数论中的局部与整体

梁 永祺

中国科学技术大学

Introduction

引言

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），一元二次方程（求根公式），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），一元二次方程（求根公式），一元三、四次方程（也有求根公式，16世纪，Cardano和Ferrari），

数学的中心问题

- 数学的中心问题是什么?
- 解方程!
- 来源于物理的偏微分方程，例：流体力学的 Navier-Stokes 方程（Clay数学所的千禧年七大数学问题之一）
- 来源于数学本身的方程：代数方程
- 例：一元一次方程，多元一次方程（线性代数：Gauss消去法），一元二次方程（求根公式），一元三、四次方程（也有求根公式，16世纪，Cardano和Ferrari），一元高次方程（19世纪，Galois：不存在求根公式，通过群论来研究域扩张：某个域扩张的Galois群不是可解群）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

什么是算术代数几何?

- 数论：研究整数的理论
- $\mathbb{Z}$：每个整数都是素数的乘积
- $\mathbb{Q} = Frac(\mathbb{Z})$ 以及它的有限扩张
- 代数几何：研究代数簇的理论
- 即（多元多次）多项式方程组所定义的几何对象（“代数的流形”称作代数簇，可以定义在任何域上，多项式的系数可以在$\mathbb{Q}$中取值，不仅仅是$\mathbb{R}$和$\mathbb{C}$）
- 算术代数几何：介于数论和代数几何之间
- 研究多项式方程组的整数解、有理数解（或更一般的在数域上的解）

丢番图方程

- 整系数多项式方程求整数解称为Diophantine方程
- Hilbert第十问题（1900s）：是否存在一种由有限步构成的一般算法来判断一个 Diophantine方程 是否可解?
- 否定的解决：1970s, Yuri Matiyasevic 不存在这样的算法。
- 仅仅是判断有没有解就很难，更不用说求解！
- 我们今天只关注在有理数里求解
- 已经非常困难，但是有一套非常有启发性的办法：可以从中看出数学家们是怎么一步一步去逼近这个问题

丢番图方程

- 整系数多项式方程求整数解称为Diophantine方程
- Hilbert第十问题（1900s）：是否存在一种由有限步构成的一般算法来判断一个 Diophantine方程 是否可解?
- 否定的解决：1970s, Yuri Matiyasevic 不存在这样的算法。
- 仅仅是判断有没有解就很难，更不用说求解！
- 我们今天只关注在有理数里求解
- 已经非常困难，但是有一套非常有启发性的办法：可以从中看出数学家们是怎么一步一步去逼近这个问题

丢番图方程

- 整系数多项式方程求整数解称为Diophantine方程
- Hilbert第十问题（1900s）：是否存在一种由有限步构成的一般算法来判断一个 Diophantine方程 是否可解?
- 否定的解决：1970s, Yuri Matiyasevic 不存在这样的算法。
- 仅仅是判断有没有解就很难，更不用说求解！
- 我们今天只关注在有理数里求解
- 已经非常困难，但是有一套非常有启发性的办法：可以从中看出数学家们是怎么一步一步去逼近这个问题

丢番图方程

- 整系数多项式方程求整数解称为Diophantine方程
- Hilbert第十问题（1900s）：是否存在一种由有限步构成的一般算法来判断一个 Diophantine方程 是否可解?
- 否定的解决：1970s, Yuri Matiyasevic 不存在这样的算法。
- 仅仅是判断有没有解就很难，更不用说求解！
- 我们今天只关注在有理数里求解
- 已经非常困难，但是有一套非常有启发性的办法：可以从中看出数学家们是怎么一步一步去逼近这个问题

丢番图方程

- 整系数多项式方程求整数解称为Diophantine方程
- Hilbert第十问题（1900s）：是否存在一种由有限步构成的一般算法来判断一个 Diophantine方程 是否可解?
- 否定的解决：1970s, Yuri Matiyasevic 不存在这样的算法。
- 仅仅是判断有没有解就很难，更不用说求解！
- 我们今天只关注在有理数里求解
- 已经非常困难，但是有一套非常有启发性的办法：可以从中看出数学家们是怎么一步一步去逼近这个问题

丢番图方程

- 整系数多项式方程求整数解称为Diophantine方程
- Hilbert第十问题（1900s）：是否存在一种由有限步构成的一般算法来判断一个 Diophantine方程 是否可解?
- 否定的解决：1970s, Yuri Matiyasevic 不存在这样的算法。
- 仅仅是判断有没有解就很难，更不用说求解！
- 我们今天只关注在有理数里求解
- 已经非常困难，但是有一套非常有启发性的办法：可以从中看出数学家们是怎么一步一步去逼近这个问题

Global study

整体研究

历史上非常著名的几个例子

- 哲学：几何决定算术！
- 对象：（光滑）代数簇 = 多项式方程组（系数在$\mathbb{Q}$中）
- 算术性质：有没有有理数解，有多少解?
- 几何性质：复数解构成一个复流形——经典的几何对象
- 例子：1维复流形 = 复曲线 = 代数曲线 = 黎曼曲面

历史上非常著名的几个例子

- 哲学：几何决定算术！
- 对象：（光滑）代数簇 = 多项式方程组（系数在$\mathbb{Q}$中）
- 算术性质：有没有有理数解，有多少解?
- 几何性质：复数解构成一个复流形——经典的几何对象
- 例子：1维复流形 = 复曲线 = 代数曲线 = 黎曼曲面

历史上非常著名的几个例子

- 哲学：几何决定算术！
- 对象：（光滑）代数簇 = 多项式方程组（系数在$\mathbb{Q}$中）
- 算术性质：有没有有理数解，有多少解?
- 几何性质：复数解构成一个复流形——经典的几何对象
- 例子：1维复流形 = 复曲线 = 代数曲线 = 黎曼曲面

历史上非常著名的几个例子

- 哲学：几何决定算术！
- 对象：（光滑）代数簇 = 多项式方程组（系数在$\mathbb{Q}$中）
- 算术性质：有没有有理数解，有多少解?
- 几何性质：复数解构成一个复流形——经典的几何对象
- 例子：1维复流形 = 复曲线 = 代数曲线 = 黎曼曲面

历史上非常著名的几个例子

- 哲学：几何决定算术！
- 对象：（光滑）代数簇 = 多项式方程组（系数在$\mathbb{Q}$中）
- 算术性质：有没有有理数解，有多少解?
- 几何性质：复数解构成一个复流形——经典的几何对象
- 例子：1维复流形 = 复曲线 = 代数曲线 = 黎曼曲面

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。它们是由圆锥和平面相交得出来的：上文提到的限制就是要求平面不要通过锥的顶点（那时正好交出一对相交直线）
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。它们是由圆锥和平面相交得出来的：上文提到的限制就是要求平面不要通过锥的顶点（那时正好交出一对相交直线）
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。它们是由圆锥和平面相交得出来的：上文提到的限制就是要求平面不要通过锥的顶点（那时正好交出一对相交直线）
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！

几何不变量：射影曲线（紧黎曼面）的亏格

- 考虑复射影平面$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}\times\mathbb{C}\times\mathbb{C}\setminus\{(0,0,0)\})/\sim$ 中由一个齐次（d次）多项式方程$P(x,y,z)=0$定义的(平面)曲线C
- 对多项式作某些限制后对应的曲线C是光滑曲线（= 紧黎曼曲面）

Definition

$g(C)=\frac{1}{2}(d-1)(d-2)$ 称为平面曲线C的亏格。

- 例：2次曲线（又称圆锥曲线：圆、椭圆、抛物线、双曲线）亏格为0。它们是由圆锥和平面相交得出来的：上文提到的限制就是要求平面不要通过锥的顶点（那时正好交出一对相交直线）
- 这个定义是个好的数学概念/数学定义吗?
- 答：不好！ 为什么不好?

几何不变量：射影曲线（紧黎曼面）的亏格

- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} H^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数

几何不变量：射影曲线（紧黎曼面）的亏格

- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} H^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数

几何不变量：射影曲线（紧黎曼面）的亏格

- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} H^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数

几何不变量：射影曲线（紧黎曼面）的亏格

- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} H^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数

几何不变量：射影曲线（紧黎曼面）的亏格

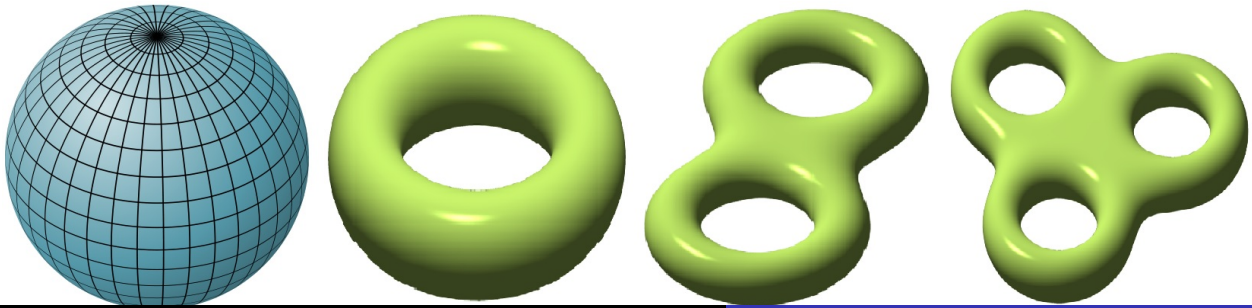
- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} \mathrm{H}^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数

几何不变量：射影曲线（紧黎曼面）的亏格

- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} \mathrm{H}^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数

几何不变量：射影曲线（紧黎曼面）的亏格

- 先验地（即未经证明论证之前），两条“同构”的曲线也许会由不同的多项式来定义，但没有任何理由认为这两个多项式的次数应该是一样的。做个坐标变换，方程就变了，但曲线本身没变，那个方程只是一个表象而不是本质。
- 几何上称这不是 内蕴 的
- 内蕴：应该从曲线自身出发来给定义，而不是从外部的表象（曲线的方程）
- 好的定义：提取曲线在同构下的不变量，例如某些同调群
- 亏格$g(C) = \dim_{\mathbb{C}} H^1(X, \mathcal{O}_X)$
- 内蕴的量才是好的不变量，亏格可以用于分类光滑射影曲线
- 直观的讲就是黎曼曲面上洞的个数



算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

算术性质

- 复数域 $\mathbb{C}$ 的算术性质是平凡的：所有多项式方程都有解。我们只关心复流形的几何性质。
- 算术性质要考虑不是代数封闭的域，例如 $\mathbb{Q}$
- 考虑两曲线 $C_1 : x^2 + y^2 = -1$ 和 $C_2 : XY = -1$
- 它们的几何性质是一样的：它们在 $\mathbb{C}$ 上是同构的（复流形双全纯等价）
- （线性可逆）变量替换：$X = x + \sqrt{-1}y$，$Y = x - \sqrt{-1}y$
- 但它们算术性质差很远：C_1 没有有理数解；C_2 有很多有理数解
- 说好的几何决定算术呢?

