么包含 V_2^+，要么包含 V_2^-.

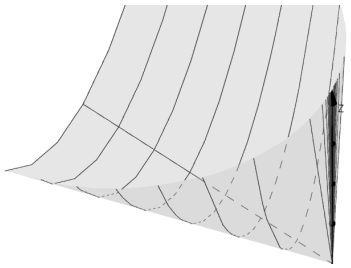
(2.2) 如果 $M\subseteq G\setminus V_1$，则集合 $N_G(V_1)\cap\overline{V_1MV_1}$ 生成的子群的闭包 $\overline{\langle N_G(V_1)\cap\overline{V_1MV_1}\rangle}$ 要么包含 V，要么包含形如 $vDV_1v^{-1}, v\in V$ 的子群.

(2.3) 设 $y\in\Omega$. 如果 $\overline{Dy}$ 在 Ω 中紧，则 $W\cap\mathrm{Stab}_G(y)=\{\mathrm{id}\}$. 此外，对任意 W 的非平凡闭子群 U，商群 $U/(U\cap\mathrm{Stab}_G(y))$ 均非紧.

(2.4) 对任意 $y\in\Omega$，$\overline{DV_1V_2^+y}$ 和 $\overline{DV_1V_2^-y}$ 均在 Ω 中非紧.

关于引理 5.5 我们作如下注释，让这些结论符合直觉，借此替代证明. 在这里我们应该从矩阵的几何意义入手，把定义 5.3 中的矩阵看成 $\mathbb{R}^3$ 中的变换，采用的工具无非是线性代数.

注意 5.6 在引理 5.5 中，(1.1′) 找到了一些在 P 之外，但对 Y 的作用又是良好定义 ($hY\subseteq Y$) 的元素，因为考虑子群 P 的作用时这部分信息不应该被忽略；(2.1) 是在讨论 V_1 中的变换 (相对复杂) 该通过何种方式与 V_2 中的切变变换 (相对容易) 联系起来，而 (2.2) 则是对该关系的进一步讨论；(2.4) 中，不妨就取二次型 $y=2x_1x_3-x_2^2\leftrightarrow(e_1,-e_2,e_3)$，这里 $\{e_i\}$ 是 $\mathbb{Z}^3$ 的标准正交基. 首先 Mahler 定理告诉我们 $\overline{H\mathbb{Z}^3}$ 紧，其次通过简单的计算可得 $DV_1V_2^+y=\left\{\left(xe_1-xye_2+(xz+\frac{xy^2}{2})e_3,-e_2+ye_3,\frac{1}{x}e_3\right): x,z>0,y\in\mathbb{R}\right\}$. 此处第一个坐标分量的取值曲面如下，破坏紧致性的原因一目了然 (图源 GeoGebra，永远的神)：



定理 5.4 的证明 证明分如下几步：

Step1：由于 $\overline{Hz}$ 紧且是 H-不变的，所以它包含了一个闭的极小 H-不变子集 T. 注意到 $H\supseteq V_1$ 且 T 是紧空间的闭子集因而紧，故 T 包含了一个闭的极小 V_1-不变子集 T'. 取 $y\in T'$，显然 $\overline{Hy}$ 在紧空间 T 中紧. 又由 $D\subseteq H$ 知 $\overline{Dy}$ 是 $\overline{Hy}$ 的闭子集因而紧，故根据引理 5.5(2.3) 得 $V_1/(V_1\cap\mathrm{Stab}_G(y))$ 非紧，再用引理 5.5(1.2) 可知集合 $K:=\{g\in G\setminus V_1: gy\in V_1y\}$ 的闭包 $\overline{K}$ 包含 id. 记 $\Psi:=\overline{\langle N_G(V_1)\cap\overline{V_1KV_1}\rangle}$，由引理 5.5(1.1′) 立得 $\Psi T'=T'$.

Step2：引理 5.5(2.2) 断言 Ψ 要么包含 V，要么包含 $vDV_1v^{-1}, v\in V$. 而当选取 $v\in V\setminus V_1$ 时利用线性代数可以直接验证 vDV_1v^{-1} 只能包含 V_2^+ 或 V_2^- 其中之一，即 $DV_1(vDV_1v^{-1})$ 要么包含 $DV_1V_2^+$，要么包含 $DV_1V_2^-$. 若 $\Psi\not\supseteq DV_1$ 且 $\Psi\not\supseteq V$，则存在 $v\in V$ 使得 $DV_1\Psi\supseteq DV(vDV_1v^{-1})\supseteq DV_1V_2^{+,-}$. 但根据 $HT=T, T'\subseteq T, DV_1\subseteq H$ 我们有 $DV_1T'\subseteq T$，由 Step1 得 $T\supseteq DV_1\Psi T'$，并且注意到 T 紧，此时引理 5.5(2.4) 蕴含 $DV_1\Psi\not\supseteq V_1V_2^+, DV_1\Psi\not\supseteq V_1V_2^-$，矛盾. 因此 $\Psi\supseteq DV_1$. 结合 Step1 可知 $DV_1T'\subseteq\Psi T'=T'\subseteq DV_1T'$.

Step3：记 $M:=\{g\in G\setminus H: gy\in\overline{Hz}\}$. 反证法，设 $\mathrm{id}\in\overline{M}$，则由引理 5.5(2.1) 知 $\overline{HMDV_1}$ 要么包含 V_2^+，要么包含 V_2^-. 此外根据 Step2($DV_1T'=T'$) 以及引理 5.5(1.1)，对任意 $g\in N_G(V_1)\cap\overline{HMDV_1}$ 均有 $gT'\subseteq\overline{Hz}$. 所以 $\overline{Hz}$ 要么包含 V_2^+T'，要么包含 V_2^-T'. 根据 Step2 且结合等式 $DV_1V_2^+=V_2^+DV_1, DV_1V_2^-=V_2^-DV_1$ 得紧集 $\overline{Hz}$ 要么包含 $DV_1V_2^+T'$，要么包含 $DV_1V_2^-T'$，而这与引理 5.5(2.4) 矛盾，因此 $\mathrm{id}\notin\overline{M}$.

Step4：因为 $\overline{Hy}\subseteq T\subseteq\overline{Hz}$，根据极小性这三个集合只能相等. 所以，Step3 连同引理 5.5(1.2) 给出 $H/(H\cap\mathrm{Stab}_G(y))$ 紧，即 $H/(H\cap\mathrm{Stab}_G(z))$ 紧.■

6、一些动力学概念

俗话说，只要有变化，就有动力系统. 本节主要引入一些动力系统中的基本概念，为之后的内容作铺垫，同时它们是动力学中永恒的研究对象. 如无特别声明，本节考虑的动力系统均是离散的，也就是映射的迭代.

定义 6.1(周期性) 设 $T:X\to X$ 是集合 X 上的映射. 对 $x\in X$ 的轨道 $\mathrm{Orb}_T(x):=\{T^n(x):n\geq 0\}$ 而言，如果 $\mathrm{Orb}_T(x)$ 是有限集，则称 x 是**预周期点** (Preperiodic Point)，记所有预周期点作成的集合为 $\mathrm{PrePer}(X,T)$；特别地如果存在 $n\geq 1$ 使 $T^n(x)=x$，则称 x 为一个**n-周期点** (注意 n- 周期点一定是 kn- 周期点)，记作 $x\in\mathrm{Per}_n(X,T)$. 记所有周期点作成的集合为 $\mathrm{Per}(X,T):=\bigcup_{n\geq 1}\mathrm{Per}_n(X,T)$. 反之若 $\mathrm{Orb}_T(x)$ 是无限集，则称 x 是**流浪点** (Wandering Point，也译作游荡点). 对子集 $U\subseteq X$ 而言，称 U 分别是 f 的**周期区域**、**预周期区域**、**流浪区域**，如果对应地，存在 $n\geq 1$ 使 $f^n(U)=U$、存在 $n\geq 1$ 使 $f^n(U)$ 是周期区域、U 非预周期区域.

上述定义虽不来源于“算术”，但却可以用于刻画算术性质. 例如，我们会关心这样的问题：对于 (次数大于 1 的) 有理函数 $f(z)\in\mathbb{Q}(z)$，集合 $\mathrm{Per}(\mathbb{P}^1(\mathbb{Q}),f)$ 与 $\mathrm{PrePer}(\mathbb{P}^1(\mathbb{Q}),f)$ 会有什么样的性质 (譬如 Mazur 证明了椭圆曲线 $E/\mathbb{Q}$ 预周期点的个数 $|E(\mathbb{Q})_{\mathrm{tor}}|$ 不超过 16)？它们如何反映 f 的几何信息？更一般地，如何描述有理点在 f 下的轨道？它什么时候无限 (譬如 Siegel 证明了亏格大于 0 的有理代数曲线的整点必为有限多个)？

现考虑 Riemann 曲面 $\mathbb{P}^1(\mathbb{C})$，它的全纯自同构群是 $\mathrm{PGL}(2,\mathbb{C})$，按分式线性变换作用. 设 $f(z)\in\mathbb{C}(z)$ 是一个有理函数，对任意 $\alpha\in\mathbb{C}$ 满足 $f(\alpha)\neq\infty$ 时，f 在 α 附近都有 Taylor 展开 $f(z)=f(\alpha)+f'(\alpha)(z-\alpha)+\frac{1}{2}f''(\alpha)(z-\alpha)^2+\cdots$. 如果 $f'(\alpha)=0$，则称 α 是一个**临界点**，此时 $f(\alpha)$ 称作**临界值**. 更精细地，我们可以引入分歧指数：若 $f(z)=f(\alpha)+c(z-\alpha)^{e_\alpha(f)}+\cdots,c\neq 0$，则称 $e_\alpha(f)\geq 1$ 为 f 在 α 处的**分歧指数** (可理解为将 α 拆成 $\{z:f(z)=f(\alpha)\}$). 如果 $e_\alpha(f)=\deg(f)$，则称 f 在 α 处**完全分歧**，此时 $f^{-1}(f(\alpha))=\{\alpha\}$. 而当 $\alpha=\infty$ 或 $f(\alpha)=\infty$ 时，可选取 $\sigma\in\mathrm{PGL}(2,\mathbb{C})$ 使得 $\sigma(\alpha),f\circ\sigma(\alpha)\neq\infty$. 在这种情况下定义 $e_\alpha(f):=e_{\sigma^{-1}(\alpha)}(\sigma^{-1}\circ f\circ\sigma)$.

定理 6.2(Riemann-Hurwitz) 设 $f\in\mathbb{C}(z)$ 且 $\deg(f)\geq 1$，则 $2\deg(f)-2=\sum_{\alpha\in\mathbb{P}^1(\mathbb{C})}(e_\alpha(f)-1)$.

定义 6.3(吸引、排斥) 设 α 是 $f\in\mathbb{C}(z)$ 的周期点，周期为 n. 称 $(f^n)'(\alpha)$ 为 f 在 α 处的**膨胀系数**，记作 $\varrho_\alpha(f)$(如果 $\infty\in\mathrm{Orb}_f(\alpha)$ 则用某个自同构 $\sigma\in\mathrm{PGL}(2,\mathbb{C})$ 作用后再约定 $\varrho_\alpha(f):=\varrho_{\sigma^{-1}(\alpha)}(\sigma^{-1}\circ f\circ\sigma)$). 由于在 f^n 在 α 附近的行为由展开式 $f^n(z)=\alpha+\varrho_\alpha(f)(z-\alpha)+O((z-\alpha)^2)$ 描述，故不难发现 $|\varrho_\alpha(f)|$ 的大小控制了 f^n 的迭代行为，因而我们称周期点 α 分别是**强吸引的** (Superattracting)、**吸引的** (Attracting)、**中性的** (Neutral)、**排斥的** (Repelling)，如果对应的 $|\varrho_\alpha(f)|=0$、$|\varrho_\alpha(f)|<1$、$|\varrho_\alpha(f)|=1$、$|\varrho_\alpha(f)|>1$.

定义 6.4(等度连续) 设 $f\in\mathbb{C}(z),\alpha\in\mathbb{P}^1(\mathbb{C})$. 称 f 在 α 处**等度连续**，如果对任意 $\epsilon>0$，总存在 $\delta>0$，若 $d(\alpha,\beta)<\delta$，则对任意 $n\in\mathbb{Z}_{\geq 0}$ 均有 $d(f^n(\alpha),f^n(\beta))<\epsilon$. 这里度量 $d:(\mathbb{C}\sqcup\{\infty\})^2\to\mathbb{R}_{\geq 0}\sqcup\{\infty\},(z_1,z_2)\mapsto\frac{|z_1-z_2|}{\sqrt{|z_1|^2+1}\sqrt{|z_2|^2+1}}$(这个度量由 Riemann 曲面上唯一的 Green 函数给出). 对于 $f\in\mathbb{C}(z)$，定义 f 的 **Fatou 集**为 $\mathbb{P}^1(\mathbb{C})$ 中最大的使 f 在其中的点处等度连续的开子集，记作 $\mathcal{F}(f)$，其补集 $\mathcal{J}(f):=\mathcal{F}(f)^c$ 称作 **Julia 集**，它由动力学行为混乱的点组成.

根据定义可以得到 Fatou 集和 Julia 集的一些拓扑性质 (证明略)：

命题 6.5 (1) 设 $f\in\mathbb{C}(z),\deg(f)\geq 2$，则：

(1.1) 称满足 $f(V)=V=f^{-1}(V)$ 的子集 $V\subseteq\mathbb{P}^1(\mathbb{C})$ 在 f 下**完全不变**. 则 $\mathcal{F}(f),\mathcal{J}(f),\partial\mathcal{J}(f)$ 均在 f 下完全不变.

(1.2) 对任意 $n\geq 1,\mathcal{F}(f^n)=\mathcal{F}(f),\mathcal{J}(f^n)=\mathcal{J}(f)$. (1.3) 集合 $\mathcal{J}(f)$ 非空. (1.4) 集合 $\mathcal{J}(f)$ 不含孤立点.

(1.5) 如果 f 的所有临界点均属于 $\mathrm{Preper}(\mathbb{P}^1(\mathbb{C}),f)\setminus\mathrm{Per}(\mathbb{P}^1(\mathbb{C}),f)$，则 $\mathcal{J}(f)=\mathbb{P}^1(\mathbb{C})$.

(2) 设 $f\in\mathbb{C}[z],\deg(f)\geq 2$，则：

(2.1) 集合 $\mathcal{J}(f)$ 是 $\mathbb{C}$ 的有界子集，因而 $\mathcal{F}(f)$ 非空(但当 $f\in\mathbb{C}(z)$ 时 Fatou 集可能为空，见 (1.5)).

(2.2) 集合 $\mathcal{J}(f)$ 连通当且仅当所有临界点 $\alpha\neq\infty$ 在 f 下的轨道 $\mathrm{Orb}_f(\alpha)$ 在 $\mathbb{C}$ 中有界.

(2.3) 如果 f 的所有临界点 α 均满足 $\lim_{n\to\infty}f^n(\alpha)=\infty$，则 $\mathcal{J}(f)$ 完全不连通.

(2.4) 集合 $\mathcal{J}(f)=\overline{\{z:z是f的排斥的周期点\}}$.

(3) 设 $f\in\mathbb{C}(z),\deg(f)\geq 2$，则下述说法等价：

(3.1)$\mathcal{J}(f)=\mathbb{P}^1(\mathbb{C})$；(3.2)$\mathrm{int}(\mathcal{J}(f))\neq\varnothing$；(3.3) 存在 $\alpha\in\mathbb{P}^1(\mathbb{C})$ 使得 $\mathrm{Orb}_f(\alpha)$ 在 $\mathbb{P}^1(\mathbb{C})$ 中稠密.

