

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor M. Reid, Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom

The titles below are available from booksellers, or from Cambridge University Press at www.cambridge.org/mathematics

- 225 A mathematical introduction to string theory, S. ALBEVERIO *et al*
 226 Novikov conjectures, index theorems and rigidity I, S. C. FERRY, A. RANICKI & J. ROSENBERG (eds)
 227 Novikov conjectures, index theorems and rigidity II, S. C. FERRY, A. RANICKI & J. ROSENBERG (eds)
 228 Ergodic theory of Z^d -actions, M. POLLICOTT & K. SCHMIDT (eds)
 229 Ergodicity for infinite dimensional systems, G. DA PRATO & J. ZABCZYK
 230 Prolegomena to a middlebrow arithmetic of curves of genus 2, J. W. S. CASSELS & E. V. FLYNN
 231 Semigroup theory and its applications, K. H. HOFMANN & M. W. MISLOVE (eds)
 232 The descriptive set theory of Polish group actions, H. BECKER & A. S. KECHRIS
 233 Finite fields and applications, S. COHEN & H. NIEDERREITER (eds)
 234 Introduction to subfactors, V. JONES & V. S. SUNDER
 235 Number theory: Séminaire de théorie des nombres de Paris 1993–94, S. DAVID (ed)
 236 The James forest, H. FETTER & B. GAMBOA DE BUEN
 237 Sieve methods, exponential sums, and their applications in number theory, G. R. H. GREAVES *et al* (eds)
 238 Representation theory and algebraic geometry, A. MARTSINKOVSKY & G. TODOROV (eds)
 240 Stable groups, F. O. WAGNER
 241 Surveys in combinatorics, 1997, R. A. BAILEY (ed)
 242 Geometric Galois actions I, L. SCHNEPS & P. LOCHAK (eds)
 243 Geometric Galois actions II, L. SCHNEPS & P. LOCHAK (eds)
 244 Model theory of groups and automorphism groups, D. M. EVANS (ed)
 245 Geometry, combinatorial designs and related structures, J. W. P. HIRSCHFELD *et al* (eds)
 246 p -Automorphisms of finite p -groups, E. I. KHUKHRO
 247 Analytic number theory, Y. MOTOHASHI (ed)
 248 Tame topology and O -minimal structures, L. VAN DEN DRIES
 249 The atlas of finite groups – Ten years on, R. T. CURTIS & R. A. WILSON (eds)
 250 Characters and blocks of finite groups, G. NAVARRO
 251 Gröbner bases and applications, B. BUCHBERGER & F. WINKLER (eds)
 252 Geometry and cohomology in group theory, P. H. KROPHOLLER, G. A. NIBLO & R. STÖHR (eds)
 253 The q -Schur algebra, S. DONKIN
 254 Galois representations in arithmetic algebraic geometry, A. J. SCHOLL & R. L. TAYLOR (eds)
 255 Symmetries and integrability of difference equations, P. A. CLARKSON & F. W. NIJHOFF (eds)
 256 Aspects of Galois theory, H. VÖLKLEIN, J. G. THOMPSON, D. HARBATER & P. MÜLLER (eds)
 257 An introduction to noncommutative differential geometry and its physical applications (2nd edition), J. MADORE
 258 Sets and proofs, S. B. COOPER & J. K. TRUSS (eds)
 259 Models and computability, S. B. COOPER & J. TRUSS (eds)
 260 Groups St Andrews 1997 in Bath I, C. M. CAMPBELL *et al* (eds)
 261 Groups St Andrews 1997 in Bath II, C. M. CAMPBELL *et al* (eds)
 262 Analysis and logic, C. W. HENSON, J. IOVINO, A. S. KECHRIS & E. ODELL
 263 Singularity theory, W. BRUCE & D. MOND (eds)
 264 New trends in algebraic geometry, K. HULEK, F. CATANESE, C. PETERS & M. REID (eds)
 265 Elliptic curves in cryptography, I. BLAKE, G. SEROUSSI & N. SMART
 267 Surveys in combinatorics, 1999, J. D. LAMB & D. A. PREECE (eds)
 268 Spectral asymptotics in the semi-classical limit, M. DIMASSI & J. SJÖSTRAND
 269 Ergodic theory and topological dynamics of group actions on homogeneous spaces, M. B. BEKKA & M. MAYER
 271 Singular perturbations of differential operators, S. ALBEVERIO & P. KURASOV
 272 Character theory for the odd order theorem, T. PETERFALVI. Translated by R. SANDLING
 273 Spectral theory and geometry, E. B. DAVIES & Y. SAFAROV (eds)
 274 The Mandelbrot set, theme and variations, T. LEI (ed)
 275 Descriptive set theory and dynamical systems, M. FOREMAN, A. S. KECHRIS, A. LOUVEAU & B. WEISS (eds)
 276 Singularities of plane curves, E. CASAS-ALVERO
 277 Computational and geometric aspects of modern algebra, M. ATKINSON *et al* (eds)
 278 Global attractors in abstract parabolic problems, J. W. CHOLEWA & T. DLOTKO
 279 Topics in symbolic dynamics and applications, F. BLANCHARD, A. MAASS & A. NOGUEIRA (eds)
 280 Characters and automorphism groups of compact Riemann surfaces, T. BREUER
 281 Explicit birational geometry of 3-folds, A. CORTI & M. REID (eds)
 282 Auslander-Buchweitz approximations of equivariant modules, M. HASHIMOTO
 283 Nonlinear elasticity, Y. B. FU & R. W. OGDEN (eds)
 284 Foundations of computational mathematics, R. DEVORE, A. ISERLES & E. SÜLI (eds)
 285 Rational points on curves over finite fields, H. NIEDERREITER & C. XING
 286 Clifford algebras and spinors (2nd Edition), P. LOUNESTO
 287 Topics on Riemann surfaces and Fuchsian groups, E. BUJALANCE, A. F. COSTA & E. MARTÍNEZ (eds)
 288 Surveys in combinatorics, 2001, J. W. P. HIRSCHFELD (ed)
 289 Aspects of Sobolev-type inequalities, L. SALOFF-COSTE
 290 Quantum groups and Lie theory, A. PRESSLEY (ed)
 291 Tits buildings and the model theory of groups, K. TENT (ed)
 292 A quantum groups primer, S. MAJID
 293 Second order partial differential equations in Hilbert spaces, G. DA PRATO & J. ZABCZYK
 294 Introduction to operator space theory, G. PISIER
 295 Geometry and integrability, L. MASON & Y. NUTKU (eds)
 296 Lectures on invariant theory, I. DOLGACHEV
 297 The homotopy category of simply connected 4-manifolds, H.-J. BAUES
 298 Higher operads, higher categories, T. LEINSTER (ed)
 299 Kleinian groups and hyperbolic 3-manifolds, Y. KOMORI, V. MARKOVIC & C. SERIES (eds)
 300 Introduction to Möbius differential geometry, U. HERTTRICH-JEROMIN
 301 Stable modules and the $D(2)$ -problem, F. E. A. JOHNSON
 302 Discrete and continuous nonlinear Schrödinger systems, M. J. ABLOWITZ, B. PRINARI & A. D. TRUBATCH
 303 Number theory and algebraic geometry, M. REID & A. SKOROBOGATOV (eds)
 304 Groups St Andrews 2001 in Oxford I, C. M. CAMPBELL, E. F. ROBERTSON & G. C. SMITH (eds)
 305 Groups St Andrews 2001 in Oxford II, C. M. CAMPBELL, E. F. ROBERTSON & G. C. SMITH (eds)
 306 Geometric mechanics and symmetry, J. MONTALDI & T. RATIU (eds)