亏格0

Theorem

令C为亏格0的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 与 $\mathbb{P}^1$ 的有理点（即$\mathbb{Q} \cup \{\infty\}$）有一个自然的一一对应。

- 其中，有理点就是指定义曲线的多项式方程在$\mathbb{Q}$中的解
- 证明用到一个精彩的几何定理

Theorem (Bézout)

复射影平面中次数分别为 m 和 n 的两条曲线相交于 mn 个交点。

- 必须是复的，否则可能无交点（圆与直线）
- 必须是射影平面中，否则可能相交在无穷远处（平行线）
- 计算个数时要算重数：例如二重点算两个（切线）

亏格0

Theorem

令C为亏格0的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 与 $\mathbb{P}^1$ 的有理点（即$\mathbb{Q} \cup \{\infty\}$）有一个自然的一一对应。

- 其中，有理点就是指定义曲线的多项式方程在$\mathbb{Q}$中的解
- 证明用到一个精彩的几何定理

Theorem (Bézout)

复射影平面中次数分别为 m 和 n 的两条曲线相交于 mn 个交点。

- 必须是复的，否则可能无交点（圆与直线）
- 必须是射影平面中，否则可能相交在无穷远处（平行线）
- 计算个数时要算重数：例如二重点算两个（切线）

亏格0

Theorem

令C为亏格0的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 与 $\mathbb{P}^1$ 的有理点（即$\mathbb{Q} \cup \{\infty\}$）有一个自然的一一对应。

- 其中，有理点就是指定义曲线的多项式方程在$\mathbb{Q}$中的解
- 证明用到一个精彩的几何定理

Theorem (Bézout)

复射影平面中次数分别为 m 和 n 的两条曲线相交于 mn 个交点。

- 必须是复的，否则可能无交点（圆与直线）
- 必须是射影平面中，否则可能相交在无穷远处（平行线）
- 计算个数时要算重数：例如二重点算两个（切线）

亏格0

Theorem

令C为亏格0的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 与 $\mathbb{P}^1$ 的有理点（即$\mathbb{Q} \cup \{\infty\}$）有一个自然的一一对应。

- 其中，有理点就是指定义曲线的多项式方程在$\mathbb{Q}$中的解
- 证明用到一个精彩的几何定理

Theorem (Bézout)

复射影平面中次数分别为 m 和 n 的两条曲线相交于 mn 个交点。

- 必须是复的，否则可能无交点（圆与直线）
- 必须是射影平面中，否则可能相交在无穷远处（平行线）
- 计算个数时要算重数：例如二重点算两个（切线）

亏格0

Theorem

令C为亏格0的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 与 $\mathbb{P}^1$ 的有理点（即$\mathbb{Q} \cup \{\infty\}$）有一个自然的一一对应。

- 其中，有理点就是指定义曲线的多项式方程在$\mathbb{Q}$中的解
- 证明用到一个精彩的几何定理

Theorem (Bézout)

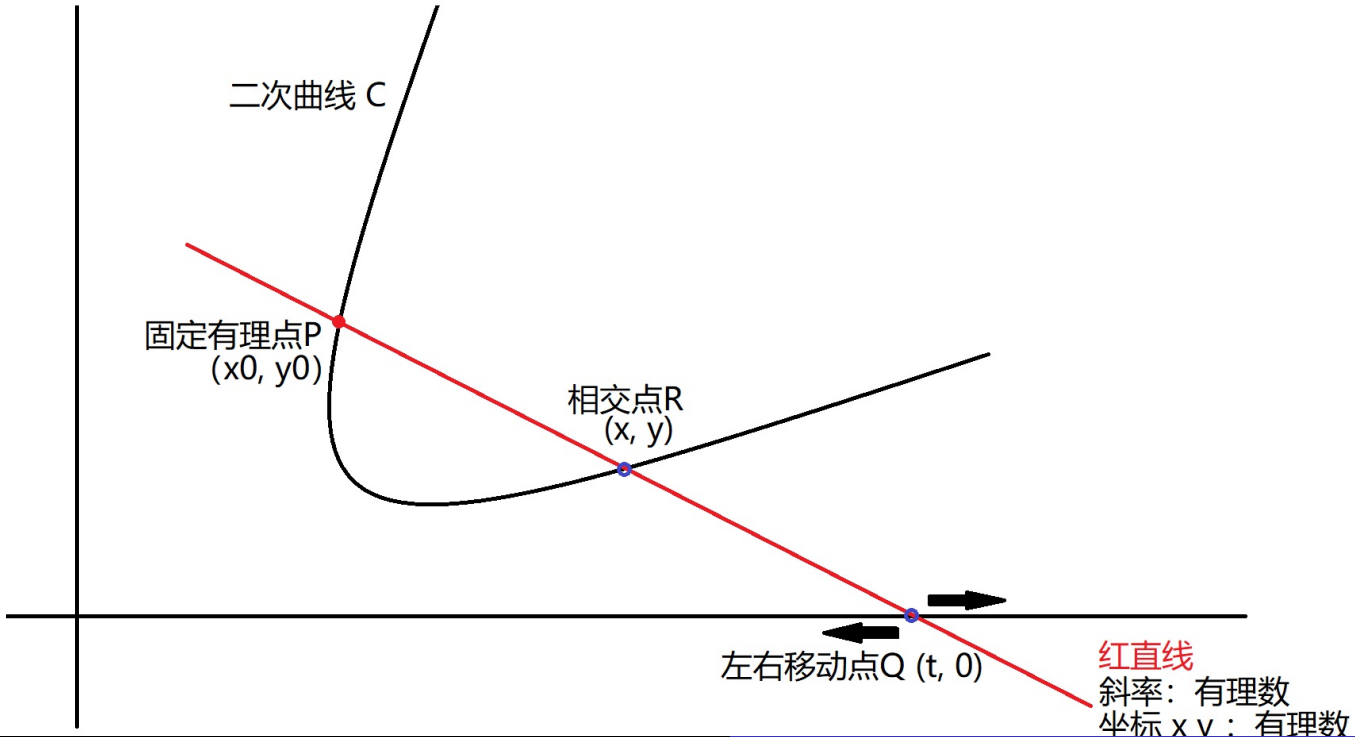
复射影平面中次数分别为 m 和 n 的两条曲线相交于 mn 个交点。

- 必须是复的，否则可能无交点（圆与直线）
- 必须是射影平面中，否则可能相交在无穷远处（平行线）
- 计算个数时要算重数：例如二重点算两个（切线）

亏格0

Theorem

令C为亏格0的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 与 $\mathbb{P}^1$ 的有理点（即$\mathbb{Q} \cup \{\infty\}$）有一个自然的一一对应。



亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的亚纯函数域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$
- 3次曲线，亏格为1
- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的函数亚纯域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$

亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的亚纯函数域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$
- 3次曲线，亏格为1
- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的函数亚纯域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$

亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的亚纯函数域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$
- 3次曲线，亏格为1
- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的函数亚纯域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$

亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的亚纯函数域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$
- 3次曲线，亏格为1

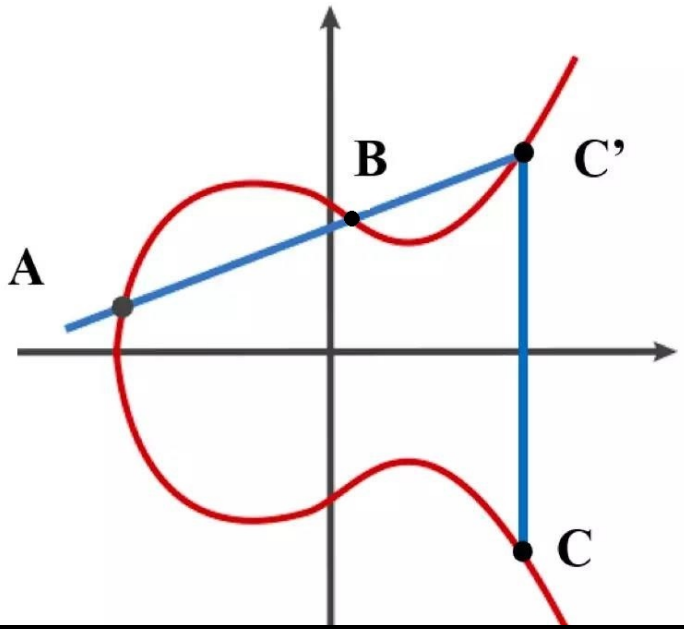
- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的函数亚纯域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$

亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Abel群结构。加法：$A+B=C$，逆元：$C'=-C$，零元：无穷远点$(0:1:0)\in\mathbb{P}^2$



亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的函数亚纯域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$
- 3次曲线，亏格为1
- Abel群结构。
- 有限生成Abel群的结构定理：$C(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus F$ （其中F是有限交换群）可为有限可为无限。
- $r = \mathrm{rank}(E)$ 称为秩

亏格1

Theorem (Mordell-Weil)

令C为亏格1的射影曲线。如果C至少有一个有理点，那么它的有理点的集合 $C(\mathbb{Q})$ 是一个有限生成的阿贝尔群。

- Mordell：$\mathbb{Q}$，Weil：一般数域（即$\mathbb{Q}$的有限扩张）
- 称C为椭圆曲线（跟椭圆没有直接关系；间接关系：求椭圆周长的积分称为椭圆函数，是椭圆曲线上的函数亚纯域中的元素）
- Weierstrass方程：$y^2 = x^3 + ax + b$, $\Delta = 4a^3 + 27b^2 \neq 0$
- 3次曲线，亏格为1
- Abel群结构。
- 有限生成Abel群的结构定理：$C(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus F$ （其中F是有限交换群）可为有限可为无限。
- $r = \mathrm{rank}(E)$ 称为秩

Birch–Swinnerton-Dyer猜想

- BSD猜想（Clay数学所的七大千禧年问题）

Conjecture

$\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E, s)$

- 左边是一个代数量
- 右边L函数是个全纯复变函数，在$s = 1$处零点的重数是一个来源于分析的量
- 先验地，$L(E, s)$是通过一个无穷乘积（每个素数对应一项：“局部”分量）定义出来的复“解析函数”（乘积仅仅在复平面右半部收敛）
- 全纯性的证明极其不平凡：1990s，Wiles，Wiles-Taylor证明Fermat大定理的关键一步

Birch–Swinnerton-Dyer猜想

- BSD猜想（Clay数学所的七大千禧年问题）

Conjecture

$\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E, s)$

- 左边是一个代数量
- 右边L函数是个全纯复变函数，在$s = 1$处零点的重数是一个来源于分析的量
- 先验地，$L(E, s)$是通过一个无穷乘积（每个素数对应一项：“局部”分量）定义出来的复“解析函数”（乘积仅仅在复平面右半部收敛）
- 全纯性的证明极其不平凡：1990s，Wiles，Wiles-Taylor证明Fermat大定理的关键一步

Birch–Swinnerton-Dyer猜想

- BSD猜想（Clay数学所的七大千禧年问题）

Conjecture

$\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E, s)$

- 左边是一个代数量
- 右边L函数是个全纯复变函数，在$s = 1$处零点的重数是一个来源于分析的量
- 先验地，$L(E, s)$是通过一个无穷乘积（每个素数对应一项：“局部”分量）定义出来的复“解析函数”（乘积仅仅在复平面右半部收敛）
- 全纯性的证明极其不平凡：1990s，Wiles，Wiles-Taylor证明Fermat大定理的关键一步