(4.**Carleson-Gamelin**) 若 $f\in\mathbb{C}(z)$，则 $\mathcal{F}(f)$ 的连通分支个数只可能为 $0,1,2,\infty$. 由于 f 是开映射，故可定义映射 $\{\mathcal{F}(f)的连通分支\}\to\{\mathcal{F}(f)的连通分支\},U\mapsto f(U)$.

(4.1.**Sullivan 流浪定理**)f 没有流浪区域.

(4.2.**Fatou 分支分类定理**) 设 U 是 $\mathcal{F}(f)$ 的一个连通分支，若 U 是周期区域，则 U 必为下述情况之一：

(4.2.1)U 含有一个吸引的周期点.

(4.2.2)$f(U)=U$ 且 $\partial(U)$ 含有一个中性的周期点 ξ，$\varrho_\xi(f)$ 是单位根，且任意 $\alpha\in U$ 有 $\lim_{n\to\infty}f^n(\alpha)=\xi$.

(4.2.3)$f(U)=U$ 且存在全纯同构 $\sigma:D:=\{z\in\mathbb{C}:|z|<1\}\to U$ 使得 $\sigma^{-1}\circ f\circ\sigma$ 是圆盘 D 的旋转.

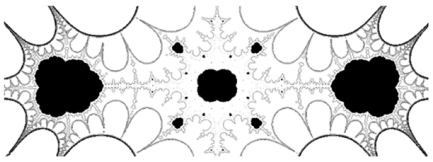
(4.2.4)$f(U)=U$ 且存在全纯同构 $\sigma:R:=\{z\in\mathbb{C}:a<|z|<b\}\to U$ 使得 $\sigma^{-1}\circ f\circ\sigma$ 是环带 R 的旋转.

例 6.6 (1) 如果 f 的周期点 α 是吸引的，则 $\alpha\in\mathcal{F}(f)$；如果周期点 α 是排斥的，则 $\alpha\in\mathcal{J}(f)$.

(2) 函数 $f(z)=z^n,n\geq 2$ 的 Julia 集为 $\mathcal{J}(f)=\{z\in\mathbb{C}:|z|=1\}$.

(3) 考虑函数 $f(z)=1-\frac{2}{z^2}$，它的临界点为 $0,\infty$. 由于 $\mathrm{Orb}_f(0)=\{0,\infty,1,-1\}$，所以这些临界点都属于 $\mathrm{Preper}(\mathbb{P}^1(\mathbb{C}),f)\setminus\mathrm{Per}(\mathbb{P}^1(\mathbb{C}),f)$，故由命题 6.5(1.5) 可知 $\mathcal{J}(f)=\mathbb{P}^1(\mathbb{C})$.

(4) 考虑 $f_c(z)=z^2+c$，若记 $\mathcal{M}:=\{c\in\mathbb{C}:\mathcal{J}(f_c)连通\}$，则 $\mathcal{M}$ 反映在复平面上就是著名的 **Mandelbrot 集** (下图左).

(5.**Collatz 猜想**) 定义 **Collatz 函数**为 $\ell:\mathbb{Z}_{\geq 1}\to\mathbb{Z}_{\geq 1},n\mapsto\begin{cases}(3n+1)/2,n是奇数\\ n/2,n是偶数\end{cases}$，它可以延拓为 $\mathbb{C}$ 上的全纯函数 $\widetilde{\ell}(z)=\frac{1+4z-(1+2z)\cos(\pi z)}{4}$. 那些在 $\widetilde{\ell}$ 迭代下收敛的点形成了一个分形 (上图右). 著名的 Collatz 猜想说，对任意 $n\geq 1$，总存在与 n 有关的 k 使得 $\mathrm{Orb}_\ell(\ell^k(n))=\{1,2\}$. 该猜想的最新进展，也是目前为止最好的结果是 Tao 在 2019 年的论文 [22]，他用随机过程和动力系统的方法证明了：若任取满足条件 $\lim_{n\to\infty}f(n)=+\infty$ 的函数 $f:\mathbb{Z}_{\geq 1}\to\mathbb{R}$，则集合 $X_f:=\left\{n\geq 1:\inf_{k\geq 0}\ell^k(n)<f(n)\right\}$ 均满足 $\lim\limits_{t\to\infty}\dfrac{\sum_{i\in X_f\cap\mathbb{Z}_{\geq 1}\cap[1,t]}\frac{1}{i}}{\sum_{i\in\mathbb{Z}_{\geq 1}\cap[1,t]}\frac{1}{i}}=1$.

7、熵

数学中的熵 (Entropy) 来自于物理学中相应概念的“不完全”抽象 (两者都用来描述“混乱”，但实际意义完全不同)，由 Kolmogorov 和 Sinai 于 1959 年引入，用来衡量系统演化的复杂程度，或者说轨道之间关系的复杂程度. 为了探究最初的想法，我们进行如下思想实验：

考虑空间 X 中的两点 $x,y\in X$，设 $T:X\to X$ 是一个变换. 现以函数 $f(n,x,y)$ 表示第 n 次迭代之后 $T^n(x)$ 与 $T^n(y)$ 的差别，差别越大则 f 的值越大，显然函数 f 刻画了轨道之间的关系. 此外相邻的几次迭代均会对 f 产生不能忽略的扰动，因为 f 随时间的变化也暗含了轨道之间关系的信息，并且探测的时间越长，获得的信息越多. 现对上述差别指定一个精度 K，如果在这个精度下随着时间的流逝有更多的信息进入了 K 不能探查的范围，则轨道之间的关系越捉摸不透，而描述这种混乱程度的表达式应该形如 $\varinjlim_K\varinjlim_n g(f(n,x,y),K)$. 我们的目标是找到合适的 f 和 g，这当然有很多选择，相应地也会导出不同的不变量，但可能会有一些不变量很差 (例如所有系统的熵都是 ∞). 关于合理选取 f 和 g 的方式将在定理 7.3 给出.

而在本节涉及到的拓扑动力系统中，我们所想象的熵表现为拓扑熵，这是一个拓扑共轭不变量 (测度熵在拓扑动力系统中的类比). 此处我们只快速地介绍有关熵的基本性质，更重要的则是理解它与算术不变量之间更精细的联系.

定义 7.1(拓扑熵) 设 X 是紧致拓扑空间，$T:X\to X$ 是连续映射. 设 $\mathcal{A},\mathcal{B}$ 是 X 的两个开覆盖，定义它们的**交** (Join) 为 $\mathcal{A}\vee\mathcal{B}:=\{A\cap B:A\in\mathcal{A},B\in\mathcal{B}\}$，这仍是一个开覆盖. 定义关于开覆盖 $\mathcal{A}$ 的**熵**为 $H(\mathcal{A}):=\ln\big(\inf\{|\mathcal{S}|:\mathcal{S}是\mathcal{A}的有限子覆盖\}\big)$. 定义变换 T 的**拓扑熵**为 $h(T):=\sup\limits_{\mathcal{A}是X的开覆盖}\lim\limits_{n\to\infty}\dfrac{1}{n}H\left(\bigvee\limits_{i=0}^{n-1}T^{-i}(\mathcal{A})\right)$，这里 $T^{-1}(\mathcal{A}):=\{T^{-1}A:A\in\mathcal{A}\}$.

由定义很容易证明：

命题 7.2 (1)$H(\mathcal{A})\geq 0$；$H(\mathcal{A})=0$ 当且仅当 $X\in\mathcal{A}$. (2) 若 $\mathcal{B}$ 是 $\mathcal{A}$ 的加细，则 $H(\mathcal{A})\leq H(\mathcal{B})$.

(3)$H(\mathcal{A}\vee\mathcal{B})\leq H(\mathcal{A})+H(\mathcal{B})$. (4)$H(T^{-1}\mathcal{A})\leq H(\mathcal{A})$，当 T 是满射时等号成立.

(5) 恒等映射的拓扑熵为 0. (6) 若 T 是同胚，则 $h(T)=h(T^{-1})$.

(7) 若 $Y\subseteq X$ 是闭子集且 $T(Y)=Y\big($也就是说 $(Y,T|_Y)$ 是 (X,T) 的一个子系统$\big)$，则 $h(T|_Y)\leq h(T)$.

(8) 若 X 还是紧致度量空间，则对任意 $m\geq 1$，$h(T^m)=mh(T)$.

(9) 设 $T_i:X_i\to X_i$ 是紧致度量空间 $(X_i,d_i),i=1,2$ 上的连续映射，则 $h(T_1\times T_2)=h(T_1)+h(T_2)$.

证明 仅证 (6) 和 (8)，需要用到定理 7.3；(6) 设 $\mathcal{A}$ 为 X 的开覆盖，则 $\lim_{n\to\infty}\frac{1}{n}H\big(\bigvee_{i=0}^{n-1}T^{-i}\mathcal{A}\big)\overset{(4)}{=}\lim_{n\to\infty}\frac{1}{n}H\big(T^{n-1}\bigvee_{i=0}^{n-1}T^{-i}\mathcal{A}\big)=\lim_{n\to\infty}\frac{1}{n}H\big(\bigvee_{i=0}^{n-1}T^{i}\mathcal{A}\big)$，由定义 7.1 和 $\mathcal{A}$ 的任意性得证；(8) 对任意 $n\geq 1$ 和 $\epsilon>0$，若采用定理 7.3 的记号则显然 $r_{T,nm}(\epsilon)\geq r_{T^m,n}(\epsilon)$，于是

$$h(T^m)=\lim_{\epsilon\to 0}\limsup_{n\to\infty}\frac{\ln r_{T^m,n}(\epsilon)}{n}\leq\lim_{\epsilon\to 0}\limsup_{n\to\infty}\frac{nm}{n}\frac{1}{mn}\ln r_{T,nm}(\epsilon)\leq mh(T).$$

另一方面，对任意 $\epsilon>0$，由 T 一致连续知存在与常数 m 有关的 $\delta>0$ 使得对任意 $x,y\in X$，当 $d(x,y)<\delta$ 时 $d(T^ix,T^iy)<\epsilon,0\leq i\leq m-1$. 注意到 $r_{T^m,n}(\delta)\geq r_{T,nm}(\epsilon)$，从而 $h(T^m)\geq mh(T)$，命题得证.■

直接用定义 7.1 来计算拓扑熵是很麻烦的——因为我们要遍历所有开覆盖. 但是 Bowen 告诉我们，如果 X 是紧致度量空间，那么用 Lebesgue 数取特殊的开覆盖就行了 (由 Lebesgue 覆盖引理可以控制开集的直径使得该开覆盖是某些标准覆盖的加细). 这也给出了度量空间上动力系统拓扑熵的等价定义 (见 [6] 定理 5.2.1)：

定理 7.3(Bowen) 设 (X,d) 是紧致度量空间，$T:X\to X$ 是连续映射. 若记 $r_n(\epsilon):=\min\big\{|F|:F\subseteq X,\forall x\in X,\exists y\in F使得\forall 0\leq i\leq n-1,d(T^ix,T^iy)<\epsilon\big\}$，记 $s_n(\epsilon):=\max\big\{|E|:E\subseteq X,\forall x,y\in E,\exists 0\leq i\leq n-1使得d(T^ix,T^iy)>\epsilon\big\}$. 令 $h_1(T):=\lim_{\epsilon\to 0}\limsup_{n\to\infty}\frac{\ln r_n(\epsilon)}{n}$，$h_2(T):=\lim_{\epsilon\to 0}\limsup_{n\to\infty}\frac{\ln s_n(\epsilon)}{n}$，则 $h(T)=h_1(T)=h_2(T)$. 此外，拓扑熵与度量的选取无关.

动力系统的熵从迭代中产生，系统随着演化可能会越来越复杂. 定理 7.3 相对直观地告诉我们：指定一个精度，若随着迭代在这个精度下不能区分的点以更快的指数级速度增多 (即 r_n 越大，相应的有用的信息以更快的指数级速度减少)，则迭代越混乱，熵也就越大. 这也是为什么拓扑熵会经常被用来研究混沌理论和分形几何.

例 7.4 (1) 设 $X=\{1,-1\},T:\pm1\mapsto\mp1$. 则 $\mathcal{A}=\{\{1\},\{-1\}\},\mathcal{B}=\{\{1,-1\}\}$ 是所有的开覆盖. 此时 $T^{-i}(\mathcal{A})=\mathcal{A},T^{-i}(\mathcal{B})=\mathcal{B}$，易得 $h(T)=0$. 注意到这里的 T 不是恒等映射 (严格来说该系统与平凡系统非拓扑共轭)，因此拓扑熵不足以完全分类所有拓扑动力系统. 类似地不难发现简单的动力系统拓扑熵都很小 (譬如有限离散空间上连续变换的熵为 0).

(2) 例 1.2(3) 中 Bernoulli 试验关于左平移的拓扑熵为 $\ln n$. 事实上可以直接算出 $r_i(\frac{1}{2^k})=n^{2k+i}$.

另一类重要的例子是所谓的线圈 (Solenoid)：

定义 7.5(线圈) 称拓扑维数有限的紧致连通 Abel 群为一个**线圈**.

例 7.6 设 $a,b\in\mathbb{Z},(a,b)=1$，则紧群 $\prod_{i\in\mathbb{Z}}\mathbb{T}$ 的闭子群 $\boldsymbol{S}:=\{\boldsymbol{x}=(x_i):bx_{i+1}=ax_i\}$ 就是一个 1 维线圈. 关于这个线圈还有另外两种定义方式：Adelic 观点下 $\boldsymbol{S}:=\big(\prod_{p|ab}\mathbb{Q}_p\times\mathbb{R}\big)\big/\mathbb{Z}[\frac{1}{ab}]$，Pontryagin 对偶观点下 $\boldsymbol{S}:=\widehat{\mathbb{Z}[\frac{1}{ab}]}$.

证明 **Step1：** $\boldsymbol{S}$ 的原始定义与 Pontryagin 对偶观点下的定义相同. **证：**只需验证 $\big\{(x_i)\in\prod_{i\in\mathbb{Z}}\mathbb{T}:x_{i+1}=\frac{a}{b}x_i\big\}\to\widehat{\mathbb{Z}[\frac{1}{ab}]},(\cdots,\frac{b}{a},1,\frac{a}{b},\cdots)\alpha\mapsto\left[e^{2\pi i\alpha(\cdot)}:\frac{1}{ab}\mapsto e^{\frac{2\pi i\alpha}{ab}}\right],\alpha\in\mathbb{T}$ 是拓扑 Abel 群同构即可.

