LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor J.W.S. Cassels, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge CB2 1SB, England

The titles below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

34 Representation theory of Lie groups, M.F. ATIYAH *et al*
46 p-adic analysis: a short course on recent work, N. KOBLITZ
50 Commutator calculus and groups of homotopy classes, H.J. BAUES
59 Applicable differential geometry, M. CRAMPIN & F.A.E. PIRANI
66 Several complex variables and complex manifolds II, M.J. FIELD
69 Representation theory, I.M. GELFAND *et al*
76 Spectral theory of linear differential operators and comparison algebras, H.O. CORDES
77 Isolated singular points on complete intersections, E.J.N. LOOIJENGA
83 Homogeneous structures on Riemannian manifolds, F. TRICERRI & L. VANHECKE
86 Topological topics, I.M. JAMES (ed)
87 Surveys in set theory, A.R.D. MATHIAS (ed)
88 FPF ring theory, C. FAITH & S. PAGE
89 An F-space sampler, N.J. KALTON, N.T. PECK & J.W. ROBERTS
90 Polytopes and symmetry, S.A. ROBERTSON
92 Representation of rings over skew fields, A.H. SCHOFIELD
93 Aspects of topology, I.M. JAMES & E.H. KRONHEIMER (eds)
94 Representations of general linear groups, G.D. JAMES
95 Low-dimensional topology 1982, R.A. FENN (ed)
96 Diophantine equations over function fields, R.C. MASON
97 Varieties of constructive mathematics, D.S. BRIDGES & F. RICHMAN
98 Localization in Noetherian rings, A.V. JATEGAONKAR
99 Methods of differential geometry in algebraic topology, M. KAROUBI & C. LERUSTE
100 Stopping time techniques for analysts and probabilists, L. EGGHE
104 Elliptic structures on 3-manifolds, C.B. THOMAS
105 A local spectral theory for closed operators, I. ERDELYI & WANG SHENGWANG
107 Compactification of Siegel moduli schemes, C-L. CHAI
108 Some topics in graph theory, H.P. YAP
109 Diophantine analysis, J. LOXTON & A. VAN DER POORTEN (eds)
110 An introduction to surreal numbers, H. GONSHOR
113 Lectures on the asymptotic theory of ideals, D. REES
114 Lectures on Bochner-Riesz means, K.M. DAVIS & Y-C. CHANG
115 An introduction to independence for analysts, H.G. DALES & W.H. WOODIN
116 Representations of algebras, P.J. WEBB (ed)
118 Skew linear groups, M. SHIRVANI & B. WEHRFRITZ
119 Triangulated categories in the representation theory of finite-dimensional algebras, D. HAPPEL
121 Proceedings of *Groups - St Andrews 1985*, E. ROBERTSON & C. CAMPBELL (eds)
122 Non-classical continuum mechanics, R.J. KNOPS & A.A. LACEY (eds)
125 Commutator theory for congruence modular varieties, R. FREESE & R. MCKENZIE
126 Van der Corput's method of exponential sums, S.W. GRAHAM & G. KOLESNIK
128 Descriptive set theory and the structure of sets of uniqueness, A.S. KECHRIS & A. LOUVEAU
129 The subgroup structure of the finite classical groups, P.B. KLEIDMAN & M.W. LIEBECK
130 Model theory and modules, M. PREST
131 Algebraic, extremal & metric combinatorics, M-M. DEZA, P. FRANKL & I.G. ROSENBERG (eds)
132 Whitehead groups of finite groups, ROBERT OLIVER
133 Linear algebraic monoids, MOHAN S. PUTCHA
134 Number theory and dynamical systems, M. DODSON & J. VICKERS (eds)
135 Operator algebras and applications, 1, D. EVANS & M. TAKESAKI (eds)
136 Operator algebras and applications, 2, D. EVANS & M. TAKESAKI (eds)
137 Analysis at Urbana, I, E. BERKSON, T. PECK, & J. UHL (eds)
138 Analysis at Urbana, II, E. BERKSON, T. PECK, & J. UHL (eds)
139 Advances in homotopy theory, S. SALAMON, B. STEER & W. SUTHERLAND (eds)
140 Geometric aspects of Banach spaces, E.M. PEINADOR & A. RODES (eds)
141 Surveys in combinatorics 1989, J. SIEMONS (ed)
144 Introduction to uniform spaces, I.M. JAMES
145 Homological questions in local algebra, JAN R. STROOKER
146 Cohen-Macaulay modules over Cohen-Macaulay rings, Y. YOSHINO
147 Continuous and discrete modules, S.H. MOHAMED & B.J. MÜLLER
148 Helices and vector bundles, A.N. RUDAKOV *et al*
149 Solitons, nonlinear evolution equations and inverse scattering, M. ABLOWITZ & P. CLARKSON
150 Geometry of low-dimensional manifolds 1, S. DONALDSON & C.B. THOMAS (eds)
151 Geometry of low-dimensional manifolds 2, S. DONALDSON & C.B. THOMAS (eds)
152 Oligomorphic permutation groups, P. CAMERON
153 L-functions and arithmetic, J. COATES & M.J. TAYLOR (eds)
154 Number theory and cryptography, J. LOXTON (ed
155 Classification theories of polarized varieties, TAKAO FUJITA
156 Twistors in mathematics and physics, T.N. BAILEY & R.J. BASTON (eds)