- 307 Surveys in combinatorics 2003, C. D. WENSLEY (ed.)
- 308 Topology, geometry and quantum field theory, U. L. TILLMANN (ed)
- 309 Corings and comodules, T. BRZEZINSKI & R. WISBAUER
- 310 Topics in dynamics and ergodic theory, S. BEZUGLYI & S. KOLYADA (eds)
- 311 Groups: topological, combinatorial and arithmetic aspects, T. W. MÜLLER (ed)
- 312 Foundations of computational mathematics, Minneapolis 2002, F. CUCKER *et al* (eds)
- 313 Transcendental aspects of algebraic cycles, S. MÜLLER-STACH & C. PETERS (eds)
- 314 Spectral generalizations of line graphs, D. CVETKOVIĆ, P. ROWLINSON & S. SIMIĆ
- 315 Structured ring spectra, A. BAKER & B. RICHTER (eds)
- 316 Linear logic in computer science, T. EHRHARD, P. RUET, J.-Y. GIRARD & P. SCOTT (eds)
- 317 Advances in elliptic curve cryptography, I. F. BLAKE, G. SEROUSSI & N. P. SMART (eds)
- 318 Perturbation of the boundary in boundary-value problems of partial differential equations, D. HENRY
- 319 Double affine Hecke algebras, I. CHEREDNIK
- 320 L-functions and Galois representations, D. BURNS, K. BUZZARD & J. NEKOVARĚ (eds)
- 321 Surveys in modern mathematics, V. PRASOLOV & Y. ILYASHENKO (eds)
- 322 Recent perspectives in random matrix theory and number theory, F. MEZZADRI & N. C. SNAITH (eds)
- 323 Poisson geometry, deformation quantisation and group representations, S. GUTT *et al* (eds)
- 324 Singularities and computer algebra, C. LOSSEN & G. PFISTER (eds)
- 325 Lectures on the Ricci flow, P. TOPPING
- 326 Modular representations of finite groups of Lie type, J. E. HUMPHREYS
- 327 Surveys in combinatorics 2005, B. S. WEBB (ed)
- 328 Fundamentals of hyperbolic manifolds, R. CANARY, D. EPSTEIN & A. MARDEN (eds)
- 329 Spaces of Kleinian groups, Y. MINSKY, M. SAKUMA & C. SERIES (eds)
- 330 Noncommutative localization in algebra and topology, A. RANICKI (ed)
- 331 Foundations of computational mathematics, Santander 2005, L. M. PARDO, A. PINKUS, E. SÜLI & M. J. TODD (eds)
- 332 Handbook of tilting theory, L. ANGELERI HÜGEL, D. HAPPEL & H. KRAUSE (eds)
- 333 Synthetic differential geometry (2nd Edition), A. KOCK
- 334 The Navier–Stokes equations, N. RILEY & P. DRAZIN
- 335 Lectures on the combinatorics of free probability, A. NICA & R. SPEICHER
- 336 Integral closure of ideals, rings, and modules, I. SWANSON & C. HUNEKE
- 337 Methods in Banach space theory, J. M. F. CASTILLO & W. B. JOHNSON (eds)
- 338 Surveys in geometry and number theory, N. YOUNG (ed)
- 339 Groups St Andrews 2005 I, C. M. CAMPBELL, M. R. QUICK, E. F. ROBERTSON & G. C. SMITH (eds)
- 340 Groups St Andrews 2005 II, C. M. CAMPBELL, M. R. QUICK, E. F. ROBERTSON & G. C. SMITH (eds)
- 341 Ranks of elliptic curves and random matrix theory, J. B. CONREY, D. W. FARMER, F. MEZZADRI & N. C. SNAITH (eds)
- 342 Elliptic cohomology, H. R. MILLER & D. C. RAVENEL (eds)
- 343 Algebraic cycles and motives I, J. NAGEL & C. PETERS (eds)
- 344 Algebraic cycles and motives II, J. NAGEL & C. PETERS (eds)
