纯粹数学前沿.

数论：几何，分析，代数相交汇的地方.

(intro. 中文
后面 英文教书)

§1 Introduction

数学中的问题：　解方程！

来源于物理：ordinary / partial differential equation.

例：流体力学 (Fluid mechanics)：Navier-Stocks 方程.

Clay 数学所提出的千禧年七大问题之一. (Millennium Pbs)

另一类重要的方程：来源于"数"本身的方程.

人类数数 ⟶ 自然数 $\mathbb{N}$.

$$\left.\begin{array}{ll} x+1=0 & \text{求解} \to \text{加入负数} \to \mathbb{Z}. \\ \left.\begin{array}{ll} 3x=1 & \text{求解} \to \text{加入有理数} \to \mathbb{Q}. \\ x^2=2 & \text{求解} \to \text{加入无理数} \to \mathbb{R} \\ x^2=-1 & \text{求解} \to \text{加入虚数} \to \mathbb{C} \end{array}\right\} \text{域} & \end{array}\right\} \text{环}.$$

↳ 多项式方程. 一元 n 次方程

Thm 所有多项式方程均在 $\mathbb{C}$ 上有解。

分析要问：多项式方程 (或更一般的方程) 什么时候在 $\mathbb{R}$ 中有解？
(实系数)

数学分析.

① 有理系数 多项式 方程 什么时候在 $\mathbb{Q}$ 中有解？

② 整系数　　　　　　　　　　　$\mathbb{Z}$　　？

② 称为丢番图 (Diophantine equation) 方程可解性问题.

Hilbert 第十问题：能否用一种由有限步构成的一般算法 (algorithm) 判断一个丢番图方程是否可解？

1970年，Yuri Matiyasevic 前苏联：不存在这样的算法！

因此②很难。今天我们看①。（也很难）

$$\boxed{\text{有理系数多项式方程(组)什么时候在 } \mathbb{Q} \text{ 中有解？}}$$

牵涉的方向：
- 数论：$\mathbb{Z}$，$\mathbb{Q}$，数域（$\mathbb{Q}$ 的有限~~维~~次数扩张）
- 代数几何：多项式方程所定义的几何对象（例：$x^2+y^2=1$ 圆）
- 算术代数几何

一些著名的例子：

“几何决定算术”

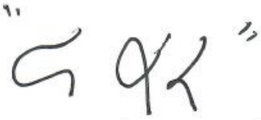
$\mathbb{P}^2_{\mathbb{C}}$ $(x:y:z)$ 复射影平面

给定一个齐次多项式 $P(x,y,z)$ degree $=d$.

$$C=\{(x:y:z)\in\mathbb{P}^2_{\mathbb{C}} \mid P(x,y,z)=0\}$$ 射影曲线（复维数 1）

Riemann surface 黎曼面（实维数 2）

亏格 是它的一个几何量。
genus



Formula If C is smooth then genus $g(C)=\frac{1}{2}(d-1)(d-2)$.

From now on assume that C is smooth.

Rk. (1) 这可以作为光滑曲线亏格的定义。

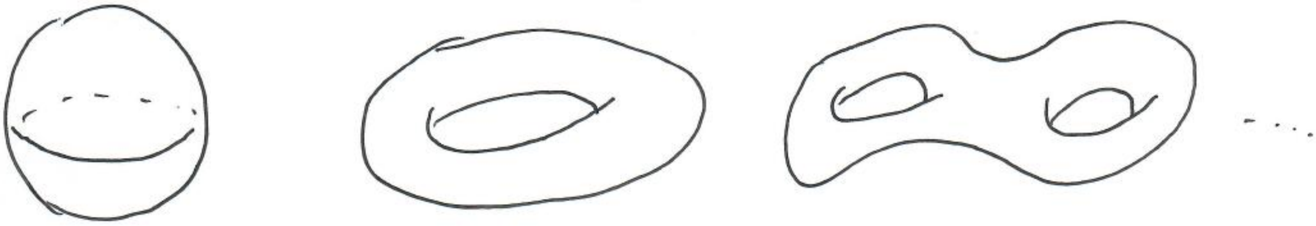
(2) 但这不是一个好的定义。亏格作为一个“几何量”应该是内蕴(intrinsic)的。同构的曲线应该有一样的亏格。但“degree”=方程的次数，同构的曲线对应的方程并不一样，~~[illegible]~~没有理由认为次数相同。

(3) "内蕴" intrinsic 的定义在是 C 的某个上同调群的维数.

(从几何体本身出发去定义, 而不是从方程出发去定义)

$$\cancel{\dim}\ g(C) = \dim_{\mathbb{C}} H^1(X, \mathcal{O}_X)$$

几何直观: 黎曼面 / (代数)射影曲线



亏格 $g = 0$. 1 . 2 .

算术性质: 当定义 C 的多项式 $P(x,y,z)$ 的系数在 $\mathbb{Q}$ 中时,

多项式 P 是否有有理数解?