158 Geometry of Banach spaces, P.F.X. MÜLLER & W. SCHACHERMAYER (eds)
159 Groups St Andrews 1989 volume 1, C.M. CAMPBELL & E.F. ROBERTSON (eds)
160 Groups St Andrews 1989 volume 2, C.M. CAMPBELL & E.F. ROBERTSON (eds)
161 Lectures on block theory, BURKHARD KÜLSHAMMER
162 Harmonic analysis and representation theory, A. FIGA-TALAMANCA & C. NEBBIA
163 Topics in varieties of group representations, S.M. VOVSI
164 Quasi-symmetric designs, M.S. SHRIKANDE & S.S. SANE
165 Groups, combinatorics & geometry, M.W. LIEBECK & J. SAXL (eds)
166 Surveys in combinatorics, 1991, A.D. KEEDWELL (ed)
167 Stochastic analysis, M.T. BARLOW & N.H. BINGHAM (eds)
168 Representations of algebras, H. TACHIKAWA & S. BRENNER (eds)
169 Boolean function complexity, M.S. PATERSON (ed)
170 Manifolds with singularities and the Adams-Novikov spectral sequence, B. BOTVINNIK
171 Squares, A.R. RAJWADE
172 Algebraic varieties, GEORGE R. KEMPF
173 Discrete groups and geometry, W.J. HARVEY & C. MACLACHLAN (eds)
174 Lectures on mechanics, J.E. MARSDEN
175 Adams memorial symposium on algebraic topology 1, N. RAY & G. WALKER (eds)
176 Adams memorial symposium on algebraic topology 2, N. RAY & G. WALKER (eds)
177 Applications of categories in computer science, M. FOURMAN, P. JOHNSTONE, & A. PITTS (eds)
178 Lower K- and L-theory, A. RANICKI
179 Complex projective geometry, G. ELLINGSRUD *et al*
180 Lectures on ergodic theory and Pesin theory on compact manifolds, M. POLLICOTT
181 Geometric group theory I, G.A. NIBLO & M.A. ROLLER (eds)
182 Geometric group theory II, G.A. NIBLO & M.A. ROLLER (eds)
183 Shintani zeta functions, A. YUKIE
184 Arithmetical functions, W. SCHWARZ & J. SPILKER
185 Representations of solvable groups, O. MANZ & T.R. WOLF
186 Complexity: knots, colourings and counting, D.J.A. WELSH
187 Surveys in combinatorics, 1993, K. WALKER (ed)
188 Local analysis for the odd order theorem, H. BENDER & G. GLAUBERMAN
189 Locally presentable and accessible categories, J. ADAMEK & J. ROSICKY
190 Polynomial invariants of finite groups, D.J. BENSON
191 Finite geometry and combinatorics, F. DE CLERCK *et al*
192 Symplectic geometry, D. SALAMON (ed)
193 Computer algebra and differential equations, E. TOURNIER (ed)
194 Independent random variables and rearrangement invariant spaces, M. BRAVERMAN
195 Arithmetic of blowup algebras, WOLMER VASCONCELOS
196 Microlocal analysis for differential operators, A. GRIGIS & J. SJÖSTRAND
197 Two-dimensional homotopy and combinatorial group theory, C. HOG-ANGELONI, W. METZLER & A.J. SIERADSKI (eds)
198 The algebraic characterization of geometric 4-manifolds, J.A. HILLMAN
199 Invariant potential theory in the unit ball of $\mathbf{C}^n$, MANFRED STOLL
200 The Grothendieck theory of dessins d'enfant, L. SCHNEPS (ed)
201 Singularities, JEAN-PAUL BRASSELET (ed)
202 The technique of pseudodifferential operators, H.O. CORDES
203 Hochschild cohomology of von Neumann algebras, A. SINCLAIR & R. SMITH
204 Combinatorial and geometric group theory, A.J. DUNCAN, N.D. GILBERT & J. HOWIE (eds)
205 Ergodic theory and its connections with harmonic analysis, K. PETERSEN & I. SALAMA (eds)
206 An introduction to noncommutative differential geometry and its physical applications, J. MADORE
207 Groups of Lie type and their geometries, W.M. KANTOR & L. DI MARTINO (eds)
208 Vector bundles in algebraic geometry, N.J. HITCHIN, P. NEWSTEAD & W.M. OXBURY (eds)
209 Arithmetic of diagonal hypersurfaces over finite fields, F.Q. GOUVÊA & N. YUI
210 Hilbert C*-modules, E.C. LANCE
211 Groups 93 Galway / St Andrews I, C.M. CAMPBELL *et al*
212 Groups 93 Galway / St Andrews II, C.M. CAMPBELL *et al*
214 Generalised Euler-Jacobi inversion formula and asymptotics beyond all orders, V. KOWALENKO, N.E. FRANKEL, M.L. GLASSER & T. TAUCHER
215 Number theory, S. DAVID (ed)
216 Stochastic partial differential equations, A. ETHERIDGE (ed)
217 Quadratic forms with applications to algebraic geometry and topology, A. PFISTER
218 Surveys in combinatorics, 1995, PETER ROWLINSON (ed)
220 Algebraic set theory, A. JOYAL & I. MOERDIJK
221 Harmonic approximation, S.J. GARDINER
222 Advances in linear logic, J.-Y. GIRARD, Y. LAFONT & L. REGNIER (eds)
223 Analytic semigroups and semilinear initial boundary value problems, KAZUAKI TAIRA
224 Computability, enumerability, unsolvability, S.B. COOPER, T.A. SLAMAN & S.S. WAINER (eds)
226 Novikov conjectures, index theorems and rigidity I, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
227 Novikov conjectures, index theorems and rigidity II, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
228 Ergodic theory of $\mathbf{Z}^d$ 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)

