Ganze Punkte auf algebraischen Mannigfaltigkeiten

Jean-Louis Colliot-Thélène (CNRS et Université Paris-Sud)

Kolloquiumsvortrag
Universität des Saarlandes
Im Rahmen des Deutsch-Französischen Diskurses
Saarbrücken, den 26. April 2013

Zusammenfassung :
Seien a, b, c ganze Zahlen. Wenn man für jede ganze Zahl $m > 0$ eine Lösung (x, y, z) in ganzen Zahlen zur linearen affinen Gleichung $ax + by = c + mz$ finden kann, dann kann man auch eine Lösung in ganzen Zahlen (x, y) für die Gleichung $ax + by = c$ finden. Gibt es ähnliche Sätze, oder zumindestens Ersätze, wenn man Gleichungen höheren Grades in mehreren Variabeln betrachtet ?

Affine lineare Abbildungen

Seien $L_i(x_1, \ldots, x_n)$, $i = 1, \ldots, r$ lineare Formen mit ganzen Koeffizienten, und seien c_i, $i = 1, \ldots, r$ ganze Zahlen.
Wenn für alle $m > 0$ die Gleichung

$$L_i(x_1, \ldots, x_n) = c_i$$

modulo m lösbar ist, dann hat sie eine Lösung $\mathbf{b} \in \mathbb{Z}^n$.
Ferner, sei $\mathbf{b}_m \in \mathbb{Z}^n$ eine Lösung modulo $m > 0$. Nehmen wir an, man kann für jede ganze Zahl $M > 0$ eine Lösung $\mathbf{b}_{mM}$ modulo mM finden, die mod m mit $\mathbf{b}_m$ übereinstimmt. Dann gibt es eine Lösung $\mathbf{b} \in \mathbb{Z}^n$ mit der Eigenschaft $\mathbf{b} \equiv \mathbf{b}_m$ mod m.

Aufpassen : $2x = 4$ hat eine Lösung in $\mathbb{Z}$, keine Lösung aber, die die Lösung $x \equiv 1 \bmod 2$ induziert.

Allgemein betrachtet man ein System von Gleichungen

$$P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

in dem die P_i Polynomen von beliebigen Grade sind, und mit ganzen Koeffizienten, und man fragt, ob es eine Lösung $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ gibt.
Eine notwendige Bedingung ist das Bestehen von Lösungen $(x_1, \ldots, x_n) \in \mathbb{R}^n$.
Eine Reihe von notwendigen Bedingungen :
Für jede ganze Zahl $m > 0$ kann man das System modulo m lösen.
Dafür reicht es, daß man das System modulo jede Potenz p^s, (p Primzahl) lösen kann.

Nehmen wir an, daß diese “lokalen” notwendigen Bedingungen erfüllt sind. Man sagt, starke Approximation gilt für das System

$$P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r,$$

wenn man für jede ganze Zahl $m > 0$ und jede Familie $(b_1, \ldots, b_n) \in \mathbb{Z}^n$, welche die obigen Gleichungen modulo m erfüllt, und welche für jede M die Reduktion modulo mM von einer Lösung modulo mM ist, eine Lösung $(c_1, \ldots, c_n) \in \mathbb{Z}^n$ vom obigen System finden kann, die congruent $(b_1, \ldots, b_n)$ modulo m ist.

Schematen

Ein System

$$P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

definiert eine affines Schema $\mathcal{X}$ von endlichen Typ über dem Ring $\mathbb{Z}$.
Sei A ein kommutativer Ring mit Eins. Wir schreiben $\mathcal{X}(A)$ für die Menge der Lösungen mit Koordinaten in A.
Sei $A \to B$ ein Homomorphismus von Ringen, dann hat man eine induzierte Abbildung $\mathcal{X}(A) \to \mathcal{X}(B)$.
Beispiel : $\mathbb{Z} \to \mathbb{Z}/m$, die Abbildung ist die Reduktion modulo $m > 1$.

p-adische Zahlen (Hensel)

Sei p eine Primzahl. Jede rationale Zahl $x \in \mathbb{Q}^\times$ kann man schreiben als $x = p^{n_p}.(u/v)$ mit $n \in \mathbb{Z}$ und u, v ganz und prim zu p.
Definition :
$abs_p(x) = 1/p^{n_p} \in \mathbb{Q}$ et $abs_p(0) = 0$.
Man hat $abs_p(xy) = abs_p(x).abs_p(y)$ und
$abs_p(x+y) \leq max(abs_p(x), abs(y)) \leq abs_p(x) + abs_p(y)$.
Also hat man eine (nicht archimedische) Metrik auf $\mathbb{Q}$.

Genau wie man den Körper $\mathbb{Q}$ bezüglich des üblichen Absolutwertes vervollständigen kann um den Körper $\mathbb{R}$ zu bekommen, so kann man $\mathbb{Q}$ bezüglich des p-adischen Absolutwertes vervollständigen. Man bekommt den Körper $\mathbb{Q}_p$. Dieser Körper ist der Fraktionskörper eines Ringes $\mathbb{Z}_p$: die Elemente dieses Ringes sind die Elemente von $\mathbb{Q}_p$ mit absolutem Wert ≤ 1.
Wir schreiben hier $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.