Birch–Swinnerton-Dyer猜想

- BSD猜想（Clay数学所的七大千禧年问题）

Conjecture

$\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E, s)$

- 左边是一个代数量
- 右边L函数是个全纯复变函数，在$s = 1$处零点的重数是一个来源于分析的量
- 先验地，$L(E, s)$是通过一个无穷乘积（每个素数对应一项：“局部”分量）定义出来的复“解析函数”（乘积仅仅在复平面右半部收敛）
- 全纯性的证明极其不平凡：1990s，Wiles，Wiles-Taylor证明Fermat大定理的关键一步

Birch–Swinnerton-Dyer猜想

- BSD猜想（Clay数学所的七大千禧年问题）

Conjecture

$\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E, s)$

- 左边是一个代数量
- 右边L函数是个全纯复变函数，在$s = 1$处零点的重数是一个来源于分析的量
- 先验地，$L(E, s)$是通过一个无穷乘积（每个素数对应一项：“局部”分量）定义出来的复“解析函数”（乘积仅仅在复平面右半部收敛）
- 全纯性的证明极其不平凡：1990s，Wiles，Wiles-Taylor证明Fermat大定理的关键一步

高亏格

Theorem (Faltings，1980s)

令C为亏格≥ 2的射影曲线。那么 $C(\mathbb{Q})$ 是一个有限集。

- 把$\mathbb{Q}$换成一般数域也成立。
- 证明Faltings定理和Mordell-Weil定理关键：引入“高度”的概念（有理数约分成既约分数后，分子分母中绝对值较大的值）
- 高度用于衡量有理点的算术复杂性
- Faltings定理的例子：$C: x^n + y^n = z^n$
- 当$n \geq 4$时$g(C) \geq 2$，Faltings：这方程只有有限个有理解。

Theorem (Fermat's last theorem. Wiles，1990s)

当$n \geq 3$时，方程$x^n + y^n = z^n$没有非平凡有理数（整数）解。

高亏格

Theorem (Faltings，1980s)

令C为亏格≥ 2的射影曲线。那么 $C(\mathbb{Q})$ 是一个有限集。

- 把$\mathbb{Q}$换成一般数域也成立。
- 证明Faltings定理和Mordell-Weil定理关键：引入“高度”的概念（有理数约分成既约分数后，分子分母中绝对值较大的值）
- 高度用于衡量有理点的算术复杂性
- Faltings定理的例子：$C: x^n + y^n = z^n$
- 当$n \geq 4$时$g(C) \geq 2$，Faltings：这方程只有有限个有理解。

Theorem (Fermat's last theorem. Wiles，1990s)

当$n \geq 3$时，方程$x^n + y^n = z^n$没有非平凡有理数（整数）解。

高亏格

Theorem (Faltings，1980s)

令C为亏格≥ 2的射影曲线。那么 $C(\mathbb{Q})$ 是一个有限集。

- 把$\mathbb{Q}$换成一般数域也成立。
- 证明Faltings定理和Mordell-Weil定理关键：引入“高度”的概念（有理数约分成既约分数后，分子分母中绝对值较大的值）
- 高度用于衡量有理点的算术复杂性
- Faltings定理的例子：$C: x^n + y^n = z^n$
- 当$n \geq 4$时$g(C) \geq 2$，Faltings：这方程只有有限个有理解。

Theorem (Fermat's last theorem. Wiles，1990s)

当$n \geq 3$时，方程$x^n + y^n = z^n$没有非平凡有理数（整数）解。

高亏格

Theorem (Faltings，1980s)

令C为亏格≥ 2的射影曲线。那么 $C(\mathbb{Q})$ 是一个有限集。

- 把$\mathbb{Q}$换成一般数域也成立。
- 证明Faltings定理和Mordell-Weil定理关键：引入“高度”的概念（有理数约分成既约分数后，分子分母中绝对值较大的值）
- 高度用于衡量有理点的算术复杂性
- Faltings定理的例子：$C : x^n + y^n = z^n$
- 当$n \geq 4$时$g(C) \geq 2$，Faltings：这方程只有有限个有理解。

Theorem (Fermat's last theorem. Wiles，1990s)

当$n \geq 3$时，方程$x^n + y^n = z^n$没有非平凡有理数（整数）解。

高亏格

Theorem (Faltings，1980s)

令C为亏格≥ 2的射影曲线。那么 $C(\mathbb{Q})$ 是一个有限集。

- 把$\mathbb{Q}$换成一般数域也成立。
- 证明Faltings定理和Mordell-Weil定理关键：引入“高度”的概念（有理数约分成既约分数后，分子分母中绝对值较大的值）
- 高度用于衡量有理点的算术复杂性
- Faltings定理的例子：$C : x^n + y^n = z^n$
- 当$n \geq 4$时$g(C) \geq 2$，Faltings：这方程只有有限个有理解。

Theorem (Fermat's last theorem. Wiles，1990s)

当$n \geq 3$时，方程$x^n + y^n = z^n$没有非平凡有理数（整数）解。

高亏格

Theorem (Faltings，1980s)

令C为亏格≥ 2的射影曲线。那么 $C(\mathbb{Q})$ 是一个有限集。

- 把$\mathbb{Q}$换成一般数域也成立。
- 证明Faltings定理和Mordell-Weil定理关键：引入“高度”的概念（有理数约分成既约分数后，分子分母中绝对值较大的值）
- 高度用于衡量有理点的算术复杂性
- Faltings定理的例子：$C: x^n + y^n = z^n$
- 当$n \geq 4$时$g(C) \geq 2$，Faltings：这方程只有有限个有理解。

Theorem (Fermat's last theorem. Wiles，1990s)

当$n \geq 3$时，方程$x^n + y^n = z^n$没有非平凡有理数（整数）解。

几何决定算术

- 曲线情形：几何不变量 $\Longrightarrow$ 算术性质
- 亏格0且存在有理点 $\Longrightarrow$ 无穷个有理点
- 亏格1且存在有理点 $\Longrightarrow$ 有理点组成有限生成的Abel群
- 亏格≥ 2（且存在有理点） $\Longrightarrow$ 有限个有理点

几何决定算术

- 曲线情形：几何不变量 $\Longrightarrow$ 算术性质
- 亏格0且存在有理点 $\Longrightarrow$ 无穷个有理点
- 亏格1且存在有理点 $\Longrightarrow$ 有理点组成有限生成的Abel群
- 亏格≥ 2（且存在有理点） $\Longrightarrow$ 有限个有理点

几何决定算术

- 曲线情形：几何不变量 $\Longrightarrow$ 算术性质
- 亏格0且存在有理点 $\Longrightarrow$ 无穷个有理点
- 亏格1且存在有理点 $\Longrightarrow$ 有理点组成有限生成的Abel群
- 亏格≥ 2（且存在有理点） $\Longrightarrow$ 有限个有理点

几何决定算术

- 曲线情形：几何不变量 $\Longrightarrow$ 算术性质
- 亏格0且存在有理点 $\Longrightarrow$ 无穷个有理点
- 亏格1且存在有理点 $\Longrightarrow$ 有理点组成有限生成的Abel群
- 亏格≥ 2（且存在有理点） $\Longrightarrow$ 有限个有理点

Local World

局部世界

代数数论：有理数域与一般数域

- 数域$K = \mathbb{Q}$的有限扩张
- 相似：$\mathbb{Q} = Frac(\mathbb{Z})$，$K = Frac(\mathcal{O}_K)$ 其中$\mathcal{O}_K$称为代数整数环
- 区别：$\mathbb{Z}$中整数可以唯一分解为素数的乘积
- $\mathcal{O}_K$中代数整数分解为不可约元的乘积不唯一
- 例：在$K = \mathbb{Q}(\sqrt{-5})$，$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$中，
$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 经典代数数论的解决办法：不考虑数的分解，而考虑环（Dedekind整环）的理想的素分解
- 以下的为表述方便只讨论$\mathbb{Q}$，换成一般数域也都成立（要把素数换成素理想）

代数数论：有理数域与一般数域

- 数域$K = \mathbb{Q}$的有限扩张
- 相似：$\mathbb{Q} = Frac(\mathbb{Z})$，$K = Frac(\mathcal{O}_K)$ 其中$\mathcal{O}_K$称为代数整数环
- 区别：$\mathbb{Z}$中整数可以唯一分解为素数的乘积
- $\mathcal{O}_K$中代数整数分解为不可约元的乘积不唯一
- 例：在$K = \mathbb{Q}(\sqrt{-5})$，$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$中，$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 经典代数数论的解决办法：不考虑数的分解，而考虑环（Dedekind整环）的理想的素分解
- 以下的为表述方便只讨论$\mathbb{Q}$，换成一般数域也都成立（要把素数换成素理想）

代数数论：有理数域与一般数域

- 数域$K = \mathbb{Q}$的有限扩张
- 相似：$\mathbb{Q} = Frac(\mathbb{Z})$，$K = Frac(\mathcal{O}_K)$ 其中$\mathcal{O}_K$称为代数整数环
- 区别：$\mathbb{Z}$中整数可以唯一分解为素数的乘积
- $\mathcal{O}_K$中代数整数分解为不可约元的乘积不唯一
- 例：在$K = \mathbb{Q}(\sqrt{-5})$，$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$中，$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 经典代数数论的解决办法：不考虑数的分解，而考虑环（Dedekind整环）的理想的素分解
- 以下的为表述方便只讨论$\mathbb{Q}$，换成一般数域也都成立（要把素数换成素理想）

代数数论：有理数域与一般数域

- 数域$K = \mathbb{Q}$的有限扩张
- 相似：$\mathbb{Q} = Frac(\mathbb{Z})$，$K = Frac(\mathcal{O}_K)$ 其中$\mathcal{O}_K$称为代数整数环
- 区别：$\mathbb{Z}$中整数可以唯一分解为素数的乘积
- $\mathcal{O}_K$中代数整数分解为不可约元的乘积不唯一
- 例：在$K = \mathbb{Q}(\sqrt{-5})$，$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$中，
  $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 经典代数数论的解决办法：不考虑数的分解，而考虑环（Dedekind整环）的理想的素分解
- 以下的为表述方便只讨论$\mathbb{Q}$，换成一般数域也都成立（要把素数换成素理想）

代数数论：有理数域与一般数域

- 数域$K = \mathbb{Q}$的有限扩张
- 相似：$\mathbb{Q} = Frac(\mathbb{Z})$，$K = Frac(\mathcal{O}_K)$ 其中$\mathcal{O}_K$称为代数整数环
- 区别：$\mathbb{Z}$中整数可以唯一分解为素数的乘积
- $\mathcal{O}_K$中代数整数分解为不可约元的乘积不唯一
- 例：在$K = \mathbb{Q}(\sqrt{-5})$，$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$中，
  $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 经典代数数论的解决办法：不考虑数的分解，而考虑环（Dedekind整环）的理想的素分解
- 以下的为表述方便只讨论$\mathbb{Q}$，换成一般数域也都成立（要把素数换成素理想）

