Universiteit Leiden
The Netherlands

Kummer theory for commutative algebraic groups

Tronto, S.

Citation
Tronto, S. (2022, September 8). *Kummer theory for commutative algebraic groups*. Retrieved from https://hdl.handle.net/1887/3455350

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/3455350

Note: To cite this publication please use the final published version (if applicable).

Bibliography

[Ach05] Jeffrey D. Achter. Detecting complex multiplication. In *Computational aspects of algebraic curves*, pages 38–50. World Scientific, 2005.

[Ara08] Keisuke Arai. On uniform lower bound of the Galois images associated to elliptic curves. *Journal de théorie des nombres de Bordeaux*, 20(1):23–43, 2008.

[Bae40] Reinhold Baer. Abelian groups that are direct summands of every containing abelian group. *Bulletin of the American Mathematical Society*, 46(10):800–806, 1940.

[BC14] Barinder S. Banwait and John E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra & Number Theory*, 8(5):1201–1229, 2014.

[BC20a] Abbey Bourdon and Pete L. Clark. Torsion points and Galois representations on CM elliptic curves. *Pacific Journal of Mathematics*, 305(1):43–88, 2020.

[BC20b] Abbey Bourdon and Pete L. Clark. Torsion points and isogenies on CM elliptic curves. *Journal of the London Mathematical Society. Second Series*, 102(2):580–622, 2020.

[BDM+19] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Annals of Mathematics. Second Series*, 189(3):885–944, 2019.

[BDM+21] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. *arXiv preprint arXiv:2101.01862*, 2021.

[Ber88] Daniel Bertrand. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge University Press, Cambridge, 1988.

[BJR91] Nigel Boston, Hendrik W. Lenstra Jr., and Kenneth A. Ribet. Quotients of group rings arising from two-dimensional representations. *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, 312(4):323–328, 1991.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Annals of Mathematics*, 173(1):569–584, 2011.

[BP21] Peter Bruin and Antonella Perucca. Reductions of points on algebraic groups, II. *Glasgow Mathematical Journal*, 63(2):484–502, 2021.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. 63(3):957–984, 2013.

[BR03] Matthew H. Baker and Kenneth A. Ribet. Galois theory and torsion points on curves. *Journal de Théorie des Nombres de Bordeaux*, 15(1):11–32, 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Mathematics of Computations*, 88:1303–1339, 2019.

[Coa70] John Coates. An application of the division theory of elliptic functions to Diophantine approximation. *Inventiones Mathematicae*, 11:167–182, 1970.

[Coh07] Henri Cohen. *Number theory: Volume I: Tools and Diophantine equations*. Springer, 2007.

[CP20] Francesco Campagna and Riccardo Pengo. Entanglement in the family of division fields of elliptic curves with complex multiplication. *arXiv preprint arXiv:2006.00883*, 2020.

[CR21] Michael Cerchia and Jeremy Rouse. Uniform bounds on the image of the arboreal Galois representations attached to non-CM elliptic curves. *Proceedings of the American Mathematical Society*, 149(2):583–589, 2021.

[Cre97] John E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[CS19] Francesco Campagna and Peter Stevenhagen. Cyclic reduction of elliptic curves. *arXiv preprint arXiv:2001.00028*, 2019.

[Dav11] Agnès David. Borne uniforme pour les homothéties dans l'image de Galois associée aux courbes elliptiques. *Journal of Number Theory*, 131(11):2175 – 2191, 2011.

[Deu53] Max Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachrichten von der Akademie der Wissenschaften Göttingen Mathematisch-Physikalische Klasse. IIa, Mathematisch-Physikalisch-Chemische Abteilung*, 1953:85–94, 1953.

[Deu58] Max Deuring. Die Klassenkorper der komplexen Multiplikation. In *Enzyklopädie der mathematischen Wissenschaften*, volume I2, Heft 10, Teil II. Teubner Verlag, Stuttgart, 1958.

[DLM21] Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow. Towards a classification of entanglements of Galois representations attached to elliptic curves. *arXiv preprint arXiv:2105:02060*, 2021.

[DP16] Christophe Debry and Antonella Perucca. Reductions of algebraic integers. *Journal of Number Theory*, 167:259–283, 2016.

[EGH+11] Pavel I. Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to representation theory.* American Mathematical Society, 2011.

[ES53] Beno Eckmann and A Schopf. Über injektive Moduln. *Archiv der Mathematik*, 4(2):75–78, 1953.

[Fle68] Isidore Fleischer. A new construction of the injective hull. *Canadian Mathematical Bulletin*, 11(1):19–21, 1968.

