North-Holland Mathematical Library

Cubic Forms
Algebra, Geometry, Arithmetic

YU. I. MANIN

VOLUME 4

Cubic Forms
Algebra, Geometry, Arithmetic

YU. I. MANIN

Mathematical Institute V. A. Steklov
Academy of Sciences of the U.S.S.R.
Moscow

Translated from Russian
by
M. Hazewinkel

Second Edition

1986

NORTH-HOLLAND
AMSTERDAM · NEW YORK · OXFORD

First edition 1974
Second edition 1986

ISBN: 0444 878238

Published by:
ELSEVIER SCIENCE PUBLISHERS B.V.
P.O. Box 1991
1000 BZ Amsterdam
The Netherlands

Sole distributors for the U.S.A. and Canada:
ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
52, Vanderbilt Avenue
New York, NY 10017
U.S.A.

Library of Congress Cataloging-in-Publication Data

Manin, IU. I.
Cubic forms.

(North-Holland mathematical library ; v. 4)
Translation of: Kubicheskie formy.
Bibliography: p
Includes index.
1. Surfaces, Cubic. I. Title. II. Series.
QA573.M2513 1986 516.3'6 83-20463
ISBN 0-444-87823-8 (U.S.)

Printed in the Netherlands

North-Holland Mathematical Library

VOLUME 4

NORTH-HOLLAND
AMSTERDAM · NEW YORK · OXFORD

PREFACE TO THE SECOND EDITION

In the ten years since this book was published in English, there has been important progress in a number of topics related to its subject. Were this book to be written anew, its title could be *Algebraic Varieties close to the Rational Ones. Algebra, Geometry, Arithmetic*. In fact, this class of varieties has crystallized as a natural domain for the methods developed and expounded in *Cubic Forms*.

In this edition the original text is left intact, except for a few corrections, but an Appendix is added together with a list of references to original papers, mainly of the last decade.

This Appendix sketches some of the most essential new results, constructions and ideas, including the solutions of the Lüroth and Zariski problems, the theory of the descent and obstructions to the Hasse principle on rational varieties, and recent applications of K-theory to arithmetic. Proofs are omitted since their complete presentation would demand a new book. Meanwhile, this modest report will hopefully be of use.

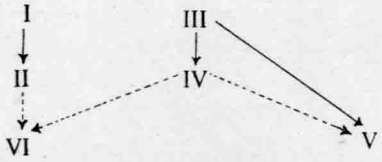
I am deeply indebted to V. E. Voskresenski and M. A. Tsfasman for their help in preparing this second edition.

Moscow, 1984. Yu. I. Manin

INSTRUCTIONS TO THE READER

1. The first sections of all chapters can be read consecutively, independently of the remaining text. These sections contain a survey of the main concepts and results of the book, as well as some motivation and examples.

2. Interdependence table of the chapters:



(Dashed arrows indicate a weak dependence.)

3. Some standard notation:

$\mathbf{Z}$ – the integers,
$\mathbf{Q}$ – the rational numbers,
$\mathbf{R}$ – the real numbers,
$\mathbf{C}$ – the complex numbers,
$\mathbf{Q}_p$ – the field of p-adic numbers,
$\mathbf{Z}_n$ – the cyclic group of order n.

4. The list of references, the author index, a list of the most frequently occurring symbols, and the subject index can be found at the end of the book.

CONTENTS

PREFACE TO THE SECOND EDITION v

CONTENTS vii

INSTRUCTIONS TO THE READER x

INTRODUCTION 1

CHAPTER I. CH-QUASIGROUPS AND MOUFANG LOOPS 6
1. A survey of definitions and results 6
2. Symmetric Abelian quasigroups 11
3. CH-quasigroups 15
4. Commutative Moufang loops 21
5. The connection between CH-quasigroups and Moufang loops . . . 25
6. Morphisms of CH-quasigroups and Moufang loops 28
7. The first structure theorem 30
8. The second structure theorem 33
9. Finite Fischer groups 34
10. Unsolved problems and bibliographical remarks 39

CHAPTER II. CLASSES OF POINTS ON CUBIC HYPERSURFACES 42
11. Admissible equivalence relations: a survey 42
12. Unirationality 46
13. Universal equivalence 54
14. R-equivalence: the basic properties 61
15. R-equivalence and quadratic extensions 65
16. Universal equivalence over local fields. Examples 69
17. Bibliographical remarks 76

