金井　和貴（Kazuki KANAI）

所属（Domain）　情報科学領域（Domain of Computer and Information Sciences）

●研究テーマ（Research theme）

① 代数的トーラスの有理性問題
（Rationality problem for algebraic tori）

② ハッセ原理
（Hasse principle）

③ カードベース暗号
（Card-based cryptography）

---

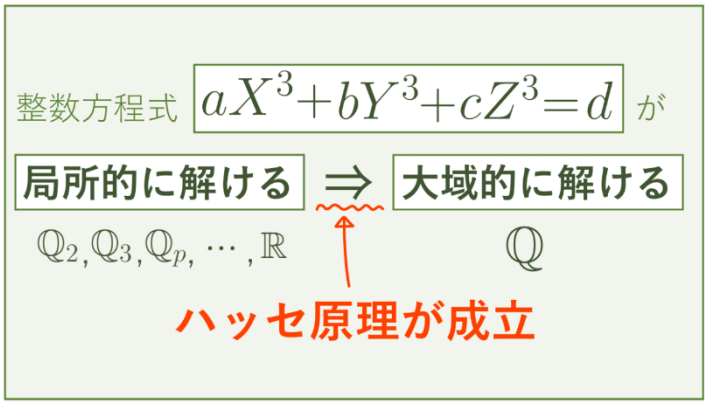
①代数的トーラスの有理性問題

有理性問題とは、与えられた図形（代数多様体）が最も簡単な図形（射影空間）と同型であるかを問う問題である。代数多様体の中でも主要なクラスである代数的トーラスに対して、この問題に取り組んでいる。

1. Rationality Problems for Algebraic Tori.
A rationality problem asks whether a given geometric object (an algebraic variety) is isomorphic to the simplest such object, namely projective space. I study this question for algebraic tori, which form one of the principal classes of algebraic varieties.

②ハッセ原理

整数論における種々の問題の可否は、素数の世界（局所）と整数の世界（大域）にどれほどのズレがあるかに集約されることがままある。この局所と大域のズレがないときにハッセ原理（局所大域原理）が成立すると言う。特にノルム方程式に対するこれを研究している。



2. The Hasse Principle.
In number theory, the solvability of various problems is often reduced to understanding the discrepancy between the world of prime numbers and the world of integers. When no such discrepancy exists, one says that the Hasse principle holds. I am interested in studying this principle for norm equations.

③カードベース暗号

カードベース暗号とはカードを用いて暗号技術を実現する研究分野である。特に秘密計算とゼロ知識証明の研究が活発に行われている。カードに対するシャッフルを群論的に解析し、数学的な道具を使える枠組みを整える研究を行っている。

3. Card-Based Cryptography.
Card-based cryptography explores cryptographic techniques using physical playing cards, with active research on secure computation and zero-knowledge proofs. I study card shuffles from a group-theoretic perspective and develop a framework for applying mathematical tools.

キーワード（Keyword）	代数的トーラス、 有理性、 ハッセ原理,、カードベース暗号
専門分野（Specialized Field）	代数的整数論、計算機群論
共同研究可能技術（Possible Technology of Cooperative research）	数学における代数的手法
関連論文・特許情報 website （Related articles･patent information）	金井 和貴(工学部 情報工学科)｜茨城大学研究者情報総覧
研究設備（Research Facility）	代数計算ソフトGAP
研究室URL（Lab. URL）	
E-mail	Kazuki.kanai.du62@vc.ibaraki.ac.jp