~~例 Thm Fermat 大定理 (Wiles) 1993.~~ ~~$P(x,y,z) = x^n + y^n - z^n$ 没有非平凡解!~~

以下为

几何决定算术的三个定理:

神奇之处在于 输入 是一个几何量. g. 亏格. 是 P 的所有复数解(组成一个复流形 —— 黎曼面.) 的一个纯几何的不变量.

而输出 的结论是关于 P 在 $\mathbb{Q}$ 中解方程的可能性!

~~Thm 1. $g(C) = 0$ 而且 C 有一个有理点(即 P 有一个有理数解)~~

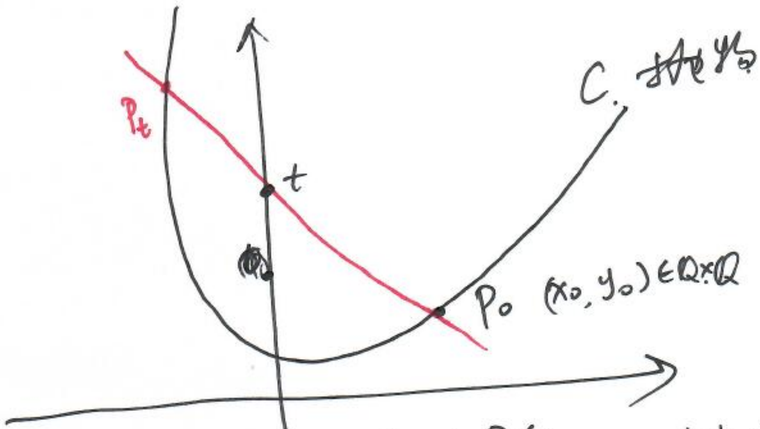
猜想

<u>Thm 1</u>. $g(C)=0$ and if C has one rational point
(i.e. P has a solution in $\mathbb{Q}$)

Then C has as many as rational points as $\mathbb{P}^1$

<u>Rk.</u> In particular, the number of rational points is infinite.

<u>proof</u>. $g=0 \Leftrightarrow d=2$. 二次曲线/圆锥曲线 $\begin{cases} \text{抛物线} \\ \text{椭圆} \\ \text{双曲线.} \end{cases}$



Fix a rational point P_0 of C.

任取 y轴上一个有理数点 t.

连直线 tP_0

代数几何里的 <u>Bézout 定理</u>: 复数域上 直线(一次曲线)与二次曲线在射影平面内相交~~的有~~的交点数 $= 2\times 1 = 2$.

C 与 相交得 P_t 与 P_0

$$\left.\begin{array}{l} t\in\mathbb{Q} \\ P_0(x_0,y_0)\in\mathbb{Q}\times\mathbb{Q} \end{array}\right\} \Longrightarrow \text{直线斜率} \in \mathbb{Q}$$

$\xRightarrow[\text{(有理系数)}]{\text{代入方程P}}$ P_t 的坐标 $\in\mathbb{Q}$.

即 P_t 是 C 的一个有理点

$$\text{(y轴)}\ \mathbb{P}^1 \longrightarrow C \quad \text{是一个双射.}$$
$$t \longmapsto P_t$$

#.

Thm 2 (Mordell–Weil). $g(C)=1$, if C has one rational point.

Then the set of rational points of C is a finitely generated abelian group.

Rk. (1) Mordell 证明 $\mathbb{Q}$ 上成立

(2) Weil 证明：一般数域上也成立 (finite extension of $\mathbb{Q}$, e.g. $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$)

(3) In this case, we say that C is an elliptic curve.

Weierstrass equation: C is isomorphic to $y^2 = x^3+ax+b$, $\Delta = 4a^3+27b^2 \neq 0$.

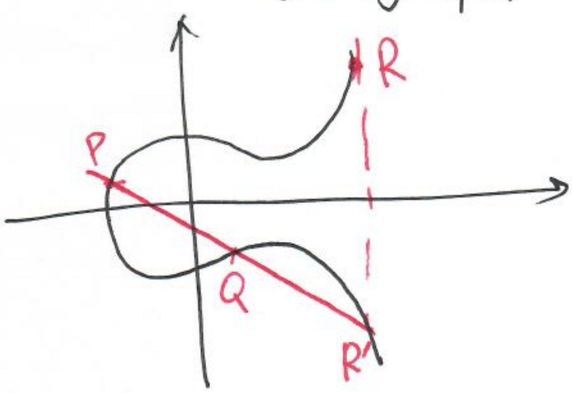
$zy^2 = x^3+axz^2+bz^3$, $(0:1:0) \in$ 曲线.

(4) the number of rational points can be finite or infinite.

~~但我们可以 Structure thm of finitely generated abelian~~

(5) the set of rational points $C(\mathbb{Q})$ (or $C(K)$, K number field) is an abelian group!