Step2： $\boldsymbol{S}$ 在 Pontryagin 对偶观点下的定义与 Adelic 观点下的定义相同. **证：**直观上来讲仅需考虑素点 $p|ab$ 处的信息，所以 [12] 定理 8.18 中给出的正合序列 $0\longrightarrow\mathbb{Q}\longrightarrow\mathbb{A}_{\mathbb{Q}}\xrightarrow{\sigma}\widehat{\mathbb{Q}}\longrightarrow 0$ 可以“限制到”$\mathbb{Z}[\frac{1}{ab}]\big($这里 $\mathbb{Q}$ 和 $\mathbb{Z}[\frac{1}{ab}]$ 均配备离散拓扑然后对角嵌入到 Adele 中$\big)$上：$0\longrightarrow\mathbb{Z}[\frac{1}{ab}]\longrightarrow\prod_{p|ab}\mathbb{Q}_p\times\mathbb{R}\longrightarrow\widehat{\mathbb{Z}[\frac{1}{ab}]}\longrightarrow 0$(因为其余素点处的信息冗余). 事实上 [12] 定理 7.7 告诉我们 $\sigma:\mathbb{A}_{\mathbb{Q}}\to\widehat{\mathbb{Q}},(x_p)\mapsto\left[\Pi\chi_p(\cdot x_p):t\mapsto\prod_{p\leq\infty}\chi_p(tx_p)\right]$，

这里 χ_p 指 [12] 注意 8.3 中的标准特征标，且至少有一个 $x_p \notin \mathbb{Q}$ 或序列 $\{x_p\}$ 非常值. 设素数 $q \nmid ab$，则 $\sigma(\cdots,0,x_q,0,\cdots)=e^{2\pi i x_q(\cdot)}$. 若要使它满足 $\exp\big(2\pi i x_q(\mathbb{Q}\backslash\mathbb{Z}[\frac{1}{ab}])\big)=\mathrm{id}$(我们想把 $\mathbb{Q}$ 上的特征标限制到 $\mathbb{Z}[\frac{1}{ab}]$)，则只能 $x_q=0$. 无穷素点的处理类似. 因此确定 $\mathbb{Z}[\frac{1}{ab}]$ 上的特征标只需考虑 $\prod_{p|ab}\mathbb{Q}_p\times\mathbb{R}$ 中的元素即可. 不难发现 $\mathbb{Z}[\frac{1}{ab}]$ 的对角嵌入恰巧贡献那些平凡的特征标.■

命题 7.7(Mahler-Jensen-Schmidt) 设有多项式 $f(z)=bz-a\in\mathbb{Z}[z],(a,b)=1$. 考虑例 7.6 中的线圈 $\boldsymbol{S}$，若定义其上的连续变换为 $T_f:\boldsymbol{S}\to\boldsymbol{S},(x_i)\mapsto(x_{i+1})$，则：

(1) 拓扑熵 $h(T_f)=\ln\max\{|a|,|b|\}$. (2)$|\mathrm{Per}_n(\boldsymbol{S},T_f)|=|a^n-b^n|$.

更一般地 (详见 [17]Chapter2.3)，设有本原多项式 $f(z)=a_dz^d+\cdots+a_0\in\mathbb{Z}[z]$，它在 $\mathbb{C}$ 上分解为一次因式的乘积 $f(z)=a_d\prod_{i=1}^d(z-\alpha_i)$. 考虑 d 维线圈

$$\boldsymbol{S}:=\left\{\boldsymbol{x}=(x_i)\in\prod_{i\in\mathbb{Z}}\mathbb{T}:\forall i\in\mathbb{Z},a_0x_i+a_1x_{i+1}+\cdots+a_dx_{i+d}=0\right\},$$

若定义其上的变换为 $T_f:\boldsymbol{S}\to\boldsymbol{S},(x_i)\mapsto(x_{i+1})$，则：

(1) 拓扑熵 $h(T_f)=\int_0^1\ln|f(e^{2\pi it})|dt=\ln|a_d|+\sum_{i=1}^d\ln^+|\alpha_i|$(第二个等号是 Mahler 测度的 Jensen 公式).

(2) 如果这些 α_i 都不是单位根，那么 $|\mathrm{Per}_n(\boldsymbol{S},T_f)|=|a_d|^n\prod_{i=1}^d|\alpha_i^n-1|$.

证明 (1) 见 [17]Chapter2.3；(2) 见 [17]Chapter2.4.■

注意 7.8 一个公开问题是：给定 $a,b\in\mathbb{Z},x_0\in\mathbb{R}$，如何判断序列 $\big\{(\frac{a}{b})^nx_0(\mathrm{mod}\ 1)\big\}$ 是否在 $\mathbb{T}$ 中稠密？这个问题是正规数问题的另一版本. 从动力系统上来讲，如果命题 7.7 中的拓扑熵 $h(T_{bz-a})=+\infty$，那就会提示该问题存在某种解决方法. 可事实并非如此.

事实上对椭圆曲线使用类似的方法也可以得到这样的结论，我们将在第 8 节中详细介绍. 不过与命题 7.7 中直接研究线圈上左平移变换不同，此处需要从某个与椭圆曲线有关的像线圈但不是线圈的系统的“Adelic 视角”入手 (这时候连通性、群结构均被破坏). 这些都是例 7.6 给我们的启发.

此外，Mahler 测度也是研究多项式算术性质的有力工具，相关内容请参考 [17]Chapter1.

8、高度

本节我们来看看熵在数论中的应用——算术高度的动力学解释. 我们知道在 Diophantine 几何或算术几何的意义上，代数数的高度是算术复杂性的度量，而熵是动力系统复杂性的度量，我们自然猜测这两者有某种联系.

定义 8.1(高度) 设 $0\neq x\in\overline{\mathbb{Q}}$，取其极小多项式 $f_x(z):=a_0z^n+\cdots+a_n\in\mathbb{Z}[z],(a_0,\cdots,a_n)=1$. 现将 f_x 在 $\mathbb{C}$ 上分解为一次因式的乘积 $f_x(z)=a_0\prod_{i=1}^n(z-x_i)$，定义 x 的**高度**为 $h(x):=\ln\left(|a_0|\prod_{i=1}^n\max\{|x_i|,1\}\right)^{1/n}$. 在补充定义 $h(0)=h(\infty):=0$ 之后 h 可以延拓到 $\mathbb{P}^1(\overline{\mathbb{Q}})$. 特别地，当 $x=\frac{m}{n}\in\mathbb{Q}$ 时 $h(x)=\ln\max\{|m|,|n|\}$.

而定义典范高度 (Canonical Height) 则比较麻烦，为此我们需要如下命题.

命题 8.2 (1) 设 $\phi=\frac{f}{g}\in\overline{\mathbb{Q}}(z)$ 是有理函数，$\deg(\phi)\geq1$，则存在常数 $C_\phi\in\mathbb{R}$ 使得对任意 $x\in\mathbb{P}^1(\overline{\mathbb{Q}})$，$|h(\phi(x))-\deg(\phi)\cdot h(x)|\leq C_\phi$. 换句话说，$h(\phi(x))=\deg(\phi)\cdot h(x)+O_\phi(1)$.

(2) 设 K 是数域，则对任意 $B>0$，集合 $\{x\in\mathbb{P}^1(K):h(x)\leq B\}$ 有限. 更一般地，对任意 $C>0$ 和 $D\geq1$，集合 $\{x\in\mathbb{P}^1(\overline{\mathbb{Q}}):h(x)\leq C,[\mathbb{Q}(x):\mathbb{Q}]\leq D\}$ 有限.

证明 (1) 此处仅以 $x\in\mathbb{Z}$ 为例，一般情形的处理虽复杂但是标准的. 设 $f=\sum_if_iz^i,g=\sum_jg_jz^j$，则由三角不等式可得 $|h(\phi(x))-\deg(\phi)\cdot h(x)|\sim\left|\ln\frac{\max\{|\sum_if_ix^i|,|\sum_jg_jx^j|\}}{|x|^{\deg(\phi)}}\right|\leq C_\phi$(与 x 无关)；(2) 在 $K=\mathbb{Q}$ 时结论显然，而当 K 是一般数域时考虑极小多项式即可.■

设 $\phi\in\overline{\mathbb{Q}}(z)$ 且 $\deg(\phi)\geq2$，此时命题 8.2(1) 告诉我们 $h(\phi(x))-\deg(\phi)h(x)$ 是上 $\mathbb{P}^1(\overline{\mathbb{Q}})$ 的有界函数. 如果我们对高度函数 h 进行一些修正 (记作 $\widehat{h}$) 使得 $\widehat{h}(\phi(x))\equiv\deg(\phi)\widehat{h}(x)$，这就得到了典范高度的定义：

定理 8.3(Tate) 设 $\phi\in\overline{\mathbb{Q}}(z)$ 且 $\deg(\phi)\geq2$，则对任意 $x\in\mathbb{P}^1(\overline{\mathbb{Q}})$，极限 $\widehat{h}_\phi(x):=\lim_{n\to\infty}\frac{1}{\deg(\phi)^n}h(\phi^n(x))$ 存在且具有如下性质：(1) 对任意 $x\in\mathbb{P}^1(\overline{\mathbb{Q}})$，$\widehat{h}_\phi(x)=h(x)+O_\phi(1)$；(2) 对任意 $x\in\mathbb{P}^1(\overline{\mathbb{Q}})$，$\widehat{h}_\phi(\phi(x))=$

$\deg(\phi)\widehat{h}_\phi(x)$；(3)$\widehat{h}_\phi(x)\geq 0$，且 $\widehat{h}_\phi(x)=0$ 当且仅当 x 是 ϕ 的预周期点；(4) 满足条件 (1) 和 (2) 的函数是唯一的.

称上述定义在 $\mathbb{P}^1(\overline{\mathbb{Q}})$ 上的函数 $\widehat{h}_\phi$ 为ϕ-**典范高度**函数，称它在代数数 x 处的取值 $\widehat{h}_\phi(x)$ 为 x 的ϕ-**高度**.

证明 根据命题 8.2(1)，对任意 $x\in\mathbb{P}^1(\overline{\mathbb{Q}})$ 有 $\left|\frac{h(\phi^n(x))}{\deg(\phi)^n}-\frac{h(\phi^m(x))}{\deg(\phi)^m}\right|=\left|\sum_{i=m}^{n-1}\left(\frac{h(\phi^{i+1}(x))}{\deg(\phi)^{i+1}}-\frac{h(\phi^i(x))}{\deg(\phi)^i}\right)\right|\leq\sum_{i=m}^{n-1}\frac{|h(\phi^{i+1}(x))-\deg(\phi)h(\phi^i(x))|}{\deg(\phi)^{i+1}}\leq C_\phi\cdot\sum_{i=m}^{n-1}\deg(\phi)^{-i-1}\to 0, m\to\infty$. 因此 $\left\{\frac{h(\phi^n(x))}{\deg(\phi)^n}\right\}$ 是 Cauchy 序列. 令上式中 $m=0$ 即得 (1)，(2) 显然，(3) 非负性显然，另设 $x\in\mathrm{Preper}(\mathbb{P}^1(\overline{\mathbb{Q}}),\phi)$，则 $h(\phi^n(x))$ 只能取到有限多个值，故由定义立得 $\widehat{h}_\phi(x)=0$；反过来设 $\widehat{h}_\phi(x)=0$，则 $h(\phi^n(x))=\deg(\phi)^n\widehat{h}_\phi(x)+O_\phi(1)=O_\phi(1)$，这意味着 $h(\mathrm{Orb}_\phi(x))\subseteq[0,r]$ 是 $\mathbb{R}$ 的有界子集. 现设 K 是使 $\phi\in K(z)$ 且 $x\in\mathbb{P}^1(K)$ 的数域，那么 $\mathrm{Orb}_\phi(x)\subseteq\mathbb{P}^1(K)$. 根据命题 8.2(2)，我们得到 $\mathrm{Orb}_\phi(x)$ 是有限集，所以 $x\in\mathrm{Preper}(\mathbb{P}^1(\overline{\mathbb{Q}}),\phi)$. 至于 (4)，设函数 σ,τ 满足条件，若存在 x 使得 $(\sigma-\tau)(x)\neq 0$，则由 (2) 可得 $|(\sigma\circ\phi^n-\tau\circ\phi^n)(x)|=\deg(\phi)^n|(\sigma-\tau)(x)|\to\infty, n\to\infty$，而 (1) 蕴含 $|\sigma-\tau|$ 有界，矛盾.■

$\widehat{h}_\phi$ 结合了算术信息 (算术复杂度) 和动力学信息 (在预周期点处取值为 0). 既然与算术有关，那肯定要问它的局部行为如何描述，以及如何用这些行为拼出整体信息. 很自然地，我们希望典范高度就是局部高度之和，而 Néron 告诉我们事实正是如此 (定理 8.5). 这种观点某种程度上比定理 8.3 更重要.

定义 8.4(局部高度) 设 K 是数域，$\phi\in K[z]$ 且 $\deg(\phi)\geq 2$. 设 v 是 K 的素点，定义ϕ,v-**局部高度**函数为 $\widehat{\lambda}_{\phi,v}(x):=\lim_{n\to\infty}\frac{1}{\deg(\phi)^n}\ln\max\{|\phi^n(x)|_v,1\}, x\in K_v$. 但一般而言当 $\phi\in K(z)$ 时定义非常复杂 (涉及约化理论)，我们置于下节详细讨论.

定理 8.5(Néron-Tate) 设 K 是数域，$\phi\in K(z)$ 且 $\deg(\phi)\geq 2$. 则任意 $x\in K$ 均成立等式 $\widehat{h}_\phi(x)=\frac{1}{[K:\mathbb{Q}]}\sum_{p\leq\infty}\sum_{v|p}[K_v:\mathbb{Q}_p]\cdot\widehat{\lambda}_{\phi,v}(x)$.

这些概念反映在椭圆曲线上就是我们熟知的典范高度 ([20]Chapter8.9)：

例 8.6 椭圆曲线 $E/\mathbb{Q}$ 的典范高度函数被定义为 $\widehat{h}_E:E(\mathbb{Q})\to\mathbb{R}, Q=(x_Q,y_Q)\mapsto\lim_{n\to\infty}4^{-n}h_E(2^nQ)$，其中 $h_E(Q):=\frac{1}{2}h(x_Q)$. 当然还可以定义 $E/\mathbb{Q}$ 在素点 p 处的局部高度函数 $\widehat{\lambda}_{E,p}$，但由于涉及复杂的约化理论故在此不表，详见 [7]. 此时对任意 $Q\in E(\mathbb{Q})$，会成立等式 $\widehat{h}_E(Q)=\sum_{p\leq\infty}\widehat{\lambda}_{E,p}(Q)$.

研究局部高度最经典的手段就是把问题约化到剩余域上，关于约化的具体内容请移步第 9 节，本节剩余篇幅旨在给出椭圆曲线典范高度的动力学解释，读者可参考 [17].

定理 8.7 (1.**无穷素点情形**) 对任意 $\beta>0$，定义β- **变换**$T_\beta:[0,1)\to[0,1), x\mapsto\beta x(\mathrm{mod}\ 1)$. 类比例 7.4(2) 和定理 2.7 可计算“拓扑熵”$h(T_\beta)=\ln^+\beta$(注意，这里 T_β 不一定连续 (也不一定保 Lebesgue 测度)，因此定义 7.1 并不适用. 此处我们需把该系统化为“Bernoulli 试验”，详见 [34]Chapter7.3). 具体来讲：

(1.1) 当 $\beta>1$ 时，$h(T_\beta)=\ln\beta$. 此外，$\ln|\mathrm{Per}_n([0,1),T_\beta)|\sim n\ln\beta, n\to\infty$.

(1.2) 当 $\beta<1$ 时，$h(T_\beta)=0$. 此外，对任意 $n\geq 1$ 均有 $\mathrm{Per}_n([0,1),T_\beta)=\{0\}$.

(2.**有限素点情形**) 对任意 $q\in\mathbb{Q}_p$，定义q- **变换**$T_q:\mathbb{Z}_p\to\mathbb{Z}_p, T_q(x):=\sum_{i=\max\{0,m\}}^{\infty}b_ip^i$，其中 $qx=\sum_{i=m}^{\infty}b_ip^i$(同样，这里 T_q 不一定连续 (仅在 $|q|_p\geq 1$ 时保 Haar 测度)，故此处计算熵时也应转化成“Bernoulli 试验”). 则 $h(T_q)=\ln^+|q|_p$，且当 $q^k\neq 1(k\geq 1)$ 时 $\ln|\mathrm{Per}_n(\mathbb{Z}_p,T_q)|=n\ln^+|q|_p$. 此外，当 $|q|_p>1$ 时 T_q 关于 Haar 测度遍历 (但 $|q|_p=1$ 时 T_q 关于 Haar 测度却不是遍历的. 在这种情况下，Coelho 和 Parry 在 [21] 中研究了 T_q- 不变测度的遍历分解).