CHAPTER III. TWO-DIMENSIONAL BIRATIONAL GEOMETRY 77
18. The main results 77
19. Monoidal transformations 82
20. Monoidal transformations and divisors 90
21. The main theorems on birational maps 100
22. Bibliographical remarks 110

CHAPTER IV. THE TWENTY-SEVEN LINES 112
23. A survey of the results 112
24. Del Pezzo surfaces 117
25. The Picard group and root systems 126
26. Exceptional curves and Weyl groups 134
27. The zeta function 143
28. Minimality and classes of conjugate elements in Weyl groups . . . 151
29. A cohomological invariant and the degree of unirationality 154
30. Rational points 162
31. Tables and comments. Calculation of H^1. The theorem of Artin and Tate 174
32. Bibliographical remarks 182

CHAPTER V. MINIMAL CUBIC SURFACES 184
33. A survey of the results 184
34. The fundamental birational invariant 189
35. A bubble space 195
36. Calculations on cubic surfaces 200
37. Birational non-triviality 202
38. Birational classification 204
39. Relations between the generators 206
40. Bibliographical remarks 219

CHAPTER VI. THE BRAUER–GROTHENDIECK GROUP 220
41. A survey of the results. Obstructions to the Hasse principle 220
42. The construction of Azumaya algebras 229
43. Brauer equivalence 234
44. The finiteness theorem 237
45. Calculations for Brauer equivalence. Examples 243
46. A negative result 264
47. Counter-examples to the Hasse principle 276
48. Bibliographical remarks 283

APPENDIX. ALGEBRAIC VARIETIES CLOSE TO THE RATIONAL ONES. ALGEBRA, GEOMETRY, ARITHMETIC

Introduction 284
1. Galois cohomology, Picard groups and birational geometry 285
2. The Hasse principle and descent on rational varieties 288
3. Geometry of rational surfaces. Complements 294

4. The Lüroth problem and the Zariski problem in dimension ≥ 3 302
5. Rational points and equivalence relations. 306
6. Cubic surfaces and commutative Moufang loops (CML) 309
References (for the Appendix) 313

REFERENCES 318

AUTHOR INDEX 323

LIST OF SYMBOLS. 324

SUBJECT INDEX 325

INTRODUCTION

0.1. Every mathematician who is not indifferent to number theory has felt the charm of Fermat's theorem on the sum of two squares of natural numbers. A psychologist of the Jungian school would probably think that such diophantine problems are archetypal to a high degree.

The basic idea for the book presented here arose from an attempt to find out what happens in the case of sums of three rational cubes. Needless to say, the result is not nearly so simple, fundamental and complete as the classical pattern. The author has generalized the problem along all the lines which occurred to him, and has used all technical resources known to him. He obtained as a result the multitude of non-associative composition laws, monoidal transformations and Galois cohomologies which make up this book.

0.2. The problem of the sum of three cubes has a respectable history. The basic result by the classical mathematicians is the following (see Dickson [1]):

Theorem. *Every rational number is a sum of three rational cubes.*

First proof (Ryley (1825); Richmond (1930)):

$$a = \left(\frac{a^3 - 3^6}{3^2a^2+3^4a+3^6}\right)^3 + \left(\frac{-a^3+3^5a+3^6}{3^2a^2+3^4a+3^6}\right)^3 + \left(\frac{3^3a^2+3^5a}{3^2a^2+3^4a+3^6}\right)^3$$

his proof is simple, but not too illuminating. It would be nice to know what es behind this identity.

Second proof: After having added an extra coordinate T_0, we can write the equation in homogeneous form:

$$aT_0^3 + T_1^3 + T_2^3 + T_3^3 = 0\,.$$

This is the equation of a smooth cubic surface V in a three-dimensional projective space. There are 'trivial' rational points on this surface, e.g. $(0, 0, 1, -1)$. Unfortunately these lie in the plane at infinity and do not give a solution to our original problem. However, rational points on a cubic surface can be multiplied, that is, we can construct new ones, starting from known points.