$y^2 = x^3+ax+b$.



C degree 3 curve

Bezout $\Rightarrow$ intersection $= 3$ points

$P+Q := R$. check that this is a group!

commutative group.

$O = (0:1:0)$

无穷远点.

(6) Structure thm for finitely generated abelian group:

$C(\mathbb{Q}) \cong \underset{\text{finite gp.}}{F} \oplus \mathbb{Z}^r$

BSD conjecture: (Clay 数学所 千禧年问题之一)

$r = \mathrm{ord}_{s=1} \underbrace{L(C,s)}$

L function of the elliptic curve.

亚纯

(7) The proof uses Fermat's descent method. 费马递降法.

and height function (高度) to measure the complexity of rational points.

<u>Thm 3</u> (Faltings) $g(C) \geq 2$ Then $C(\mathbb{Q})$ (or $C(K)$) is finite.

C has at most finitely many rational points.

→ Fields medal 1986

The proof uses Faltings' height. → 袁新意 2019年5月在科大的短课程.(科大网络课堂有视频).

几何
⇓
算术

$g = 0$

$|C(\mathbb{Q})| = \infty$.

$g = 1$

$C(\mathbb{Q})$ finitely generated abelian group.

$g \geq 2$

$|C(\mathbb{Q})| < \infty$

Fermat's last Theorem (Wiles 1993)

$C: \quad x^n + y^n = z^n \quad n \geq 3$ has no non-trivial solution.

$n = 3, 4$ proved by Fermat.

$n = 5$. $g = \frac{1}{2}(n-1)(n-2) \geq 2$. Faltings ⇒ only finitely many solution!

Wiles ⇒ no non-trivial solution! much stronger!

proof uses $\begin{cases} \text{elliptic curve} \\ \text{modular form (~~number theory~~)} \\ \text{galois representation.} \end{cases}$

§2. How to study rational solutions of polynomials?

K = number field = finite extension of $\mathbb{Q}$

$X_{/K}$ = algebraic variety = a set of polynomials with coeff. in K

$\forall$ field extension L/K $\quad X(L)$ = the set of solutions in L of the polynomials.

= set of rational points

Suppose that X is smooth (i.e. $X(\mathbb{C})$ is a smooth complex manifold)

example: X defined by $P(x,y) = x^2+y^2+1$ over $k=\mathbb{Q}$.

~~$X(\mathbb{Q})=\phi$, $X(\mathbb{R})=\phi$, $X(\mathbb{C})\neq\phi$.~~

$X(\mathbb{C}) \neq \phi \qquad \mathbb{C}$: algebraically closed.

$X(\mathbb{Q}) = \phi$ why? Since $X(\mathbb{R}) = \phi$.

$$\text{real analysis} \Rightarrow \begin{cases} x^2 \geq 0 \\ y^2 \geq 0 \end{cases} \Rightarrow X(\mathbb{R}) = \phi. \xRightarrow{\boxed{\mathbb{Q}\subseteq\mathbb{R}}} X(\mathbb{Q})=\phi$$

advantage of $\mathbb{R}$: ① can do real analysis (i.e. can take limit. complete
Cauchy sequences are convergent)

② $\mathbb{R}$ is not far from $\mathbb{Q}$.

$\mathbb{Q} \subseteq \mathbb{R}$ is dense

$\mathbb{R}$ solutions may be approximated by $\mathbb{Q}$ solutions.

①+②: $\mathbb{R}$ is a completion of $\mathbb{Q}$.

Natural question: other completions?

$d_\infty(a,b)=$

$\mathbb{Q}$, $a,b\in\mathbb{Q}$. $|a-b|_\infty := |a-b| \leftarrow$ absolute value $\cancel{d_\infty(a,b)}$ is a distance on $\mathbb{Q}$

① $d(a,b)\geq 0\ \forall a,b$; $d(a,b)=0$ iff $a=b$.

② $d(a,b)=d(b,a)$

③ $d(a,b)+d(b,c)\geq d(a,c)$

$$\xrightarrow{\text{Completion.}} \mathbb{R}$$

add limits of all Cauchy sequence

Define a new distance:

$p\in\mathbb{Z}$ prime number.

$\forall n\in\mathbb{Z}$. $v_p(n):=r$ if $p^r | n$ but $p^{r+1}\nmid n$.