Übersetzungen

"Sei p eine Primzahl. Das System $P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$ kann man modulo alle p^r lösen", Übersetzung :

$$\mathcal{X}(\mathbb{Z}_p) \neq \emptyset.$$

"Das System $P_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$ kann man modulo alle ganze Zahlen $m > 0$ und in $\mathbb{R}$ lösen " , Übersetzung :

$$\mathcal{X}(\mathbb{R}) \times \prod_p \mathcal{X}(\mathbb{Z}_p) \neq \emptyset.$$

Unter der Annahme, daß dieses Produkt von topologischen Mengen nicht leer ist, dann lautet *Starke Approximation* für X so : **Das diagonale Bild von $\mathcal{X}(\mathbb{Z})$ liegt dicht in $\prod_{p \text{ Primzahl}} \mathcal{X}(\mathbb{Z}_p)$.**

Diese Begriffe kann man für alle $\mathbb{Z}$-Schemata von endlichem Typ definieren.
Mit $X = \mathcal{X} \times_{\mathbb{Z}} \mathbb{Q}$ bezeichnen wir das Schema mit den selben Gleichungen, betrachtet aber über dem Körper $\mathbb{Q}$ der rationalen Zahlen.
Falls das Schema $\mathcal{X}$ projektiv über $\mathbb{Z}$ ist, das heisst ist geschlossen in einem projektiven Raum $\mathbb{P}^n_{\mathbb{Z}}$, dann hat man $\mathcal{X}(\mathbb{Z}) = X(\mathbb{Q})$ und $\mathcal{X}(\mathbb{Z}_p) = X(\mathbb{Q}_p)$.
In diesem Fall, sind die Probleme, die wir hier besprechen, Probleme von rationalen Punkten. Der richtige Begriff hier lautet Schwache Approximation.

Die Antwort zu diesen arithmetischen Problemen hängt stark von der Geometrie der assoziierten geometrischen Räumen ab.

Existenz und Dichtigkeit von Punkten in der Menge $\mathcal{X}(\mathbb{Z})$ werden also untersucht in Bezug auf die Geometrie von $X \times_{\mathbb{Q}} \mathbb{C}$, einer Varietät über dem komplexen Körper.

Unser einführendes Beispiel

$$L_i(x_1, \ldots, x_n) = c_i$$

entspricht einer Varietät $X \times_{\mathbb{Q}} \mathbb{C}$, die enteweder leer oder isomorph zu einem affinen Raum $\mathbb{A}^n_{\mathbb{C}}$ ist.
Für $ax + by = c$ mit $(a, b) \neq (0, 0)$ erhalten wir $\mathbb{A}^1_{\mathbb{C}}$, das heißt $\mathbb{P}^1_{\mathbb{C}}$ minus ein Punkt.

Gleichungen in einer Variabel

Bei $(2x-1)(3x-1)=0$ gibt es Lösungen in allen $\mathbb{Z}_p$, nicht aber in $\mathbb{Z}$.

Bei $(x^2-13)(x^2-17)(x^2-221)$ gibt es Lösungen in allen $\mathbb{Z}_p$ und $\mathbb{R}$, nicht aber in $\mathbb{Z}$.

Elementar :
Wenn eine Gleichung $x^2+bx+c=0$ eine Lösung in allen $\mathbb{Z}_p$ und in $\mathbb{R}$ hat, dann auch in $\mathbb{Z}$.

Schwieriger : Wenn die Gleichung $x^2 + bx + c = 0$ eine Lösung in fast allen $\mathbb{Z}_p$ (d. h. in allen bis auf möglicherweise einer endlichen Anzahl) hat, dann auch in $\mathbb{Z}$, also auch in allen $\mathbb{Z}_p$.

Allgemeiner :
Satz (Chebotarev) : Wenn ein Polynom
$P(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ *irreduzibel* ist, dann gibt es eine unendliche Anzahl von Primzahlen p, so daß $P(x) = 0$ keine Lösung in $\mathbb{Z}_p$ hat.

Von jetzt an werden wir nur Schemata $\mathcal{X}$ sur $\mathbb{Z}$ betrachen, für welche gilt : $X \times_{\mathbb{Q}} \mathbb{C}$ ist *irreduzibel* und *glatt* ($=$ singularitätsfrei).

Falls $\mathcal{X}/\mathbb{Z}$ affin (d. h. geschlossene Menge in $\mathbb{A}^n_{\mathbb{Z}}$), $\mathcal{X}(\mathbb{Z}) \neq \emptyset$ und $X(\mathbb{R})$ kompakt, dann kann starke Approximation für X nicht gelten : da $\mathbb{Z}$ diskret in $\mathbb{R}$ liegt, wäre $\mathcal{X}(\mathbb{Z}) \subset X(\mathbb{R})$ endlich. Jede $X(\mathbb{Z}_p)$ ist aber unendlich.