The first idea. Let $x \in V$ be some rational point. Construct the tangent plane to V at x and let us denote by $C(x)$ its intersection with V.

'Generally speaking', $C(x)$ is an irreducible cubic curve in this plane with x as a double point. Through x we draw all the lines in rational directions which are tangent to V. Each of these lines must intersect the cubic curve $C(x)$ in three points (counting multiplicities); but the intersection at x has multiplicity two, which leaves only one point. The coordinates of this point are necessarily rational. In fact, the coordinates of the intersection points in terms of the parameters of the equations of the line are the roots of a cubic equation with rational coefficients. This equation has a double rational root, corresponding to x; therefore the third root is also rational. After this one can apply the same procedure to the rational points of the curve $C(x)$ and so on.

Unfortunately, for $x = (0, 0, 1, -1)$ the curve $C(x)$ consists of three lines which are conjugate over $\mathbf{Q}$, and there are no rational points on it except for x.

The second idea. In this case we draw a line in an arbitrary rational direction. We only take care that the two other points of intersection of this line with V, say y and $\bar{y}$, do not coincide and that the curves $C(y)$ and $C(\bar{y})$ are 'good' as described above.

Then the previous argument on cubic polynomials shows that $y, \bar{y}$ are defined and conjugate over some quadratic extension K of the field of rational numbers $\mathbf{Q}$. (It can happen by accident that $y, \bar{y}$ even have rational coordinates, but then the problem is solved.)

As above, we construct 'many' points on $C(y)$ with coordinates in K. Take one of those points, say z, construct its conjugate $\bar{z}$, and draw the line through z and $\bar{z}$. Because z and $\bar{z}$ are conjugate, we can assume that the coefficients of the parameter equation of this line are rational. The third (besides z and $\bar{z}$) of its intersection points with V, which we denote by $z \circ \bar{z}$, then also has rational coordinates (by the same argument on cubic polynomials).

Of course, if we start with $z = y$, we simply return to $y \circ \bar{y} = x$, but it is not difficult to show that other points $z \in C(y)$ give many new rational points including points which do not lie in the plane at infinity.

0.3. Although the second proof is considerably longer than the first, it contains, in embryo form, interesting possibilities for establishing approaches towards getting a review of all solutions of the equation, instead of giving only an existence proof.

Multiplying points by means of $C(x)$ gives an infinite family of solutions of our diophantine equation. These solutions depend on as many independent parameters as desired (the directions of the lines which occur in the construction). Can all solutions be covered by a finite number of such families? How many parameters are sufficient for this?

The composition law $x \circ y$ is not defined everywhere (e.g., what is $x \circ x$?); all the same it permits us to obtain new solutions from old ones. Is it possible, by combining this composition with the construction of points on $C(x)$, to obtain all solutions out of a finite number of them?

0.4. A positive answer to the latter question is known; not for cubic surfaces, but only for cubic curves (without singular points), say $aT_0^3 + T_1^3 + T_2^3 = 0$. This is the famous Mordell–Weil theorem on elliptic curves. The algebra, geometry and arithmetic of cubic curves (one could add analysis, e.g. theta functions) constitute a vast and actively developing field; see the survey of Cassels [3] in the list of references.

The natural more-dimensional generalizations of elliptic curves, however, are the Abelian varieties (and homogeneous spaces over them) and in general not the cubic (hyper)surfaces. Nevertheless, it turns out that over non-closed fields (in particular over number fields), there is a whole series of results from the theory of elliptic curves which admit non-trivial analogues in the theory of cubic surfaces. (Sometimes the statement of the theorem carries over almost verbatim, although the mechanics of the proofs in dimension 2 have nothing in common with the one-dimensional case; see Section 33.)

Three fundamental parallels follow.

0.5. (a) The composition law $xy = u \circ (x \circ y)$ (u fixed) on an elliptic curve turns its set of points into an Abelian group. (As above, the point $x \circ y$ is defined by the property that $x, y, x \circ y$ are on one line.) On a cubic surface one can divide the set of points into classes such that these classes can be composed in a unique way by means of lines through representatives. After this the composition law $XY = U \circ (X \circ Y)$ turns the set of classes E into an 'almost' Abelian group of exponent six. 'Almost' because this composition can apparently be

non-associative. A slightly weaker associativity condition than the usual one, which can be successfully proved, defines on E the structure of a 'commutative Moufang loop'. This structure is studied in Chapter I of this book, and the composition of classes of points in Chapter II.