(3.**局部整体原则**) 设 $E/\mathbb{Q}$ 是椭圆曲线，对任意 $Q:=(x_Q,y_Q)\in\{Q\in E(\mathbb{Q}):p=\infty$或坏约化时$\widehat{\lambda}_{E,p}(Q)>0\}$，考虑

$$X_E:=\prod_{p<\infty}p\,\mathbb{Z}_p\times[0,1),\quad T_Q:=\prod_{p<\infty}T_{x_Q}\times T_{e^{2\widehat{\lambda}_{E,\infty}(Q)}},$$

则该系统的拓扑熵 $h(T_Q)=2\widehat{h}_E(Q)$，且 $\ln|\mathrm{Per}_n(X_E,T_Q)|\sim n\big(\sum_{p<\infty}\ln^+|x_Q|_p+\ln\exp(2\widehat{\lambda}_{E,\infty}(Q))\big), n\to\infty$.

证明 无穷素点情形不再赘述，类比例 7.4(2) 即可. 其余断言仅陈述证明思路，具体细节见 [15].

Step1：$h(T_q)=\ln^+|q|_p$. **证**：注意 T_q 的平移性，由定理 7.3 有 $h(T_q)=\lim\limits_{m\to\infty}\lim\limits_{n\to\infty}\frac{-\ln\mu\left(\bigcap_{k=0}^{n-1}T_q^{-k}(p^m\,\mathbb{Z}_p)\right)}{n}$. 当 $|q|_p\leq 1$ 时，显然 $\bigcap_{k=0}^{n-1}T_q^{-k}(p^m\,\mathbb{Z}_p)=p^m\,\mathbb{Z}_p$，直接代入计算得 $h(T_q)=0$；当 $|q|_p=p^r>1$ 时，显然 $T_q^{-1}(p^m\,\mathbb{Z}_p)=p^{m+r}\,\mathbb{Z}_p$，故 $\bigcap_{k=0}^{n-1}T_q^{-k}(p^m\,\mathbb{Z}_p)=p^{m+rn}\,\mathbb{Z}_p$，直接代入计算得 $h(T_q)=r\ln p$.

Step2：当 $q^k\neq 1(k\geq 1)$ 时 $\ln|\mathrm{Per}_n(\mathbb{Z}_p,T_q)|=n\ln^+|q|_p$. **证**：$|q|_p\leq 1$ 时显然. 当 $q=p^{-k},k>0$ 时，显

然 $T_q^n(\sum_i a_ip^i)=\sum_{i=0}^{\infty}a_{i+nk}p^i$，所以方程 $T_q^nx=x$ 的解由满足 $a_{i+nk}=a_i, i=0,\cdots,kn-1$ 的 p^{kn} 个点给出.

Step3：当 $|q|_p>1$ 时 T_q 关于 Haar 测度遍历. **证**：类比例 2.4(3). 设 E 满足 $T_q^{-1}E=E$. 对任意 $\epsilon>0$，可选取 A 使 $\mu(E\triangle A)<\epsilon$，显然 $|\mu(E)-\mu(A)|<\epsilon$. 现选取合适的 n 使得 $\mu(A\cap T_q^{-n}A)=\mu(A)\mu(T_q^{-n}A)=\mu(A)^2$. 注意到 $T_q^{-n}E=E$，所以 $\mu(E\triangle T_q^{-n}A)<\epsilon$. 又因为 $\mu(E\triangle(A\cap T_q^{-n}A))\le\mu((E\triangle A)\cup(E\triangle T_q^{-n}A))<2\epsilon$，故有 $|\mu(E)-\mu(E)^2|\le|\mu(E)-\mu(A\cap T_q^{-n}A)|+|\mu(A\cap T_q^{-n}A)-\mu(E)^2|<4\epsilon$. 由 ϵ 的任意性立得 $\mu(E)=0$ 或 1.

Step4：$h(T_Q)=2\widehat{h}_E(Q)$. **证**：不难发现在几乎所有的有限素点处 $h(T_{x_Q})=0$，故由命题 7.2(9) 有 $h(T_Q)=h\big(T_{\exp(2\widehat{\lambda}_{E,\infty}(Q))}\big)+\sum_{p<\infty}h(T_{x_Q})=\ln\exp(2\widehat{\lambda}_{E,\infty}(Q))+\sum_{p<\infty}\ln\max\{|x_Q|_p,1\}=2\widehat{h}_E(Q)$.■

定理 8.7 相当于定理 8.5 的椭圆曲线版本，因为我们用到了整体熵是局部熵之和这一事实.

注意 8.8 (1) 我们只能说定理 8.7(3) 是线圈情形 (命题 7.7) 的类比，理由如下：设 $E/\mathbb{Q}$ 是椭圆曲线，考虑其约化核 $E_1(\mathbb{Q}_p)$. 解析几何告诉我们 $E_1(\mathbb{R})\cong\mathbb{T}$；形式群告诉我们当 $p\ge3$ 时 $E_1(\mathbb{Q}_p)\cong p\mathbb{Z}_p$；$p=2$ 的情况见 [20]Chapter4. 此时我们可以粗略地认为 $X_E=\prod_{p\le\infty}E_1(\mathbb{Q}_p)$，但事实上 X_E 并没有群结构.

(2) 定理 8.7(1) 和 (2) 暗示局部情形下周期点的增长比率等于 (局部) 熵，这与线圈上的结论 (命题 7.7) 是一致的. 前者的动力系统由多项式给出$\big($熵对应 Mahler 测度 $\mathrm{Mah}(f):=\int_0^1\ln|f(e^{2\pi it})|dt\big)$，后者的动力系统由椭圆曲线的方程给出$\Big($与熵对应的则是椭圆版的 Mahler 测度 $\mathrm{Mah}_E(f):=\int_{\text{基本区域}}\ln|f(\wp_E(z))|dz$，此时 $2\widehat{h}_E(Q)=\mathrm{Mah}_E(nz-m)$ 对任意 $Q\in\{(x_Q,y_Q):x_Q=\frac{m}{n},p|\Delta_E\Rightarrow p|n\}$ 均成立. 详见 [17]Chapter6.2$\Big)$——这也在暗示我们整体情形下有理曲线诱导的某个合理系统上的 (整体) 熵，与某类多项式的 Mahler 测度、曲线的高度函数相比蕴含的信息大同小异. 这相当于是用动力系统解释了我们为什么认为高度是一种“(算术) 复杂性”的度量.

9、约化方法

本节中，我们约定 K 是整体域，v 是 K 的一个有限素点，对应的离散赋值记作 $|\cdot|_v$. 记 K 关于 v 的赋值环为 $\mathcal{O}_v$，它有唯一极大理想 $\mathfrak{m}_v$，相应的剩余域记作 $k_v:=\mathcal{O}_v/\mathfrak{m}_v$. 我们称 $\bmod\mathfrak{m}_v:\mathcal{O}_v\to k_v$ 为**约化映射**，记作 $\widetilde{(\cdot)}:=(\bmod\mathfrak{m}_v)(\cdot)$. 下面的命题指出可以将约化映射定义到 $\mathbb{P}^n(K)$ 上：

命题 9.1 设 $P\in\mathbb{P}^n(K)$，则存在 $[a_0,a_1,\cdots,a_n]\in\mathbb{P}^n(K), a_{0\le i\le n}\in\mathcal{O}_K$ 使得 $P=[a_0,a_1,\cdots,a_n]$(称为 P 的一个**标准表示**)，且至少有某个 i 使 $a_i\in\mathcal{O}_K^\times$. 此时可以定义 P 的**模 $\mathfrak{m}_v$ 约化**为 $\widetilde{P}:=[\widetilde{a_0},\widetilde{a_1},\cdots,\widetilde{a_n}]\in\mathbb{P}^n(k_v)$.

证明 仅需证 $\widetilde{(\cdot)}$ 是良好定义的. 首先标准表示确保约化后的坐标分量不全为 0，从而落在 $\mathbb{P}^n(k_v)$ 中. 又因 P 的两个标准表示 $[a_0,a_1,\cdots,a_n],[b_0,b_1,\cdots,b_n]$ 仅相差 $\mathcal{O}_K^\times$ 中的某个可逆元，从而 $[\widetilde{a_0},\widetilde{a_1},\cdots,\widetilde{a_n}]$ 与 $[\widetilde{b_0},\widetilde{b_1},\cdots,\widetilde{b_n}]$ 仅相差 $k_v^\times$ 中的一个非零元，所以这两个表示在 $\mathbb{P}^n(k_v)$ 中确定同一个点.■

我们的目标是研究有理函数的动力学行为及其约化的动力学行为，特别是它们之间的联系. 为简单起见，如无特别声明本节出现的 $\mathbb{P}^n(\cdot)$ 均以 $n=1$ 为例.

对多项式 $f(x)=\sum_{i=0}^m a_ix^i\in\mathcal{O}_K[x]$，同样可以定义 $f(x)$ 的模 $\mathfrak{m}_v$ 约化 $\widetilde{f}(x)$ 为 $\sum_{i=0}^m\widetilde{a_i}x^i\in k_v[x]$. 而对于有理函数 $\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$，可以把 ϕ 表成 $\phi=[f(x,y),g(x,y)]$，这里 $f(x,y),g(x,y)\in K[x,y]$ 均是齐次多项式. 类似于命题 9.1，ϕ 应该也有所谓的标准表示：称 $[f(x,y),g(x,y)]$ 是 ϕ 的一个**齐次标准表示**，如果 $f(x,y),g(x,y)\in\mathcal{O}_K[x,y]$ 且至少有一个 $f(x,y),g(x,y)$ 的系数落入 $\mathcal{O}_K^\times$.

定义 9.2 设 ϕ 具有齐次标准表示 $[f(x,y),g(x,y)]$，定义 ϕ 的**模 $\mathfrak{m}_v$ 约化**为 $\widetilde{\phi}:=[\widetilde{f}(x,y),\widetilde{g}(x,y)]:\mathbb{P}^1(k_v)\to\mathbb{P}^1(k_v)$. 与命题 9.1 同理，$\widetilde{\phi}$ 良好定义.

例 9.3 设 $\phi=[ax^d,y^d],a\in K^\times$，则 $a\in\mathcal{O}_K^\times$ 当且仅当 $\widetilde{\phi}=[\widetilde{a}x^d,y^d]$. 其余情况 $\widetilde{\phi}$ 均为常值映射.

通过类似的方式还可以定义射影簇的约化，以及簇之间正则映射的约化. 一个经典的例子是整体域上椭圆曲线的约化情况.

命题 9.4 设 $\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$ 是有理函数，$[f,g]$ 是 ϕ 的齐次标准表示，则 $\deg(\phi)=\deg(\widetilde{\phi})$ 当且仅当 $\widetilde{f},\widetilde{g}$ 在 $\mathbb{P}^1(\overline{k_v})$ 中无公共解. 称满足该条件的有理函数 ϕ 是**好约化**的.

证明 由 $\widetilde{\phi}$ 的定义，若 $\deg(\phi)=\deg(\widetilde{\phi})$，则 $\widetilde{f}$ 与 $\widetilde{g}$ 不能在 $\overline{k_v}[x]$ 中有公因式，反之亦然.■

类比定义 6.4，对于赋值 $|\cdot|_v$，现定义 $\mathbb{P}^1(K)$ 上的度量为 $d_v:\mathbb{P}^1(K)^2\to\mathbb{R}_{\ge0}\sqcup\{\infty\},([x_1,y_1],[x_2,y_2])\mapsto\frac{|x_1y_2-x_2y_1|_v}{\max\{|x_1|_v,|y_1|_v\}\cdot\max\{|x_2|_v,|y_2|_v\}}$. 此时便可利用度量 d_v 研究 ϕ 的动力学行为. 例如我们可以得到好约化的 ϕ 具有

较好的动力学性质：

命题 9.5 若有理函数 $\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$ 好约化，则：

(1) 对任意 $P\in\mathbb{P}^1(K)$，$\widetilde{\phi(P)}=\widetilde{\phi}(\widetilde{P})$. (2)Julia 集 $\mathcal{J}(\phi)=\varnothing$.

(3) 若 ψ 也是好约化的，则 $\psi\circ\phi$ 好约化，且 $\widetilde{\psi\circ\phi}=\widetilde{\psi}\circ\widetilde{\phi}$.

(4) 约化映射 $\widetilde{(\cdot)}:\mathbb{P}^1(K)\to\mathbb{P}^1(k)$ 把周期点映为周期点，预周期点映为预周期点. 具体来讲，若 $\widetilde{(\cdot)}$ 把 n-周期点 P 映为 m-周期点 $\widetilde{P}$，则 $m|n$.

(5) 设 K_v 是局部域，有理函数 ϕ 好约化且 $\deg(\phi)\geq 2$. 若 $P\in\mathbb{P}^1(K_v)$ 的最小正周期为 n，$\widetilde{P}$ 的最小正周期为 m，则 $n=m$ 或 $n=m\cdot r\cdot\mathrm{Char}(k_v)^e, e\in\mathbb{Z}_{\geq 0}$，其中 r 指元素 $\varrho_{\widetilde{P}}(\widetilde{\phi})\in k_v^\times$ 的阶 (定义 6.3).

证明 见 [1]Chapter2.■

定理 9.6 设 K 是数域，$\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$ 是有理函数且 $\deg(\phi)\geq 2$，则 $|\mathrm{Per}(\mathbb{P}^1(K),\phi)|$ 有限.

证明 已知 ϕ 在 K 的几乎所有素点处好约化，现取其中两个素点 v,w 使得 $\mathrm{Char}(k_v)\neq\mathrm{Char}(k_w)$. 任取 $P\in\mathrm{Per}(\mathbb{P}^1(K),\phi)$，设 n 是 P 的最小正周期，则根据命题 9.5(5) 有 $n=m_vr_vp_v^{e_v}=m_wr_wp_w^{e_w}$. 注意到 p_v,p_w 是两个不同的素数，故 $n\leq m_vr_vm_wr_w\leq(|k_v|^2-1)(|k_w|^2-1)$. 由于给定 n 之后 ϕ 只有有限个 n-周期点，因而 $|\mathrm{Per}(\mathbb{P}^1(K),\phi)|<\infty$.■

应用第 8 节中介绍的高度函数，我们可以证明定理 9.6 的更强版本：

定理 9.7 设 K 是数域，$\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$ 是有理函数且 $\deg(\phi)\geq 2$，则 $|\mathrm{PrePer}(\mathbb{P}^1(K),\phi)|$ 有限.