Also, *für $\mathcal{X}/\mathbb{Z}$ affin, notwendige Bedingung für starke Approximation : $X(\mathbb{R})$ nicht kompakt.*

Grad 2, zwei Variabeln

Gleichungen $ax^2 + bxy + cy^2 = d$ mit $d.(b^2 - 4ac) \neq 0$

Geometrisch :

$\mathbb{P}^1_{\mathbb{C}}$ **minus 2 Punkte**

oder auch

$\mathbb{G}_{m,\mathbb{C}}$

$n \in \mathbb{Z}$ gegeben

Äquivalenz (Fermat, p-adisch übersetzt) :

(a) Die Gleichung $n = x^2 + y^2$ kann man in allen $\mathbb{Z}_p$ lösen.

(b) Die Gleichung $n = x^2 + y^2$ kann man in $\mathbb{Z}$ lösen.

Also : lokal-global Prinzip.

Lokale Lösungen in $\mathbb{Z}_p$ und $\mathbb{R}$, *aber* keine Lösung in $\mathbb{Z}$ für folgende (Systeme von) Gleichungen :

- $23 = x(x + 7y)$ (klar, da $\mathbb{Z}^\times = \{\pm 1\}$)
- $\{2x - 5y = 1, xt = 1\}$ (klar, da $\mathbb{Z}^\times = \{\pm 1\}$)

($\mathbb{P}^1_{\mathbb{Q}}$ mit zwei rationalen Punkten abgenommen.)

- $1 = 4x^2 + 25y^2$ (leicht, da $X(\mathbb{R})$ kompakt ist)
- $1 = 4x^2 - 475y^2$ (Beweis schwer)

($\mathbb{P}^1_{\mathbb{Q}}$ minus zwei konjugierte Punkte)

q Primzahl

Äquivalenz :

(a) $q \equiv 1 \bmod 3$

(b) für jede Primzahl p hat $q = x^2 + 27y^2$ eine Lösung in $\mathbb{Z}_p$

(c) *eine* von den beiden Gleichungen

$$q = x^2 + 27y^2$$
$$q = 4x^2 + 2xy + 7y^2$$

kann man mit $x, y \in \mathbb{Z}$ lösen.

(Euler, Lagrange)

q Primzahl. Die Gleichung $q = x^2 + 27y^2$ kann man in $\mathbb{Z}$ lösen dann und nur dann, wenn

(a) es gibt Lösungen in allen $\mathbb{Z}_p$

UND

(b) 2 ist eine dritte Potenz modulo q.

(vermutet von Euler, bewiesen von Gauß)

Grad 2, drei Variabeln

Gleichungen $q(x, y, z) = a$ mit $q \in \mathbb{Z}[x, y, z]$ quadratische Form, vom Rank 3 über $\mathbb{Q}$

Geometrisch, d. h. über $\mathbb{C}$:

Quadrik in $\mathbb{P}^3$ mit einem glatten Ebenenschnitt abgezogen

oder auch

$\mathbb{P}^1 \times \mathbb{P}^1$ mit einem diagonalen $\mathbb{P}^1$ abgezogen

oder auch

$Spin(3)/\mathbb{G}_m$

$n \in \mathbb{Z}$ gegeben
$n = x^2 + y^2 + z^2$ hat eine Lösung über $\mathbb{Z}$, dann und nur dann, wenn sie eine Lösung über jedem $\mathbb{Z}_p$ hat, was darauf ankommt, daß $n > 0$ und $n \neq 4^r(8m + 7)$.

Beispiel von Borovoi und Rudnick (Gegenbeispiel zum lokal-globalen Prinzip)
$(y-x)(9x+7y) = 1-2z^2$
Lösungen in allen $\mathbb{Z}_p$, nicht in $\mathbb{Z}$.

Beweis :
Lösungen (x,y,z) in $\mathbb{Q}$: $(-1/2, 1/2, 1)$ et $(1/3, 0, 1)$, also Lösung in jedem $\mathbb{Z}_p$.
Lösung (x,y,z) in $\mathbb{Z}_2$, dann $y-x \equiv \pm 3 \bmod 8$ (kurze Berechnung).
Nehmen wir an, es gibt eine Lösung (x,y,z) in $\mathbb{Z}$. Falls Primzahl p teilt $y-x$, dann $1-2z^2 \equiv 0 \bmod p$, also p ungerade und 2 Quadrat mod p. Also
(Zweiter Ergänzungssatz der quadratischen Reziprozitätsgesetzes)
$p \equiv \pm 1 \bmod 8$. Also $y-x \equiv \pm 1 \bmod 8$. Unmöglich.

Seien $n, m, k \in \mathbb{N}_{>0}$, $(n, m) = 1$. Die Gleichung

$$m^2x^2 + n^{2k}y^2 - nz^2 = 1$$

kann man umschreiben :

$$(1 + n^k y)(1 - n^k y) = m^2x^2 - nz^2.$$

Bei jeder solcher Gleichung gibt es Lösungen in allen $\mathbb{Z}_p$.
Unter Benutzung von Geschlechtstheorie (Gauß), F. Xu und R. Schulze-Pillot beweisen : Die Gleichung hat keine Lösung in $\mathbb{Z}$ dann und nur dann, wenn

(i) $n \equiv 5\ (8)$ und 2 teilt m
oder
(ii) $n \equiv 3\ (8)$ und 4 teilt m.