(b) The translations by means of a rational point generate almost all of the group of birational maps of an elliptic curve into itself (more precisely, they generate a subgroup of finite index). In the two-dimensional case, the translation by x defines analogously a birational map $t_x : v \mapsto x \circ v$ of a surface into itself. These maps (and similar ones connected with quadratic extensions of the base field) also generate a subgroup of finite index in the group of all birational maps of V into itself; in any case, if V is minimal. The proof (with substantial specifications) is contained in Chapter V.

(c) An algorithm for settling the question of whether there are rational points on a given plane elliptic curve has up till now not been found. The first necessary condition is that there exist points 'everywhere locally'. This being fulfilled, there is the second necessary condition that the so-called Cassels–Tate form becomes zero. In Chapter VI it will be shown that the second condition admits a quite general formulation, which is in particular applicable to cubic surfaces. There we also obtain (rather restricted) results on the questions formulated in section 0.3. They give lower estimates for the necessary number of parameters and for the number of generators of the set of points.

These three subjects also represent, respectively, algebra, geometry and arithmetic. Analysis and topology could essentially complete the picture. For instance, starting with dimension 3, the 'intermediate Jacobians' of A. Weil appear. In a less traditional direction we can expect that the group generated by the maps t_x has interesting ergodic properties. All this is not touched upon in this book.

0.6. A part of the results expounded here has been taken from the journal literature, old and new (including papers of the author). Another part is published here for the first time, for example the discussion on universal equivalence in Chapter II and almost all calculations of Chapter VI.

Mainly classical material is contained in Chapter IV, where the geometry of the famous configuration of the 27 lines and its generalisations and applications are studied. Chapter III presents the necessary preparatory information on birational maps.

The required algebraic–geometric background of the reader increases mono-

tonically with the numbers of the chapters. In Chapter I, in general no algebraic geometry is required. To understand Chapter II, it suffices if the reader is familiar with the lectures of Šafarevič [2] (by no means to its fullest extent). Chapters III–V require the mastery of approximately half of Mumford's book [2], if the reader is willing to take a series of theorems on trust. Finally in Chapter VI already the ghosts of étale cohomology faintly stir. To understand it, it is also necessary to have some acquaintance with class field theory (structure of the Brauer group for local and global fields).

I.R. Šafarevič taught me the algebraic–geometric approach to number theory. Around ten years ago he drew my attention to cubic surfaces. He conjectured, in particular, that some non-associative structure must play a role in the description of the set of rational points. When these structures started to appear, I was assisted in dealing with them by B B. Venkov, A.I. Kostrikin and V.A. Belousov. The talks with V.A. Iskovskih on the Brauer group have been very useful to me. Some of the results of Chapter II are due to A. Bel'skii; he has also been of considerable assistance in preparing the manuscript for printing. The identification of the root systems R_r in Chapter IV has been done by means of a method communicated to me by P. Deligne in a private letter. To all these persons I am deeply indebted.

The papers of Grothendieck [2], Segre [3] and Châtelet [1] have most of all influenced the formation of the new ideas of this treatise.

Moscow, 1969–1970 Yu. I. Manin

CHAPTER I

CH-QUASIGROUPS AND MOUFANG LOOPS

First Scene:

An open place. Thunder and lightning.
Enter three witches.

Shakespeare. Macbeth, Act I

1. A survey of definitions and results

In this chapter we introduce and study some algebraic structures which emerge in the theory of cubic hypersurfaces. The first section contains a survey of those results which have immediate applications in that theory. I strongly recommend to restrict oneself at first to this survey and to go on directly to the second chapter, returning to the first when necessary. Here we give the exact definitions, state the theorems and give some motivation; the proofs are contained in the next sections.

Definition 1.1. A set E with a binary composition law $E \times E \to E$: $(x, y) \mapsto x \circ y$ is called a *symmetric quasigroup* if it satisfies one of the following equivalent conditions:

(i) The three-place relation $L(x, y, z) : x \circ y = z$ is invariant under all permutations of x, y, z.

