Graduate Texts in Mathematics

Joseph H. Silverman

The Arithmetic of Elliptic Curves

椭圆曲线的算术理论

Springer-Verlag
世界图书出版公司

Joseph H. Silverman

The Arithmetic of Elliptic Curves

With 13 Illustrations

Springer

书　　名：The Arithmetic of Elliptic Curves
作　　者：J.H.Silverman
中 译 名：椭圆曲线的算术理论
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
发　　行：世界图书出版公司北京公司（北京市朝阳门内大街 137 号　100010）
开　　本：1/24　711×1245　　印　张：17.5
出版年代：1999 年 11 月
书　　号：ISBN7-5062-0135-6
定　　价：68.00 元

Preface

The preface to a textbook frequently contains the author's justification for offering the public "another book" on the given subject. For our chosen topic, the arithmetic of elliptic curves, there is little need for such an apologia. Considering the vast amount of research currently being done in this area, the paucity of introductory texts is somewhat surprising. Parts of the theory are contained in various books of Lang (especially [La 3] and [La 5]); and there are books of Koblitz ([Ko]) and Robert ([Rob], now out of print) which concentrate mostly on the analytic and modular theory. In addition, survey articles have been written by Cassels ([Ca 7], really a short book) and Tate ([Ta 5], which is beautifully written, but includes no proofs). Thus the author hopes that this volume will fill a real need, both for the serious student who wishes to learn the basic facts about the arithmetic of elliptic curves; and for the research mathematician who needs a reference source for those same basic facts.

Our approach is more algebraic than that taken in, say, [La 3] or [La 5], where many of the basic theorems are derived using complex analytic methods and the Lefschetz principle. For this reason, we have had to rely somewhat more on techniques from algebraic geometry. However, the geometry of (smooth) curves, which is essentially all that we use, does not require a great deal of machinery. And the small price paid in learning a little bit of algebraic geometry is amply repaid in a unity of exposition which (to the author) seems to be lacking when one makes extensive use of either the Lefschetz principle or lengthy (but elementary) calculations with explicit polynomial equations.

This last point is worth amplifying. It has been the author's experience that "elementary" proofs requiring page after page of algebra tend to be quite uninstructive. A student may be able to verify such a proof, line by line, and

at the end will agree that the proof is complete. But little true understanding results from such a procedure. In this book, our policy is always to state when a result can be proven by such an elementary calculation, indicate briefly how that calculation might be done, and then give a more enlightening proof which is based on general principles.

The basic (global) theorems in the arithmetic of elliptic curves are the Mordell–Weil theorem, which is proven in chapter VIII and analyzed more closely in chapter X; and Siegel's theorem, which is proven in chapter IX. The reader desiring to reach these results fairly rapidly might take the following path:

I and II (briefly review), III (§1–8), IV (§1–6), V (§1),
VII (§1–5), VIII (§1–6), IX (§1–7), X (§1–6).

This material also makes a good one-semester course, possibly with some time left at the end for special topics. The present volume is built around the notes for such a course, taught by the author at M.I.T. during the spring term of 1983. [Of course, there are many other possibilities. For example, one might include all of chapters V and VI, skipping IX and (if pressed for time) X.] Other important topics in the arithmetic of elliptic curves, which do not appear in this volume due to time and space limitations, are briefly discussed in appendix C.

It is certainly true that some of the deepest results in this subject, such as Mazur's theorem bounding torsion over $\mathbb{Q}$ and Faltings' proof of the isogeny conjecture, require many of the resources of modern "SGA-style" algebraic geometry. On the other hand, one needs no machinery at all to write down the equation of an elliptic curve and to do explicit computations with it; and so there are many important theorems whose proof requires nothing more than cleverness and hard work. Whether your inclination leans toward heavy machinery or imaginative calculations, you will find much that remains to be discovered in the arithmetic theory of elliptic curves. Happy hunting!

Acknowledgments

In writing this book, I have consulted a great many sources. Citations have been included for major theorems, but many results which are now considered "standard" have been presented as such. In any case, I can claim no originality for any of the unlabeled theorems in this book, and apologize in advance to anyone who may feel slighted. The excellent survey articles of Cassels [Ca 7] and Tate [Ta 5] served as guidelines for organizing the material. (The reader is especially urged to peruse the latter.) In addition to [Ca 7] and [Ta 5], other sources which were extensively consulted include [La 5], [La 7], [Mum], [Rob], and [Se 10].