Grad 2, wenigstens 4 Variabeln

Satz (Eichler, Kneser)
Sei $q(x_1, \ldots, x_n)$ eine ganze, nicht entartete, **indefinite** *quadratische Form in $n \geq 4$ Variabeln. Die Gleichung*

$$m = q(x_1, \ldots, x_n)$$

hat eine Lösung in $\mathbb{Z}$ dann und nur dann, wenn sie eine Lösung in allen $\mathbb{Z}_p$ hat. Allgemeiner : Starke Approximation an den endlichen Stellen gilt für solche Gleichungen.

Dieses Theorem ist eng mit dem Fall $G = Spin(q)$ des folgenden Satzes verknüpft.

Satz (Kneser, Platonov). *Sei $\mathcal{X}/\mathbb{Z}$ ein affines Schema von endlichem Typ. Nehmen wir an :*
(a) $\prod_{p\cup\infty} \mathcal{X}(\mathbb{Z}_p) \neq \emptyset$
(b) $X_{\mathbb{Q}}$ ist eine halbeinfache, fast $\mathbb{Q}$-einfache, einfach zusammenhängende lineare algebraische Gruppe G.
(c) $X(\mathbb{R})$ ist nicht kompakt.
Dann gilt starke Approximation für $\mathcal{X}$:

$\mathcal{X}(\mathbb{Z})$ liegt dicht in $\prod_{p \text{ fini}} \mathcal{X}(\mathbb{Z}_p)$.

Ein allgemeiner Begriff, der viele Gegenbeispiele zum lokal-globalen Prinzip erklärt :

Das ganzzahlige Brauer-Maninsche Hindernis

Die Brauergruppe eines Schemas

Auf einer algebraischen Mannigfaltigkeit und allgemeiner auf einem Schema X sind die Vektorbündel das Analog von Vektorräumen auf einem Körper.
Azumaya Algebren auf einem Schema sind die natürliche Objekte, die zentral einfache Algebren (Vorkriegszeit Hyperkomplexe Systemen) verallgemeinern.
Auf solche Algebren kann man eine Äquivalenzrelation einführen, die die Brauer-Äquivalenz auf zentral einfachen Algebren verallgemeinert.

Tensorprodukt induziert auf die Menge der Äquivalenzklassen die Struktur einer abelschen Gruppe $\mathrm{Br}(X)$, die (Azumaya) Brauergruppe von X.
Für gute Schemata stimmt diese Gruppe mit der von Grothendieck definierte Brauergruppe überein.
Sei $\mathcal{X}/\mathbb{Z}$ ein Schema. Für jeden kommutativen Ring R hat man eine natürliche Paarung $\mathcal{X}(R) \times \mathrm{Br}(\mathcal{X}) \to \mathrm{Br}(R)$.

Klassenkörpertheorie

$$\mathrm{inv}_\infty : \mathrm{Br}\,\mathbb{R} = \mathbb{Z}/2$$
$$\mathrm{inv}_p : \mathrm{Br}\,\mathbb{Q}_p \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

Reziprozitätsgesetz für die Brauergruppe eines globalen Körpers : exakte Folge

$$0 \to \mathrm{Br}\,\mathbb{Q} \to \oplus_{p \cup \infty} \mathrm{Br}\,\mathbb{Q}_p \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Die quadratische Reziprozitätsgesetze von Gauß erhält man durch Anwendung auf die Klassen von Quaternionalgebren $(a, b) \in \mathrm{Br}\,\mathbb{Q}$.

Seien $\mathcal{X}$ ein $\mathbb{Z}$-Schema und $X = \mathcal{X} \times_{\mathbb{Z}} \mathbb{Q}$.
Aus dem Reziprozitätsgesetz für die Brauergruppe bekommt man :
Das Bild von $\mathcal{X}(\mathbb{Z})$ in $\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)$ liegt im Linkskern der (wohldefinierten) Paarung

$$\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p) \times \mathrm{Br}\,(X) \to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{inv}_p(\alpha(M_p)).$$

Auf der rechten Seite hängt die Paarung nur von der Klasse im Quotient $\mathrm{Br}\,(X)/\mathrm{Br}\,(\mathbb{Q})$ ab.
Der Linkskern, auch unter dem Namen Brauer-Maninsche Menge bekannt, wird $[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p]^{\mathrm{Br}\,(X)}$ geschrieben.

Aus $\mathcal{X}(\mathbb{Z}) \subset [\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)}$ folgt :

Falls $[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset$, dann ist $\mathcal{X}(\mathbb{Z}) = \emptyset$: es gibt keinen ganzen Punkt.
Dies ist eine "ganze" Version des Brauer-Maninschen Hindernisses (1970).

Dieses Hindernis wurde meistens im Fall $\mathcal{X}/\mathbb{Z}$ projektiv studiert. In diesem Falle hat man $\mathcal{X}(\mathbb{Z}) = X(\mathbb{Q})$ und $\mathcal{X}(\mathbb{Z}_p) = X(\mathbb{Q}_p)$: es werden *rationale Punkte* studiert.

Das Studium von *ganzen Punkten* von diesem Standpunkt aus würde erst seit 2005 systematisch entwickelt.