[GM20] Aurélien Galateau and César Martínez. Homothéties explicites des représentations ℓ-adiques. *arXiv preprint arXiv:2006.07401*, 2020.

[Gou97] Fernando Q. Gouvêa. *p-adic Numbers.* Springer, 1997.

[Gre12] Ralph Greenberg. The image of Galois representations attached to elliptic curves with an isogeny. *American Journal of Mathematics*, 134(5):1167–1196, 2012.

[Gro91] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, pages 235–256. Cambridge University Press, Cambridge, 1991.

[GRSS14] Ralph Greenberg, Karl Rubin, Alice Silverberg, and Michael Stoll. On elliptic curves with an isogeny of degree 7. *American Journal of Mathematics*, 136(1):77–109, 2014.

[Har20] David Harari. *Galois cohomology and class field theory.* Springer, 2020.

[Hin88] Marc Hindry. Autour d'une conjecture de Serge Lang. *Inventiones Mathematicae*, 94(3):575–603, 1988.

[Jac12] Nathan Jacobson. *Basic algebra I.* Courier Corporation, 2012.

[Jon10] Nathan Jones. Almost all elliptic curves are Serre curves. *Transactions of the American Mathematical Society*, 362(3):1547–1570, 2010.

[JP21] Abtien Javan Peykar. *Division points in arithmetic.* PhD thesis, Leiden University, 2021.

[JR10] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proceedings of the London Mathematical Society*, 100(3):763–794, 2010.

[Ken82] Monsur A. Kenku. On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class. *Journal of Number Theory*, 15(2):199–202, 1982.

[Lan02] Serge Lang. *Algebra.* Springer-Verlag, New York, 2002.

[LFL21] Samuel Le Fourn and Pedro Lemos. Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan. *Algebra & Number Theory*, 15(3):747–771, 2021.

[LJ96] Hendrik W. Lenstra Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022. [Online; accessed 25 January 2022].

[Lom15] Davide Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra & Number Theory*, 9(10):2347–2395, 2015.

[Lom17] Davide Lombardo. Galois representations attached to abelian varieties of CM type. *Bulletin de la Société Mathématique de France*, 145(3):469–501, 2017.

[Lom19] Davide Lombardo. Computing the geometric endomorphism ring of a genus-2 Jacobian. *Mathematics of Computation*, 88(316):889–929, 2019.

[LP17] Davide Lombardo and Antonella Perucca. The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. *New York Journal of Mathematics*, 23, 2017.

[LP21] Davide Lombardo and Antonella Perucca. Reductions of points on algebraic groups. *Journal of the Institute of Mathematics of Jussieu*, 20(5):1637–1669, 2021.

[LR18] Álvaro Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. *arXiv preprint arXiv:1809.02584*, 2018.

[LT21a] Davide Lombardo and Sebastiano Tronto. Effective Kummer Theory for Elliptic Curves. *International Mathematics Research Notices*, 08 2021.

[LT21b] Davide Lombardo and Sebastiano Tronto. Some uniform bounds for elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:2106.09950*, 2021. Submitted for publication.

[LV14] Eric Larson and Dmitry Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *Journal de l'Institut de Mathématiques de Jussieu*, 13(3):517–559, 2014. With an appendix by Brian Conrad.

[LW15] Tyler Lawson and Christian Wuthrich. Vanishing of some Galois cohomology groups for elliptic curves. In *Elliptic Curves, Modular Forms and Iwasawa Theory – Conference in honour of the 70th birthday of John Coates*, pages 373–399. Springer, 2015.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, (47):33–186, 1977. With an appendix by Barry Mazur and Michael Rapoport.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1-3):437–449, 1996.

[MG78] Barry Mazur and Dorian Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[Mor12] Pieter Moree. Artin's primitive root conjecture–a survey. *Integers*, 12(6):1305–1416, 2012.

[Mor19] Jackson S. Morrow. Composite images of Galois for elliptic curves over $\mathbb{Q}$ and entanglement fields. *Mathematics of Computation*, 88(319):2389–2421, 2019.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Springer Science & Business Media, 2013.

[Ogg73] Andrew P. Ogg. Rational points on certain elliptic modular curves. In *Proceedings of Symposia in Pure Mathematics*, volume 24, pages 221–231, 1973.

[Pal04] Willem J. Palenstijn. Galois action on division points. Master's thesis, Leiden University, 2004.

[Pal14] Willem J. Palenstijn. *Radicals in arithmetic*. PhD thesis, Leiden University, 2014.

[Par96] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *Journal für die reine und angewandte Mathematik*, 1999:116 – 85, 1996.

[Per08] Antonella Perucca. *On the order of the reductions of points on abelian varieties and tori*. PhD thesis, Tor Vergata University of Rome, 2008.