It would not be possible to catalogue all of the mathematicians from whom

I learned this beautiful subject; but to all of them, my deepest thanks. I would especially like to thank John Tate, Barry Mazur, Serge Lang, and the "Elliptic Curves Seminar" group at Harvard (1977–1982), whose help and inspiration set me on the road which led to this book. I would also like to thank David Rohrlich and Bill McCallum for their careful reading of the original draft, Gary Cornell and the editorial staff of Springer-Verlag for encouraging me to undertake this project in the first place, and Ann Clee for her meticulous preparation of the manuscript. Finally, I would like to thank my wife, Susan, for her patience and understanding through the turbulent times during which this book was written; and also Deborah and Daniel, for providing most of the turbulence.

Cambridge, Massachusetts
September, 1985

JOSEPH H. SILVERMAN

Acknowledgements For The Second Printing

I would like to thank the following people who kindly provided corrections which have been incorporated in this second revised printing: Andrew Baker, Arthur Baragar, Wah Keung Chan, Yen-Mei (Julia) Chen, Bob Coleman, Fred Diamond, David Fried, Dick Gross, Ron Jacobwitz, Kevin Keating, Masato Kuwata, Peter Landweber, H. W. Lenstra Jr., San Ling, Bill McCallum, David Masser, Hwasin Park, Elisabeth Pyle, Ken Ribet, John Rhodes, David Rohrlich, Mike Rosen, Rene Schoof, Udi de Shalit, Alice Silverberg, Glenn Stevens, John Tate, Jaap Top, Paul van Mulbregt, Larry Washington, Don Zagier.

It has unfortunately not been possible to include in this second printing many important results proven during the past six years, such as the work of Kolyvagin and Rubin on the Birch and Swinnerton-Dyer conjectures (C.16.5) and the finiteness of the Tate-Shafarevich group (X.4.13), Ribet's proof that the conjecture of Shimura-Taniyama-Weil (C.16.4) implies Fermat's Last Theorem, and recent work of Mestre on elliptic curves of high rank (C §20). The inclusion of such material (and more) will have to await an eventual second edition, so the reader should be aware that some of our general discussion, especially in Appendix C, is out of date. In spite of this obsolescence, it is our hope that this book will continue to provide a useful introduction to the study of the arithmetic of elliptic curves.

Providence, Rhode Island
August, 1992

JOSEPH H. SILVERMAN

Contents

Preface v

Introduction 1

CHAPTER I

Algebraic Varieties 5

§1. Affine Varieties 5
§2. Projective Varieties 10
§3. Maps between Varieties 15

CHAPTER II

Algebraic Curves 21

§1. Curves 21
§2. Maps between Curves 23
§3. Divisors 31
§4. Differentials 34
§5. The Riemann–Roch Theorem 37

CHAPTER III

The Geometry of Elliptic Curves 45

§1. Weierstrass Equations 46
§2. The Group Law 55
§3. Elliptic Curves 63
§4. Isogenies 70
§5. The Invariant Differential 79

§6. The Dual Isogeny 84
§7. The Tate Module 90
§8. The Weil Pairing 95
§9. The Endomorphism Ring 100
§10. The Automorphism Group 103

CHAPTER IV

The Formal Group of an Elliptic Curve 110

§1. Expansion around O 110
§2. Formal Groups 115
§3. Groups Associated to Formal Groups 117
§4. The Invariant Differential 119
§5. The Formal Logarithm 121
§6. Formal Groups over Discrete Valuation Rings 123
§7. Formal Groups in Characteristic p 126

CHAPTER V

Elliptic Curves over Finite Fields 130

§1. Number of Rational Points 130
§2. The Weil Conjectures 132
§3. The Endomorphism Ring 137
§4. Calculating the Hasse Invariant 140