$\forall \frac{m}{n}\in\mathbb{Q}$ $v_p\left(\frac{m}{n}\right):=v_p(m)-v_p(n)$ well-defined.

$$\left|\frac{m}{n}\right|_p := p^{-v_p\left(\frac{m}{n}\right)}$$

$$d_p\left(\frac{m_1}{n_1},\frac{m_2}{n_2}\right):=\left|\frac{m_1}{n_1}-\frac{m_2}{n_2}\right|_p$$

①✓ ②✓, ③': $d_p(a,c)\leq \max\left(d_p(a,b),d_p(b,c)\right)$

$\Rightarrow$ ③

p-adic distance.

p进

example $p=3$

$n_1=36=3^2\times 2^2$ $v_p(n_1)=2$, $|n_1|_p=\frac{1}{9}$ 中

$n_2=3$ $v_p(n_2)=1$, $|n_2|_p=\frac{1}{3}$ 大

$n_3=27=3^3$ $v_p(n_3)=3$, $|n_3|_p=\frac{1}{27}$ 小

$$\mathbb{Q} \xrightarrow[|\cdot|_p]{\text{Completion}} \mathbb{Q}_p \qquad \mathbb{Q} \underset{\text{dense}}{\subseteq} \mathbb{Q}_p$$

can do p-adic analysis on $\mathbb{Q}_p$.

<u>Thm</u> (Ostrowski 1916) Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_p$ or $|\cdot|_\infty$.

$\Rightarrow$ We <u>should</u> consider $\mathbb{R}$ and all $\mathbb{Q}_p$.

分析表述

$$\begin{cases} \mathbb{Q} \xrightarrow{\text{Completion}} \mathbb{Q}_p = \{p\text{-adic numbers}\} \\ \mathbb{Z} \longrightarrow \mathbb{Z}_p = \{p\text{-adic integers}\} \end{cases}$$

代数表述：

$\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$, $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$ fraction field

~~代数表述~~ $\underbrace{\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}}_{:= \{(a_n)_{n \geq 1} \ a_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t. } a_n \bmod p^n = a_{n+1} \bmod p^n \ \forall n \geq 1\}} \subseteq \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$ $\boxed{\mathbb{Q}_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q}.} = \mathrm{Frac}(\mathbb{Z}_p)$

Consider ~~$\mathbb{Z}_p$-solut~~ solutions in $\mathbb{Z}_p$ or in $\mathbb{Q}_p$.

$\mathbb{Z}_p$-solutions $\underset{\text{more or less}}{=}$

~~solut~~
mod p solutions
mod p^2 solutions
$\vdots$
mod p^n solutions.

p-adic analysis :

Hensel's Lemma :

$f(x) \in \mathbb{Z}[x]$, $k \in \mathbb{N}$, $r \in \mathbb{Z}$ s.t. $f(r) \equiv 0 \mod p^k$

(i.e. $|f(r)|_p \le \frac{1}{p^k}$)

$m \in \mathbb{N}$, $m \le k$

If $f'(r) \not\equiv 0 \mod p$ (i.e. $|f'(r)|_p = 1$)

Then $\exists\, s \in \mathbb{Z}$ st. $\begin{cases} f(s) \equiv 0 \mod p^{k+m} & (\text{i.e. } |f(s)|_p \le \frac{1}{p^{k+m}}) \\ s \equiv r \mod p^k & (\text{i.e. } |s-r|_p \le \frac{1}{p^k}) \end{cases}$

Moreover, s is unique mod p^{k+m}.

$\hookrightarrow$ f has a mod p^k solution $\xRightarrow[f \text{ is "good"}]{}$ f has a mod p^{k+m} solution.

$\to$ get mod p, mod p^2, $\cdots$ mod $p^n \cdots$ solution

$\to$ get $\mathbb{Z}_p$-solution.

(~~母~~ 数学分析：牛顿迭代，求收敛的极限) 几何： $\left.\begin{array}{l} f(x)=0 \\ f'(x)\neq 0 \end{array}\right\}$ 对应 Jacobi矩阵的性质 . 光滑性.

Geometric version :

If X is smooth mod p, then $X(\mathbb{F}_p) \neq \phi \Rightarrow X(\mathbb{Z}_p) \neq \phi$
$X(\mathbb{Q}_p)$?

$\hookrightarrow$ good reduction mod p.

Rk (1) $X(\mathbb{F}_p)$ is "easy" to compute (by computer!)

(2) Hensel's lemma says : easy to get $\mathbb{Q}_p$-solution

if X has good reduction mod p

(3) X has good reduction mod p for all but finitely many p.

<u>example</u> X defined by $P(x,y) = x^2 + 45y^2 - 75$

has good reduction mod p if $p \neq \cancel{0}\, 3, 5$.

$p = 3$ or 5 : ~~X mod~~ X mod p is ~~def~~ defined by $x^2 = 0$. mod p.

double point, not smooth.

§3. global and local in number theory.

— global field

— local fields

(different topology).

in geometry.

locally looks the same

$\boxed{\text{Why call it local}}$

In alg. geo. $\mathrm{Spec}(\mathbb{Z})$ global geom. object. prime ~~md~~ numbers are points on $\mathrm{Spec}(\mathbb{Z})$. each p is a "local object".

globally different. $g = 0$, $g = 1$.