证明 由命题 8.2(1)，存在常数 C_ϕ，使得对任意 $P\in K$ 均有 $h(\phi(P))\geq\deg(\phi)h(P)-C_\phi$，归纳可得 $h(\phi^n(P))\geq\deg(\phi)^nh(P)-C_\phi\cdot(1+\deg(\phi)+\cdots+\deg(\phi)^{n-1})\geq\deg(\phi)^n\cdot(h(P)-C_\phi)$. 现设 $Q\in\mathrm{PrePer}(K,\phi)$，则存在 $m\geq 1,n\geq 0$ 使得 $\phi^{m+n}(Q)=\phi^n(Q)$，故 $h(\phi^n(Q))=h(\phi^m(\phi^n(Q)))\geq\deg(\phi)^m\cdot(h(\phi^n(Q))-C_\phi)$. 又由于 $h(\phi^n(Q))\geq\deg(\phi)^n\cdot(h(Q)-C_\phi)$，因此可解出 $h(Q)\leq\frac{\deg(\phi)^m}{\deg(\phi)^n\cdot(\deg(\phi)^m-1)}C_\phi+C_\phi\leq 3C_\phi$. 应用命题 8.2(2) 即得结论.■

定理 9.7 中的 K 也可以替换成 $\mathbb{P}^n(K)$、椭圆曲线或 Abel 簇等几何对象，此时 Weil 高度机器 (Weil Height Machine) 保证了我们总可以讨论高度函数，换言之我们之前思考的“算术复杂性”本质上应该来自于几何.

定理 9.8(Weil 高度机器) 设 X 是数域 K 上的光滑射影簇，记 X 上所有余维数为 1 的闭子簇生成的自由 Abel 群为 $\mathrm{Div}(X)$，称为 X 上的**除子群**. 此时存在映射 $h_X:\mathrm{Div}(X)\longrightarrow\{\text{函数}X(\overline{K})\to\mathbb{R}\}, D\longmapsto h_{X,D}$，它满足：

(1.**在射影空间上标准**) 设 $H\subseteq\mathbb{P}^n(\overline{K})$ 是超平面，L/K 是有限扩张，则对任意 $P=[x_0,\cdots,x_n]\in\mathbb{P}^n(L)$，有 $h_{\mathbb{P}^n,H}(P)=\frac{1}{[L:K]}\sum_v\ln\max\{|x_0|_v,\cdots,|x_n|_v\}+O(1)$.

(2.**函子性**) 设 $f:X\to Y$ 是簇之间的态射，$D\in\mathrm{Div}(Y)$，则对任意 $P\in X(\overline{K})$，有 $h_{X,f^*D}(P)=h_{Y,D}(f(P))+O(1)$.

(3.**加性**) 设 $D,E\in\mathrm{Div}(X)$，则对任意 $P\in X(\overline{K})$，有 $h_{X,D+E}(P)=h_{X,D}(P)+h_{X,E}(P)+O(1)$.

(4.**线性等价**) 设 $D,E\in\mathrm{Div}(X)$ 线性等价，则对任意 $P\in X(\overline{K})$，有 $h_{X,D}(P)=h_{X,E}(P)+O(1)$.

(5.**代数等价**) 设 $D,E\in\mathrm{Div}(X)$，D 丰沛 (Ample) 且 E 代数等价于 0，则 $\lim\limits_{P\in X(\overline{K}),h_{X,D}(P)\to\infty}\frac{h_{X,E}(P)}{h_{X,D}(P)}=0$.

(6.**有限性**) 设 $D\in\mathrm{Div}(X)$ 丰沛，则对任意有限扩张 L/K 以及任意 $B>0$，集合 $\{P\in X(L):h_{X,D}(P)\leq B\}$ 有限.

(7.**唯一性**) 函数 $h_{X,D}$ 在相差一个 $O(1)$ 的前提下被 (1)，(2)，(3) 唯一确定.

定理 9.8 中的映射 h_X 当然还满足很多其它性质，此处不一一列举了. 值得一提的是，Weil 高度反映在具体的例子上便是我们熟知的各种高度.

第 8 节遗留的问题之一便是局部高度函数的定义. 当时我们说这个定义的最终形式非常复杂，造成这种现象的原因在于极限 $\lim_{n\to\infty}\frac{1}{\deg(\phi)^n}\ln\max\{|\phi^n(x)|_v,1\}$ 并不总是存在. 所以我们需要寻找一种可以放心求极限的替代物——Green 函数.

对有理函数 $\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$，考虑提升 $\Phi:=(f,g):\mathbb{A}^2_*(K)\to\mathbb{A}^2_*(K)$ 使得 f,g 作为齐次多项式没有公因式，其中 $\mathbb{A}^2_*(K)$ 指 2 维穿孔仿射平面，$\mathbb{P}^1(K)\cong\mathbb{A}^2_*(K)/\text{相似}$. 此处不需要使 $\phi=[f,g]$ 是齐次标准表示. 赋予 $\mathbb{A}^2_*(K)$ 绝对值 $\|(x,y)\|_v:=\max\{|x|_v,|y|_v\}$.

命题 9.9(Green 函数) 设 K 是域，$|\cdot|_v$ 是有限素点. 设有理函数 $\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$ 满足 $\deg(\phi)\geq 2$，

若指定提升 $\Phi=(f,g)$，则极限 $\lim_{n\to\infty}\frac{1}{\deg(\phi)^n}\ln\|\Phi^n(x,y)\|_v$ 存在，记作 $\mathcal{G}_{\Phi,v}(x,y)$. 称 $\mathcal{G}_{\Phi,v}$ 为 **Green 函数**，它具有以下性质：

(1)$\mathcal{G}_{\Phi,v}(\Phi(x,y))=\deg(\phi)\mathcal{G}_{\Phi,v}(x,y)$; $\mathcal{G}_{\Phi,v}(x,y)=\ln\|(x,y)\|_v+O_\phi(1)$. (2)$\mathcal{G}_{\Phi,v}:\mathbb{A}^2_*(K)\to\mathbb{R}$ 是连续映射.

(3) 若 K 是数域，则对任意 $P:=[x,y]\in\mathbb{P}^1(K)$，有 $\widehat{h}_\phi(P)=\sum_{p\le\infty}\sum_{v|p}[K_v:\mathbb{Q}_p]\cdot\mathcal{G}_{\Phi,v}(x,y)$.

该命题的证明类似定理 8.3，此处不再赘述. 至此我们便可完善定义 8.4：

定义 8.4′(局部高度) 记号如上，定义ϕ,v**-局部高度**函数为 $\widehat{\lambda}_{\phi,v}:\mathbb{P}^1(K)\to\mathbb{R}, P=[x,y]\mapsto\mathcal{G}_{\Phi,v}(x,y)-\ln|y|_v$. 可以证明它确实是良好定义的 ([1] 定理 5.60).

回顾定义 8.4，我们期待在好约化的时候局部高度函数会有更简单的表达式，关于此有如下命题：

命题 9.10 设 K 是数域，v 是有限素点，$\phi:\mathbb{P}^1(K)\to\mathbb{P}^1(K)$ 是有理函数满足 $\deg(\phi)\ge 2$. 若 ϕ 在 v 处好约化，则有 $|\phi(P)|_v=|P|_v^{\deg(\phi)}$，从而 $\mathcal{G}_{\Phi,v}(x,y)=\ln\|(x,y)\|_v$，$\widehat{\lambda}_{\phi,v}(P)=\ln\max\{|P|_v,1\}$.

10、映射类群的作用

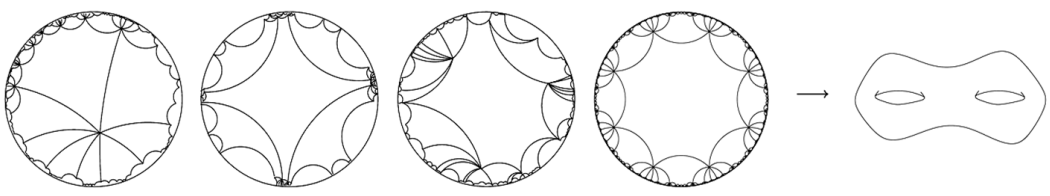
接下来介绍一些几何拓扑的概念，许多结论将会用示意图替代证明，因为我们更关心这些拓扑直观对于数论的启发，例如将复流形的代数几何合理地搬运为数域上的算术几何. 我们知道射影代数曲线上函数域扩张的 Galois 群相当于在描述曲线的分歧复叠，所以 Galois 表示应当可以来自于复叠变换群 (即底空间基本群) 的表示. 不过这里的表示空间是所谓的模空间，其上的“变换”可看成“纤维在基本群作用下的变化”. 我们称这样的表示为 Monodromy 表示，在 11 节中会介绍代数版本的 Monodromy 理论，并依此构建 Galois 表示. 本节除了刻画 Teichmuller 空间和模空间的几何拓扑，最重要的是在动力系统的观点下对闭曲面映射类群中的元素进行分类，而该分类的技术可用于使用 Monodromy 理论证明**几何 Shafarevich 刚性猜想**(设 X 是 Riemann 曲面 (从紧 Riemann 曲面挖去有限多个点得到)，给定 $g\ge 2$，考虑非局部常值的纤维丛 $\pi:Y\to X$ 使得 $\pi^{-1}(t)$ 均是亏格 g 的紧 Riemann 曲面 (见下面的拉回图表)，则满足上述这些条件的二元对 (Y/X) 仅有有限多个)，这种有限性类比到数域上就是曲线的**有限 Femart 定理**(方程 $X^n+Y^n=Z^n,(X,Y,Z)=1$ 在 $n\ge 4$ 时仅有有限多组整数解，详见第 12 节). 该工作来自于 Faltings，在历史上是解决 Femart 猜想的重要进展之一.

$$\begin{array}{ccccc}
\text{亏格}g\text{的紧 Riemann 曲面} & \xrightarrow{\quad\sim\quad} & \pi^{-1}(\cdot) & \longrightarrow & Y \\
 & \searrow^{\text{标准模型}} & \downarrow & \lrcorner & \downarrow\pi \\
 & & \mathrm{Spec}(\mathbb{C}) & \xrightarrow{\sim}\ \{\cdot\}\hookrightarrow & X
\end{array}$$

首先给出一个预备定理：

定理 10.1(Gauss-Bonnet) 亏格 $g\ge 2$ 的可定向光滑闭曲面 S 一定容许一个双曲度量 (此时称 S 为**双曲曲面**)，此时 $\pi_1(S)$ 的中心平凡；亏格 $g=1$ 的环面 $\mathbb{T}^2$ 容许一个平坦度量 (此时称 $\mathbb{T}^2$ 为**平坦曲面**)；亏格 $g=0$ 的球面 S^2 容许一个球度量(如果 S 上存在完备且使 $\mathrm{Vol}(S)$ 有限的 Riemann 度量，它对应的截面曲率分别为常数 -1、0、1，则分别称 S 容许一个**双曲度量**、**平坦度量**、**球度量**).

当 $g\ge 2$ 时，选取万有复叠空间 Poincaré 圆盘 $\left(\mathcal{D}:=\{z\in\mathbb{C}:|z|<1\},\frac{4|dz|^2}{(1-|z|^2)^2}\right)$ 中内角和为 2π 的一个测地 $4g$ 边形，下放其 Riemann 度量 $\frac{4|dz|^2}{(1-|z|^2)^2}$ 即得到闭曲面 S(只需合适地粘接对边即可) 上的一个双曲度量(记作 $\boldsymbol{d}$. 严格来说由于基本区域有多种选择故得到的应该是一个度量的共形等价类. 此外该度量也依赖于测地多边形的选取，如下图所示).

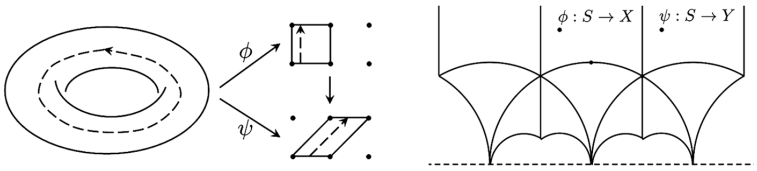


定义 10.2(模空间) 设 S 是亏格 $g\ge 0$ 的可定向光滑闭曲面，定义 S 的**映射类群** (Mapping Class Group)

为 $\mathrm{Mod}(S):=\{$保定向微分同胚$\}$/同痕，定义 S 的 **Teichmuller 空间**为

$$\begin{aligned}\mathrm{Teich}(S):&=\frac{\{\phi:S\to X\text{是微分同胚}:X\text{是双曲曲面 (即}S\text{上所有双曲度量)}\}}{(\phi:S\to X)\sim(\psi:S\to Y)\Leftrightarrow\text{存在等距同构}i:X\to Y\text{，使得映射}i\circ\phi\text{同伦于}\psi}\\&\xrightarrow{\sim}\frac{\{\text{离散单同态}\rho:\pi_1(S)\to\mathrm{PSL}(2,\mathbb{R})\cong\mathrm{Isom}^+(\mathcal{D})\}}{\rho_1\sim\rho_2\Leftrightarrow\exists A\in\mathrm{PGL}(2,\mathbb{R})\cong\mathrm{Isom}(\mathcal{D}),\forall\gamma\in\pi_1(S),\rho_2(\gamma)=A\rho_1(\gamma)A^{-1}}\\&[\phi:S\to X]\longmapsto\big[(S^1\xrightarrow{\gamma}S)\mapsto\phi\circ\gamma\in\pi_1(X)\cong\mathrm{Deck}(\mathcal{D}/X)\subseteq\mathrm{PSL}(2,\mathbb{R})\big].\end{aligned}$$

注意到 $\mathcal{D}$ 是万有复叠空间，故直观上说 $\mathrm{Teich}(S)$ 中的元素是 S 上“被基本群记录”的双曲结构 $\mathcal{D}/\rho(\pi_1(S))$，因为 $\mathrm{Teich}(S)$ 中每个元素都指定了 $\pi_1(S)$ 中各道路自由同伦类中最短闭测地线的长度. 由于度量结构比复结构更加刚性，故 Teichmuller 空间中不同点可能对应相同 Riemann 曲面，例如下图：



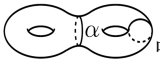
自然地，我们有群作用 $\mathrm{Mod}(S)\times\mathrm{Teich}(S)\to\mathrm{Teich}(S),(\sigma,[\phi:S\to X])\mapsto[\phi\circ\sigma^{-1}:S\to X]$. 称此时的轨道空间 $\mathcal{M}(S):=\mathrm{Teich}(S)/\mathrm{Mod}(S)$ 为同胚于 S 的 Riemann 曲面的**模空间** (Moduli Space). 直观上说 $\mathcal{M}(S)$ 中的元素是 S 上所有不同的双曲结构.

我们关心 $\mathrm{Mod}(S)$ 的代数结构 (实际上它是基本群 $\pi_1(S)$ 的保定向外自同构群)、$\mathrm{Teich}(S)$ 和 $\mathcal{M}(S)$ 的几何拓扑结构 (它们在某种意义上是“参数空间”)，这些结构通过 S 的组合拓扑联系起来.

定义 10.3(相交数) 设 S 是亏格 $g\geq 0$ 的可定向光滑闭曲面，称光滑单射 $S^1\hookrightarrow S$ 是 S 中的一条**简单闭曲线**. 记 $\mathrm{Loop}(S):=\{S$上的简单闭曲线$\}$/自由同伦，定义**几何相交形式**为 $i:\mathrm{Loop}(S)^2\to\mathbb{Z}_{\geq 0},(\alpha,\beta)\mapsto\min\{|a\pitchfork b|:a,b\text{是简单闭曲线},a\in\alpha,b\in\beta\}$，这里“$\pitchfork$”指**横截相交** (即 $x\in a\cap b$ 且满足 $T_xa\oplus T_xb\cong T_xS$). 整数 $i(\alpha,\beta)$ 称为 α 和 β 的**几何相交数** (Intersection Number). 当然也有代数相交的概念：定义**代数相交形式**为 $\widetilde{i}:H_1(S,\mathbb{Z})^2\to\mathbb{Z},(\alpha,\beta)\mapsto\sum_{t\in a\cap b}\frac{(a_t'\times b_t')\cdot\boldsymbol{n}_t}{|a_t'\times b_t'|}$，这里随意选取 $a\in\alpha,b\in\beta$，$\boldsymbol{n}_t$ 指由 S 的定向给出的 t 处的单位法向量. 整数 $\widetilde{i}(\alpha,\beta)$ 称为 α 和 β 的**代数相交数**.