London Mathematical Society Lecture Note Series. 230

Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2

J.W.S. Cassels
University of Cambridge

E.V. Flynn
University of Liverpool

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521483704

First published 1996

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

ISBN-13 978-0-521-48370-4 paperback
ISBN-10 0-521-48370-0 paperback

Transferred to digital printing 2005

Contents

Chapters are divided into sections. Some topics occupy several sections. We give a name to a section and list it here only when it starts a new topic.

Foreword

The arithmetic (= number theory) of curves of genus 0 is well understood. For genus 1, there is a rich body of theory and conjecture, and in recent years notable success has been achieved in transforming the latter into the former. For curves of higher genus there is a rich body of theory with some spectacular successes (e.g. Faltings' proof of 'Mordell's Conjecture'), but our command is still rudimentary. For genus 1, a concrete question about an individual curve can usually be answered by one means or another: for higher genus, this is far from the case.

For curves of genus 0 and 1 the road between general theory and particular cases is no one-way street. Numerous individual cases were investigated by amateurs as well as as by distinguished mathematicians such as Diophantos, Fermat, Euler, Sylvester, Mordell, Selmer, Birch and Swinnerton-Dyer. Regularities which emerged, sometimes quite unexpectedly, suggested theorems, which could sometimes be proved. The new theorems suggested new questions. For higher genus, existing theory is notoriously unadapted to the study of individual curves, and few have been elucidated. What is needed is a corpus of explicit concrete cases and a middlebrow arithmetic theory which would provide both a practicable means to obtain them and a framework to understand any unexpected regularities.

Such a theory will, of course, draw freely from the existing body of knowledge, but the emphasis on feasibility gives new perspectives. Classical geometers worked over an algebraically closed field, usually the complexes. Modern geometers take account of the ground field, but regard a field extension as a cheap manoeuvre. For practical computations it is desperately expensive: the theory we seek must avoid them at almost all costs.

A natural place to begin is with a curve of genus 2 defined over the rationals and a natural first problem is to determine its Mordell-Weil group (or at least the rank). General theory suggests an approach through the (arithmetic) jacobian, the arithmetic analogue of the complex manifold studied in the 19th century. Although it figures prominently in the general theory, we appear to have been the first to describe it explicitly, as a surface in 15-dimensional projective space. It is an inconveniently large object, but fortunately much information is retained in its Kummer surface. These are surfaces of degree 4, which were also the subject of intensive 19th century study over the reals and complexes.

Our first attack on the Mordell-Weil group was a simple-minded generalization of an algorithm for elliptic curves. The study of the classical geometrical literature gave a deeper understanding of the algorithm and also new perspectives on the geometric theory. The algorithm is still not easy. In appropriate cases, however, there is an isogeny of degree 4 analogous to that of degree 2 for elliptic curves which, where it exists, permits the determination of the rank on a production-line basis.¶