代数数论：有理数域与一般数域

- 数域$K = \mathbb{Q}$的有限扩张
- 相似：$\mathbb{Q} = Frac(\mathbb{Z})$，$K = Frac(\mathcal{O}_K)$ 其中$\mathcal{O}_K$称为代数整数环
- 区别：$\mathbb{Z}$中整数可以唯一分解为素数的乘积
- $\mathcal{O}_K$中代数整数分解为不可约元的乘积不唯一
- 例：在$K = \mathbb{Q}(\sqrt{-5})$，$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$中，
  $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 经典代数数论的解决办法：不考虑数的分解，而考虑环（Dedekind整环）的理想的素分解
- 以下的为表述方便只讨论$\mathbb{Q}$，换成一般数域也都成立（要把素数换成素理想）

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

如何在有理数中解方程

- 例：$x^2 + y^2 = -1$有有理数解吗？为什么？
- 没有！因为$\mathbb{Q} \subset \mathbb{R}$所以$X(\mathbb{R}) = \emptyset \implies X(\mathbb{Q}) = \emptyset$
- $\mathbb{R}$的好处：
  - 对求极限封闭：即可以运用分析工具
  - 离目标$\mathbb{Q}$不太遥远：有理数是稠密的
- 称$\mathbb{R}$是$\mathbb{Q}$的完备化
- $\mathbb{Q}$的其他的完备化？如果有，对研究有理点将很有帮助

完备化

- 回顾$\mathbb{Q}$完备化得到$\mathbb{R}$的过程：
- 在绝对值给出的距离之下：从$\mathbb{Q}$开始，加入所有Cauchy列，然后把收敛于相同极限的柯西列等同起来（即作一个等价关系再求商），得到$\mathbb{R}$
- 如果在$\mathbb{Q}$上能造出某种不一样的“绝对值”，那么同样的过程将得到不一样的完备化。

完备化

- 回顾$\mathbb{Q}$完备化得到$\mathbb{R}$的过程：
- 在绝对值给出的距离之下：从$\mathbb{Q}$开始，加入所有Cauchy列，然后把收敛于相同极限的柯西列等同起来（即作一个等价关系再求商），得到$\mathbb{R}$
- 如果在$\mathbb{Q}$上能造出某种不一样的“绝对值”，那么同样的过程将得到不一样的完备化。

完备化

- 回顾$\mathbb{Q}$完备化得到$\mathbb{R}$的过程:
- 在绝对值给出的距离之下：从$\mathbb{Q}$开始，加入所有Cauchy列，然后把收敛于相同极限的柯西列等同起来（即作一个等价关系再求商），得到$\mathbb{R}$
- 如果在$\mathbb{Q}$上能造出某种不一样的“绝对值”，那么同样的过程将得到不一样的完备化。

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0, |a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0, |a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0, |a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0, |a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0$, $|a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0$, $|a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 取定素数$p \in \mathbb{Z}$
- 对任意$n \in \mathbb{Z}$，若$p^r | n$但$p^{r+1} \nmid n$，则定义p-adic赋值$v_p(n) = r \in \mathbb{N}$。约定$v_p(0) = +\infty$。
- 自然地扩展到$\mathbb{Q}$：$v_p(\frac{m}{n}) = v_p(m) - v_p(n)$ 定义不依赖于分数表达式的选取
- p-adic绝对值：$\forall a \in \mathbb{Q}, |a|_p = (\frac{1}{p})^{v_p(a)}$
- 这是一个范数：
  - $|a|_p \geq 0$, $|a|_p = 0 \Leftrightarrow a = 0$
  - $|ab|_p = |a|_p \cdot |b|_p$
  - $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$（强三角不等式）

p-adic绝对值

- 最后一条$|a+b|_p \leq \max(|a|_p, |b|_p)$也称为非Archimedes性质，与实数很不一样
- $\mathbb{R}$具有 Archimedes性质：

$$\forall x \in \mathbb{R}, x > 0, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx > y$$

- 即$\mathbb{Q}$取$\mathbb{R}$诱导的传统绝对值时，nx的绝对值随着n的增大而增大
- 但在p-adic绝对值下可能出现$|nx|_p < |x|_p$的情形，例如$\frac{1}{p} = |p \cdot 1|_p < |1|_p = 1$

p-adic绝对值

- 最后一条$|a+b|_p \leq \max(|a|_p, |b|_p)$也称为非Archimedes性质，与实数很不一样
- $\mathbb{R}$具有 Archimedes性质：

$$\forall x \in \mathbb{R}, x > 0, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx > y$$

- 即$\mathbb{Q}$取$\mathbb{R}$诱导的传统绝对值时，nx的绝对值随着n的增大而增大
- 但在p-adic绝对值下可能出现$|nx|_p < |x|_p$的情形，例如$\frac{1}{p} = |p \cdot 1|_p < |1|_p = 1$

p-adic绝对值

- 最后一条$|a+b|_p \leq \max(|a|_p, |b|_p)$也称为非Archimedes性质，与实数很不一样
- $\mathbb{R}$具有 Archimedes性质：

$$\forall x \in \mathbb{R}, x > 0, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx > y$$

- 即$\mathbb{Q}$取$\mathbb{R}$诱导的传统绝对值时，nx的绝对值随着n的增大而增大
- 但在p-adic绝对值下可能出现$|nx|_p < |x|_p$的情形，例如$\frac{1}{p} = |p \cdot 1|_p < |1|_p = 1$

p-adic绝对值

- 最后一条$|a+b|_p \leq \max(|a|_p, |b|_p)$也称为非Archimedes性质，与实数很不一样
- $\mathbb{R}$具有 Archimedes性质：

$$\forall x \in \mathbb{R}, x > 0, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx > y$$

- 即$\mathbb{Q}$取$\mathbb{R}$诱导的传统绝对值时，nx的绝对值随着n的增大而增大
- 但在p-adic绝对值下可能出现$|nx|_p < |x|_p$的情形，例如$\frac{1}{p} = |p \cdot 1|_p < |1|_p = 1$

p-adic绝对值

- 例子：$p = 3$
  - （大）$n_1 = 36 = 3^2 \cdot 2^2, v_p(n_1) = 2, |n_1|_p = \frac{1}{9}$（中）
  - （中）$n_2 = 27 = 3^3, \quad v_p(n_2) = 3, |n_2|_p = \frac{1}{27}$（小）
  - （小）$n_3 = 3, \quad v_p(n_3) = 1, |n_3|_p = \frac{1}{3}$（大）
- 回顾两个范数等价是指存在非零常数c使得对任意x有

$$\frac{1}{c}||x||_1 \leq ||x||_2 \leq c||x||_1$$

- 对于不同的素数p上面定义了互不等价的绝对值$|\cdot|_p$
- 它们与经典的绝对值$|\cdot| = |\cdot|_\infty$也不等价
- 用$|\cdot|_p$作为度量，对$\mathbb{Q}$作完备化（添加Cauchy列，再作等价关系求商），得到的记为$\mathbb{Q}_p$：$\mathbb{Q} \subset \mathbb{Q}_p$稠密，在$\mathbb{Q}_p$中可以做分析学研究
- 统一记号：$\mathbb{R} = \mathbb{Q}_\infty$及 $\Omega = \{\text{素数}\} \cup \{\infty\}$

p-adic绝对值

- 例子：$p = 3$
  - （大）$n_1 = 36 = 3^2 \cdot 2^2, v_p(n_1) = 2, |n_1|_p = \frac{1}{9}$（中）
  - （中）$n_2 = 27 = 3^3, \quad v_p(n_2) = 3, |n_2|_p = \frac{1}{27}$（小）
  - （小）$n_3 = 3, \quad v_p(n_3) = 1, |n_3|_p = \frac{1}{3}$（大）
- 回顾两个范数等价是指存在非零常数c使得对任意x有

$$\frac{1}{c}||x||_1 \leq ||x||_2 \leq c||x||_1$$

- 对于不同的素数p上面定义了互不等价的绝对值$|\cdot|_p$
- 它们与经典的绝对值$|\cdot| = |\cdot|_\infty$也不等价
- 用$|\cdot|_p$作为度量，对$\mathbb{Q}$作完备化（添加Cauchy列，再作等价关系求商），得到的记为$\mathbb{Q}_p$：$\mathbb{Q} \subset \mathbb{Q}_p$稠密，在$\mathbb{Q}_p$中可以做分析学研究
- 统一记号：$\mathbb{R} = \mathbb{Q}_\infty$及 $\Omega = \{\text{素数}\} \cup \{\infty\}$

p-adic绝对值

- 例子：$p = 3$
  - （大）$n_1 = 36 = 3^2 \cdot 2^2, v_p(n_1) = 2, |n_1|_p = \frac{1}{9}$（中）
  - （中）$n_2 = 27 = 3^3, \quad v_p(n_2) = 3, |n_2|_p = \frac{1}{27}$（小）
  - （小）$n_3 = 3, \quad v_p(n_3) = 1, |n_3|_p = \frac{1}{3}$（大）
- 回顾两个范数等价是指存在非零常数c使得对任意x有

$$\frac{1}{c}||x||_1 \leq ||x||_2 \leq c||x||_1$$

- 对于不同的素数p上面定义了互不等价的绝对值$|\cdot|_p$
- 它们与经典的绝对值$|\cdot| = |\cdot|_\infty$也不等价
- 用$|\cdot|_p$作为度量，对$\mathbb{Q}$作完备化（添加Cauchy列，再作等价关系求商），得到的记为$\mathbb{Q}_p$：$\mathbb{Q} \subset \mathbb{Q}_p$稠密，在$\mathbb{Q}_p$中可以做分析学研究
- 统一记号：$\mathbb{R} = \mathbb{Q}_\infty$及 $\Omega = \{\text{素数}\} \cup \{\infty\}$

p-adic绝对值

- 例子：$p=3$
  - （大）$n_1=36=3^2\cdot 2^2, v_p(n_1)=2, |n_1|_p=\frac{1}{9}$（中）
  - （中）$n_2=27=3^3, \quad v_p(n_2)=3, |n_2|_p=\frac{1}{27}$（小）
  - （小）$n_3=3, \quad v_p(n_3)=1, |n_3|_p=\frac{1}{3}$（大）
- 回顾两个范数等价是指存在非零常数c使得对任意x有

$$\frac{1}{c}||x||_1 \leq ||x||_2 \leq c||x||_1$$

- 对于不同的素数p上面定义了互不等价的绝对值$|\cdot|_p$
- 它们与经典的绝对值$|\cdot| = |\cdot|_\infty$也不等价
- 用$|\cdot|_p$作为度量，对$\mathbb{Q}$作完备化（添加Cauchy列，再作等价关系求商），得到的记为$\mathbb{Q}_p$：$\mathbb{Q}\subset\mathbb{Q}_p$稠密，在$\mathbb{Q}_p$中可以做分析学研究
- 统一记号：$\mathbb{R}=\mathbb{Q}_\infty$及$\Omega=\{\text{素数}\}\cup\{\infty\}$