[Per11] Antonella Perucca. On the reduction of points on abelian varieties and tori. *International Mathematics Research Notices*, 2011(2):293–308, 2011.

[Per15] Antonella Perucca. The order of the reductions of an algebraic integer. *Journal of Number Theory*, 148:121–136, 2015.

[Pet06] Clayton Petsche. Small rational points on elliptic curves over number fields. *The New York Journal of Mathematics*, 12:257–268, 2006.

[Pin93] Richard Pink. Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime. *Compositio Mathematica*, 88(3):251–264, 1993.

[Pin04] Richard Pink. On the order of the reduction of a point on an abelian variety. *Mathematische Annalen*, 330(2):275–291, 2004.

[Pon66] Lev S. Pontryagin. *Topological groups*. Gordon and Breach, 1966.

[PS19] Antonella Perucca and Pietro Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *International Journal of Number Theory*, 15, 04 2019.

[PST20a] Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. The degree of Kummer extensions of number fields. *International Journal of Number Theory*, 17:1–20, 10 2020.

[PST20b] Antonella Perucca, Pietro Sgobba, and Sebastiano Tronto. Explicit Kummer theory for the rational numbers. *International Journal of Number Theory*, 16, 06 2020.

[Rei75] Irving Reiner. Maximal orders. *New York-London*, 1975.

[RG20] Gaël Rémond and Eric Gaudron. Nouveaux théorèmes d'isogénies. Preprint available at https://hal.archives-ouvertes.fr/hal-02445032, January 2020.

[Rib79] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Mathematical Journal*, 46(4):745–761, 1979.

[Ros95] Jonathan Rosenberg. *Algebraic K-theory and its applications*. Springer Science & Business Media, 1995.

[RSZB21] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:2106.11141*, 2021.

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Research in Number Theory*, 1(1):1–34, 2015.

[Sah68] Chih-Han Sah. Automorphisms of finite groups. *Journal of Algebra*, 10(1):47–68, 1968.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.

[Ser97] Jean-Pierre Serre. *Abelian l-Adic Representations and Elliptic Curves*. CRC Press, 1997.

[Ser13] Jean-Pierre Serre. *Local fields*. Springer Science & Business Media, 2013.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer Science & Business Media, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, 2009.

[The] The Sage Developers. *SageMath, the Sage Mathematics Software System*. `https://www.sagemath.org`.

[The19] The PARI Group, University of Bordeaux. *PARI/GP version 2.11.2*, 2019. available from `http://pari.math.u-bordeaux.fr/`.

[Tro19] Sebastiano Tronto. Kummer Degrees, 2019. GitHub repository `https://github.com/sebastianotronto/kummer-degrees`.

[Tro20] Sebastiano Tronto. Radical entanglement for elliptic curves. *arXiv preprint arXiv:2009.08298*, 2020. Submitted for publication.

[Tro21] Sebastiano Tronto. Division in modules and Kummer theory. *arXiv preprint arXiv:2111.14363*, 2021. Submitted for publication.

[Yel15] Jeffrey Yelton. Dyadic torsion of elliptic curves. *European Journal of Mathematics*, 1(4):704–716, 2015.

[Zyw11] David Zywina. Bounds for Serre's open image theorem. *arXiv preprint arXiv:1102.4656*, 2011.

[Zyw15a] David Zywina. On the possible images of the $\bmod \ell$ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015.

[Zyw15b] David Zywina. On the surjectivity of $\bmod \ell$ representations associated to elliptic curves. *arXiv preprint arXiv:1508.07661*, 2015.

[Zyw15c] David Zywina. Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07663*, 2015.

Curriculum Vitae

Sebastiano Tronto was born in Feltre, Italy in 1994. During high school he competed in many Mathematics and programming competitions, obtaining multiple medals at the national level and a qualification for the *International Olympiad in Informatics* in 2012.

In 2013 he enrolled at the University of Trento, where he obtained his bachelor degree *with honour* in 2016 with a thesis on Galois groups and fundamental groups, under the supervision of prof. Edoardo Ballico.

He then joined the ALGANT Master program, spending one year at the University of Milan and one year at Leiden University. He wrote his thesis, entitled *The Brauer-Manin obstruction to strong approximation*, under the supervision of Dr. Martin Bright at Leiden University. He was awarded his Masters diploma *cum laude* by the University of Milan and *summa cum laude* by Leiden University.

After completing his master program, he started his PhD in a cotutelle between the University of Luxembourg and Leiden University, under the supervision of Antonella Perucca and Peter Bruin.

After his PhD he is starting a carreer outside academia, where he can put to work the problem-solving skills he developed as a Mathematics student.