CHAPTER VI

Elliptic Curves over $\mathbb{C}$ 146

§1. Elliptic Integrals 147
§2. Elliptic Functions 150
§3. Construction of Elliptic Functions 153
§4. Maps–Analytic and Algebraic 159
§5. Uniformization 161
§6. The Lefschetz Principle 164

CHAPTER VII

Elliptic Curves over Local Fields 171

§1. Minimal Weierstrass Equations 171
§2. Reduction Modulo π 173
§3. Points of Finite Order 175
§4. The Action of Inertia 178
§5. Good and Bad Reduction 179
§6. The Group E/E_0 183
§7. The Criterion of Néron–Ogg–Shafarevich 184

CHAPTER VIII
Elliptic Curves over Global Fields 189

§1. The Weak Mordell–Weil Theorem 190
§2. The Kummer Pairing via Cohomology 196
§3. The Descent Procedure 199
§4. The Mordell–Weil Theorem over $\mathbb{Q}$ 201
§5. Heights on Projective Space 205
§6. Heights on Elliptic Curves 215
§7. Torsion Points 220
§8. The Minimal Discriminant 223
§9. The Canonical Height 227
§10. The Rank of an Elliptic Curve 233

CHAPTER IX
Integral Points on Elliptic Curves 241

§1. Diophantine Approximation 242
§2. Distance Functions 245
§3. Siegel's Theorem 247
§4. The S-Unit Equation 252
§5. Effective Methods 256
§6. Shafarevich's Theorem 263
§7. The Curve $Y^2 = X^3 + D$ 266
§8. Roth's Theorem—An Overview 269

CHAPTER X
Computing the Mordell–Weil Group 276

§1. An Example 277
§2. Twisting—General Theory 284
§3. Homogeneous Spaces 287
§4. The Selmer and Shafarevich–Tate Groups 296
§5. Twisting—Elliptic Curves 306
§6. The Curve $Y^2 = X^3 + DX$ 309

APPENDIX A
Elliptic Curves in Characteristics 2 and 3 324

APPENDIX B
Group Cohomology (H^0 and H^1) 330

§1. Cohomology of Finite Groups 330
§2. Galois Cohomology 333
§3. Non-Abelian Cohomology 335

APPENDIX C
Further Topics: An Overview 338

§11. Complex Multiplication 338
§12. Modular Functions 342
§13. Modular Curves 351
§14. Tate Curves 355
§15. Néron Models and Tate's Algorithm 357
§16. *L*-Series 360
§17. Duality Theory 364
§18. Local Height Functions 364
§19. The Image of Galois 366
§20. Function Fields and Specialization Theorems 367

Notes on Exercises 369

Bibliography 372

List of Notation 379

Index 385

Introduction

The study of Diophantine equations, that is the solution of polynomial equations in integers or rational numbers, has a history stretching back to ancient Greece and beyond. The term *Diophantine geometry* is of more recent origin, and refers to the study of Diophantine equations through a combination of techniques from algebraic number theory and algebraic geometry. On the one hand, the problem of finding integer and rational solutions to polynomial equations calls into play the tools of algebraic number theory, which describes the rings and fields wherein those solutions lie. On the other hand, such a system of polynomial equations describes an algebraic variety, which is a geometric object. It is the interplay between these two points of view which is the subject of Diophantine geometry.

The simplest sort of equation is linear:

$$aX + bY = c \qquad a, b, c \in \mathbb{Z}, \qquad a \text{ or } b \neq 0.$$

Such an equation always has rational solutions. It will have integer solutions if and only if the greatest common divisor of a and b divides c; and if this occurs, then one can find all solutions by using the Euclidean algorithm.

Next in order of difficulty come quadratic equations:

$$aX^2 + bXY + cY^2 + dX + eY + f = 0 \qquad a, \ldots, f \in \mathbb{Z}, \qquad a, b, \text{or } c \neq 0.$$

They describe conic sections, and by a suitable linear change of coordinates *with rational coefficients*, one can transform a given equation into one of the following forms:

$$AX^2 + BY^2 = C \qquad \text{ellipse}$$

$$AX^2 - BY^2 = C \qquad \text{hyperbola}$$

$$AX + BY^2 = 0 \qquad \text{parabola.}$$

For quadratic equations, one has the following powerful theorem which aids in their solution.