- 345 Algebraic and analytic geometry, A. NEEMAN
- 346 Surveys in combinatorics 2007, A. HILTON & J. TALBOT (eds)
- 347 Surveys in contemporary mathematics, N. YOUNG & Y. CHOI (eds)
- 348 Transcendental dynamics and complex analysis, P. J. RIPPON & G. M. STALLARD (eds)
- 349 Model theory with applications to algebra and analysis I, Z. CHATZIDAKIS, D. MACPHERSON, A. PILLAY & A. WILKIE (eds)
- 350 Model theory with applications to algebra and analysis II, Z. CHATZIDAKIS, D. MACPHERSON, A. PILLAY & A. WILKIE (eds)
- 351 Finite von Neumann algebras and masas, A. M. SINCLAIR & R. R. SMITH
- 352 Number theory and polynomials, J. MCKEE & C. SMYTH (eds)
- 353 Trends in stochastic analysis, J. BLATH, P. MÖRTERS & M. SCHEUTZOW (eds)
- 354 Groups and analysis, K. TENT (ed)
- 355 Non-equilibrium statistical mechanics and turbulence, J. CARDY, G. FALKOVICH & K. GAWEDZKI
- 356 Elliptic curves and big Galois representations, D. DELBOURGO
- 357 Algebraic theory of differential equations, M. A. H. MACCALLUM & A. V. MIKHAILOV (eds)
- 358 Geometric and cohomological methods in group theory, M. R. BRIDSON, P. H. KROPHOLLER & I. J. LEARY (eds)
- 359 Moduli spaces and vector bundles, L. BRAMBILA-PAZ, S. B. BRADLOW, O. GARCÍA-PRADA & S. RAMANAN (eds)
- 360 Zariski geometries, B. ZILBER
- 361 Words: Notes on verbal width in groups, D. SEGAL
- 362 Differential tensor algebras and their module categories, R. BAUTISTA, L. SALMERÓN & R. ZUAZUA
- 363 Foundations of computational mathematics, Hong Kong 2008, F. CUCKER, A. PINKUS & M. J. TODD (eds)
- 364 Partial differential equations and fluid mechanics, J. C. ROBINSON & J. L. RODRIGO (eds)
- 365 Surveys in combinatorics 2009, S. HUCZYNSKA, J. D. MITCHELL & C. M. RONEY-DOUGAL (eds)
- 366 Highly oscillatory problems, B. ENGQUIST, A. FOKAS, E. HAIRER & A. ISERLES (eds)
- 367 Random matrices: High dimensional phenomena, G. BLOWER
- 368 Geometry of Riemann surfaces, F. P. GARDINER, G. GONZÁLEZ-DIEZ & C. KOUROUNIOTIS (eds)
- 369 Epidemics and rumours in complex networks, M. DRAIEF & L. MASSOULIÉ
- 370 Theory of p -adic distributions, S. ALBEVERIO, A. YU. KHRENNIKOV & V. M. SHELKOVICH
- 371 Conformal fractals, F. PRZYTYCKI & M. URBANSKI
- 372 Moonshine: The first quarter century and beyond, J. LEPOWSKY, J. MCKAY & M. P. TUIITE (eds)
- 373 Smoothness, regularity, and complete intersection, J. MAJADAS & A. RODICIO
- 374 Geometric analysis of hyperbolic differential equations: An introduction, S. ALINHAC
- 375 Triangulated categories, T. HOLM, P. JØRGENSEN & R. ROQUIER (eds)
- 376 Permutation patterns, S. LINTON, N. RUŠKUC & V. VATTER (eds)
- 377 An introduction to Galois cohomology and its applications, G. BERHUY
- 378 Probability and mathematical genetics, N. H. BINGHAM & C. M. GOLDIE (eds)
- 379 Finite and algorithmic model theory, J. ESPARZA, C. MICHAUX & C. STEINHORN (eds)
- 380 Real and Complex Singularities, M. MANOEL, M. C. ROMERO FUSTER & C. T. L. WALLS (eds)