根据定义不难验证：$\widetilde{i}(\alpha,\beta)\leq i(\alpha,\beta)$，$i(\alpha,\beta)=i(\beta,\alpha)$，$\widetilde{i}(\alpha,\beta)=-\widetilde{i}(\beta,\alpha)$.

在此我们需要强调同调、同伦、自由同伦、同痕之间的区别.

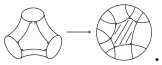
注意 10.4 同痕是稍微加强版的同伦，也就是说在伦移的过程中不允许坍缩或自交，它要求每时每刻都是嵌入，例如所有的扭结都是同伦等价的，所以对扭结而言需要使用同痕这个更精细的不变量；同伦 (某种意义上) 是加强版的同调，例如 

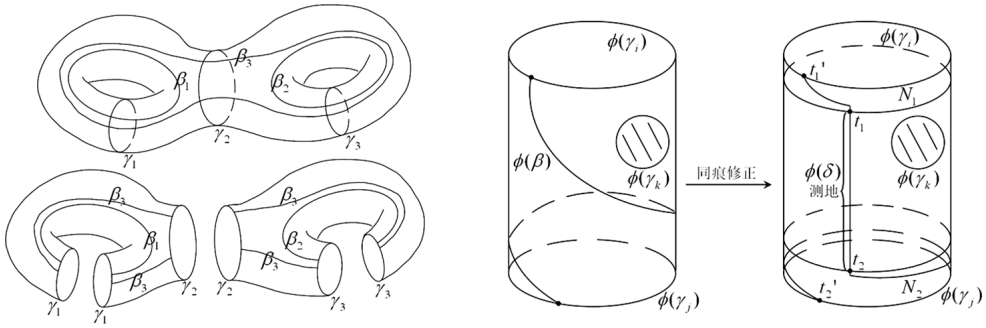
中闭曲线 α 零调但不零伦；同伦和自由同伦的区别在于是否强调基点，[27] 命题 4A.2 指出存在一一对应 $\frac{\{S\text{上过}x_0\text{的简单闭曲线}\}/\text{固定端点}x_0\text{的同伦}}{\pi_1(S,x_0)}\xrightarrow{\sim}\mathrm{Loop}(S)$.

可以证明紧致 Riemann 流形上任何闭曲线的自由同伦类中必有测地线，特别地对于双曲曲面而言这里存在的测地线还是唯一的. 这些不同自由同伦类连同扭转 (Twist) 参数贡献了空间 $\mathrm{Teich}(S)$ 的自由度.

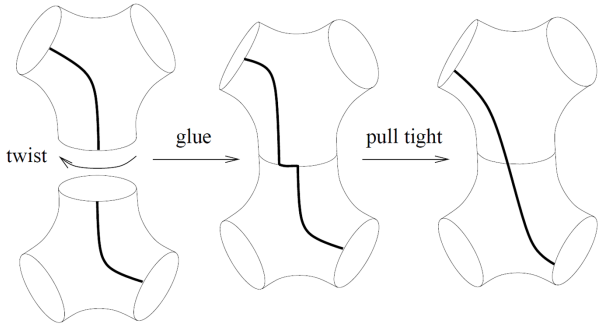
定理 10.5(Fricke) 定义**长度函数**$\ell:\mathrm{Loop}(S)\times\mathrm{Teich}(S)\to\mathbb{R}_{\geq 0},(\alpha,[\phi:S\to X])\mapsto\inf\{\boldsymbol{d}_X(\gamma):\gamma\subseteq X\text{光滑},\gamma\text{同痕于}\phi(\alpha)\}$. 当亏格 $g\geq 2$ 时，我们有同胚 $\Psi:\mathrm{Teich}(S)\to\mathbb{R}_{>0}^{3g-3}\times\mathbb{R}^{3g-3},[\phi:S\to X]\mapsto\big(\ell(\gamma_1,\phi),\cdots,\ell(\gamma_{3g-3},\phi),\theta(\gamma_1,\phi),\cdots,\theta(\gamma_{3g-3},\phi)\big)$，这里 γ_i 为 S 胖次分解对应的 $3g-3$ 条简单闭曲线，$\theta(\cdot,\cdot)$ 为粘接胖次时出现的“扭转参数”(见 Step2). 因此 $\mathrm{Teich}(S)\cong\mathbb{R}^{6g-6}$ 是同胚于开球的度量空间.

证明 **Step1：**根据定义 10.2，定义 $\mathrm{Teich}(S)$ 上的拓扑为 $\mathrm{Hom}(\pi_1(S),\mathrm{PSL}(2,\mathbb{R}))$ 配备紧开拓扑之后的子空间拓扑的商拓扑，其中 $\pi_1(S)$ 配备离散拓扑，$\mathrm{PSL}(2,\mathbb{R})$ 配备通常拓扑$\Big($实际上该拓扑可由 **Teichmuller 度量**$d_{\mathrm{Teich}}\big([S\xrightarrow{\phi}X],[S\xrightarrow{\psi}Y]\big):=\frac{1}{2}\ln\inf\{K\geq 1:\text{存在}K\text{-拟共形映射}f:X\to Y\}$ 诱导. 此处我们称微分同胚 $f:X\to Y$ 是**K-拟共形映射**，如果切映射 $df:TX\to TY$ 将无穷小的圆送到长轴和短轴之比落在区间 $[1,K]$ 中的椭圆. 可以证明，如果存在 K- 拟共形映射 $f:X\to Y$，则 $\frac{1}{K}\ell(\alpha,[S\xrightarrow{\phi}X])\leq\ell(\alpha,[S\xrightarrow{\psi}Y])\leq K\ell(\alpha,[S\xrightarrow{\phi}X])$. 还可以证明 $\mathrm{Teich}(S)$ 配备度量 d_{Teich} 之后 $\mathrm{Mod}(S)$ 在其上的作用等距，见 [25]Chapter11.8$\Big)$.

Step2：(胖次分解与扭转数)称亏格为 0 的紧曲面 P 为一只**胖次** (Pants)，如果 $\partial P\cong S^1\sqcup S^1\sqcup S^1$. 当 $g\geq 2$ 时，所谓**胖次分解**即如下资料：(1)$3g-3$ 条简单闭曲线 $\{\gamma_1,\cdots,\gamma_{3g-3}\}\subseteq S$ 将 S 切割为 $2g-2$ 只胖次 $P_1,\cdots,P_{2g-2}$，使得 $\partial P_k=\gamma_{k_1}\sqcup\gamma_{k_2}\sqcup\gamma_{k_3}$；(2)$3g-3$ 条简单闭曲线 $\{\beta_1,\cdots,\beta_{3g-3}\}\subseteq S$ 使 $\left(\bigcup_{i=1}^{3g-3}\beta_i\right)\cap P_k$ 为连接 ∂P_k 三个连通分支的三条无交曲线 (下图左). 现设 β 是胖次 P 上满足上述条件 (2) 的曲线，不妨设它连接了边界 γ_i,γ_j. 利用 $[\phi:S\to X]\in\mathrm{Teich}(S)$ 赋予 S 双曲度量之后存在唯一测地线 $\phi(\delta_{ij})$ 连接了 $\phi(\gamma_i),\phi(\gamma_j)\Big($我们可适当调整胖次 P 的选取使 $\partial(\phi P)$ 均是测地线，这样由变分原理可知 $\phi(\delta_{ij})\perp\phi(\gamma_i),\phi(\delta_{ij})\perp\phi(\gamma_j)$. 沿这 3 条测地线 $\phi(\delta_{ij}),\phi(\delta_{ik}),\phi(\delta_{jk})$ 剪开胖次后即得到两个各临边互相垂直的双曲 6 边形，它们均可自然地放入 $\mathcal{D}$：  . 这样的 6 边形的形状是唯一的，它由其中 3 条不相邻的边唯一确定. 因此胖次上带测地边界的双曲结构被边界的长度唯一确定$\Big)$. 不妨设 $\phi(\delta_{ij})\cap\phi(\gamma_i)=t_1,\phi(\beta)\cap\phi(\gamma_i)=t_1'$. 定义在映射 ϕ 下曲线 β 在 γ_i 处的**扭转数**为 $\theta(\gamma_i,\phi):=2\pi\frac{t_1-t_1'}{\ell(\gamma_i,\phi)}$(下图右). 直观上来讲，扭转数即衡量“同痕地修正 $\phi(\beta)$ 使得在 $P\setminus(N_2\cup N_2)$ 中 $\phi(\beta)=\phi(\delta_{ij})$”这个操作的困难程度，此处 N_1,N_2 是 $\phi(\gamma_i),\phi(\gamma_j)$ 的某个合适邻域.



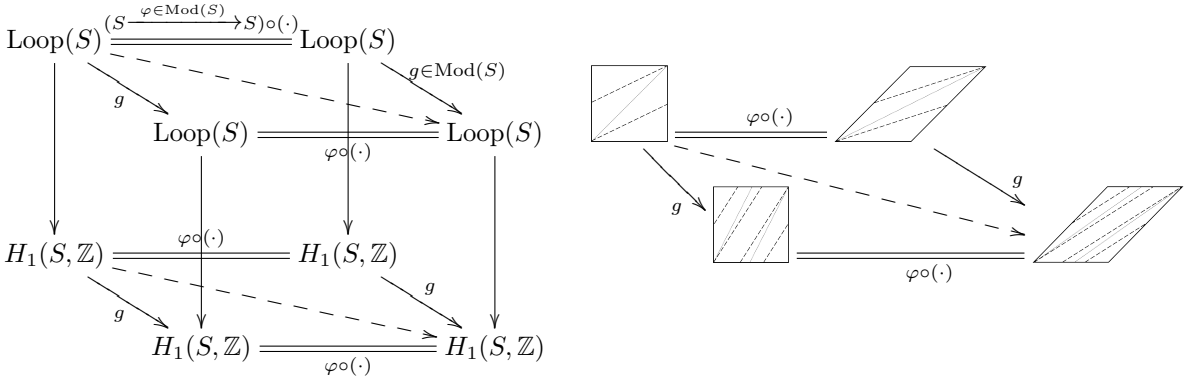
Step3：(Fenchel-Nielsen 坐标)设 $\mathrm{Teich}(S)$ 配备了 Step1 中的拓扑. 用 $3g-3$ 条简单闭曲线将 S 分解成 $2g-2$ 只胖次，这 $3g-3$ 个长度参数决定了每一只胖次的双曲结构 (Step2)；此外还有 $3g-3$ 个扭转参数用于确定这些胖次如何粘在一起 (如下图). 因此 $\mathrm{Teich}(S)$ 总共有 $6g-6$ 个自由度，换言之 Ψ 是同胚.■



代数上可以这样理解定理 10.5：显然 $\dim\mathrm{PGL}(2,\mathbb{R})=3$，并且它在集合 $\Sigma(S):=\{$离散单同态$\rho:\pi_1(S)\to\mathrm{PSL}(2,\mathbb{R})\}$ 上的作用诱导的轨道空间也是 3 维的，因此 $\dim\mathrm{Teich}(S)=\dim\Sigma(S)-3$. 可以证明 $\dim\Sigma(S)=\dim\mathrm{Hom}(\pi_1(S),\mathrm{PSL}(2,\mathbb{R}))$，而同态 $\rho:\pi_1(S):=\langle\gamma_1,\cdots,\gamma_{2g}:[\gamma_1,\gamma_2]\cdots[\gamma_{2g-1},\gamma_{2g}]\rangle\to\mathrm{PSL}(2,\mathbb{R})$ 又由 $\rho(\gamma_i),1\leq i\leq 2g$ 确定，但生成关系 $[\rho(\gamma_1),\rho(\gamma_2)]\cdots[\rho(\gamma_{2g-1}),\rho(\gamma_{2g})]=\mathrm{id}$ 暗含 $\rho(\gamma_{2g})$ 由 $\rho(\gamma_i),1\leq i\leq 2g-1$ 完全确定，这导致这些 $\rho(\gamma_i)$ 的选取 (即同态 ρ) 只有 $3(2g-1)$ 个自由度. 由于共轭表示等价又削减 3 个自由度，故综上 $\dim\mathrm{Teich}(S)=3(2g-1)-3$，即 $\mathrm{Teich}(S)$ 的自由度是 $6g-6$.

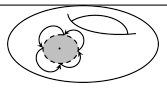
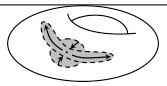
例 10.6 当 $g=1$ 时，我们知道 $\mathrm{Mod}(\mathbb{T}^2)\cong\mathrm{SL}(2,\mathbb{Z})$，$\mathrm{Teich}(\mathbb{T}^2)=\mathcal{H}$，$\mathrm{Loop}(\mathbb{T}^2)=\mathbb{P}^1(\mathbb{Q})\xrightarrow{\sim}(\mathbb{Z}\times\mathbb{Z})/\sim$，这里 $(a,b)\sim(c,d)\Leftrightarrow\exists\lambda\in\mathbb{Q}^\times,(a,b)=(\lambda c,\lambda d)$. 事实上，$\mathrm{Loop}(\mathbb{T}^2)$ 中的元素即有限长度的周期性轨道 (无理流无法回到原点). 此外，我们还可以考虑群作用 $\mathrm{Mod}(\mathbb{T}^2)\times\mathrm{Loop}(\mathbb{T}^2)\to\mathrm{Loop}(\mathbb{T}^2),\left(\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right),\frac{p}{q}\right)\mapsto\frac{ap+bq}{cp+dq}\Big($显然该作用可直接迁移至同调群 $H_1(S,\mathbb{Z})\Big)$，不难发现该作用保持几何相交形式 $i(\frac{p}{q},\frac{r}{s})=\left|\det\left(\begin{smallmatrix}p&r\\q&s\end{smallmatrix}\right)\right|$(例如下图，我们称斜着的虚线箭头为 g 相伴于微分同胚 φ 的作用. 事实上该性质对亏格 ≥ 2 或代数相交形式也成立). 换句话说如果将 $\mathrm{Loop}(\mathbb{T}^2)$ 类比为线性空间，将 $\mathrm{Mod}(\mathbb{T}^2)$ 中的元素看成可逆线性变换，则几何相交形式类似于一个“二

次型”.



我们可以按照动力学行为利用 Jordan 标准型对 $\mathrm{Mod}(\mathbb{T}^2)$ 中的元素分类：

定理 10.7(Nielsen-Thurston) 当亏格为 1 时，任意 $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\neq g\in\mathrm{Mod}(\mathbb{T}^2)$ 必属于下述三类之一：

$g\in\mathrm{Mod}(\mathbb{T}^2)$	定义	在 $\mathrm{GL}(2,\mathbb{R})$ 中对应的 Jordan 标准型	在 $\mathbb{T}^2$ 上的行为	迹
周期型 (椭圆)	$gz=z$ 在 $\mathcal{H}$ 中有解	$g^n=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),n\in\{2,3,4,6\}$		$0,1$
可约型 (抛物)	$gz=z$ 有两相同实根	$\left(\begin{smallmatrix}1&a\\0&1\end{smallmatrix}\right),a\in\mathbb{R}^\times$		2
Anosov(双曲)	$gz=z$ 有两不同实根	$\left(\begin{smallmatrix}a&0\\0&a^{-1}\end{smallmatrix}\right),a\neq\pm1$		≥ 3

一般地，当亏格 ≥ 2 时，任意 $g\in\mathrm{Mod}(S)$ 必属于周期型(存在 $n\geq 1$ 使得 $g^n=\mathrm{id}$)、可约型(存在有限集 $\{\alpha_1,\cdots,\alpha_n\}\subseteq\mathrm{Loop}(S)$ 满足 $i(\alpha_i,\alpha_j)=0$，使得 g 在其上的作用为置换)、pseudo-Anosov(存在 $K>1$ 使得对任意 $\alpha,\beta\in\mathrm{Loop}(S)$，$C_1K^n\leq i(g^n(\alpha),\beta)\leq C_2K^n$，这里 C_1,C_2 依赖于 α,β 的选取)这三类之一.

