Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

326

Alain Robert

Elliptic Curves

Notes from Postgraduate Lectures Given in Lausanne 1971/72

Springer-Verlag
Berlin Heidelberg New York Tokyo

Author

Alain Robert
Université de Neuchâtel, Institut de Mathématiques
Chantemerle 20, 2000 Neuchâtel, Switzerland

1st Edition 1973
2nd Corrected Printing 1986

Mathematics Subject Classification (1980): 12B35, 12B37, 14G10, 14H15, 14H45, 32G15

ISBN 3-540-06309-9 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-06309-9 Springer-Verlag New York Heidelberg Berlin Tokyo

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2146/3140-543210

NOTATIONS AND CONVENTIONS

We have used the usual letters for the basic sets of numbers : $\mathbb{N}$ (natural integers 0,1,2,...), $\mathbb{Z}$ (ring of rational integers), $\mathbb{Q}$ (field of rational numbers), $\mathbb{R}$ (field of real numbers), $\mathbb{C}$ (field of complex numbers), $\mathbb{F}_q$ (finite field with q elements). As a rule, we denote by $A^\times$ the multiplicative group of units (invertible elements) in a ring A. In formulas, the cypher 1 always represents the number one (except in log x ... so that in one occurence I have used log -1 to avoid ambiguities). Also $e(x) = e^{2\pi ix}$ (normalized exponential).

In a theorem, I list properties under Latin letters a), b), ... keeping i), ii), ... for equivalent properties, but the meaning is always clear by the context.

The following system has been adopted for cross-references. All theorems, propositions, corollaries, lemmas, remarks, definitions, formulas, errata,... are numbered in one sequence. Such a cypher as (III.3.4) refers to the item (3.4) of chapter III , i.e. the fourth numbered in section 3. (This happens to be a lemma 3.) From inside chapter III we would refer to (3.4) (in section 3, sometimes simply to lemma 3 : this last system of numeration has not been used systematically, but only when it can be more suggestive locally).

TABLE OF CONTENTS

INTRODUCTION

Elliptic curves are special cases of two theories, namely the theory of Riemann surfaces (or algebraic curves) and the theory of abelian varieties, so that any book concerned with these more general topics will cover elliptic curves as example. However, in a series of lectures, it seemed preferable to me to have a more limited scope and introduce students to both theories by giving them relevant theorems in their simplest case. I think that the recent recrudescence of popularity of elliptic curves amply justifies this point of view. I have not chosen the most concise style possible and sometimes have committed the "crime of lèse-Bourbaki" by giving several proofs of one theorem, illustrating different methods or point of views.

I shall not give here any idea of the topics covered by these notes, because each chapter has its own introduction for that purpose (prerequisites are also listed there). Let me just mention that I have omitted complex multiplication theory for lack of time (only integrality of singular invariants is proved in chapter III). In the short commented bibliography (given for each chapter at the end of the notes), I quote most of my sources and indicate some books and articles which should provide ample material for anyone looking for further reading.

The origin of my interest in elliptic curves has to be traced to a series of lectures given by M. Demazure (Paris Orsay, oct.-dec. 67) on elliptic curves over $\mathbb{C}$. Although the presentation I have adopted differs somewhat from his, I have been much influenced by the notes from these lectures (especially in the section on theta functions). I would also like to seize the opportunity of thanking here Y. Ihara,

J.-P. Serre, G. Shimura for very helpful discussions, correspondence... Only at the end of the lectures did I learn through S. Lang that he had also written a book on elliptic curves. It seemed however that the material covered was sufficiently different to allow the publication of my notes, and I hope that they will still have some use.

Finally it is a pleasure to thank the audience of the lectures whose interest stimulated me, my wife who gave me some hints on language and L.-O. Pochon who proof-read most of the notes, pointed out some mistakes and established an index. However, I take full responsability for remaining mistakes and would be grateful to anyone bothering to let me know about them !

September 1972

A. Robert
Institut de Mathématiques
Université de Neuchâtel
CH-2000 NEUCHATEL
(Switzerland)