London Mathematical Society Lecture notes series: 377

An Introduction to Galois Cohomology and its Applications

GRÉGORY BERHUY
Université Joseph Fourier, Grenoble



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom
One Liberty Plaza, 20th Floor, New York, NY 10006, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India
103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.
It furthers the University's mission by disseminating knowledge in the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521738668

© G. Berhuy 2010
Foreword © J.-P. Tignol 2010

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press.

First published 2010

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-73866-8 Paperback

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party internet websites referred to in
this publication, and does not guarantee that any content on such websites is,
or will remain, accurate or appropriate.

Cambridge University Press

978-0-521-73866-8 — An Introduction to Galois Cohomology and its Applications

Grégory Berhuy

Frontmatter

[More Information](#)

To my dear friend Frédérique

Contents

<i>Foreword</i>	<i>page xi</i>
Introduction	1
Part I An introduction to Galois cohomology	11
I Infinite Galois theory	13
I.1 Reminiscences on field theory	13
I.2 Galois theory	17
I.2.1 Definitions and first examples	17
I.2.2 The Galois correspondence	18
I.2.3 Morphisms of Galois extensions	19
I.2.4 The Galois group as a profinite group	21
Exercises	24
II Cohomology of profinite groups	26
II.3 Cohomology sets: basic properties	26
II.3.1 Definitions	26
II.3.2 Functoriality	36
II.3.3 Cohomology sets as a direct limit	41
II.4 Cohomology sequences	45
II.4.1 The case of a subgroup	46
II.4.2 The case of a normal subgroup	51
II.4.3 The case of a central subgroup	52
II.5 Twisting	56
II.6 Cup-products	61
Exercises	64
III Galois cohomology	69
III.7 Warm-up	69
III.7.1 Digression: categories and functors	69