(ii) The following identities hold for all $x, y \in E$:

$$x \circ y = y \circ x , \tag{I.1}$$

$$x \circ (x \circ y) = y . \tag{I.2}$$

The equivalence can be verified immediately.

The following geometric example may serve as background and motivation

for this definition: let E be the set of non-singular points of an irreducible cubic curve V, embedded in a projective plane over a field k; and let the relation $L(x, y, z)$ be 'the cycle $x+y+z$ is the intersection of V with some line' (counting multiplicities). Here condition (i) is geometrically obvious but condition (ii) is easier to work with algebraically.

In this example the quasigroup E satisfies the following additional property: let $u \in E$ be some fixed element; we introduce on E the new composition law $xy = u \circ (x \circ y)$. Then E becomes an Abelian group with u as unit element. As the structure of Abelian groups is well known, one usually prefers to work with this (new) composition law.

An axiomatization of this situation leads to the following:

Definition 1.2. A symmetric quasigroup E is called *Abelian* if it satisfies one of the following equivalent conditions:

(i) There exists an Abelian group structure on E with composition law $(x, y) \mapsto xy$, and there is an element $c \in E$ such that $x \circ y = cx^{-1}y^{-1}$ for all $x, y \in E$.

(ii) For any element $u \in E$ the composition law $xy = u \circ (x \circ y)$ turns E into an Abelian group.

The equivalence of conditions (i) and (ii) will be verified in the next section.

Let us now consider an irreducible cubic hypersurface V of dimension $\geqslant 2$ embedded in some projective space; let E be the set of non-singular points. The three-place relation $L(x, y, z)$ on V is defined as before in the case of a cubic curve. It is symmetric. However, in general, *it does not come from a binary composition law on V.* This has to do with two geometric circumstances:

(a) When $\dim V = 1$, the point $x \circ x$ is defined as 'the third intersection point with V of the tangent line to V at x'. But, when $\dim V > 1$, there are many tangent lines at x: they fill up a whole tangent hyperplane.

(b) When $\dim V > 1$, there can be lines completely lying in V. For two points on such a line it is impossible to find a third such that the set of these three forms the whole intersection cycle with some line.

In the next chapter we shall avoid these difficulties by considering instead of E a quotient set of E such that the induced relation of 'collinearity' comes from a symmetric quasigroup composition law. We cannot guarantee that this quasigroup will be Abelian, as in the one-dimensional case. However, any three points of V are contained in the intersection of V with a plane. This intersec-

tion is a cubic curve. Hence, as the lines through these points and the points derived from them all stay in this plane, we obtain the result that any set of three elements of the quasigroup generates an Abelian quasigroup.

This justifies the following definition:

Definition 1.3. A *CH-quasigroup* (CH stands for Cubic Hypersurface) is a symmetric quasigroup in which any three elements generate an Abelian subquasigroup.

We shall now state the main known results on the structure of CH-quasigroups.

Let E be a CH-quasigroup. By analogy with the Abelian case we introduce on E a new composition law $xy = u \circ (x \circ y)$, where u is some fixed element. It is a remarkable fact that the structure thus obtained has been introduced before in non-associative algebra theory, and has been thoroughly studied by Bruck [2].

Definition 1.4. A set E with composition law $(x, y) \mapsto xy$ is called a *commutative Moufang loop* (henceforth abbreviated CML) if it satisfies the following axioms:

(i) Commutativity: $xy = yx$ for all $x, y \in E$.

(ii) Unit element: $ux = x$ for all $x \in E$.

(iii) Inverses: there exists a map $E \to E: x \mapsto x^{-1}$ such that $x^{-1}(xy) = y$ for all $x, y \in E$.

(iv) Weak associativity:

for three factors: $x(xy) = x^2y$; (I.3)

for four factors: $(xy)(xz) = x^2(yz)$, (I.4)

$x(y(xz)) = (x^2y)z$. (I.5)

Theorem 1.5. *If E is a CH-quasigroup, then the composition law $xy = u \circ (x \circ y)$ turns E into a CML.*

The axioms for a CML, as introduced in Definition 1.4, are not independent. For example, it is possible to deduce (I.3), (I.4) and (I.5) from either (I.4) or (I.5) alone. We have included these identities because they immedi-