Tatsache 1 : Alle die Gegenbeispiele zum lokal-globalen Prinzip, die wir weiter oben erwähnt haben, kann man mittels des ganzen Brauer-Maninschen Hindernisses erklären, d. h. :

$$[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset.$$

Tatsache 2 : Für bestimmte Klassen von Gleichungen, die wir erwähnt haben, mit assoziierten Schema $\mathcal{X}/\mathbb{Z}$, wenn $[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} \neq \emptyset$, dann hat man $\mathcal{X}(\mathbb{Z}) \neq \emptyset$, und $\mathcal{X}(\mathbb{Z})$ liegt dicht in der grössten Untermenge von $\prod_{p \text{ endlich}} \mathcal{X}(\mathbb{Z}_p)$ welche das Brauer-Maninsche Hindernis erlaubt.

Machen wir eine Ausnahme mir der Irreduzibilitätshypothese.
Wir haben das folgende Gegenbeispiel zum lokal-globalen Prinzip erwähnt :

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0.$$

Sei $\mathcal{X}/\mathbb{Z}$ das entsprechende Schema. Für die Quaternionalgebra $A = (x, 13)$ auf X findet man :
Für einen beliebigen $M_p \in \mathcal{X}(\mathbb{Z}_p)$ hat man $A(M_p) = 0 \in \mathbb{Q}/\mathbb{Z}$ wenn $p \neq 13$ und $A(M_{13}) = 1/2 \in \mathbb{Q}/\mathbb{Z}$.

Also $[\prod_p \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset$.

Bemerkung : unter der Einbettung $\mathcal{X}_{\mathbb{Q}} \hookrightarrow \mathbb{G}_{m,\mathbb{Q}}$, die durch x gegeben ist, kommt die Klasse $(x, 13)$ von einer Klasse in $\mathrm{Br}\,\mathbb{G}_{m,\mathbb{Q}}$ her.
Dies ist ein spezieller Fall einer "torischer" Version (CT/Xu 2010) eines Satzes von M. Stoll (2006) über endliche Unterschemata von abelschen Varietäten.

Borovoi–Rudnick

$$(y - x)(9x + 7y) = 1 - 2z^2$$

Es wird die Klasse $A = (y - x, 2) = (9x + 7y, 2)$ benutzt.
Es wird (leicht) geprüft : $A = 0$ auf $\mathcal{X}(\mathbb{Z}_p)$ wenn $p \neq 2$, und $A = 1/2$ auf $\mathcal{X}(\mathbb{Z}_2)$.
Also :
$[\prod_p \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)} = \emptyset$.

Satz (CT-Xu 2006/2009). *Sei $q(x,y,z)$ eine ganze ternäre quadratische Form, die nicht entartet und indefinit über $\mathbb{R}$ ist. Sei $n \in \mathbb{Z}, n \neq 0$ und $\mathcal{X}/\mathbb{Z}$ das Schema $q(x,y,z) = n$. Es liegt $\mathcal{X}(\mathbb{Z})$ dicht in der Projektion von $[\prod_{p \cup \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\, X}$ auf $\prod_{p \text{ endlich}} \mathcal{X}(\mathbb{Z}_p)$.*

Weiter ist $\mathrm{Br}\, X/\mathrm{Br}\,(\mathbb{Q}) \subset \mathbb{Z}/2$, und man kann einen Erzeuger berechnen, also kann man algorithmisch entscheiden, ob es eine ganzzahlige Lösung gibt.

So erhält man einen neuen Beweis des Satzes von Schulze-Pillot und Xu.

$$(1 + n^k y)(1 - n^k y) = m^2 x^2 - n z^2.$$

Die Klasse $A = (1 + n^k y, m) = (1 - n^k y, m)$ liegt in $\mathrm{Br}\, X$ und erzeugt $\mathrm{Br}\, X / \mathrm{Br}\, \mathbb{Q}$.
Für $p \neq 2$, auch für $p = \infty$, verschwindet A auf $\mathcal{X}(\mathbb{Z}_p)$.
Auf $\mathcal{X}(\mathbb{Z}_2)$, A ist konstant mit Wert entweder 0 oder $1/2$, und ist gleich $1/2$ dann und nur dann, wenn

(i) $n \equiv 5\ (8)$ und 2 teilt m
oder
(ii) $n \equiv 3\ (8)$ und 4 teilt m.

Die Gegenbeispiele zum lokal-globalen Prinzip für $q(x, y) = n$, wo q eine nicht entartete *binäre* quadratische Form mit ganzen Koeffizienten ist, die wir früher erwähnt haben, kann man auch mittels der Brauergruppe erklären.

Satz (spezieller Fall eines Satzes von D. Harari 2008 für Tori, Methode : Klassenkörpertheorie).
Für eine solche Gleichung $q(x, y) = n$ *stimmt der topologische Abschluß von* $\mathcal{X}(\mathbb{Z})$ *in* $\prod_\bullet \mathcal{X}(\mathbb{Z}_p)$ *mit der Brauer-Maninsche Menge* $[\prod_\bullet \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)}$ *überein.*
[$\bullet$: es werden alle Punkte in derselben Komponente von $X(\mathbb{R})$ identifiziert.]