证明 亏格为 1 的情形就是基本的线性代数，详见 [28]Chapter1.3. 亏格 ≥ 2 时的证明见 [25]. 基本想法是把 $f:S\to S$ 提升为 $\widetilde{f}:\mathcal{D}\to\mathcal{D}$，再延拓到无穷远边界得到 $\partial\widetilde{f}:S^1\to S^1$，然后对 $\partial\widetilde{f}$ 的不动点集进行分类.■

当亏格 ≥ 2 时，定理 10.5 已经完美地刻画了 Teichmuller 空间. 当然我们还希望刻画模空间，而这至少需要弄清楚映射类群 (即模空间基本群) 的代数结构而非其中元素的动力学行为 (定理 10.7). 研究这个代数结构是尤其困难的，此处我们仅列出它的若干性质：

命题 10.8 $\mathrm{Mod}(S)$ 是有限表示的. 当 $g\geq 3$ 时，$\mathrm{Mod}(S)$ 的中心平凡；$H_1(\mathrm{Mod}(S),\mathbb{Z})=\{0\}$. 当 $g\geq 4$ 时，$H_2(\mathrm{Mod}(S),\mathbb{Z})=\mathbb{Z}$.

映射类群的复杂导致我们无法妥善地描述模空间的拓扑，即便我们已经确定其上的度量. 不同于几何所关心的，模空间的另一意义在于其“参数化了一些结构”：

定理 10.9 当 $g\geq 2$ 时，模空间 $\mathcal{M}(S)$ 是 S 上如下结构的参数化：(1)S 上常曲率度量的等距自同构类；(2)S 上双曲度量的共形等价类；(3)S 上复结构的双全纯同构类；(4)S 上光滑复代数结构的同构类.

11、单值性

定义 11.1(族) 设 B 是 Riemann 曲面 (称为**底空间**)，它可从一个紧 Riemann 曲面挖去有限多个点得到. 设有 2 维复流形 C(称为**全空间**) 连同一个全纯映射 $\pi:C\to B$ 使纤维 $\pi^{-1}(t):=C_t$ 均是亏格 g 的紧 Riemann 曲面，则称二元对 C/B 是一个**族** (Family). 称族 C/B **局部常值**，如果对任意 $s,t\in B$，$C_s\cong C_t$，否则称其为**非局部常值** (Truly Varying) 的.

“族”的一般定义见 [33]Chapter2.3. 有了这个定义之后便可如下描述几何 Shafarevich 刚性猜想：

定理 11.2(几何 Shafarevich 刚性定理) 设 B 是 Riemann 曲面 (可非紧致). 给定 $g\geq 2$，则纤维亏格均

为 g 的非局部常值族 C/B 仅有有限多个. 具体来讲，这有限多个非局部常值族 C/B 被同态 $\pi_1(B)\to\pi_1(\mathcal{M}_g)$ 完全决定 (这里 $\mathcal{M}_g$ 表示亏格 g 的紧 Riemann 曲面作成的模空间，Teich_g 同理).

该定理的证明请参考 [16]. 定理中出现的同态 $\pi_1(B)\to\pi_1(\mathcal{M}_g)$ 是一种 **Monodromy 表示**，它的算术版本才是我们关注的，不过此处还是先从 Monodromy 理论的几何版本开始介绍.

设 B 是紧 Riemann 曲面，$\mathcal{P}\subseteq B$ 是有限集，考虑族 $C\big/(B\setminus\mathcal{P})$. 定义**分类映射** $f:B\setminus\mathcal{P}\to\mathcal{M}_g, t\mapsto[C_t]$，它诱导 Monodromy 表示

$$\widetilde{f}_{\mathcal{P}}\langle t\rangle:\pi_1(B\setminus\mathcal{P},t)\to\pi_1(\mathcal{M}_g)=\mathrm{Deck}\left(\mathrm{Teich}_g\Big/\frac{\mathrm{Teich}_g}{\mathrm{Mod}(C_t)}\right)\cong\mathrm{Mod}(C_t).$$

由于映射类群 $\mathrm{Mod}(C_t)$ 太过复杂，加之我们又希望研究简单的线性表示，故可利用同调函子对上述 Monodromy 表示稍作修正：考虑同态 $\pi_1(B\setminus\mathcal{P},t)\to\mathrm{Aut}(H_1(C_t,\mathbb{Z}))=\mathrm{GL}(2g,\mathbb{Z}),\gamma\mapsto H_1\circ(\widetilde{f}_{\mathcal{P}}\langle t\rangle(\gamma))$，该表示记录了同调的变化. 通过这个修正版本的 Monodromy 表示可以构造 Galois 表示，而这首先要将基本群和 Galois 群联系起来. 我们的思路是抽象基本群的复叠解释.

先回顾一下 Riemann 曲面的复叠理论，借此引入 etale 基本群的定义. 我们称 $\widehat{G}:=\varprojlim_{N\lhd G,[G:N]<\infty}G/N$ 为群 G 的 **Profinite 完备化**，它配备了自然的 Profinite 拓扑之后成为一个拓扑群.

设 X 是紧 Riemann 曲面 (当然道路连通)，则亚纯函数域 $\mathcal{M}_X$ 的任意有限 (可分) 代数扩张均形如 $\mathcal{M}_Y$，其中 Y 是紧 Riemann 曲面且 $Y\to X$ 是有限分歧复叠. 记分歧点作成的集合为 $\mathrm{Ram}_{Y\to X}\subseteq X$，这是个有限集.

命题 11.3 称 n 次扩张 $\mathcal{M}_Y/\mathcal{M}_X$ 在 $\mathcal{M}_X$ 上的离散赋值 $v_p:f\mapsto\mathrm{ord}_p(f), p\in X$ 处**分歧**，如果只有小于 n 种方式将 v_p 提升为 $\mathcal{M}_Y$ 上的离散赋值. 我们有一一对应

$$\mathrm{Ram}_{Y\to X}\xrightarrow{\sim}\{\mathcal{M}_X\text{上的离散赋值}v:\mathcal{M}_Y/\mathcal{M}_X\text{在}v\text{处分歧}\},\quad p\longmapsto v_p.$$

此外，若定义 $\overline{\mathcal{M}_X^{\mathcal{P}}}:=\big\langle\mathcal{M}_X\text{的有限扩张}:\text{仅在}v_p\text{处分歧},p\in\mathcal{P}\subseteq X\big\rangle\subseteq\overline{\mathcal{M}_X}$，则对任何有限集 $\mathcal{P}\subseteq X$，有拓扑群同构 $\mathrm{Gal}\big(\overline{\mathcal{M}_X^{\mathcal{P}}}/\mathcal{M}_X\big)\cong\widehat{\pi}_1(X\setminus\mathcal{P})$. 特别地，若 $\mathcal{P}=\varnothing$，则 $\mathrm{Gal}\big(\overline{\mathcal{M}_X^{\varnothing}}/\mathcal{M}_X\big)\cong\widehat{\pi}_1(X)$.

例 11.4 注意到所有紧 Riemann 曲面上的所有亚纯函数都是到 $\mathbb{P}^1(\mathbb{C})$ 的复叠映射，因而简单起见考虑 $X:=\mathbb{P}^1(\mathbb{C})$，此时 $\mathcal{M}_X=\mathbb{C}(z)$. 显然 $\widehat{\pi}_1(X)$ 平凡，故 $\mathbb{C}(z)$ 的所有非平凡代数扩张都有分歧点$\Big($或抽象来讲，射影概型 $\mathbb{P}^1(\mathbb{C})$ 上没有“有限 etale 覆盖”. 类似地在代数数论中，Hermite-Minkowski 定理告诉我们对于有限扩张 $K/\mathbb{Q}$，判别式 d_K 满足不等式 $\sqrt{|d_K|}\geq\frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$. 由此可得 $\mathbb{Q}$ 没有非分歧扩张，即 $\mathrm{Spec}(\mathbb{Z})$ 上也没有所谓的有限 etale 覆盖，因此之后定义的 etale 基本群 $\pi_1^{\mathrm{et}}(\mathrm{Spec}(\mathbb{Z}))$ 平凡，详见定义 11.5 和例 11.8$\Big)$. 例如指定分歧点 $\mathcal{P}:=\{0,\infty\}\subseteq X$，则由 $\pi_1(X\setminus\mathcal{P})=\mathbb{Z}$ 可知 $\mathrm{Gal}\big(\overline{\mathbb{C}(z)^{\{0,\infty\}}}/\mathbb{C}(z)\big)=\widehat{\mathbb{Z}}$. 例如，2 次代数扩张 $\mathbb{C}(z)\subseteq\mathbb{C}(\sqrt{z})\subseteq\overline{\mathbb{C}(z)^{\{0,\infty\}}}$ 对应极小多项式 $x^2-z=0$，倘若取 $Y:=\mathbb{P}^1(\mathbb{C})$，则根据 Riemann-Hurwitz 公式可计算得该扩张对应 X 上的分歧点正好就是 $\mathcal{P}\Big($或者从赋值来看 v_0 仅有一种提升；或者从代数来看 Zariski 闭点 0 对应的素理想 $(z)\in\mathrm{Spec}(\mathbb{C}[z])$ 在环 $\mathbb{C}[\sqrt{z}]$ 中分解 $\mathrm{Im}((z))\,\mathbb{C}[\sqrt{z}]=(\sqrt{z})^2$ 的分歧指数为 2；或者从几何来看 0 显然是分歧点$\Big)$.

考虑穿孔曲面基本群 $\pi_1(X\setminus\mathrm{Ram}_{Y\to X})$ 的 Profinite 完备化并关于所有可能的分歧复叠作反向极限得 $\varprojlim\widehat{\pi}_1(X\setminus\mathrm{Ram}_{Y\to X})$，这个群直观上记录所有穿刺曲面 X 的方式，而绝对 Galois 群 $\mathrm{Gal}(\overline{\mathcal{M}_X}/\mathcal{M}_X)$ 记录所有可能的分歧方式，所以我们自然期待这两个群存在某种联系，而该联系可由命题 11.3 得到：

$$\begin{array}{ccccc}
\varprojlim\limits_{\mathrm{Ram}_{Y\to X}\neq\varnothing}\mathrm{Gal}\big(\overline{\mathcal{M}_X^{\mathrm{Ram}_{Y\to X}}}/\mathcal{M}_X\big) & \xleftarrow{\text{分歧部分}} & \mathrm{Gal}(\overline{\mathcal{M}_X}/\mathcal{M}_X) & \xrightarrow{\text{非分歧部分}} & \mathrm{Gal}\big(\overline{\mathcal{M}_X^{\varnothing}}/\mathcal{M}_X\big) \\
\| & & \| & & \| \\
\varprojlim\limits_{\mathrm{Ram}_{Y\to X}\neq\varnothing}\widehat{\pi}_1(X\setminus\mathrm{Ram}_{Y\to X}) & & \varprojlim\limits_{\text{所有复叠}Y\to X}\widehat{\pi}_1(X\setminus\mathrm{Ram}_{Y\to X}) & & \widehat{\pi}_1(X)
\end{array}$$

对于非分歧的部分，在代数几何中有严肃的语言重新建立这套理论，从而得到所谓的 etale 基本群. 上面的例子也正好解释了为什么 etale 态射需要“非分歧”的条件以及为什么 Galois 群会与基本群有联系 (命题 11.7). 此处限于篇幅仅作简要介绍：

定义 11.5(etale 基本群) 设 $(f,f^\sharp):(X,\mathcal{O}_X)\to(S,\mathcal{O}_S)$ 是**局部有限型**(Locally of Finite Type，即 S 存在仿射开覆盖 $\{\mathrm{Spec}(B_i)\}$ 使得 $f^{-1}(\mathrm{Spec}(B_i))=\bigcup_j\mathrm{Spec}(A_{ij})$ 且 A_{ij} 均是有限生成 B_i-**代数**)的概型态射. 称 f 在 $x\in X$ 处 **etale**，如果 f 在 x 处**平坦**(即 $\mathcal{O}_{X,x}$ 作为 $\mathcal{O}_{S,f(x)}$-模是平坦的) 且**非分歧**(即 $(f_x^\sharp)^{-1}(\mathfrak{m}_{\mathcal{O}_{X,x}})=\mathfrak{m}_{\mathcal{O}_{S,f(x)}}$，$f_x^\sharp(\mathfrak{m}_{\mathcal{O}_{S,f(x)}})\mathcal{O}_{X,x}=\mathfrak{m}_{\mathcal{O}_{X,x}}$ 且 $(\mathcal{O}_{X,x}/\mathfrak{m}_{\mathcal{O}_{X,x}})\big/(\mathcal{O}_{S,f(x)}/\mathfrak{m}_{\mathcal{O}_{S,f(x)}})$ 是有限可分扩张)). 如果 f 在任意 $x\in X$ 处 etale，则称 f 是一个 **etale 态射**. 现要求 S 是一个带有**几何点** $\overline{x}:\mathrm{Spec}(\Omega)\to S$(Ω 是一个可分闭域. 取可分闭域是因为此时 Galois 群平凡 (见例 11.8)，而代数拓扑的直觉告诉我们这样的点作为基本群的基点才是合理的)的连通概型，记所有**有限**(即 S 存在仿射开覆盖 $\{\mathrm{Spec}(B_i)\}$ 使得对任意 i，$f^{-1}(\mathrm{Spec}(B_i))=\mathrm{Spec}(A_i)$ 且 A_i 是有限生成 B_i-**模**)etale S- 态射 $p:X\to S$ 作成的范畴为 $\mathbf{FEt}_S$. 考虑函子 $F_{\overline{x}}:\mathbf{FEt}_S\longrightarrow\mathbf{FSets},[p:X\to S]\longmapsto p^{-1}(\overline{x})=\mathrm{Spec}(\Omega)\times_S X$(看作集合)，其自同构群 $\mathrm{Aut}(F_{\overline{x}})$ 称为 **etale 基本群**，记作 $\pi_1^{\mathrm{et}}(S,\overline{x})$.

注意 11.6 (1) 设 K 是一个域，则 $X\to\mathrm{Spec}(K)$ 是 etale 态射当且仅当 $X\cong\bigsqcup_i\mathrm{Spec}(L_i)$，其中 L_i/K 是有限可分扩张. 因此代数上来讲 etale 态射可以看成有限可分扩张的推广. 拓扑上来讲 etale 态射模拟了复叠映射的“局部同胚”.

(2) 虽然 etale 基本群这个概念抽象自拓扑，但它本质上是代数的构造，并不直接反映概型的拓扑信息. 但由于开浸入均是 etale 态射，因而某种意义上会出现一个比 Zariski 拓扑更细的“拓扑”——etale 拓扑，更精细的信息来自于局部环剩余域的扩张行为. 注意，etale 基本群也并不是“etale 拓扑”在代数拓扑意义下的基本群！实际上“etale 拓扑”并非由通常的拓扑公理定义，但层上同调 (即 etale 上同调，这是 Galois 上同调的推广) 或 Čech 上同调的技术却依然可以合理地移植于此，详见 [35]Chapter6.