A less sophisticated, but deeper, problem is to ask for all the rational points on a curve of genus 2. The number is finite by Faltings' Theorem, but the proof gives no hope of a reasonable algorithm. An old theorem of Chabauty states (as a special case) that the number is finite if the Mordell-Weil rank is (0 or) 1. As a theorem, it is superseded by Faltings, but the proof gives a feasible approach. Until recently, no actual example was known. The first was given by† Gordon & Grant (1993), and now there are many.

Some chapters do not require everything that goes before. In particular, the computational Chapters 8, 10, 11, 12, 13 do not depend on Chapters 4, 5.

Even with the emphasis on feasibility, the manipulations would have daunted a Gauss or a Salmon. Our investigations would have been impossible without the resources of computer algebra. We have not attempted to reproduce the larger formulae in the text, but have made them available‡ in machine-readable form by ftp. We give in Appendix I programs which enable the reader to check our assertions and to produce formulae for herself. They are in the computer language MAPLE, the algebra package we have mainly used, and are heavily annotated: a reader who prefers another package should have no difficulty in adapting them. The MAPLE programs are also available by ftp.

This volume is a progress report on a project which has lasted, on and off, more than ten years. We are grateful to SERC and its successor EPSRC for grants to JWSC which supported EVF for four years. The text has benefited from Ed Schaefer's criticism of an earlier draft. The canonical disclaimer applies.

¶ As for elliptic curves, the algorithm is not effective in the logical sense. But it usually works.

† References are cited by name(s) and date, with a possible further letter.

‡ See Appendix II.

Background and conventions

0 Introduction. In writing we have had in mind a beginning graduate student with some exposure to algebraic geometry.¶ Here we indicate our point of view. We fix some notation and recall some definitions and background. These are illustrated by a simple computation.

We shall be working over a ground field such as the rationals $\mathbb{Q}$ or the p-adics $\mathbb{Q}_p$. First, however, we look at an algebraically closed field.

1 Algebraically closed ground field. Let $\bar{k}$ be an algebraically closed field, for simplicity of characteristic 0, and let $\mathcal{B}$ be a complete curve defined over $\bar{k}$. For example $\mathcal{B}$ may be a nonsingular curve in a projective space defined by equations with coefficients in $\bar{k}$. A *divisor* $\mathfrak{A} = \sum_{\mathfrak{a}} n_{\mathfrak{a}} \mathfrak{a}$ on $\mathcal{B}$ is an element of the free abelian group Div on (symbols for) the points on $\mathcal{B}$ defined over $\bar{k}$. A point $\mathfrak{a}$ of $\mathcal{B}$ has a multiplicity $n_{\mathfrak{a}}$ in $\mathfrak{A}$ which is an integer, and is 0 for all except finitely many $\mathfrak{a}$. The set of points with nonzero multiplicity in a divisor is its *support*. The *degree* of a divisor is the sum $\sum_{\mathfrak{a}} n_{\mathfrak{a}}$ of the multiplicities of the points.