Hier gibt es keine Einschränkung zu indefiniten Formen, es liegt aber ein grosses Problem vor, der Quotient $\mathrm{Br}\,(X)/\mathrm{Br}\,(\mathbb{Q})$ ist hier unendlich, im Prinzip haben wir eine unendliche Anzahl von Bedingungen nachzuprüfen um zu entscheiden ob $\mathcal{X}(\mathbb{Z}) \neq \emptyset$!

In bestimmen Fällen kommt man mit einer endlichen Anzahl von expliziten Bedingungen aus, wie wir am Beispiel $p = x^2 + 27y^2$ (Gauß), p Primzahl, gesehen haben.

Beide Sätze (CT-Xu, Harari) haben Demarche und dann Borovoi-Demarche verallgemeinert.

Satz (Borovoi-Demarche 2011) *Sei $\mathcal{X}$ ein $\mathbb{Z}$-Schema und $X = \mathcal{X}_{\mathbb{Q}}$ homogener Raum von einer zusammenhängender linearer algebraischer Gruppe G. Nehmen wir an, die geometrische Trägheitsgruppen sind zusammenhängend, und jeder einfacher halbeinfacher $\mathbb{Q}$-Faktor H von G ist $\mathbb{R}$-isotrop (d. h. $H(\mathbb{R})$ nicht kompakt).*
Dann stimmt der topologische Abschluß von $\mathcal{X}(\mathbb{Z})$ in $\prod_{p \text{ endlich}} \mathcal{X}(\mathbb{Z}_p)$ mit der Projektion der Brauer-Maninschen Menge $[\prod_p \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)}$ überein.

Jenseits von homogenen Räumen

- Einparameter Familien von homogenen Räumen
- Einige affine Geichungen $f(x, y, z) = 0$.
- Einige "Gleichungen" $F(X, Y, Z) \neq 0$.
- Hyperbolische Kurven.
- Was mit $\mathbb{F}_p[t]$ anstelle von $\mathbb{Z}$?

Einparameter Familien von homogenen Räumen

Mit F. Xu haben wir (2010/11) Gleichungen

$$q(x, y, z) = P(t)$$

studiert. Hier ist q eine ternäre quadratische Form mit ganzzahligen Koeffizienten, indefinit, und $P(t) \in \mathbb{Z}[t]$ ein nichtkonstantes Polynom.
Wir zeigten : *Der topologische Abschluß von* $\mathcal{X}(\mathbb{Z})$ *in* $\prod_{p \text{ endlich}} \mathcal{X}(\mathbb{Z}_p)$ *stimmt mit der Projektion der Brauer-Maninschen Menge* $[\prod_p \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}\,(X)}$ *überein.*
Ist $P(t)$ *separabel, dann ist* $\mathrm{Br}\,(X) = \mathrm{Br}\,(\mathbb{Q})$, *also gilt starke Approximation.*

1994/1996 hat D. Harari Methoden entwickelt, um *rationale* Punkte auf einparameter Familien von *projektiven Varietäten* $X \to \mathbb{P}^1$ zu untersuchen.
Vor kurzem haben Harari und ich ähnliche Methoden benutzt, um *ganze* Punkte von einparameter Familien von *affinen, homogenen Räumen* $X \to \mathbb{A}^1$ zu studieren.
Der folgende spezielle Fall stellt schon eine grosse Verallgemeinerung des Satzes mit Xu :

Satz (CT-Harari 2011/12) *Seien* $a_i(t), i = 1, 2, 3,$ *und* $p(t)$ *in* $\mathbb{Z}[t]$ *Polynome. Nehmen wir an, das Produkt* $p(t).\prod_i a_i(t)$ *ist nicht konstant und is quadratfrei in* $\mathbb{Q}[t]$.
Sei $\mathcal{X} \subset \mathbb{A}^4_{\mathbb{Z}}$ *das affine Schema*

$$\sum_{i=0}^{2} a_i(t)x_i^2 = p(t).$$

Nehmen wir an, für fast alle $t \in \mathbb{R}$ *hat der Kegelschnitt* $\sum_{i=0}^{2} a_i(t)x_i^2 = 0$ *einen Punkt auf* $\mathbb{R}$.
Dann gelten das lokal-global Prinzip und starke Approximation für ganze Punkte von $\mathcal{X}$ *:* $\mathcal{X}(\mathbb{Z})$ *liegt dicht im Produkt* $\prod_{p \text{ fini}} \mathcal{X}(\mathbb{Z}_p)$.

Affine Flächen. Ein klassisches Problem

Kann man jede ganze Zahl $n \neq \pm 4 \mod 9$ als Summe von drei Kuben in $\mathbb{Z}$ darstellen ? (Der Fall $n = 33$ ist offen.)

Der folgende Satz zeigt : mit Reziprozitätsgesetzen kann man keine solche n ausschließen.

Satz (CT-Wittenberg 2009/12). *Sei n ganz, $n \neq \pm 4 \bmod 9$, und sei $\mathcal{X}_n/\mathbb{Z}$ definiert durch*

$$x^3 + y^3 + z^3 = n.$$

Sei $X_n = \mathcal{X}_n \times_{\mathbb{Z}} \mathbb{Q}$. Dann hat man :

$$[\prod_{p \cup \infty} \mathcal{X}_n(\mathbb{Z}_p)]^{\mathrm{Br}\,(X_n)} \neq \emptyset.$$

Es ist nicht leicht, Gruppen $\mathrm{Br}\,(X)/\mathrm{Br}\,(\mathbb{Q})$ bei affinen Varietäten zu berechnen. Hier zum Beispiel hängt die Antwort von der Arithmetik der Kurve "im unendlichen" $x^3 + y^3 + z^3 = 0$.