	III.7.2	Algebraic group-schemes	77
	III.7.3	The Galois cohomology functor	85
III.8		Abstract Galois descent	96
	III.8.1	Matrices reloaded	97
	III.8.2	Actions of group-valued functors	99
	III.8.3	Twisted forms	101
	III.8.4	The Galois descent condition	103
	III.8.5	Stabilizers	104
	III.8.6	Galois descent lemma	106
	III.8.7	Hilbert's Theorem 90	110
III.9		First applications of Galois descent	117
	III.9.1	Galois descent of algebras	117
	III.9.2	The conjugacy problem	121
	III.9.3	Cup-products with values in μ_2	126
		Exercises	130
IV		Galois cohomology of quadratic forms	134
IV.10		Algebraic group-schemes associated to quadratic forms	134
	IV.10.1	Quadratic forms over rings	134
	IV.10.2	Orthogonal groups	136
	IV.10.3	Clifford groups and spinors	139
IV.11		Galois cohomology of quadratic forms	145
	IV.11.1	Galois cohomology of orthogonal groups	145
	IV.11.2	Galois cohomology of spinors	147
IV.12		Cohomological invariants of quadratic forms	152
	IV.12.1	Classification of quadratic forms over \mathbb{Q}	152
	IV.12.2	Higher cohomological invariants	154
		Exercises	158
V		Étale and Galois algebras	160
V.13		Étale algebras	160
V.14		Galois algebras	164
	V.14.1	Definition and first properties	164
	V.14.2	Galois algebras and Galois cohomology	170
		Exercises	177
VI		Group extensions, Galois embedding problems and Galois cohomology	179
VI.15		Group extensions	179
VI.16		Galois embedding problems	185
		Exercises	187
Part II		Applications	189
VII		Galois embedding problems and the trace form	191
VII.17		The trace form of an étale algebra	192

<i>Contents</i>		ix
VII.18	Computation of $e^*(s_n)$	196
VII.19	Applications to inverse Galois theory	200
	Exercises	205
VIII	Galois cohomology of central simple algebras	207
VIII.20	Central simple algebras	207
VIII.21	Algebras with involutions	217
	VIII.21.1 Basic concepts	217
	VIII.21.2 Hyperbolic involutions	222
	VIII.21.3 Similitudes	226
	VIII.21.4 Cohomology of algebras with involution	228
	VIII.21.5 Trace forms	231
	Exercises	245
IX	Digression: a geometric interpretation of $H^1(-, G)$	249
IX.22	Reminiscences on schemes	249
IX.23	Torsors	253
	Exercises	259
X	Galois cohomology and Noether's problem	261
X.24	Formulation of Noether's problem	261
X.25	The strategy	262
X.26	Residue maps	265
X.27	An unramified cohomological invariant	271
X.28	Proof of Theorem X.24.1	272
XI	The rationality problem for adjoint algebraic groups	274
XI.29	R -equivalence groups	275
XI.30	The rationality problem for adjoint groups	278
XI.31	Examples of non-rational adjoint groups	281
	Exercises	287
XII	Essential dimension of functors	290
XII.32	Essential dimension: definition and first examples	290
XII.33	First results	292
XII.34	Cohomological invariants and essential dimension	296
XII.35	Generic objects and essential dimension	298
XII.36	Generically free representations	300
XII.37	Some examples	301
XII.38	Complements and open problems	306
	Exercises	308
<i>References</i>		310
<i>Index</i>		314

Foreword

Like an idea whose time has come, nonabelian Galois cohomology burst into the world in the mid 50's. There had been harbingers, of course. Châtelet's *méthode galoisienne* for genus 1 curves and Weil's observations on homogeneous spaces had opened the way, and it was a small step to write down the basic operations so that they make sense in a noncommutative situation. Within a few years, several pioneers realized almost simultaneously that the formalism of Galois cohomology could be used to classify various algebraic structures and to illuminate the definition of some of their invariants. This simple and remarkably penetrating idea, soon popularized by Serre's famous monograph *Cohomologie galoisienne*, immediately took hold. Galois cohomology is indeed algebra at its best: a few formal basic operations with a broad spectrum of far-reaching applications.

Grégory Berhuy's monograph provides a very welcome introduction to Galois descent techniques and nonabelian Galois cohomology, aimed at people who are new to the subject. Beginners will find here a thorough discussion of the technical details that are usually left to the reader. Together with advanced readers, they will appreciate a tasteful tour of applications, including some to which the author, himself an avid cocyclist, has contributed. (Incidentally, the title of Section III.8.1 also offers a glimpse into his taste in movies.) As may be expected, the list of applications discussed here is far from exhaustive, and in the last chapters the exposition is more demanding. It strikes a nice balance between a thorough account and a survey, and it provides a unique introduction to several of the exciting developments of the last decade, such as essential dimension and new advances on rationality problems. The many who did not have the good fortune to take his course at the University of Southampton will be thankful to Grégory Berhuy for making available the text of his lectures. I trust it will give to a large audience an idea of the scope and beauty of the subject, and inspire many of them to contribute to it in their turn.

Jean-Pierre Tignol