A nonzero function f on $\mathcal{B}$ determines a divisor $[f]$ as follows. The multiplicity† of a point $\mathfrak{a}$ in $[f]$ is the order to which f vanishes at $\mathfrak{a}$ measured in terms of a *local uniformizer*: so the multiplicity is negative if $\mathfrak{a}$ is a pole. A divisor of the form $[f]$ is a *principal divisor*. Principal divisors have degree 0.

The principal divisors are a subgroup of Div. Two divisors differing by a principal divisor are *linearly equivalent* or in the same *divisor class*. The divisor classes form the *Picard group* Pic. Pic inherits a degree from Div. The set of elements of Pic of degree j is denoted by Pic^j. Clearly Pic^0 is a subgroup of Pic.

¶ e.g. Chapters I, II of Silverman (1986). We shall also assume that the reader is familiar with the idea of a field with a valuation, in particular the p-adic numbers $\mathbb{Q}_p$ [see Chapter 2 of Cassels (1991) or the first few chapters of Cassels (1986)]. It would be helpful for the reader to have had a brief introduction to elliptic curves; either Cassels (1991) or Chapters III, IV, VII, VIII of Silverman (1986) would be more than sufficient.

† A Mickey Mouse example follows.

Similarly we can define the divisor of a *differential* $h\mathrm{d}f$, where f, h are functions, in terms of local uniformizers. The divisors of differentials are all in the same divisor class, the *canonical class*. The degree of the canonical class is $2g-2$, where g is the *genus*. A divisor $\mathfrak{A}$ is *effective* if all the points of its support have nonnegative multiplicity. There is a partial order $\succ$ on Div: by definition $\mathfrak{A} \succ \mathfrak{B}$ if $\mathfrak{A}-\mathfrak{B}$ is effective. For given divisor $\mathfrak{A}$, the set of functions f with¶ $[f] \succ -\mathfrak{A}$ together with $f=0$ form a vector space over $\bar{k}$. It has a finite dimension given by the *Riemann-Roch Theorem*, which we do not rehearse.

Still working over an algebraically closed field $\bar{k}$, we suppose that the characteristic is not 2 and take as an example the curve $\mathcal{C}$ given in the affine plane by

$$Y^2 = \prod_{j=1}^{6}(X-\theta_j).$$

It is not complete: there are two points $\mathfrak{b}_1$, $\mathfrak{b}_2$ 'at infinity'. The points $\mathfrak{a}_j = (\theta_j, 0)$ are the *Weierstrass points*. Then Y is a local uniformizer at the $\mathfrak{a}_j$ and X^{-1} is a local uniformizer at the $\mathfrak{b}_j$. Otherwise, $(X-x)$ is a local uniformizer at (x,y). Hence the divisor of $\mathrm{d}X$ is†

$$-2\mathfrak{b}_1 - 2\mathfrak{b}_2 + \sum \mathfrak{a}_j,$$

which is by definition in the canonical class. It has degree

$$6-2-2 = 2 = 2g-2,$$

so the genus g is 2. Since

$$[Y] = -3\mathfrak{b}_1 - 3\mathfrak{b}_2 + \sum \mathfrak{a}_j,$$

it follows that $\mathfrak{b}_1 + \mathfrak{b}_2$, the divisor of poles of X, is in the canonical class.

2 Perfect ground field. One can develop algebraic geometry from scratch over a general ground field k [e.g. Chevalley (1951)]. We are concerned only with k of characteristic 0 or, very occasionally, of finite cardinality, so a less sophisticated approach suits us better. Let $\bar{k}$ be the algebraic

¶ The negative sign here is traditional.