Hasse–Minkowski Theorem ([Se 7, IV Thm. 8]). *Let $f(X, Y) \in \mathbb{Q}[X, Y]$ be a quadratic polynomial. Then the equation $f(X, Y) = 0$ has a solution $(x, y) \in \mathbb{Q}^2$ if and only if it has a solution $(x, y) \in \mathbb{R}^2$ and a solution $(x, y) \in \mathbb{Q}_p^2$ for every prime p. (Here $\mathbb{Q}_p$ is the field of p-adic numbers.)*

In other words, a quadratic polynomial has a solution in $\mathbb{Q}$ if and only if it has a solution in every completion of $\mathbb{Q}$. Now checking for solutions in $\mathbb{Q}_p$ will, by Hensel's lemma, be more or less the same as checking for solutions in the finite field $\mathbb{Z}/p\mathbb{Z}$; and this, in turn, is easily accomplished by using quadratic reciprocity. Let us summarize the steps which go into the Diophantine analysis of quadratic equations.

(1) Analyze the equations over finite fields. [Quadratic reciprocity]
(2) Use this information to study the equations over complete local fields $\mathbb{Q}_p$. [Hensel's lemma] (We must also analyze them over $\mathbb{R}$.)
(3) Piece together all the local information to obtain results for the global field $\mathbb{Q}$. [Hasse principle]

Where does the geometry appear? Linear and quadratic equations in two variables define curves of genus 0. The above discussion says that we have a fairly good understanding of the arithmetic of curves of genus 0. The next simplest case, namely the arithmetic properties of curves of genus 1 (which are given by cubic equations in two variables), is our object of study in this book. The arithmetic of these so-called *elliptic curves* already presents complexities on which much current research is centered. Further, they provide a standard testing ground for conjectures and techniques which can then be fruitfully applied to the study of curves of higher genus and (abelian) varieties of higher dimension.

Briefly, the organization of this book is as follows. After two introductory chapters giving basic material on algebraic geometry, we start by studying the geometry of elliptic curves over algebraically closed fields (chapter III). We then follow the program outlined above and investigate the properties of elliptic curves over finite fields (chapter V), local fields (chapters VI, VII), and global (number) fields (chapters VIII, IX, X). Our understanding of elliptic curves over finite and local fields will be fairly satisfactory. However, it turns out that the analogue of the Hasse–Minkowski theorem is false for polynomials of degree greater than 2; this means that the transition from local to global is far more tenuous than in the degree 2 case. We study this problem in some detail in chapter X.

The theory of elliptic curves is rich, varied, and amazingly vast. The original aim of this book was to provide an essentially self-contained introduction to the basic arithmetic properties of elliptic curves. Even such a

limited goal proved to be too ambitious. The material described above is approximately half of what the author had hoped to include. The reader will find a brief discussion and list of references for the omitted topics in appendix C.

Our other goal, that of being self-contained, has been more successful. We have, of course, felt free to state results that every reader should be aware of, even when the proofs are far beyond the scope of this book. However, we have endeavored not to use such results for making further deductions. There are three major exceptions to this general policy. First, we have not proven that every elliptic curve over $\mathbb{C}$ is uniformized by elliptic functions (VI.5.1). This result fits most naturally into a discussion of modular functions, which is one of the topics which had to be omitted. Second, we have not proven that over a complete local field, the "non-singular" points sit with finite index inside the set of all points (VII.6.2). This can actually be proven by quite explicit polynomial computations (cf. [Ta 6]), but they are rather lengthy, and again have not been included due to lack of space. Finally, in the study of integral points on elliptic curves, we have made use of Roth's theorem (IX.1.4) without giving a proof. However, a brief discussion of the proof has been given in (IX §8), and the reader who then wishes to see the myriad details can proceed to one of the references listed there.