In number theory

$\exists\ \mathbb{Q}$ solutions (global solutions) $\Rightarrow$ $\exists\ \mathbb{Q}_p$, $\mathbb{R}$ solutions (local solutions)

$\overset{?}{\Leftarrow}$ Question

~~Question~~

$\Omega = \{\text{primes}\} \cup \{\infty\}$, $\mathbb{Q}_\infty = \mathbb{R}$.

Def. Hasse principle holds if $X(\mathbb{Q}_p) \neq \phi\ \forall p \in \Omega \Rightarrow X(\mathbb{Q}) \neq \phi$.
(Local-global principle) ~~$X(\mathbb{R}) \neq \phi$~~

<u>Thm</u> (Hasse-Minkowski) If X is defined by quadratic form, then ~~Hasse~~ local-global principle holds for X.

<u>Rk</u>. (1) Hasse proved it for $\mathbb{Q}$. Minkowski for a general number field.

(2) An elementry proof $\rightarrow$ J.P.Serre « A Course in Arithmetic ».

(3) We ~~will~~ are going to give a "proof" for a special case.

X defined by
$$P(x,y,z) = \underbrace{x^2 \pm ay^2 \pm bz^2}_{\text{quadratic form.}} \qquad a, b \in \mathbb{Q}^*$$

<u>Def</u> (Hilbert Symbol) $K/\mathbb{Q}$ field extension.

$$(a,b)_K := \begin{cases} 1 & \text{if } X(K) \neq \phi \\ -1 & \text{if } X(K) = \phi. \end{cases}$$

<u>Notation</u>:
$$(a,b)_p := (a,b)_{\mathbb{Q}_p}$$
$$(a,b)_\infty := (a,b)_{\mathbb{R}}$$
$$(a,b) := (a,b)_{\mathbb{Q}}$$

Want to prove <u>Hasse principle</u>: $\boxed{\left.\begin{array}{l} (a,b)_p = 1 \quad \forall p \\ (a,b)_\infty = 1 \end{array}\right\} \Rightarrow (a,b) = 1.}$

Before ~~the~~ to prove, get a feeling of local and global in Number theory.

<u>Question</u>: for each $p \in \Omega$ ~~(and ∞)~~ fix $n_p \in \{\pm 1\}$.

Does there exist $a, b \in \mathbb{Q}^*$ s.t. $(a,b)_p = n_p \ \forall p$, $(a,b)_\infty = n_\infty$?

Necessary conditions: (a local condition and a global condition)

Thm. For any $a, b \in \mathbb{Q}^*$

(C1) $(a,b)_p = 1$ for almost all p. (local property, follows from Hensel's lemma for good reduction primes)

(C2) product formula. $\prod_{p \in \Omega} (a,b)_p = 1$. (① "$\prod$" makes sense since (1) ② global property: the values $(a,b)_p$ are not independant they have at least this relation $\prod (a,b)_p = 1$ ③ this follows from quadratic reciprocity law of Gauss 二次互反律)

We reduce Question 1 to

Question 2: Are these conditions C1, C2 sufficient conditions for Question 1 ?

We are going to answer to Q2 and prove the Hasse principle for X.

Def. K field, a K-algebra A is a ring A containing K. $K \subseteq A$. (in particular, A has identity element $1_A = 1_K$)

A may be non-commutative.

~~From now on suppose that~~ $\dim_K A < \infty$ ~~(viewed as a K-vector space)~~

(i.e. K-algebra = ring + K-vector space structure. all operations are compatible)

Suppose that $\dim_K A < \infty$ from now on.

We say that A is a simple algebra if it has no non-trivial

A is a <u>central simple algebra</u> if $\mathrm{center}(A) = K$.

example: $A = M_n(K)$ $n\times n$ matrices

<u>Prop</u>. A: K-algebra. TFAE.

(1) A is a central simple algebra

(2) $A \otimes_K K^s \underset{K^s\text{-alg}}{\cong} M_n(K^s)$ (K^s ~~alg~~ separable closure)

(3) $\exists$ finite extension L/K s.t. $A \otimes_K L \underset{L\text{-alg}}{\cong} M_n(L)$ (之后再讲到)

~~representation~~ ~~(4) (Wedderburn) $A \cong M_m(D)$ where D is a division algebra.~~ ~~representation theory of algebras~~ 之后讲

<u>Rk</u>: (1) $\otimes$ = tensor product (homological algebra, commutative algebra)

coefficient $\in K$. $\rightsquigarrow$ in L (L/K)

e.g. $M_n(K) \otimes_K L = M_n(L)$ for matrix algebra.

(2) central simple algebra $\underset{\substack{\uparrow \\ \text{after a finite seperable extension}}}{\overline{\overline{\text{more or less}}}}$ matrix algebra.

It is a "<u>twist</u>" of the matrix algebra

<u>example</u>: $\mathbb{H}$: Hamilton's quaternion algebra over $K = \mathbb{R}$

As K-vector space $\mathbb{H} = 1\cdot K \oplus i\cdot K \oplus j\cdot K \oplus k\cdot K$

basis $\{1, i, j, k\}$ coef $\in K = \mathbb{R}$

product in $\mathbb{H}$ is given by $i^2 = -1$, $j^2 = -1$, $ij = -ji = k$.

