Kummer theory for commutative algebraic groups

Tronto, S.

Stellingen

Kummer theory for commutative algebraic groups

by Sebastiano Tronto

1. The failure of maximality of Kummer extensions of number fields arising from non-torsion points on elliptic curves is bounded by a constant that depends only on computable quantities associated with the base field, with the chosen curve and with divisibility properties of the chosen points.

2. The elliptic curve E over $\mathbb{Q}$ defined by the equation

$$y^2 + y = x^3 - 216x - 1861$$

is such that the point

$$P = \left(\frac{23769}{400}, \frac{3529853}{8000} \right) \in E(\mathbb{Q})$$

cannot be written as $3Q + T$ for any $Q \in E(\mathbb{Q})$ and $T \in E(\mathbb{Q})_{\text{tors}}$, but over the 3-torsion field $K = \mathbb{Q}(\sqrt[6]{-3})$ of E the point

$$Q = \left(\frac{803}{400}\sqrt[6]{-3}^4 - \frac{416}{400}\sqrt[6]{-3}^2 + \frac{507}{400}, \frac{89133}{8000}\sqrt[6]{-3}^4 - \frac{199071}{8000}\sqrt[6]{-3}^2 - \frac{95323}{8000} \right) \in E(K)$$

is such that $3Q = P$.

3. For every elliptic curve E over $\mathbb{Q}$ and every positive integer N, the group

$$H^1(\text{Gal}(\mathbb{Q}(E_{\text{tors}}) \mid \mathbb{Q}), E[N])$$

has finite exponent dividing

$$2^{12} \times 3^8 \times 5^3 \times 7^3 \times 11^2 \,.$$

If E has complex multiplication, this exponent divides 12.

4. There is a notion of divisibility with respect to a filter of ideals for modules over any unitary ring that extends the concepts of injective module and of p-divisible group. Important theorems such as Baer's criterion and the existence of an injective hull can be generalized to this setting, which moreover offers a framework for the study of modules of division points of commutative algebraic groups and their associated Kummer extensions.

5. There exists an algorithm that, given as input r rational numbers $a_1, \ldots, a_r$, produces as output a formula for the degrees over $\mathbb{Q}$ of all cyclotomic-Kummer extensions of the form

$$\mathbb{Q}\left(\zeta_m, \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}\right)$$

for any pair of positive integers (m, n) with n dividing m.

6. The number 41389051340965630239434436 7 is prime.

7. Let n be a natural number and let p be a prime number different from 2 and 5. Then n is divisible by p if and only if the number obtained from n by removing its last digit, multiplying this digit by a certain factor $\acute{e}_p$, and adding the result to the remaining number is divisible by p. The factor $\acute{e}_p$ can be any inverse of 10 modulo p, and one can determine a possible value for it by writing $p = 10x + y$ with $0 \leqslant y \leqslant 9$ and using the following table:

$$\acute{e}_p = \begin{cases} -x & \text{if } y = 1, \\ 3x + 1 & \text{if } y = 3, \\ -3x - 2 & \text{if } y = 7, \\ x + 1 & \text{if } y = 9. \end{cases}$$

8. In 1981 Morwen Thistlethwaite devised an algorithm to prove that every configuration of the Rubik's cube can be solved in 52 moves or less. This algorithm can be applied by human solvers to find remarkably efficient solutions.

9. Computers and the Internet offer an incredibly powerful yet fragile way of storing and sharing information: as old software and technologies get deprecated, old documents become unreadable and old applications impossible to run. Open-source software and formats can help mitigate this, but the fundamental problems remain.

10. In the present day, the existence of peer-reviewed academic journals that do not offer open access is unacceptable.