The prerequisites for reading this book are fairly modest. We assume that the reader has had a first course in algebraic number theory, and so is acquainted with number fields, rings of integers, prime ideals, ramification, absolute values, completions, etc. The contents of any basic text in algebraic number theory, such as [La 2, Part I] or [Bo–Sh], should more than suffice. Chapter VI, which deals with elliptic curves over $\mathbb{C}$, assumes a familiarity with the basic principles of complex analysis. In chapter X we will need a little bit of group cohomology, but just H^0 and H^1. The reader will find the cohomological facts needed to read chapter X given in appendix B. Finally, since our approach is mainly algebraic, there is the question of background material in algebraic geometry. On the one hand, since much of the theory of elliptic curves can be obtained through the use of explicit equations and calculations, we do not want to require the reader to already know a great deal of algebraic geometry. On the other hand, this being a book on number theory and not algebraic geometry, it would not be reasonable to spend half of the book developing from first principles the algebro-geometric facts that we will use. As a compromise, the first two chapters give an introduction to the algebraic geometry of varieties and curves, stating all of the facts which we will need, giving complete references, and providing enough proofs so that the reader can gain a flavor for some of the basic techniques used in algebraic geometry.

Numerous exercises have been included at the end of each chapter. The reader desiring to gain a real understanding of the subject is urged to attempt as many as possible. Some of these exercises are (special cases of) results which have appeared in the literature. A list of comments and citations for

the exercises will be found at the end of the book. Exercises with a single asterisk are somewhat more difficult, and two asterisks signal an unsolved problem.

References

Bibliographical references are enclosed in square brackets, e.g. [Ta 5, thm. 6]. Cross references to theorems, propositions, lemmas within the same chapter are given by number in parentheses, e.g. (4.3). Reference to an exercise is given by (exer. 3.6). References from within one chapter to another chapter or an appendix are preceded by the appropriate Roman numeral or letter, e.g. (IV.3.1), (B.2.1).

Standard Notation

Throughout this book, we use the symbols

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \text{ and } \mathbb{Z}_\ell$$

to represent the integers, rational numbers, real numbers, complex numbers, field with q elements, and ℓ-adic integers respectively. Further, if R is any ring, then R^* denotes the group of invertible elements of R; and if A is an abelian group, then $A[m]$ denotes the subgroup of A consisting of elements of order dividing m. A more complete list of notation is included on p. 379.

CHAPTER I

Algebraic Varieties

In this chapter we describe the basic objects which arise in the study of algebraic geometry. We set the following notation, which will be used throughout this book.

K	a perfect field (i.e. every algebraic extension of K is separable).
$\bar{K}$	a fixed algebraic closure of K
$G_{\bar{K}/K}$	the Galois group of $\bar{K}/K$

For this chapter, we also let m and n denote positive integers.

The assumption that K is a perfect field is made solely to simplify our exposition. However, since our eventual goal is to do arithmetic, the field K will eventually be taken as an algebraic extension of $\mathbb{Q}$, $\mathbb{Q}_p$, or $\mathbb{F}_p$. Thus this restriction on K need not concern us unduly.

For a more extensive exposition of the basic concepts which appear in this chapter, we refer the reader to any introductory book on algebraic geometry, such as [Har], [Sha 2], [Ful].

§1. Affine Varieties

We begin our study of algebraic geometry with Cartesian (or affine) n-space and its subsets defined by zeros of polynomials.

Definition. *Affine n-space (over K)* is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \ldots, x_n) : x_i \in \bar{K}\}.$$

Similarly, the *set of K-rational points in* $\mathbb{A}^n$ is the set

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n : x_i \in K\}.$$

Notice that the Galois group $G_{\bar{K}/K}$ acts on $\mathbb{A}^n$; for $\sigma \in G_{\bar{K}/K}$ and $P \in \mathbb{A}^n$,

$$P^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

Then $\mathbb{A}^n(K)$ may be characterized by

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Let $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$ be a polynomial ring in n variables, and let $I \subset \bar{K}[X]$ be an ideal. To each such I we associate a subset of $\mathbb{A}^n$,

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Definition. An (*affine*) *algebraic set* is any set of the form V_I. If V is an algebraic set, the *ideal of* V is given by

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\}.$$

An algebraic set V is *defined over* K if its ideal $I(V)$ can be generated by polynomials in $K[X]$. We denote this by V/K. If V is defined over K, the *set of K-rational points of* V is the set

$$V(K) = V \cap \mathbb{A}^n(K).$$

Remark 1.1. Note that by the Hilbert basis theorem ([A–M, 7.6]), all ideals in $\bar{K}[X]$ and $K[X]$ are finitely generated.