p-adic绝对值

- 例子：$p = 3$
  - （大）$n_1 = 36 = 3^2 \cdot 2^2, v_p(n_1) = 2, |n_1|_p = \frac{1}{9}$（中）
  - （中）$n_2 = 27 = 3^3, \quad v_p(n_2) = 3, |n_2|_p = \frac{1}{27}$（小）
  - （小）$n_3 = 3, \quad v_p(n_3) = 1, |n_3|_p = \frac{1}{3}$（大）
- 回顾两个范数等价是指存在非零常数c使得对任意x有

$$\frac{1}{c}||x||_1 \leq ||x||_2 \leq c||x||_1$$

- 对于不同的素数p上面定义了互不等价的绝对值$|\cdot|_p$
- 它们与经典的绝对值$|\cdot| = |\cdot|_\infty$也不等价
- 用$|\cdot|_p$作为度量，对$\mathbb{Q}$作完备化（添加Cauchy列，再作等价关系求商），得到的记为$\mathbb{Q}_p$：$\mathbb{Q} \subset \mathbb{Q}_p$稠密，在$\mathbb{Q}_p$中可以做分析学研究
- 统一记号：$\mathbb{R} = \mathbb{Q}_\infty$及 $\Omega = \{\text{素数}\} \cup \{\infty\}$

p-adic绝对值

- 例子：$p = 3$
  - （大）$n_1 = 36 = 3^2 \cdot 2^2, v_p(n_1) = 2, |n_1|_p = \frac{1}{9}$（中）
  - （中）$n_2 = 27 = 3^3, \quad v_p(n_2) = 3, |n_2|_p = \frac{1}{27}$（小）
  - （小）$n_3 = 3, \quad v_p(n_3) = 1, |n_3|_p = \frac{1}{3}$（大）
- 回顾两个范数等价是指存在非零常数c使得对任意x有

$$\frac{1}{c}||x||_1 \leq ||x||_2 \leq c||x||_1$$

- 对于不同的素数p上面定义了互不等价的绝对值$|\cdot|_p$
- 它们与经典的绝对值$|\cdot| = |\cdot|_\infty$也不等价
- 用$|\cdot|_p$作为度量，对$\mathbb{Q}$作完备化（添加Cauchy列，再作等价关系求商），得到的记为$\mathbb{Q}_p$：$\mathbb{Q} \subset \mathbb{Q}_p$稠密，在$\mathbb{Q}_p$中可以做分析学研究
- 统一记号：$\mathbb{R} = \mathbb{Q}_\infty$及 $\Omega = \{\text{素数}\} \cup \{\infty\}$

$\mathbb{Q}$上的绝对值

Theorem (Ostrowski, 1916)

$\mathbb{Q}$上任何一个非平凡的绝对值等价于$|\cdot|_p (p \in \Omega)$之一。

- 即$\mathbb{Q}$的完备化只有$\mathbb{R} = \mathbb{Q}_\infty$与$\mathbb{Q}_p$
- 因此考虑在$\mathbb{Q}$中解多项式方程，首先要考虑如何在上述这些完备化中解方程
- $\mathbb{R}$中：经典的实分析/数学分析
- $\mathbb{Q}_p$中：p-adic分析

$\mathbb{Q}$上的绝对值

Theorem (Ostrowski, 1916)

$\mathbb{Q}$上任何一个非平凡的绝对值等价于$|\cdot|_p (p \in \Omega)$之一。

- 即$\mathbb{Q}$的完备化只有$\mathbb{R} = \mathbb{Q}_\infty$与$\mathbb{Q}_p$
- 因此考虑在$\mathbb{Q}$中解多项式方程，首先要考虑如何在上述这些完备化中解方程
- $\mathbb{R}$中：经典的实分析/数学分析
- $\mathbb{Q}_p$中：p-adic分析

$\mathbb{Q}$上的绝对值

Theorem (Ostrowski, 1916)

$\mathbb{Q}$上任何一个非平凡的绝对值等价于$|\cdot|_p (p \in \Omega)$之一。

- 即$\mathbb{Q}$的完备化只有$\mathbb{R} = \mathbb{Q}_\infty$与$\mathbb{Q}_p$
- 因此考虑在$\mathbb{Q}$中解多项式方程，首先要考虑如何在上述这些完备化中解方程
- $\mathbb{R}$中：经典的实分析/数学分析
- $\mathbb{Q}_p$中：p-adic分析

$\mathbb{Q}$上的绝对值

Theorem (Ostrowski, 1916)

$\mathbb{Q}$上任何一个非平凡的绝对值等价于$|\cdot|_p (p \in \Omega)$之一。

- 即$\mathbb{Q}$的完备化只有$\mathbb{R} = \mathbb{Q}_\infty$与$\mathbb{Q}_p$
- 因此考虑在$\mathbb{Q}$中解多项式方程，首先要考虑如何在上述这些完备化中解方程
- $\mathbb{R}$中：经典的实分析/数学分析
- $\mathbb{Q}_p$中：p-adic分析

p-adic分析

- 对$\mathbb{Z}$作相应的完备化得到p-adic整数$\mathbb{Z}_p$，　$Frac(\mathbb{Z}_p) = \mathbb{Q}_p$
- 想法：把p-adic分析归结为初等数论！
- 代数的表达：

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(a_n)_{n\geq 1} | a_n \in \mathbb{Z}/p^n\mathbb{Z}, a_n \equiv a_{n+1} \mod p^n\}$$

- 换言之，在$\mathbb{Z}_p$中求解方程相当于 mod p求解，　mod p^2求解，……，　mod p^n求解，……（初等数论！）
- 在绝大部分情况下，其实可以更简单：　mod p就够了

p-adic分析

- 对$\mathbb{Z}$作相应的完备化得到p-adic整数$\mathbb{Z}_p$，　$Frac(\mathbb{Z}_p) = \mathbb{Q}_p$
- 想法：把p-adic分析归结为初等数论！
- 代数的表达：

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(a_n)_{n\geq 1} | a_n \in \mathbb{Z}/p^n\mathbb{Z}, a_n \equiv a_{n+1} \mod p^n\}$$

- 换言之，在$\mathbb{Z}_p$中求解方程相当于 mod p求解，　mod p^2求解，……，　mod p^n求解，……（初等数论！）
- 在绝大部分情况下，其实可以更简单：　mod p就够了

p-adic分析

- 对$\mathbb{Z}$作相应的完备化得到p-adic整数$\mathbb{Z}_p$，　$Frac(\mathbb{Z}_p) = \mathbb{Q}_p$
- 想法：把p-adic分析归结为初等数论！
- 代数的表达：

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(a_n)_{n\geq 1} | a_n \in \mathbb{Z}/p^n\mathbb{Z}, a_n \equiv a_{n+1} \mod p^n\}$$

- 换言之，在$\mathbb{Z}_p$中求解方程相当于 mod p求解，　mod p^2求解，……，　mod p^n求解，……（初等数论！）
- 在绝大部分情况下，其实可以更简单：　mod p就够了

p-adic分析

- 对$\mathbb{Z}$作相应的完备化得到p-adic整数$\mathbb{Z}_p$，　$Frac(\mathbb{Z}_p) = \mathbb{Q}_p$
- 想法：把p-adic分析归结为初等数论！
- 代数的表达：

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(a_n)_{n\geq 1} | a_n \in \mathbb{Z}/p^n\mathbb{Z}, a_n \equiv a_{n+1} \mod p^n\}$$

- 换言之，在$\mathbb{Z}_p$中求解方程相当于 mod p求解，　mod p^2求解，……，　mod p^n求解，……（初等数论！）
- 在绝大部分情况下，其实可以更简单：　mod p就够了

p-adic分析

- 对$\mathbb{Z}$作相应的完备化得到p-adic整数$\mathbb{Z}_p$，　$Frac(\mathbb{Z}_p) = \mathbb{Q}_p$
- 想法：把p-adic分析归结为初等数论！
- 代数的表达：

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(a_n)_{n\geq 1} | a_n \in \mathbb{Z}/p^n\mathbb{Z}, a_n \equiv a_{n+1} \mod p^n\}$$

- 换言之，在$\mathbb{Z}_p$中求解方程相当于 mod p求解，　mod p^2求解，……，　mod p^n求解，……（初等数论！）
- 在绝大部分情况下，其实可以更简单：　mod p就够了

Hensel引理

Lemma (Hensel)

令$f(x) \in \mathbb{Z}[x]$为整系数多项式，令$k \in \mathbb{N}, k \geq 1$，$r \in \mathbb{Z}$使得$|f(r)|_p \leq \frac{1}{p^k}$（即$f(r) \equiv 0 \mod p^k$）。

若$|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）那么存在$s \in \mathbb{Z}$使得

$$|f(s)|_p \leq \frac{1}{p^{k+1}}$$（即$f(s) \equiv 0 \mod p^{k+1}$）且

$$|s - r|_p \leq \frac{1}{p^k}$$（即$s \equiv r \mod p^k$）

- 初等数论角度：存在 mod p解 $\Longrightarrow$ 存在 mod p^2解 $\Longrightarrow$ 存在 mod p^3解 $\Longrightarrow \cdots\cdots$（从而存在$\mathbb{Z}_p$解）而$X(\mathbb{F}_p)$容易计算（计算机可以处理有限域）
- 分析角度：Newton迭代法的类比，近似解逐步逼近
- $|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）的几何意义：$X$ mod p后仍“光滑”（除去有限个素数外总是成立的）

Hensel引理

Lemma (Hensel)

令$f(x) \in \mathbb{Z}[x]$为整系数多项式，令$k \in \mathbb{N}, k \geq 1$，$r \in \mathbb{Z}$使得$|f(r)|_p \leq \frac{1}{p^k}$（即$f(r) \equiv 0 \mod p^k$）。

若$|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）那么存在$s \in \mathbb{Z}$使得

$$|f(s)|_p \leq \frac{1}{p^{k+1}}$$（即$f(s) \equiv 0 \mod p^{k+1}$）且

$$|s - r|_p \leq \frac{1}{p^k}$$（即$s \equiv r \mod p^k$）

- 初等数论角度：存在 $\mod p$解 $\Longrightarrow$ 存在 $\mod p^2$解 $\Longrightarrow$ 存在 $\mod p^3$解 $\Longrightarrow \cdots\cdots$（从而存在$\mathbb{Z}_p$解）而$X(\mathbb{F}_p)$容易计算（计算机可以处理有限域）
- 分析角度：Newton迭代法的类比，近似解逐步逼近
- $|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）的几何意义：$X \mod p$后仍“光滑”（除去有限个素数外总是成立的）

Hensel引理

Lemma (Hensel)

令$f(x) \in \mathbb{Z}[x]$为整系数多项式，令$k \in \mathbb{N}, k \geq 1$，$r \in \mathbb{Z}$使得$|f(r)|_p \leq \frac{1}{p^k}$（即$f(r) \equiv 0 \mod p^k$）。