† The multiplicity $n_{\mathfrak{p}}$ of $\mathfrak{p}$ is the order of $\mathrm{d}X/\mathrm{d}t_{\mathfrak{p}}$ at $\mathfrak{p}$, where $t_{\mathfrak{p}}$ is a local uniformizer: that is $t_{\mathfrak{p}}^{-n_{\mathfrak{p}}}\mathrm{d}X/\mathrm{d}t_{\mathfrak{p}}$ has neither a zero nor a pole at $\mathfrak{p}$.

closure of k. Then Gal $= \mathrm{Gal}(\bar{k}/k)$ acts on all the objects in the algebraic geometry over $\bar{k}$. We say that a divisor, etc. is *defined over* k if it is fixed under the action of Galois. If there is only one ground field k of interest at the time, we may say *rational* instead of 'defined over k'. (But we have to avoid the phrase 'a rational curve' since this is established as a synonym of 'a curve of genus 0'.) The only slightly tricky point to note is that if a divisor is defined over k and principal, then it is the divisor of a function defined over k. This is a special case of a general principle proved in the following Appendix. On the other hand, and this will turn out to be crucial, a rational divisor class does not necessarily contain a rational divisor, see the Appendix to Chapter 4.

Appendix

Finite-dimensional Galois modules

The following theorem is often useful in deducing results over k from those over $\bar{k}$ [Cartier (1960)].

THEOREM. *Let $\mathfrak{M}$ be a finite-dimensional $\bar{k}$-module. Suppose given an action of* Gal *on $\mathfrak{M}$ compatible with the $\bar{k}$-structure. We shall say that $\mu \in \mathfrak{M}$ is defined over an extension K of k if μ is fixed by every $\sigma \in$ Gal which leaves K elementwise fixed. Suppose that every element of $\mathfrak{M}$ is defined over some finite extension of k. Then $\mathfrak{M}$ has a $\bar{k}$-basis consisting of elements defined over k.*

Note. The 1-dimensional case is the standard generalization of Hilbert 90 under a light disguise, cf. Serre (1962), p. 159.

Proof. We denote by $\mathfrak{M}_k$ the set of elements of $\mathfrak{M}$ defined over k. It inherits a structure as k-vector space from $\mathfrak{M}$.
(i) *$\mathfrak{M}$ is $\bar{k}$-spanned by the elements of $\mathfrak{M}_k$.* Let $\mu \in \mathfrak{M}$, so μ is defined over a finite extension K of k, which without loss of generality may be supposed to be normal. Let $\omega_1, \dots, \omega_n$ be a basis of K/k and let $\tau_1, \dots, \tau_n$ be representatives in Gal of the Galois group of K/k. Put

$$\begin{aligned} m_j &= \sum_{i=1}^{n} \tau_i(\omega_j \mu) \\ &= \sum_{i=1}^{n} (\tau_i \omega_j)(\tau_i \mu) \qquad (1 \leqslant j \leqslant n). \end{aligned}$$

Clearly $m_j \in \mathfrak{M}_k$. Since $\det_{i,j}(\tau_i \omega_j) \neq 0$ by a basic theorem of Galois theory, μ is a $\bar{k}$-linear combination of the m_j.

(ii) *If m_j $(1 \leqslant j \leqslant J)$ in $\mathfrak{M}_k$ are linearly dependent over $\bar{k}$, then they are already linearly dependent over k.* The proof is similar. Suppose that $\sum \lambda_j m_j = 0$, where the λ_j are not all 0 and, without loss of generality, are all in some finite normal extension K of k. Then by multiplying the relation by the elements of a basis of K/k and taking traces, we get linear relations between the m_j with coefficients in k, not all 0.

(iii) We can now complete the proof. By hypothesis $\mathfrak{M}$ is $\bar{k}$-spanned by a finite set of elements, and so, by (i), it is $\bar{k}$-spanned by a finite set $\mathcal{S} \subset \mathfrak{M}_k$. Let $\mathcal{S}_0$ be a maximal k-independent subset of $\mathcal{S}$. Then $\mathcal{S}_0$ is $\bar{k}$-independent by (ii), and so is the required $\bar{k}$-basis of $\mathfrak{M}$.