Affine Flächen. Gleichungen $q(x, y) = P(t)$, q binäre quadratische Form

Gegenbeispiele zum lokal-globalen Prinzip für ganze Punkte auf

$$x^2 + y^2 = P_1(z)P_2(z),$$

mit Polynomen $P_i(z) \in \mathbb{Z}[z]$, prim zu einander, kann man leicht konstruieren.
Solche Gegenbeispiele werden durch die Quaternionalgebra $A = (P_1(z), -1) = (P_2(z), -1)$ erklärt.

Einer berühmten Annahme von Bouniakowsky, Dickson, und Schinzel nach, sollte die Vermutung über Primzwillinge ein spezieller Fall der simultanen Darstellbarkeit von Primzahlen durch eine endliche Anzahl von irreduziblen Polynomen $P_i(t)$. Das könnte man heranziehen (CT-Sansuc 1979) um das Bestehen von rationalen Punkten auf bestimmen Varietäten vorherzusagen.

F. Gundlach (2012/13) hat gemerkt, daß aus dem selben Argument folgt :
Hat die Gleichung

$$x^2 + y^2 = P(z),$$

mit $P(z) = \mathbb{Z}[z]$ *einem irreduziblen Polynom von ungeradem Grad, Lösungen in allen* $\mathbb{Z}_p$*, und gilt die Schinzel Hypothese, dann hat die Gleichung eine Lösung mit* $(x, y, z) \in \mathbb{Z}$*.*
Dass man in der linken Seite $x^2 + y^2$, mit nur einer Form im Geschlecht, und nicht eine beliebige quadratische Form $q(x, y)$ hat, spielt leider eine grosse Rolle im Beweis.

Einige "Gleichungen" $F(X, Y, Z) \neq 0$

Sei $F(x, y, z)$ homogen mit Koeffizienten in $\mathbb{Z}$.
Sei $\mathcal{U}$ das $\mathbb{Z}$-Schema $\mathcal{X} \subset \mathbb{P}^2_{\mathbb{Z}}$, das durch die "Gleichung" $F \neq 0$ definiert ist.
Die ganzen Punkte werden hier durch Tripeln $(x, y, z) \in \mathbb{Z}^3$ dargestellt, bis auf Multiplikation durch eine Einheit, d.h. ± 1, mit der Eigenschaft

$$F(x, y, z) = \pm 1.$$

Ist Grad$(F) \leq 2$, da ist $U = \mathcal{U} \times_{\mathbb{Z}} \mathbb{Q}$ eine "log-del Pezzo" Fläche.
Ist Grad$(F) = 3$, da findet man ein Analog von einer $K3$ Fläche.
Ist Grad$(F) > 3$, da findet man ein Analog von einer Fläche von allgemeinem Typ.
Für ganze Punkte solcher Flächen hat man das Gegenstück zu wohlbekannten Fragen über rationale Punkte.

Das (leichte) Gegenbeispiel zum lokal-globalen Prinzip $2x^2 + 2y^2 + 3z^2 = \pm 1$ kann man in Brauer-Maninscher Art erklären, unter Benutzung von der Quaternionalgebra $A = ((2x^2 + 2y^2 + 3z^2)/z^2, -1)$.

Das Gegenbeispiel $16x^2 + 9y^2 - 3z^2 = \pm 1$ (CT-Wittenberg) kann man nicht in Brauer-Maninscher Art erklären, wohl aber (leicht) in "étale Brauer-Maninscher" Art : dies ist ein Analog – in dem Fall von ganzen Punkten – der Gegenbeispielen von Skorobogatov (1999) für rationale Punkte.
Für F vom Grad d, kann man allgemein die unverzweigte Galois Überdeckung von $F \neq 0$, mit Gruppe μ_d benutzen, die durch die affine Gleichung $F(x, y, z) = 1$ gegeben ist. Da kann man "Abstieg" anwenden.

Hyperbolische Kurven

Eine glatte Kurve nennt mant hyperbolisch wenn sie auf $\mathbb{C}$ isomorph ist zu einer von den folgenden Kurven

- $\mathbb{P}^1_{\mathbb{C}}$ minus wenigstens 3 Punkte
- Eine elliptische Kurve minus wenigstens 1 Punkt
- Eine Zariski offene Menge einer Kurve vom Geschlecht wenigstens 2.

Sei $\mathcal{U}/\mathbb{Z}$ eine affine Kurve mit $U = \mathcal{U}_{\mathbb{Q}}$ hyperbolisch.
Nach C. L. Siegel ist $\mathcal{U}(\mathbb{Z})$ endlich.