若$|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）那么存在$s \in \mathbb{Z}$使得

$$|f(s)|_p \leq \frac{1}{p^{k+1}}$$（即$f(s) \equiv 0 \mod p^{k+1}$）且

$$|s - r|_p \leq \frac{1}{p^k}$$（即$s \equiv r \mod p^k$）

- 初等数论角度：存在 $\mod p$解 $\Longrightarrow$ 存在 $\mod p^2$解 $\Longrightarrow$ 存在 $\mod p^3$解 $\Longrightarrow \cdots\cdots$（从而存在$\mathbb{Z}_p$解）而$X(\mathbb{F}_p)$容易计算（计算机可以处理有限域）
- 分析角度：Newton迭代法的类比，近似解逐步逼近
- $|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）的几何意义：$X \mod p$后仍“光滑”（除去有限个素数外总是成立的）

Hensel引理

Lemma (Hensel)

令$f(x) \in \mathbb{Z}[x]$为整系数多项式，令$k \in \mathbb{N}, k \geq 1$，$r \in \mathbb{Z}$使得$|f(r)|_p \leq \frac{1}{p^k}$（即$f(r) \equiv 0 \mod p^k$）。

若$|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）那么存在$s \in \mathbb{Z}$使得

$$|f(s)|_p \leq \frac{1}{p^{k+1}}$$（即$f(s) \equiv 0 \mod p^{k+1}$）且

$$|s - r|_p \leq \frac{1}{p^k}$$（即$s \equiv r \mod p^k$）

- 初等数论角度：存在 $\mod p$解 $\Longrightarrow$ 存在 $\mod p^2$解 $\Longrightarrow$ 存在 $\mod p^3$解 $\Longrightarrow \cdots\cdots$（从而存在$\mathbb{Z}_p$解）而$X(\mathbb{F}_p)$容易计算（计算机可以处理有限域）
- 分析角度：Newton迭代法的类比，近似解逐步逼近
- $|f'(r)|_p = 1$（即$f'(r) \not\equiv 0 \mod p$）的几何意义：$X \mod p$后仍“光滑”（除去有限个素数外总是成立的）

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

数论中的局部

- $\mathbb{Q}_p$称为局部域。为什么叫“局部”？
- 两个原因：1.$\mathbb{Q}_p$的拓扑是局部紧的。2.……
- Grothendick的现代代数几何语言：把$\mathbb{Z}$看作一条“曲线”（1维概型）$C = \mathrm{Spec}(\mathbb{Z})$
- 每个素数p成为C上的一个点
- $\mathbb{Z}_p$的一个子环$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$称为$\mathbb{Z}$在$p$处的局部化。$\mathrm{Spec}(\mathbb{Z}_{(p)}) \to C$的像是p这一点的所有开邻域的交。确实是几何意义上的“局部”
- $\mathbb{Q}$称为整体域，对应于C的point générique，这个点的闭包是C（对应于“整体”）
- 注意：跟经典的几何一样，各个局部之间并不是独立的，是相互有联系的！

二次互反律

- Legendre记号：设$p \nmid a$，若$a \mod p$是平方数，则令$\left(\frac{a}{p}\right) = 1$，否则为$-1$.

Theorem (Gauss二次互反律)

令p, q为奇素数，则$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

- 这是关于$x^2 = a$这个方程在$\mod p$和$\mod q$在a变化时的可解性的关系。
- 由Hensel引理，这相当于是讨论在$\mathbb{Q}_p$和$\mathbb{Q}_q$这两个不同的局部中的解。Gauss的定理表明各个局部不是相互独立的。
- 这个结果是一个“整体性”的结果（同时关注了至少两个不同的局部）

二次互反律

- Legendre记号：设$p \nmid a$，若$a \mod p$是平方数，则令$\left(\frac{a}{p}\right) = 1$，否则为$-1$.

Theorem (Gauss二次互反律)

令p, q为奇素数，则$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

- 这是关于$x^2 = a$这个方程在 $\mod p$和 $\mod q$在a变化时的可解性的关系。
- 由Hensel引理，这相当于是讨论在$\mathbb{Q}_p$和$\mathbb{Q}_q$这两个不同的局部中的解。Gauss的定理表明各个局部不是相互独立的。
- 这个结果是一个“整体性”的结果（同时关注了至少两个不同的局部）

二次互反律

- Legendre记号：设$p \nmid a$，若$a \mod p$是平方数，则令$\left(\frac{a}{p}\right) = 1$，否则为$-1$.

Theorem (Gauss二次互反律)

令p, q为奇素数，则$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

- 这是关于$x^2 = a$这个方程在 $\mod p$和 $\mod q$在a变化时的可解性的关系。
- 由Hensel引理，这相当于是讨论在$\mathbb{Q}_p$和$\mathbb{Q}_q$这两个不同的局部中的解。Gauss的定理表明各个局部不是相互独立的。
- 这个结果是一个“整体性”的结果（同时关注了至少两个不同的局部）

二次互反律

- Legendre记号：设$p \nmid a$，若$a \mod p$是平方数，则令$\left(\frac{a}{p}\right) = 1$，否则为$-1$.

Theorem (Gauss二次互反律)

令p, q为奇素数，则$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

- 这是关于$x^2 = a$这个方程在 $\mod p$和 $\mod q$在a变化时的可解性的关系。
- 由Hensel引理，这相当于是讨论在$\mathbb{Q}_p$和$\mathbb{Q}_q$这两个不同的局部中的解。Gauss的定理表明各个局部不是相互独立的。
- 这个结果是一个“整体性”的结果（同时关注了至少两个不同的局部）

二次互反律

- Legendre记号：设$p \nmid a$，若$a \mod p$是平方数，则令$\left(\frac{a}{p}\right) = 1$，否则为$-1$.

Theorem (Gauss二次互反律)

令p, q为奇素数，则$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

- 这是关于$x^2 = a$这个方程在 $\mod p$和 $\mod q$在a变化时的可解性的关系。
- 由Hensel引理，这相当于是讨论在$\mathbb{Q}_p$和$\mathbb{Q}_q$这两个不同的局部中的解。Gauss的定理表明各个局部不是相互独立的。
- 这个结果是一个“整体性”的结果（同时关注了至少两个不同的局部）

From local to global

从局部到整体

局部-整体

- 应该关注所有局部 $\mathbb{Q} \to \prod_{p\in\Omega} \mathbb{Q}_p; a \mapsto (a, a, \ldots)$
- 诱导出单射$X(\mathbb{Q}) \to \prod_{p\in\Omega} X(\mathbb{Q}_p)$

Question

如果$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$（即$\forall p \in \Omega, X(\mathbb{Q}_p) \neq \emptyset$），是否有$X(\mathbb{Q}) \neq \emptyset$? 方程在每个局部有解，是否就在整体有解?

- 如果答案肯定，我们称有局部整体原则

局部-整体

- 应该关注所有局部 $\mathbb{Q} \to \prod_{p\in\Omega} \mathbb{Q}_p; a \mapsto (a, a, \ldots)$
- 诱导出单射$X(\mathbb{Q}) \to \prod_{p\in\Omega} X(\mathbb{Q}_p)$

Question

如果$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$（即$\forall p \in \Omega, X(\mathbb{Q}_p) \neq \emptyset$），是否有$X(\mathbb{Q}) \neq \emptyset$? 方程在每个局部有解，是否就在整体有解?

- 如果答案肯定，我们称有局部整体原则

局部-整体

- 应该关注所有局部 $\mathbb{Q} \to \prod_{p\in\Omega} \mathbb{Q}_p; a \mapsto (a, a, \ldots)$
- 诱导出单射$X(\mathbb{Q}) \to \prod_{p\in\Omega} X(\mathbb{Q}_p)$

Question

如果$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$（即$\forall p \in \Omega, X(\mathbb{Q}_p) \neq \emptyset$），是否有$X(\mathbb{Q}) \neq \emptyset$? 方程在每个局部有解，是否就在整体有解?

- 如果答案肯定，我们称有局部整体原则

局部-整体

- 应该关注所有局部 $\mathbb{Q} \to \prod_{p\in\Omega} \mathbb{Q}_p; a \mapsto (a, a, \ldots)$
- 诱导出单射$X(\mathbb{Q}) \to \prod_{p\in\Omega} X(\mathbb{Q}_p)$

Question

如果$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$（即$\forall p \in \Omega, X(\mathbb{Q}_p) \neq \emptyset$），是否有$X(\mathbb{Q}) \neq \emptyset$? 方程在每个局部有解，是否就在整体有解?

- 如果答案肯定，我们称有局部整体原则

局部整体原则

Theorem (Hasse)

如果代数簇X是由一个二次型定义的，那么它满足局部整体原则。即二次型${}^tXMX = a$有有理数解当且仅当它在所有$\mathbb{Q}_p$中有解，其中$M \in \mathrm{Mat}_n(\mathbb{Q})$是$n \times n$对称矩阵。

- Minkowski证明了这对一般数域也是成立的。
- 证明概要：用某种数学归纳法，归结为三元二次型Hilbert符号的局部整体原则
  - 考虑二次型$P(x,y,z) = x^2 - ay^2 - bz^2$在$\mathbb{Q}_p$中是否有（非零）解，若有则记Hilbert符号$(a,b)_p = 1$，否则$-1$。
  - 上述定理就是说$\forall p \in \Omega, (a,b)_p = 1 \Leftrightarrow (a,b)_{\mathbb{Q}} = 1$

Theorem

$\prod_{p \in \Omega} (a,b)_p = 1$ （有限乘积，各个局部之间不是独立的！）

局部整体原则

Theorem (Hasse)

如果代数簇X是由一个二次型定义的，那么它满足局部整体原则。即二次型${}^tXMX = a$有有理数解当且仅当它在所有$\mathbb{Q}_p$中有解，其中$M \in \mathrm{Mat}_n(\mathbb{Q})$是$n \times n$对称矩阵。

- Minkowski证明了这对一般数域也是成立的。
- 证明概要：用某种数学归纳法，归结为三元二次型Hilbert符号的局部整体原则
  - 考虑二次型$P(x,y,z) = x^2 - ay^2 - bz^2$在$\mathbb{Q}_p$中是否有（非零）解，若有则记Hilbert符号$(a,b)_p = 1$，否则$-1$。
  - 上述定理就是说$\forall p \in \Omega, (a,b)_p = 1 \Leftrightarrow (a,b)_{\mathbb{Q}} = 1$

Theorem

$\prod_{p \in \Omega} (a,b)_p = 1$ （有限乘积，各个局部之间不是独立的！）

局部整体原则

Theorem (Hasse)

如果代数簇X是由一个二次型定义的，那么它满足局部整体原则。即二次型${}^tXMX = a$有有理数解当且仅当它在所有$\mathbb{Q}_p$中有解，其中$M \in \mathrm{Mat}_n(\mathbb{Q})$是$n \times n$对称矩阵。

- Minkowski证明了这对一般数域也是成立的。
- 证明概要：用某种数学归纳法，归结为三元二次型Hilbert符号的局部整体原则
  - 考虑二次型$P(x,y,z) = x^2 - ay^2 - bz^2$在$\mathbb{Q}_p$中是否有（非零）解，若有则记Hilbert符号$(a,b)_p = 1$，否则$-1$。
  - 上述定理就是说$\forall p \in \Omega, (a,b)_p = 1 \Leftrightarrow (a,b)_{\mathbb{Q}} = 1$

