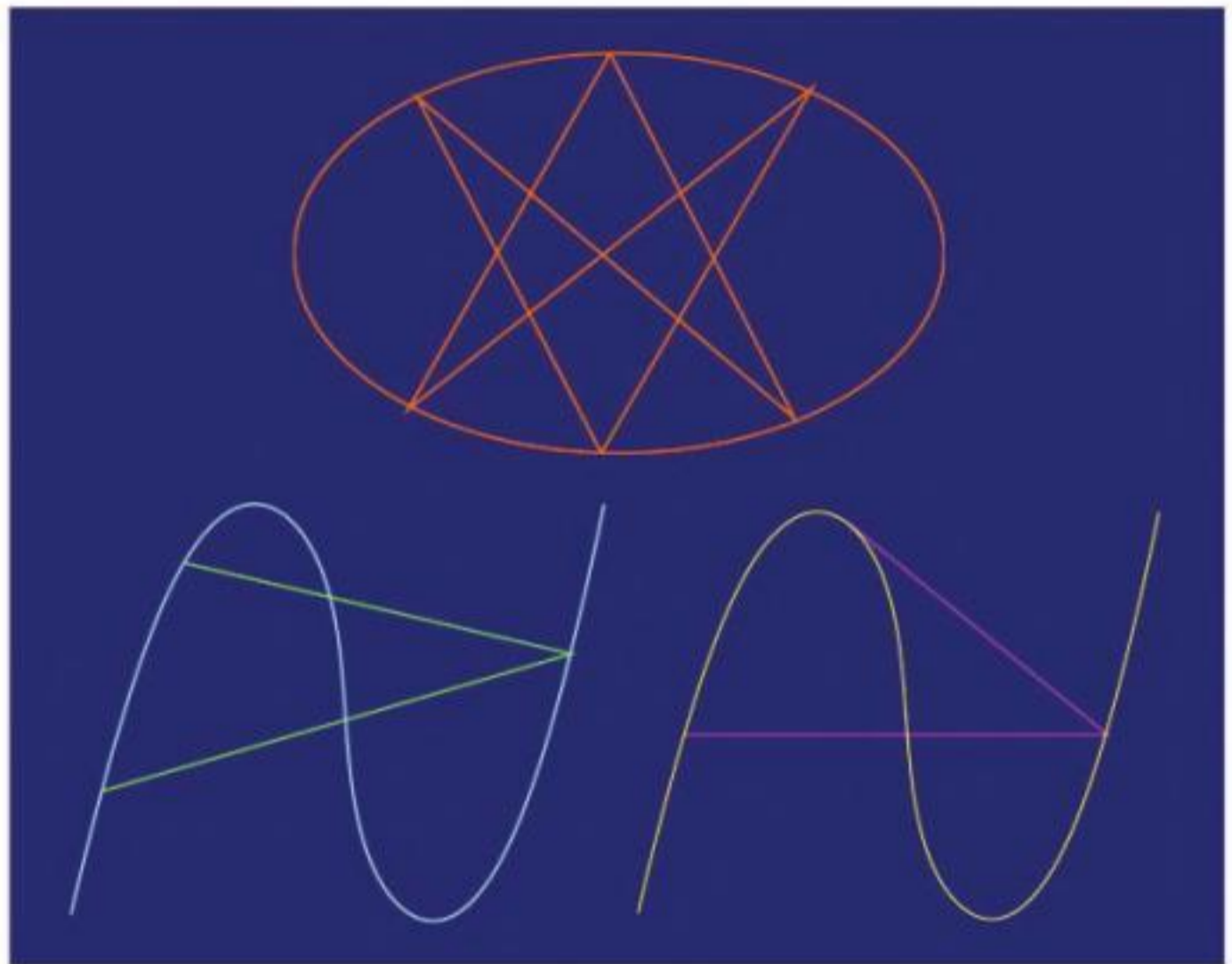


# Algebraic Curves Over a Finite Field



J.W.P. Hirschfeld,  
G. Korchmáros,  
F. Torres

---

---

# Contents

Preface	xi
<b>PART 1. GENERAL THEORY OF CURVES</b>	<b>1</b>
Chapter 1. Fundamental ideas	3
1.1 Basic definitions	3
1.2 Polynomials	6
1.3 Affine plane curves	6
1.4 Projective plane curves	9
1.5 The Hessian curve	13
1.6 Projective varieties in higher-dimensional spaces	18
1.7 Exercises	18
1.8 Notes	19
Chapter 2. Elimination theory	21
2.1 Elimination of one unknown	21
2.2 The discriminant	30
2.3 Elimination in a system in two unknowns	31
2.4 Exercises	35
2.5 Notes	36
Chapter 3. Singular points and intersections	37
3.1 The intersection number of two curves	37
3.2 Bézout's Theorem	45
3.3 Rational and birational transformations	49
3.4 Quadratic transformations	51
3.5 Resolution of singularities	55
3.6 Exercises	61
3.7 Notes	62
Chapter 4. Branches and parametrisation	63
4.1 Formal power series	63
4.2 Branch representations	75
4.3 Branches of plane algebraic curves	81
4.4 Local quadratic transformations	84
4.5 Noether's Theorem	92
4.6 Analytic branches	99
4.7 Exercises	107