Für rationale Punkte von einer projektiven Kurve $C/\mathbb{Q}$ von Geschlecht wenigstens 2 wurde die Frage untersucht, ob $C(\mathbb{Q})$ mit der Brauer-Maninschen Menge $C(\mathbb{A}_{\mathbb{Q}})_{\bullet}^{\mathrm{Br}}$ übereinstimmt (Scharaschkin, Skorobogatov, Stoll, Poonen, Mordell-Weil Sieb).

Sei jetzt $\mathcal{U}/\mathbb{Z}$ eine affine Kurve mit $U = \mathcal{U}_{\mathbb{Q}}$ hyperbolisch. Analog könnte man fragen :

(i) Falls $[\prod_p \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)} \neq \emptyset$, ist $\mathcal{U}(\mathbb{Z}) \neq \emptyset$?

(ii) Stimmt das diagonale Bild von $\mathcal{U}(\mathbb{Z})$ im Produkt $\prod_{\bullet} \mathcal{U}(\mathbb{Z}_p)$ mit $[\prod_{\bullet} \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)}$ überein ?

Dazu gibt es eine Arbeit von Harari und Voloch (2010).

Fall U der Gestalt $\mathbb{P}^1$ minus 3 Punkte ist , dann ist die Frage (i) eng mit einem Problem von Skolem verknüpft.

Stabilität der Frage (ii) : Sei $\mathcal{U}_1 \to \mathcal{U}_2$ ein dominanter Morphismus zwischen solchen Kurven über $\mathbb{Z}$. Nehmen wir an, (ii) gilt für $\mathcal{U}_2$. Dann gilt es auch für $\mathcal{U}_1$, im Besonderen, ist $\mathcal{U}_1(\mathbb{Z}) = \emptyset$, dann ist $[\prod_p \mathcal{U}_1(\mathbb{Z}_p)]^{\mathrm{Br}\,(U_1)} = \emptyset$.

Eine Variante. Sei f invertierbar auf $\mathcal{U}$, also $f : \mathcal{U} \to \mathbb{G}_{m,\mathbb{Z}}$. Dann ist offensichtlich $\mathcal{U}(\mathbb{Z})$ endlich, da $\mathbb{G}_m(\mathbb{Z}) = \pm 1$. Wenn $\mathcal{U}(\mathbb{Z}) = \emptyset$, dann ist $[\prod_p \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)} = \emptyset$.

Im selben Artikel findet man aber eine negative Antwort zur Frage (ii). Ein Beispiel bietet die affine Kurve $\mathcal{U}$ mit Gleichung $y^2 = x^3 + 3$. Hier hat man $(x, y) = (1, 2) \in \mathcal{U}(\mathbb{Z})$. Im Beweis wird die Tatsache benutzt, daß $U/\mathbb{Q}$ das Komplement von einem einzigen rationalen Punkt in einer elliptischen Kurve E ist, also $\mathrm{Br}\,(E) = \mathrm{Br}\,(U)$.

Was mit $\mathbb{F}_p[t]$ anstelle von $\mathbb{Z}$?
Sei $K = \mathbb{F}_p(t)$. Sei Ω die Menge der Stellen von K.
Für $P \in \Omega$, sei A_P die Komplettierung von A in P, und K_P der Fraktionskörper. Man hat $K_\infty = \mathbb{F}_p((1/t))$
Satz (Harari-Voloch 2012)
Sei $\mathcal{X}$ über $\mathbb{F}_p[t]$ affin. Wenn ein Punkt

$$\{P_v\} \in X(K_\infty) \times \prod_{P \text{ endlich}} \mathcal{X}(A_P)$$

in der Brauer-Maninschen Menge liegt, dann IST dieses Element das diagonale Bild von einem Punkt in $\mathcal{X}(A)$.

Im Beweis wird nur die p-torsion von $\mathrm{Br}\,(X)$ benutzt, die sehr gross ist.

Eine Frage

Seien $a, b, c \in \mathbb{Z}$ mit $c.(a-b) \neq 0$. Sei $\mathcal{V} \subset A^4_{\mathbb{Z}}$ (Koordinaten x, y, z, t) das geschlossene Schema mit den Gleichungen

$$y^2 = c(z-at)(z-bt), \;\; zt = x^2.$$

Sei $\mathcal{U} \subset \mathcal{V}$ das Komplement von $(0,0,0,0)_{\mathbb{Z}}$. Die $\mathbb{Q}$-Varietät $U = \mathcal{U}_{\mathbb{Q}}$ ist der Kegel über der Geschlecht Eins Kurve $C \subset \mathbb{P}^3_{\mathbb{Q}}$, die durch die selben Gleichungen definiert ist.

Ist es möglich, daß $[\prod_{p \cup \infty} \mathcal{U}(\mathbb{Z}_p)]^{\mathrm{Br}\,(U)} = \emptyset$ – also $\mathcal{U}(\mathbb{Z}) = \emptyset$, also $C(\mathbb{Q}) = \emptyset$ – aber $[\prod_{p \cup \infty} C(\mathbb{Q}_p)]^{\mathrm{Br}\,(C)} \neq \emptyset$?

Zum Beispiel liegt die Algebra

$A = (z-at, t) = (z-at, z) = (c(z-bt), t) = (c(z-bt), z)$

in $\mathrm{Br}\,(U)$, kommt aber nicht von $\mathrm{Br}\,(C)$.