Theorem

$\prod_{p \in \Omega} (a,b)_p = 1$ （有限乘积，各个局部之间不是独立的！）

局部整体原则

Theorem (Hasse)

如果代数簇X是由一个二次型定义的，那么它满足局部整体原则。即二次型${}^tXMX = a$有有理数解当且仅当它在所有$\mathbb{Q}_p$中有解，其中$M \in \mathrm{Mat}_n(\mathbb{Q})$是$n \times n$对称矩阵。

- Minkowski证明了这对一般数域也是成立的。
- 证明概要：用某种数学归纳法，归结为三元二次型Hilbert符号的局部整体原则
  - 考虑二次型$P(x,y,z) = x^2 - ay^2 - bz^2$在$\mathbb{Q}_p$中是否有（非零）解，若有则记Hilbert符号$(a,b)_p = 1$，否则$-1$。
  - 上述定理就是说$\forall p \in \Omega, (a,b)_p = 1 \Leftrightarrow (a,b)_{\mathbb{Q}} = 1$

Theorem

$\prod_{p\in\Omega}(a,b)_p = 1$ （有限乘积，各个局部之间不是独立的！）

局部整体原则

Theorem (Hasse)

如果代数簇X是由一个二次型定义的，那么它满足局部整体原则。即二次型${}^tXMX = a$有有理数解当且仅当它在所有$\mathbb{Q}_p$中有解，其中$M \in \mathrm{Mat}_n(\mathbb{Q})$是$n \times n$对称矩阵。

- Minkowski证明了这对一般数域也是成立的。
- 证明概要：用某种数学归纳法，归结为三元二次型Hilbert符号的局部整体原则
  - 考虑二次型$P(x,y,z) = x^2 - ay^2 - bz^2$在$\mathbb{Q}_p$中是否有（非零）解，若有则记Hilbert符号$(a,b)_p = 1$，否则$-1$。
  - 上述定理就是说$\forall p \in \Omega, (a,b)_p = 1 \Leftrightarrow (a,b)_{\mathbb{Q}} = 1$

Theorem

$\prod_{p\in\Omega}(a,b)_p = 1$ （有限乘积，各个局部之间不是独立的！）

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效？

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: \ P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效？

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效？

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效？

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效？

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效？

局部整体原则的失效

- 一个局部整体原则失效的简单例子：
- $X: P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$
- 明显：在$\mathbb{Q}$中它无解，在$\mathbb{R}$中有解
- $2^2 \equiv 17 \mod 13$即$X(\mathbb{F}_{13}) \neq \emptyset$从而由Hensel引理知道$X(\mathbb{Q}_{13}) \neq \emptyset$
- 对$p = 17$，由$8^2 \equiv 13 \mod 17$同理可得$X(\mathbb{Q}_{17}) \neq \emptyset$
- 最后对$p \neq 13, 17$，观察到$\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{13 \cdot 17}{p}\right)$，这三个Legendre符号至少有一个必须是1，因此$X(\mathbb{F}_p) \neq \emptyset$以及$X(\mathbb{Q}_p) \neq \emptyset$。（对于$p = 2$，mod 2不光滑，需要考虑更精细的Hensel引理，考虑 mod 8）
- 问题：为什么局部整体原则失效?

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega} \mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度?
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega} \mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效?

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？答：上同调理论。
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer： $C : P(x, y, z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？答：上同调理论。
- C的Jacobian： $E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E, \mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q}, E) \to \prod_{p\in\Omega} \mathrm{H}^1(\mathbb{Q}_p, E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E, \mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer： $C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？答：上同调理论。
- C的Jacobian： $E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？答：上同调理论。
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？答：上同调理论。
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？

局部整体原则的失效又一例

- 一旦把2次换成3次就不对了！
- 最著名的例子：
  Selmer：$C: P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$在$\mathbb{Q}_p$中均有（非零）解，但在$\mathbb{Q}$中没有解。
- 回顾：这是一条亏格为1的曲线，它不是一条椭圆曲线（它没有有理点）
- 问题：怎么去衡量局部整体原则失效的程度？答：上同调理论。
- C的Jacobian：$E = \mathrm{Jac}(C)$是一条椭圆曲线
- Tate-Shafarevich群
  $Ш(E,\mathbb{Q}) = Ker\left[\mathrm{H}^1(\mathbb{Q},E) \to \prod_{p\in\Omega}\mathrm{H}^1(\mathbb{Q}_p,E)\right]$
- BSD猜想的一部分：它是一个有限群（就是局部整体原则失效得并不严重）曲线被看作一个上同调类$[C] \in Ш(E,\mathbb{Q})$
- 问题：如何解释局部整体原则失效？答：上同调理论。

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能:
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能:
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能：
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能：
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能：
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能:
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能:
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 = 概型（代数簇）X
- 数域K = 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 = 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能:
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 $=$ 概型（代数簇）X
- 数域K $=$ 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 $=$ 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：如何看待方程的解

- Grothendieck创造的现代代数几何语言有强大的功能:
- 定义了“概型”：一个同时包含几何信息与算术信息的对象
- 一个极端：代数几何；另一个极端：数论。
- 研究算术代数几何的最佳语言。例：Galois群是某种意义的拓扑基本群 [SGA1]
- “多项式方程的解”在这套语言里翻译成“概型之间的映射”
- 多项式方程 $=$ 概型（代数簇）X
- 数域K $=$ 概型$\mathrm{Spec}(K)$
- 多项式方程在K中的解 $=$ 映射 $x : \mathrm{Spec}(K) \to X$
- 有理点的集合$X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$

Grothendieck的代数几何语言：étale上同调群，Brauer群

- étale上同调群：Grothendieck的另一大发明
- 代数簇上的Zariski拓扑太粗糙，用它构造上同调无法保留充分多的几何信息
- 为了模拟实/复拓扑，需要更广义的“Grothendieck拓扑”——例如“étale拓扑”，从此出发构造的上同调模拟了复流形的经典的上同调。这种上同调同时可以用于处理算术问题。
- Brauer群：$\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$
- 概型之间的态射$X \to Y$自然诱导同调群间的同态$\mathrm{Br}(Y) \to \mathrm{Br}(X)$
- 特别的，对有理点$x \in X(K)$即$x : \mathrm{Spec}(K) \to X$诱导“取值映射”$x^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathrm{Spec}(K)) = \mathrm{Br}(K)$

Grothendieck的代数几何语言：étale上同调群，Brauer群

- étale上同调群：Grothendieck的另一大发明
- 代数簇上的Zariski拓扑太粗糙，用它构造上同调无法保留充分多的几何信息
- 为了模拟实/复拓扑，需要更广义的“Grothendieck拓扑”——例如“étale拓扑”，从此出发构造的上同调模拟了复流形的经典的上同调。这种上同调同时可以用于处理算术问题。
- Brauer群：$\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$
- 概型之间的态射$X \to Y$自然诱导同调群间的同态$\mathrm{Br}(Y) \to \mathrm{Br}(X)$
- 特别的，对有理点$x \in X(K)$即$x : \mathrm{Spec}(K) \to X$诱导“取值映射”$x^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathrm{Spec}(K)) = \mathrm{Br}(K)$

Grothendieck的代数几何语言：étale上同调群，Brauer群

- étale上同调群：Grothendieck的另一大发明
- 代数簇上的Zariski拓扑太粗糙，用它构造上同调无法保留充分多的几何信息
- 为了模拟实/复拓扑，需要更广义的“Grothendieck拓扑”——例如“étale拓扑”，从此出发构造的上同调模拟了复流形的经典的上同调。这种上同调同时可以用于处理算术问题。
- Brauer群：$\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$
- 概型之间的态射$X \to Y$自然诱导同调群间的同态$\mathrm{Br}(Y) \to \mathrm{Br}(X)$
- 特别的，对有理点$x \in X(K)$即$x : \mathrm{Spec}(K) \to X$诱导“取值映射”$x^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathrm{Spec}(K)) = \mathrm{Br}(K)$

Grothendieck的代数几何语言：étale上同调群，Brauer群

- étale上同调群：Grothendieck的另一大发明
- 代数簇上的Zariski拓扑太粗糙，用它构造上同调无法保留充分多的几何信息
- 为了模拟实/复拓扑，需要更广义的“Grothendieck拓扑”——例如“étale拓扑”，从此出发构造的上同调模拟了复流形的经典的上同调。这种上同调同时可以用于处理算术问题。
- Brauer群：$\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$
- 概型之间的态射$X \to Y$自然诱导同调群间的同态$\mathrm{Br}(Y) \to \mathrm{Br}(X)$
- 特别的，对有理点$x \in X(K)$即$x : \mathrm{Spec}(K) \to X$诱导“取值映射”$x^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathrm{Spec}(K)) = \mathrm{Br}(K)$

Grothendieck的代数几何语言：étale上同调群，Brauer群

- étale上同调群：Grothendieck的另一大发明
- 代数簇上的Zariski拓扑太粗糙，用它构造上同调无法保留充分多的几何信息
- 为了模拟实/复拓扑，需要更广义的“Grothendieck拓扑”——例如“étale拓扑”，从此出发构造的上同调模拟了复流形的经典的上同调。这种上同调同时可以用于处理算术问题。
- Brauer群：$\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$
- 概型之间的态射$X \to Y$自然诱导同调群间的同态$\mathrm{Br}(Y) \to \mathrm{Br}(X)$
- 特别的，对有理点$x \in X(K)$即$x : \mathrm{Spec}(K) \to X$诱导“取值映射”$x^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathrm{Spec}(K)) = \mathrm{Br}(K)$

Grothendieck的代数几何语言：étale上同调群，Brauer群

- étale上同调群：Grothendieck的另一大发明
- 代数簇上的Zariski拓扑太粗糙，用它构造上同调无法保留充分多的几何信息
- 为了模拟实/复拓扑，需要更广义的“Grothendieck拓扑”——例如“étale拓扑”，从此出发构造的上同调模拟了复流形的经典的上同调。这种上同调同时可以用于处理算术问题。
- Brauer群：$\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$
- 概型之间的态射$X \to Y$自然诱导同调群间的同态$\mathrm{Br}(Y) \to \mathrm{Br}(X)$
- 特别的，对有理点$x \in X(K)$即$x : \mathrm{Spec}(K) \to X$诱导“取值映射”$x^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathrm{Spec}(K)) = \mathrm{Br}(K)$

Manin配对

- 当X是一个域时Brauer群有一个（通过中心单代数的）相对简单的描述
- 代数数论的局部类域论：
  - $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) = \mathrm{Br}(\mathrm{Spec}(\mathbb{Q}_p)) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$
  - $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$
- 若有一族局部有理点$(x_p)_{p\in\Omega} \in \prod_{p\in\Omega} X(\mathbb{Q}_p)$以及$b \in \mathrm{Br}(X)$则有 $\mathrm{inv}_p(x_p^*(b)) \in \mathbb{Q}/\mathbb{Z}$
- （ICM 1970）Manin定义了一个配对（X是射影代数簇）
  - $\mathrm{Br}(X) \times \prod_{p\in\Omega} X(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$
  - $(b, (x_p)_{p\in\Omega}) \mapsto \sum_{p\in\Omega} \mathrm{inv}_p(x_p^*(b))$
- 整体类域论：$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \to 0$
  $\Longrightarrow$ 整体点在上述配对中给出0。