<u>Prop</u> $\mathbb{H}$ is a division algebra (i.e. non-zero elements are invertible)

<u>proof</u>: Norm map $N: \mathbb{H} \to \mathbb{R}$

$q = x + yi + zj + tk$, $\quad x, y, z, t \in \mathbb{R}$.

$$N(q) = q \cdot \bar{q} = (x+yi+zj+tk)(x-yi-zj-tk)$$

$$= \cdots$$

$$= x^2+y^2+z^2+t^2 \in \mathbb{R}$$

$$q \neq 0 \Leftrightarrow \text{one of } x, y, z, t \neq 0 \underset{\substack{\uparrow \\ x,y,z,t \in \underline{\underline{\mathbb{R}}}}}{\Leftrightarrow} \underset{\substack{\| \\ N(q)}}{x^2+y^2+z^2+t^2} \neq 0$$

$$\Leftrightarrow \quad q^{-1} = \frac{\bar{q}}{N(q)} \qquad \#.$$

<u>Rk.</u> The proof use the fact that $\overset{\text{coefficients}}{x, y, z, t} \in \mathbb{R}$.

after tensor with $\mathbb{C}$. coeff $\in \mathbb{C}$, the same proof fails!

Indeed.

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$$

$$1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i \longmapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$

$$j \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$k \longmapsto \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$$

($\Rightarrow$ $\mathbb{H}$ is a twist of the matrix algebra.
i.e. a central simple algebra)

<u>Rk</u> in $M_2(\mathbb{C})$ not all non-zero elements are invertible.

Norm map $\otimes_{\mathbb{R}} \mathbb{C} \rightsquigarrow \det$.

Generalization. $a, b \in K^\times$.

$$Q_{a,b} := 1\cdot K \oplus i\cdot K \oplus j\cdot K \oplus k\cdot K \quad \text{as vector space.}$$

$$\begin{aligned} i^2 &= a \\ j^2 &= b \\ ij &= -ji = k. \end{aligned}$$

$Q_{a,b}$: quaternion algebra.

Thm (Wedderburn) ($\leftarrow$ representation theory for finite dimensional semi-simple algebras.)

$Q_{a,b}$ is either ① a division algebra

or ② isomorphic to $M_2(K)$ (② definition split)

relation with solution over $K = \mathbb{Q}, \mathbb{Q}_p, \mathbb{R} \cdots$.

Thm TFAE.

(1) ~~x^2+a~~ $P(x,y,z) = x^2 - ay^2 - bz^2$ has non-trivial solution in K

(2) $(a,b)_K = 1$

(3) $Q_{a,b}$ splits over K.

[key point: norm map ~~$N(x+a$~~ $N(x+yi+zj) = x^2 - ay^2 - bz^2$]

Question 2 $\Longleftrightarrow$ " $Q_{a,b}$ splits over $\mathbb{Q}_p\ \forall p$, $\mathbb{R}$ $\} \Longrightarrow Q_{a,b}$ splits over $\mathbb{Q}$? "

Now we can use powerful tools from algebra. ~~(and number~~

(actually, form algebraic number theory)

Brauer group :

Def. $\mathrm{Br}K = \{\text{central simple algebra over } K\} / \sim$

$\sim$: equivalent relation. $A \sim B \overset{\text{def.}}{\Longleftrightarrow} \exists\, m, n \in \mathbb{N}$ st. $M_n(A) \cong M_m(B)$ as K-algebra.

$\left(\text{e.g. } A = M_r(K) \sim B = K \quad \text{take } n=1,\ m=r. \right)$

$\mathrm{Br}K$ is an abelian group. (Brauer group of K)

product : $A \otimes_K B$

identity elemt : K, $\quad A \otimes_K K \cong A$.

inverse : $A \otimes_K A^{op} \cong M_n(K) \sim K$.

$\left(A^{op} = \text{opposite ring of } A \text{ 反环 i.e. } \underset{\text{in } A^{op}}{a \cdot b} := ba \text{ in } A \right)$

Now quaternion algebras are central simple algebras, they are elements in $\mathrm{Br}K$.