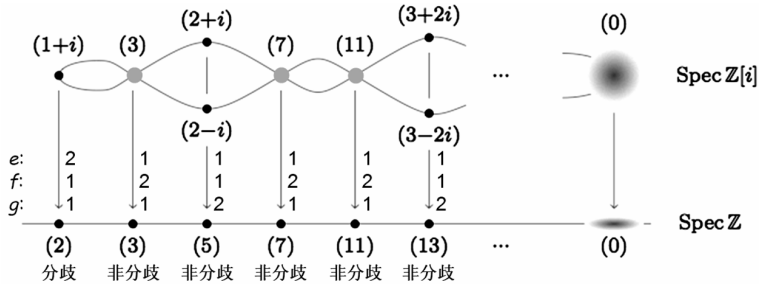
命题 11.7(正规概型的基本群) 设 X 是正规 (即所有 Stalk 均是整闭整环) 连通局部 Noether 概型，其函数域记作 $\boldsymbol{k}(X)$. 设 $\boldsymbol{k}(X)\subseteq\Omega$ 是一个可分闭域，取几何点 $\overline{x}:\mathrm{Spec}(\Omega)\to X$. 若记

$$L:=\big\langle\boldsymbol{k}(X)\text{的有限可分扩张，且在}X\text{上非分歧}\big\rangle\subseteq\Omega,$$

则 $\mathrm{Gal}(L/\boldsymbol{k}(X))=\pi_1^{\mathrm{et}}(X,\overline{x})$.

例 11.8 (1) 取域 K 的可分闭包 K_{sep} 得到一个几何点 $\overline{x}:\mathrm{Spec}(K_{\mathrm{sep}})\to\mathrm{Spec}(K)$. 此时 $\pi_1^{\mathrm{et}}(\mathrm{Spec}(K),\overline{x})=\mathrm{Gal}(K_{\mathrm{sep}}/K)$. 特别地，若 K 是可分闭域，则 etale 基本群平凡.

(2) 事实上，代数几何、代数数论、代数拓扑中对“分歧”一词的理解是一致的. 例如考虑环同态 $\mathbb{Z}\to\mathbb{Z}[i]$，它对应的函数域扩张次数是 2，此即代数数论中 efg 的值、代数拓扑中复叠的次数. 下图是该态射的几何图像，各信息均已标于图中.



对于分歧的部分，类似于命题 11.4 同样可以归结为非分歧 (即 etale) 的情形. 总的来说，我们有如下命题：

命题 11.9 设 X 是光滑曲线，记其函数域为 $\boldsymbol{k}(X)$. 此时有 $\pi_1^{\mathrm{et}}(X)\cong\mathrm{Gal}(\boldsymbol{k}(X)_{\mathrm{sep}}/\boldsymbol{k}(X))/N$，这里 N 是由所有惯性子群 I_x 生成的闭子群，其中 x 跑遍 X 的所有 Zariski 闭点.

回到 Galois 表示的问题. 给定族 $C\big/(B\setminus\mathcal{P})$，这里 $\mathcal{P}$ 是紧 Riemann 曲面 B 上取定的有限多个点. 之前我们已经构造了 Monodromy 表示 $\rho_{\mathcal{P}}:\pi_1(B\setminus\mathcal{P})\to\mathrm{GL}(2g,\mathbb{Z})$，mod ℓ^n 之后得到 $\pi_1(B\setminus\mathcal{P})\to\mathrm{GL}(2g,\mathbb{Z}/\ell^n\mathbb{Z})$. 再取反向极限有 $\widehat{\rho}_\ell:\mathrm{Gal}\big(\overline{\mathcal{M}_B^{\mathcal{P}}}/\mathcal{M}_B\big)\to\mathrm{GL}(2g,\mathbb{Z}_\ell)$，这是一个 ℓ-进 Galois 表示.

12、有限 Femart 定理

本节将大致介绍下述定理的证明思路：

定理 12.1(Faltings) 方程 $X^n+Y^n=Z^n, (X,Y,Z)=1$ 在 $n\geq 4$ 时仅有有限多组整数解.

证明 我们首先证明几何 Shafarevich 猜想的算术版本，**算术 Shafarevich 刚性定理**：设 K 是数域，S 是 K 的若干素点作成的有限集. 给定 $g\geq 2$，则定义在 K 上，亏格为 g 且在 S 之外的素点处是好约化的曲线 C 仅有有限多个.

仅证 $K=\mathbb{Q}$ 的情形，约定素数 $\ell\in S$. 考虑由 Monodromy 表示得到的 ℓ-进 Galois 表示 $\widehat{\rho}_\ell:\mathrm{Gal}(\overline{\mathbb{Q}^S}/\mathbb{Q})\to \mathrm{GL}(2g,\mathbb{Q}_\ell)$. 对任意 $p\notin S$，取 Frobenius 生成元 $[\sigma_p: x\mapsto x^p]\in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)\cong\widehat{\mathbb{Z}}$ 在映射 $D_{\mathfrak{p}|p}:=\{\sigma:\sigma\mathfrak{p}=\mathfrak{p}\}\longrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p), \sigma\longmapsto[x+\mathfrak{p}\mapsto\sigma(x)+\mathfrak{p}]$ 下的一个原像，即 $\mathrm{Gal}(\overline{\mathbb{Q}^S}/\mathbb{Q})$ 中的一个元素，它所在的共轭类由 p 唯一确定，因此**迹**$\mathrm{Tr}(\sigma_p)=\mathrm{Tr}(\widehat{\rho}_\ell(\sigma_p))$ 对素数 p 良好定义. 我们的证明思路是断言固定 S,g 之后 $\widehat{\rho}_\ell$ 仅有有限多个 (Step2-Step4)，并且每一个这样的 Galois 表示 $\widehat{\rho}_\ell$ 都仅有有限多个 Abel 簇 $A/\mathbb{Q}$ 与之对应 (Step5-Step7)，加之由 Abel 簇 $A=\mathrm{Jac}(C)$ 确定的曲线 C 仅有有限多个 (Step8)，从而证明算术 Shafarevich 刚性定理并得到推论：亏格 $g\geq 2$(即 $n\geq 4$) 的光滑曲线 $C/\mathbb{Q}$ 只有有限多个有理点 (Step1,Step9)，而这蕴含定理 12.1.

Step1：(Parshin 引理，函数域情形)给定 Riemann 曲面 B(从一个紧 Riemann 曲面挖去有限多个点得到) 以及 $g\geq 1$，则存在 $h\geq 2$ 以及映射

$$\Phi:\frac{\{(C/B,s):C/B\text{是纤维亏格为}g\text{的族，}s:B\to C\text{是}C/B\text{的一个全纯截面}\}}{(C/B,s)\sim(C'/B,s')\text{当且仅当存在同构}i,i(s)=s'\text{且满足下述交换图}}\longrightarrow\{\text{纤维亏格为}h\text{的族}D/B\},$$

$$\begin{array}{ccc} C & \xrightarrow[\sim]{i} & C' \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi'} & \\ & B & \end{array}$$

使得 $\Phi^{-1}(\Phi(C/B,s))$ 均是有限集，且对任意 $t\in B$，$D_t\to C_t$ 是只有一个分歧点 $s(t)\in C_t$ 的分歧复叠. **证：**给定 D/B，它可视作在 $s(t)$ 处分歧的复叠映射 $D_t\to C_t, t\in B$ 作成的族. 此时 C/B 即 D/B 关于 $\mathrm{Deck}(D/B)$ 的某个子群的商空间，而截面 $s(B)\subseteq C$ 是 $\mathrm{Deck}(D/B)$ 中某个元素的不动点集. 详细证明见 [16] 定理 4.1.

考虑由方程 $X^n+Y^n=Z^n$ 定义的“族 (曲线)” $C/\mathrm{Spec}(S^{-1}\mathbb{Z})$，显然方程的一个整数解 mod p 之后确定了该族的一个截面. 由于曲线 C 在 S 之外的素点处好约化，所以 $C/\mathrm{Spec}(S^{-1}\mathbb{Z})$ 的纤维是定义在 $\mathbb{F}_p$ 上的光滑曲线 $C_p:=\mathrm{Spec}(\mathbb{F}_p)\times_{\mathrm{Spec}(S^{-1}\mathbb{Z})}C$. 而 11 节的相应内容告诉我们 $\mathrm{Gal}(\overline{\mathbb{Q}^S}/\mathbb{Q})\cong\pi_1^{\mathrm{et}}(\mathrm{Spec}(S^{-1}\mathbb{Z}))\big($我们可以把 $p\notin S$ 看成 $\mathrm{Spec}(\mathbb{Z})\setminus S$ 中的道路，或 S^3 上的扭结，把 σ_p 看成它在 $\pi_1^{\mathrm{et}}(\mathrm{Spec}(S^{-1}\mathbb{Z}))$ 中对应的元素. 在这种观点下，类域论类似于研究 S^3 分歧复叠的同调，而 Iwasawa 理论类似于研究素数的 Alexander 多项式. 这种观点来自于 Kapranov-Reznikov-Mazur 扭结字典，详见网站 http://www.neverendingbooks.org/mazurs-dictionary 和 [41]$\big)$，故本质上我们需要研究 Monodromy 表示. 换句话说，Faltings 定理相当于是 Parshin 引理的算术版本.

Step2：(Monodromy 表示的半单性)表示 $\widehat{\rho}_\ell$ 是一些不可约表示的直和，并且在共轭的意义下 $\widehat{\rho}_\ell$ 由函数 $\mathrm{Tr}(\widehat{\rho}_\ell(\cdot)):p\mapsto\mathrm{Tr}(\widehat{\rho}_\ell(\sigma_p))$ 唯一确定. **证：**注意到 $\widehat{\rho}_\ell$ 来自于 Monodromy 表示 $\widetilde{f}_S\langle p\rangle:\pi_1^{\mathrm{et}}(\mathrm{Spec}(S^{-1}\mathbb{Z}),p)\to\mathrm{Mod}(C_p)$，因而 $\widehat{\rho}_\ell$ 的半单性由 $\widetilde{f}_S\langle p\rangle$ 给出. 由 Dehn-Lickorish 定理 ([25] 定理 4.1) 知映射类群由有限多个 Dehn 扭转 (阶为无穷) 生成，它们在 $\mathrm{Im}(\widetilde{f}_S\langle p\rangle)$ 作用下生成的子空间恰巧确定了 $\widehat{\rho}_\ell$ 所有可能的不可约子表示，并且 $\widehat{\rho}_\ell$ 也随 Dehn 扭转的迹确定.

Step3：(表示被有限个素数确定)更精细地，存在由素数作成的有限集 T，$T\cap S=\varnothing$，使得 $\mathrm{Tr}(\sigma_p), p\in T$ 就能确定 $\widehat{\rho}_\ell$. **证：**首先可以证明存在有限扩张 $K/\mathbb{Q}$(这里 K 依赖于 S,g)，在其上可以区分不同的表示. 根据 Hermite-Minkowski 定理，只有有限多个这样的扩张在 S 外非分歧，而 Čebotarev 定理告诉我们存在有限集 T 使得对每一个这样的 K，$\sigma_p, p\in T$ 确定了 $\mathrm{Gal}(K/\mathbb{Q})$ 中的每个共轭类. 这些 $\mathrm{Tr}(\sigma_p)$ 确定了 $\widehat{\rho}_\ell$.

Step4：(Weil 上界)对任意 $p\notin S$，$\mathrm{Tr}(\sigma_p)\in\mathbb{Z}$ 且存在仅与 p,g 有关的常数 N 使得 $|\mathrm{Tr}(\sigma_p)|\leq N$. **证：**由 Frobenius 元的 Lefschetz 不动点公式有 $|C(\mathbb{F}_p)|=1-\mathrm{Tr}(\sigma_p)+p$. 注意到有限域上的 Riemann-Roch 定理给出 $|C(\mathbb{F}_p)|<\infty$，因此断言成立.

Step5：($\widehat{\rho}_\ell$ 决定 Abel 簇)表示 $\widehat{\rho}_\ell$ 在同源的意义下确定了 Abel 簇 $A/\mathbb{Q}$. **证：**类似定理 11.2，底空间的

Monodromy 表示 (即 $\widehat{\rho}_\ell$) 决定有限多个 Abel 簇. 此外易见两个同源的 Abel 簇对应的 ℓ-进 Galois 表示一致.

Step6：(与 A 同源的 Abel 簇高度有界)给定 Abel 簇 $A/\mathbb{Q}$，则 $\{h_{\mathrm{F}}(B) : B与A同源\}$ 有界，这里 h_{F} 指 Faltings 高度. **证：**以 $A=\mathbb{C}^g/\Lambda$ 为例，则 $h_{\mathrm{F}}(A):=-\frac{1}{2}\ln\left(\frac{1}{2^g}\int_{A(\mathbb{C})}|\theta_A|^2\right)$，这里 θ_A 是某个 g-形式. 若有同源 $f:A\to B$，则可以证明 $\int_{A(\mathbb{C})}|f^*(\theta_B)|^2=[\mathbb{Z}\theta_A:f^*(\mathbb{Z}\theta_B)]^2\cdot\int_{B(\mathbb{C})}|\theta_B|^2$，因此 $h_{\mathrm{F}}(A)=h_{\mathrm{F}}(B)$. 但一般来讲仅可以证明高度有界，详见 [40] 定理 4.1.6.

Step7：(高度有界的 Abel 簇只有有限多个)给定 $C>0$，则集合 $\{A : A/\mathbb{Q}是\ \text{Abel}\ 簇且h_{\mathrm{F}}(A)\le C\}$ 有限. **证：**定义初始 Faltings 高度函数 $\widetilde{h}_{\mathrm{F}}(A):=\ln\max\{|p_1|,|q_1|,\cdots,|p_n|,|q_n|\}$，其中 $\frac{p_i}{q_i},1\le i\le n$ 是出现在定义 A 的某个合适方程中的有理系数，它可被 Faltings 高度 h_{F} 控制. 以椭圆曲线 $A/\mathbb{Q}:y^2=x(x-1)(x-\frac{p}{q}),0<\frac{p}{q}<\frac{1}{2}$ 为例，此时 $\widetilde{h}_{\mathrm{F}}(A)=\ln q$，$\theta_A=\frac{dy}{x(x-1)(qx-p)}$. 根据计算可得 $\int_{A(\mathbb{C})}|\theta_A|^2=2\int_{\mathbb{C}}\frac{|dx|^2}{|x(x-1)(qx-p)|}\sim\frac{\ln q}{q^2}$，这意味着给定 h_{F} 的界就能控制 A 的个数.

Step8：(极化，Polarization)由 Abel 簇 $A/\mathbb{Q}$ 通过 $A=\mathrm{Jac}(C)$ 确定的曲线 C 仅有有限多个. **证：**证明思路是研究相交形式 $\omega:H_1(A,\mathbb{Z})^2\cong H_1(C,\mathbb{Z})^2\to\mathbb{Z}$，Torelli 定理告诉我们 C 被二元对 (A,ω) 决定. 更详细的论证则需要分析 $\mathrm{Aut}(A)$ 在所有相交形式作成的集合上的作用，详见 [16].

Step9：(有理点有限，算术 Mordell 猜想)设 C 是定义在数域 K 上亏格 $g\ge 2$ 的光滑曲线，则 C 仅有有限多个 K-点. **证：**由算术 Shafarevich 刚性定理和 Step1 的算术版本立得.■