Manin配对

- 当X是一个域时Brauer群有一个（通过中心单代数的）相对简单的描述
- 代数数论的局部类域论：
  - $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) = \mathrm{Br}(\mathrm{Spec}(\mathbb{Q}_p)) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$
  - $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$
- 若有一族局部有理点$(x_p)_{p\in\Omega} \in \prod_{p\in\Omega} X(\mathbb{Q}_p)$以及$b \in \mathrm{Br}(X)$则有 $\mathrm{inv}_p(x_p^*(b)) \in \mathbb{Q}/\mathbb{Z}$
- （ICM 1970）Manin定义了一个配对（X是射影代数簇）
  - $\mathrm{Br}(X) \times \prod_{p\in\Omega} X(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$
  - $(b, (x_p)_{p\in\Omega}) \mapsto \sum_{p\in\Omega} \mathrm{inv}_p(x_p^*(b))$
- 整体类域论：$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \to 0$
  $\Longrightarrow$ 整体点在上述配对中给出0。

Manin配对

- 当X是一个域时Brauer群有一个（通过中心单代数的）相对简单的描述
- 代数数论的局部类域论：
  - $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) = \mathrm{Br}(\mathrm{Spec}(\mathbb{Q}_p)) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$
  - $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$
- 若有一族局部有理点$(x_p)_{p\in\Omega} \in \prod_{p\in\Omega} X(\mathbb{Q}_p)$以及$b \in \mathrm{Br}(X)$则有 $\mathrm{inv}_p(x_p^*(b)) \in \mathbb{Q}/\mathbb{Z}$
- （ICM 1970）Manin定义了一个配对（X是射影代数簇）
  - $\mathrm{Br}(X) \times \prod_{p\in\Omega} X(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$
  - $(b, (x_p)_{p\in\Omega}) \mapsto \sum_{p\in\Omega} \mathrm{inv}_p(x_p^*(b))$
- 整体类域论：$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \to 0$
  $\Longrightarrow$ 整体点在上述配对中给出0。

Manin配对

- 当X是一个域时Brauer群有一个（通过中心单代数的）相对简单的描述
- 代数数论的局部类域论：
  - $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) = \mathrm{Br}(\mathrm{Spec}(\mathbb{Q}_p)) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$
  - $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$
- 若有一族局部有理点$(x_p)_{p\in\Omega} \in \prod_{p\in\Omega} X(\mathbb{Q}_p)$以及$b \in \mathrm{Br}(X)$则有 $\mathrm{inv}_p(x_p^*(b)) \in \mathbb{Q}/\mathbb{Z}$
- （ICM 1970）Manin定义了一个配对（X是射影代数簇）
  - $\mathrm{Br}(X) \times \prod_{p\in\Omega} X(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$
  - $(b, (x_p)_{p\in\Omega}) \mapsto \sum_{p\in\Omega} \mathrm{inv}_p(x_p^*(b))$
- 整体类域论：$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \to 0$
  $\Longrightarrow$ 整体点在上述配对中给出0。

Manin配对

- 当X是一个域时Brauer群有一个（通过中心单代数的）相对简单的描述
- 代数数论的局部类域论：
  - $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) = \mathrm{Br}(\mathrm{Spec}(\mathbb{Q}_p)) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$
  - $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$
- 若有一族局部有理点$(x_p)_{p\in\Omega} \in \prod_{p\in\Omega} X(\mathbb{Q}_p)$以及$b \in \mathrm{Br}(X)$则有 $\mathrm{inv}_p(x_p^*(b)) \in \mathbb{Q}/\mathbb{Z}$
- （ICM 1970）Manin定义了一个配对（X是射影代数簇）
  - $\mathrm{Br}(X) \times \prod_{p\in\Omega} X(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$
  - $(b, (x_p)_{p\in\Omega}) \mapsto \sum_{p\in\Omega} \mathrm{inv}_p(x_p^*(b))$
- 整体类域论：$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v\in\Omega} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sum \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \to 0$
  $\Longrightarrow$ 整体点在上述配对中给出0。

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
-
$$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$ 那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$ 那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$ 那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$ 那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$ 那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍

- $[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \{(x_p) \in \prod_p X(\mathbb{Q}_p) \mid (x_p) \perp b, \forall b \in \mathrm{Br}(X)\}$
- $$X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$
- 即使所有局部都有解$\prod_{p\in\Omega} X(\mathbb{Q}_p) \neq \emptyset$，但是若$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} = \emptyset$ 那么就没有整体有理点。
- 这称为 Brauer-Manin障碍
- 这足以解释当时几乎所有已知的局部整体原则失效的例子！
- 问题：$[\prod_p X(\mathbb{Q}_p)]^{\mathrm{Br}} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$？？
- 称：对于局部整体原则Brauer-Manin障碍是唯一的障碍。
- 成立的例子：亏格1的曲线（要求某Ш群有限），线性代数群的某些齐次空间，Châtelet曲面（$y^2 - az^2 = P(x)$，P为4次多项式）……

Brauer-Manin障碍的不足

Brauer-Manin障碍不足以解释局部整体原则的失效

$$(\emptyset =) X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} (\neq \emptyset) \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$

- 例子:
  - Skorobogatov（1999）：bielliptic surface
  - Poonen（2010）：Châtelet surface bundle over a high genus curve
- 维数>1，不是有理连通簇

Brauer-Manin障碍的不足

Brauer-Manin障碍不足以解释局部整体原则的失效

$$(\emptyset =) X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} (\neq \emptyset) \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$

- 例子:
  - Skorobogatov（1999）：bielliptic surface
  - Poonen（2010）：Châtelet surface bundle over a high genus curve
- 维数>1，不是有理连通簇

Brauer-Manin障碍的不足

Brauer-Manin障碍不足以解释局部整体原则的失效

$$(\emptyset =) X(\mathbb{Q}) \subset [\prod_{p\in\Omega} X(\mathbb{Q}_p)]^{\mathrm{Br}} (\neq \emptyset) \subset \prod_{p\in\Omega} X(\mathbb{Q}_p)$$

- 例子:
  - Skorobogatov（1999）：bielliptic surface
  - Poonen（2010）：Châtelet surface bundle over a high genus curve
- 维数>1，不是有理连通簇

有理连通代数簇

- 令X为一个$\mathbb{C}$上射影代数簇

Definition

称X是一个有理连通簇，若对X上任意两点P和Q，都存在一个定义在$\mathbb{C}$上的代数映射$f : \mathbb{P}^1 \to X$使得$f(0) = P$及$f(1) = Q$。

- 这里“代数映射”是指代数簇之间的态射，即可由多项式定义的映射。
- 即任两点可以用一条有理曲线连起来
- 这个要求比拓扑里的“道路连通”要强很多（要求f是代数的映射）
- 有理连通 $\Longrightarrow$ “单连通”
- 这是一个纯粹几何的概念（全是定义在$\mathbb{C}$上的）

有理连通代数簇

- 令X为一个$\mathbb{C}$上射影代数簇

Definition

称X是一个有理连通簇，若对X上任意两点P和Q，都存在一个定义在$\mathbb{C}$上的代数映射$f : \mathbb{P}^1 \to X$使得$f(0) = P$及$f(1) = Q$。

- 这里“代数映射”是指代数簇之间的态射，即可由多项式定义的映射。
- 即任两点可以用一条有理曲线连起来
- 这个要求比拓扑里的“道路连通”要强很多（要求f是代数的映射）
- 有理连通 $\Longrightarrow$ “单连通”
- 这是一个纯粹几何的概念（全是定义在$\mathbb{C}$上的）

有理连通代数簇

- 令X为一个$\mathbb{C}$上射影代数簇

Definition

称X是一个有理连通簇，若对X上任意两点P和Q，都存在一个定义在$\mathbb{C}$上的代数映射$f : \mathbb{P}^1 \to X$使得$f(0) = P$及$f(1) = Q$。

- 这里“代数映射”是指代数簇之间的态射，即可由多项式定义的映射。
- 即任两点可以用一条有理曲线连起来
- 这个要求比拓扑里的“道路连通”要强很多（要求f是代数的映射）
- 有理连通 $\Longrightarrow$ “单连通”
- 这是一个纯粹几何的概念（全是定义在$\mathbb{C}$上的）

有理连通代数簇

- 令X为一个$\mathbb{C}$上射影代数簇

Definition

称X是一个有理连通簇，若对X上任意两点P和Q，都存在一个定义在$\mathbb{C}$上的代数映射$f : \mathbb{P}^1 \to X$使得$f(0) = P$及$f(1) = Q$。

- 这里“代数映射”是指代数簇之间的态射，即可由多项式定义的映射。
- 即任两点可以用一条有理曲线连起来
- 这个要求比拓扑里的“道路连通”要强很多（要求f是代数的映射）
- 有理连通 $\Longrightarrow$ “单连通”
- 这是一个纯粹几何的概念（全是定义在$\mathbb{C}$上的）

有理连通代数簇

- 令X为一个$\mathbb{C}$上射影代数簇

Definition

称X是一个有理连通簇，若对X上任意两点P和Q，都存在一个定义在$\mathbb{C}$上的代数映射$f : \mathbb{P}^1 \to X$使得$f(0) = P$及$f(1) = Q$。

- 这里“代数映射”是指代数簇之间的态射，即可由多项式定义的映射。
- 即任两点可以用一条有理曲线连起来
- 这个要求比拓扑里的“道路连通”要强很多（要求f是代数的映射）
- 有理连通 $\Longrightarrow$ “单连通”
- 这是一个纯粹几何的概念（全是定义在$\mathbb{C}$上的）

有理连通代数簇

- 令X为一个$\mathbb{C}$上射影代数簇

Definition

称X是一个有理连通簇，若对X上任意两点P和Q，都存在一个定义在$\mathbb{C}$上的代数映射$f : \mathbb{P}^1 \to X$使得$f(0) = P$及$f(1) = Q$。

- 这里“代数映射”是指代数簇之间的态射，即可由多项式定义的映射。
- 即任两点可以用一条有理曲线连起来
- 这个要求比拓扑里的“道路连通”要强很多（要求f是代数的映射）
- 有理连通 $\Longrightarrow$ “单连通”
- 这是一个纯粹几何的概念（全是定义在$\mathbb{C}$上的）

几何决定算术

Conjecture (Colliot-Thélène–Sansuc)

对于光滑有理连通代数簇，*Brauer-Manin*障碍是局部整体原则的唯一障碍。

Conjecture (Skorobogatov)

对于光滑射影曲线，*Brauer-Manin*障碍是局部整体原则的唯一障碍。

- 这两个猜想的哲学依然是 几何决定算术！

结语

- 通过局部来研究整体。
- 几何决定算术。