$Q_{a,b} \in \mathrm{Br}K$. $\quad$ ($Q_{a,b} \in {}_2\mathrm{Br}K$ 2-torsion part)

Thm (Global class field theory — algebraic number theory)

$$0 \to \mathrm{Br}\mathbb{Q} \xrightarrow{\varphi} \mathrm{Br}\mathbb{R} \oplus \left(\bigoplus_p \mathrm{Br}\mathbb{Q}_p \right) \xrightarrow{\psi} \mathbb{Q}/\mathbb{Z} \to 0 \qquad (*)$$

is an exact sequence.
正合列

Tate's thesis (harmonic analysis over local fields and number fields)

homological method (~~g~~ cohomology of groups, galois cohomology)

Rk. (1) class field theory is a generalization of Gauss' reciprocity law.
(Takagi. E. Artin)

(2) try to generalise class field theory → $\boxed{\text{Langlands program.}}$

GL_1 (abelian) ⇝ GL_n ⇝ reductive algebraic groups

galois representation $\xleftrightarrow{1:1}$ automorphic representation

(rep. of Galois gp) (rep. of algebraic groups)

Lie gp. / Lie algebra acting on the space of modular forms / automorphic forms.

Back to Thm

$$\mathrm{Br}\,\mathbb{R} \xrightarrow{\mathrm{inv}_{\mathbb{R}}} \mathbb{Q}/\mathbb{Z}$$

$$\mathrm{Br}\,\mathbb{Q}_p \xrightarrow{\mathrm{inv}_p} \mathbb{Q}/\mathbb{Z}$$

$$Q_{a,b} \longmapsto \begin{cases} 0 \bmod \mathbb{Z}, & \text{if } Q_{a,b} \text{ splits in } \mathbb{Q}_p, \quad (a,b)_p = 1 \\ \frac{1}{2} \bmod \mathbb{Z}, & \text{otherwise}, \quad (a,b)_p = -1 \end{cases}$$

product formula $\prod_{p \in \Omega} (a,b)_p = 1 \Rightarrow$ (*) is a complex. i.e. $\psi \circ \varphi = 0$ (for the 2-torsion part)

~~exactness~~ exactness at the middle : $\ker(\psi) = \mathrm{im}(\varphi)$ means:

$n_p \in \{\pm 1\}$, almost all v, and $\prod_{p \text{ or } \infty} n_p = 1$
n_∞

then $(n_p)_{p \in \Omega} \in \ker(\psi)$.

$\Rightarrow \exists\, (a,b) \in \mathrm{Br}\,K$ st. $(a,b)_p = n_p \quad \forall p$ prime or ∞.

This answers to Question 2.

exactness ~~at~~ on the left means φ is injective:

$(a,b)_p = 1 \quad \forall p \in \Omega \Rightarrow (a,b) = 1.$

~~$(a,b)_\infty = 1$~~

i.e. Local-global principle holds for X (defined by $P(x,y,z) = x^2 - ay^2 - bz^2 = 0$)

§4. failure of Hasse principle

quadratic form ✓.

cubic form ✗

Selmer: X defined by $P(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$

has solutions in all $\mathbb{Q}_p$ and $\mathbb{R}$,

but no solution in $\mathbb{Q}$.

Another easy counter example:

X: $P(x) = (x^2 - 13)(x^2 - 17)(x^2 - 13 \times 17)$

$13, 17, 13 \times 17$ are not squares $\Rightarrow X(\mathbb{Q}) = \phi$.

$X(\mathbb{R}) \neq \phi \quad x = \sqrt{13}$ ✓.

$2^2 = 17 \mod 13 \Rightarrow X(\mathbb{F}_{13}) \neq \phi \xRightarrow{\text{Hensel}} X(\mathbb{Q}_{13}) \neq \phi$

$8^2 = 13 \mod 17 \Rightarrow X(\mathbb{F}_{17}) \neq \phi \xRightarrow{\text{Hensel}} X(\mathbb{Q}_{17}) \neq \phi$.

for $p \neq 13, 17$. Legendre symbol $\underbrace{\left(\frac{13}{p}\right)} \cdot \underbrace{\left(\frac{17}{p}\right)} = \underbrace{\left(\frac{13 \cdot 17}{p}\right)}$ ~~can not~~ one of these must be 1.

$\Rightarrow X(\mathbb{F}_p) \neq \phi$ [illegible]

§5 Weak approximation.

existence of solution, $\rightsquigarrow$ how many solution.

$$X(\mathbb{Q}) \subset \prod_{p \in \Omega} X(\mathbb{Q}_p)$$

~~($p=\infty$, $\mathbb{Q}_\infty = \mathbb{R}$)~~

product topology

Weak approximation for X : $X(\mathbb{Q})$ dense in $\prod X(\mathbb{Q}_p)$.

means many $\mathbb{Q}$-solutions.

example. $X = \mathbb{P}^1$ weak approx $\Longleftrightarrow$ chinese remainder theorem.

it may fail : X: $x^2 - 2y^2 = -(z^2+3)(z^2-3)$ $/\mathbb{Q}$.

$$\underset{(x,y,z)=(3,0,0)}{\phi \neq X(\mathbb{Q})} \subsetneq \prod_{p \in \Omega} X(\mathbb{Q}_p)$$

($\mathbb{Q}_3$ 와 Br obs)

§6. Brauer-Manin obstruction

Aim: to explain the failure of Hasse principle and Weak approximation

Brauer group $Br(K)$ central simple algebra.