Remark 1.2. Let V be an algebraic set, and consider the ideal

$$I(V/K) = \{f \in K[X] : f(P) = 0 \text{ for all } P \in V\} = I(V) \cap K[X].$$

Then we see that V is defined over K if and only if

$$I(V)' = I(V/K)\bar{K}[X].$$

Now suppose V is defined over K, and let $f_1, \ldots, f_m \in K[X]$ be generators for $I(V/K)$. Then $V(K)$ is precisely the set of solutions $(x_1, \ldots, x_n)$ to the polynomial equations

$$f_1(X) = \cdots = f_m(X) = 0$$

with $x_1, \ldots, x_n \in K$. Thus one of the fundamental problems in the subject of *Diophantine geometry*, namely the solution of polynomial equations in rational numbers, may be said to be the problem of describing sets of the form $V(K)$ when K is a number field.

Notice that if $f(X) \in K[X]$ and $P \in \mathbb{A}^n$, then for any $\sigma \in G_{\bar{K}/K}$,

$$f(P^\sigma) = f(P)^\sigma.$$

Hence if V is defined over K, then the action of $G_{\bar{K}/K}$ on $\mathbb{A}^n$ induces an action on V, and clearly

$$V(K) = \{P \in V : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Example 1.3.1. Let V be the algebraic set in $\mathbb{A}^2$ given by the single equation

$$X^2 - Y^2 = 1.$$

Clearly V is defined over K for any field K. Let us assume that $\mathrm{char}(K) \neq 2$. Then the set $V(K)$ is in one-to-one correspondence with $\mathbb{A}^1(K) - \{0\}$, one possible map being

$$\mathbb{A}^1(K) - \{0\} \to V(K)$$
$$t \to ((t^2 + 1)/2t, (t^2 - 1)/2t).$$

Example 1.3.2. The algebraic set

$$V: X^n + Y^n = 1$$

is defined over $\mathbb{Q}$. Fermat's last "theorem" states that for all $n \geqslant 3$,

$$V(\mathbb{Q}) = \begin{cases} \{(1, 0), (0, 1)\} & n \text{ odd} \\ \{(\pm 1, 0), (0, \pm 1)\} & n \text{ even.} \end{cases}$$

Example 1.3.3. The algebraic set

$$V: Y^2 = X^3 + 17$$

has many $\mathbb{Q}$-rational points, for example

$$(-2, 3) \qquad (5234, 378661) \qquad (137/64, 2651/512).$$

In fact, $V(\mathbb{Q})$ is infinite. See (2.8) and (III.2.4) for further discussion of this example.

Definition. An affine algebraic set V is called an *(affine) variety* if $I(V)$ is a prime ideal in $\bar{K}[X]$. (Note that if V is defined over K, it is not enough to check that $I(V/K)$ is prime. For example, consider the ideal $(X_1^2 - 2X_2^2)$ in $\mathbb{Q}[X_1, X_2]$.) Let V/K be a variety (i.e. V is a variety defined over K). Then the *affine coordinate ring of* V/K is defined by

$$K[V] = \frac{K[X]}{I(V/K)}.$$

It is an integral domain; and its quotient field, denoted $K(V)$, is called the *function field of* V/K. Similarly $\bar{K}[V]$ and $\bar{K}(V)$ are defined by replacing K with $\bar{K}$.

Note that since an element $f \in \bar{K}[V]$ is well-defined up to a polynomial vanishing on V, it induces a well-defined function $f: V \to \bar{K}$. Now if $f(X) \in \bar{K}[X]$, then $G_{\bar{K}/K}$ acts on f by acting on its coefficients. Hence if V is defined over K, so $G_{\bar{K}/K}$ takes $I(V)$ into itself, then we obtain an action of $G_{\bar{K}/K}$ on $\bar{K}[V]$ and $\bar{K}(V)$. One can check (exer. 1.12) that $K[V]$ and $K(V)$ are respectively the subsets of $\bar{K}[V]$ and $\bar{K}(V)$ fixed by $G_{\bar{K}/K}$. We denote