$\wr$ $\wr$

Azumaya algebra

$Br(X)$ (a certain "sheaf of algebra" over X)

X = algebraic variety

scheme. (algebraic geometry, Grothendieck) the Azumaya alg. definition is not a good definition.

Grothendieck $\overset{\text{developed}}{\leadsto}$ étale cohomology

$$\mathrm{Br}(X) := \underset{\substack{\uparrow \\ \text{use étale topology on } X.}}{H^2_{et}}(X, \underset{\substack{\uparrow \\ \text{sheaf on } X}}{\mathbb{G}_m})$$

This is good: functorial. 函子性 (Category language 范畴论的抽象语言).

i.e. $X \xrightarrow{f} Y$ map (morphism) $\overset{\text{induces}}{\leadsto}$ $f^*: \mathrm{Br}(Y) \to \mathrm{Br}(X)$

algebraic geometry language: $X(k) = \mathrm{Hom}(\mathrm{Spec}\,k, X)$

rational points are maps between certain geometric objects!

$x \in X(k)$

$x: \mathrm{Spec}\,k \to X$

induces $x^*: \mathrm{Br}\,X \longrightarrow \mathrm{Br}\,k$.

$b \longmapsto x^*(b) =: b(x)$

Yu. I. Manin (1970 ICM 国际数学家大会)

$$\mathrm{Br}\,X \times \prod_{p \in \Omega} X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

$$b, \quad (x_p)_{p\in\Omega} \longmapsto \sum_p \mathrm{inv}_p(b(x_p))$$

$$0 \to \underset{\text{global}}{\mathrm{Br}\,\mathbb{Q}} \to \underset{\text{local.}}{\bigoplus_{p\in\Omega} \mathrm{Br}(\mathbb{Q}_p)} \to \mathbb{Q}/\mathbb{Z} \to 0$$

$\Rightarrow$ global things are 0 in $\mathbb{Q}/\mathbb{Z}$

$$X(\mathbb{Q}) \subset \overline{X(\mathbb{Q})} \subset \underbrace{\left[\prod_p X(\mathbb{Q}_p)\right]^{Br}}_{\text{closed.}} \subsetneq \prod_p X(\mathbb{Q}_p)$$

$$\left[\prod_p X(\mathbb{Q}_p)\right]^{Br} = \{(x_p)_{p\in\Omega} \mid (x_p) \perp b \ \forall b \in \mathrm{Br}X\}$$

Rk

(1) $\subsetneq$ ⟹ weak approximation fails!

(2) $\left[\prod_p X(\mathbb{Q}_p)\right]^{Br} = \phi \implies X(\mathbb{Q}) = \phi$ even if $\prod_p X(\mathbb{Q}_p) \neq \phi$.

Local-global principle fails!

This is called the <u>Brauer–Manin obstruction</u>

This explains ~~many~~ failure of local-global principle / weak approx.
for many algebraic ~~variety~~ varieties.

<u>example</u>. ~~elli~~ genus 1 curves. (e.g. $C: 3x^3 + 4y^3 + 5z^3 = 0$)

$E = \mathrm{Jac}(C)$ Jacobian variety of C.
↳ elliptic curve.

obstruction lies in $Ш^1(E^\vee) \in \mathrm{Br}(E^\vee)$ $(E^\vee = \text{dual of } E)$
Tate–Shafarevich group.

<u>Conjecture</u> (Colliot-Thélène et al.)

For <u>rationally connected varieties</u>, the Brauer–Manin obstruction controls the failure of Hasse principle and weak approximation.

(1) Rationally connected: 有理连通. geometric condition.:

$X(\mathbb{C})$: complex manifold. every 2 points can be connected by a projective line.

$\forall P_1, P_2 \in X(\mathbb{C})$. $\exists f: \mathbb{P}^1_{\mathbb{C}} \to X$ algebraic morphism.

s.t. $f(0) = P_1$ and $f(1) = P_2$ (stronger than path connected) 道路连通.

(actually. $RC \Rightarrow \pi_1^{et}(X) = 0$. simply connected)

(2) This conjecture is of the style: geometry determines arithmetic.

(3) Conj $\Rightarrow$ inverse galois problem.:

$\forall G$ finite gp, $\exists K/\mathbb{Q}$ finite galois extension s.t.:

$$\mathrm{Gal}(K/\mathbb{Q}) = G.$$

[it suffices to prove the conj. for X = smooth compactification of SL_n/G]

(4) for non-rationally connected varieties,

$\exists$ counter examples by Skorobogatov 90's

Poonen 2000's

(5) further obstructions?

Summary

$$X(\mathbb{Q}) \ \frac{\text{local-global}}{\text{obstructions.}} \ \forall p.\ X(\mathbb{Q}_p) \ \frac{\text{Hensel's lem}}{} \ X(\mathbb{F}_p)$$