4.8	Notes	109
Chapter 5. The function field of a curve		110
5.1	Generic points	110
5.2	Rational transformations	112
5.3	Places	119
5.4	Zeros and poles	120
5.5	Separability and inseparability	122
5.6	Frobenius rational transformations	123
5.7	Derivations and differentials	125
5.8	The genus of a curve	130
5.9	Residues of differential forms	138
5.10	Higher derivatives in positive characteristic	144
5.11	The dual and bidual of a curve	155
5.12	Exercises	159
5.13	Notes	160
Chapter 6. Linear series and the Riemann–Roch Theorem		161
6.1	Divisors and linear series	161
6.2	Linear systems of curves	170
6.3	Special and non-special linear series	177
6.4	Reformulation of the Riemann–Roch Theorem	180
6.5	Some consequences of the Riemann–Roch Theorem	182
6.6	The Weierstrass Gap Theorem	184
6.7	The structure of the divisor class group	190
6.8	Exercises	196
6.9	Notes	198
Chapter 7. Algebraic curves in higher-dimensional spaces		199
7.1	Basic definitions and properties	199
7.2	Rational transformations	203
7.3	Hurwitz’s Theorem	208
7.4	Linear series composed of an involution	211
7.5	The canonical curve	216
7.6	Osculating hyperplanes and ramification divisors	217
7.7	Non-classical curves and linear systems of lines	228
7.8	Non-classical curves and linear systems of conics	230
7.9	Dual curves of space curves	238
7.10	Complete linear series of small order	241
7.11	Examples of curves	254
7.12	The Linear General Position Principle	257
7.13	Castelnuovo’s Bound	257
7.14	A generalisation of Clifford’s Theorem	260
7.15	The Uniform Position Principle	261
7.16	Valuation rings	262
7.17	Curves as algebraic varieties of dimension one	268
7.18	Exercises	270
7.19	Notes	271

<b>PART 2. CURVES OVER A FINITE FIELD</b>	<b>275</b>
Chapter 8. Rational points and places over a finite field	277
8.1 Plane curves defined over a finite field	277
8.2 $\mathbf{F}_q$ -rational branches of a curve	278
8.3 $\mathbf{F}_q$ -rational places, divisors and linear series	281
8.4 Space curves over $\mathbf{F}_q$	287
8.5 The Stöhr–Voloch Theorem	292
8.6 Frobenius classicality with respect to lines	305
8.7 Frobenius classicality with respect to conics	314
8.8 The dual of a Frobenius non-classical curve	326
8.9 Exercises	327
8.10 Notes	329
Chapter 9. Zeta functions and curves with many rational points	332
9.1 The zeta function of a curve over a finite field	332
9.2 The Hasse–Weil Theorem	343
9.3 Refinements of the Hasse–Weil Theorem	348
9.4 Asymptotic bounds	353
9.5 Other estimates	356
9.6 Counting points on a plane curve	358
9.7 Further applications of the zeta function	369
9.8 The Fundamental Equation	373
9.9 Elliptic curves over $\mathbf{F}_q$	378
9.10 Classification of non-singular cubics over $\mathbf{F}_q$	381
9.11 Exercises	385
9.12 Notes	388
<b>PART 3. FURTHER DEVELOPMENTS</b>	<b>393</b>
Chapter 10. Maximal and optimal curves	395
10.1 Background on maximal curves	396
10.2 The Frobenius linear series of a maximal curve	399
10.3 Embedding in a Hermitian variety	407
10.4 Maximal curves lying on a quadric surface	421
10.5 Maximal curves with high genus	428
10.6 Castelnuovo’s number	431
10.7 Plane maximal curves	439
10.8 Maximal curves of Hurwitz type	442
10.9 Non-isomorphic maximal curves	446
10.10 Optimal curves	447
10.11 Exercises	453
10.12 Notes	454
Chapter 11. Automorphisms of an algebraic curve	458
11.1 The action of $K$ -automorphisms on places	459
11.2 Linear series and automorphisms	464
11.3 Automorphism groups of plane curves	468

11.4	A bound on the order of a $K$ -automorphism	470
11.5	Automorphism groups and their fixed fields	473
11.6	The stabiliser of a place	476
11.7	Finiteness of the $K$ -automorphism group	480
11.8	Tame automorphism groups	483
11.9	Non-tame automorphism groups	486
11.10	$K$ -automorphism groups of particular curves	501
11.11	Fixed places of automorphisms	509
11.12	Large automorphism groups of function fields	513
11.13	$K$ -automorphism groups fixing a place	532
11.14	Large $p$ -subgroups fixing a place	539
11.15	Notes	542
Chapter 12. Some families of algebraic curves		546
12.1	Plane curves given by separated polynomials	546
12.2	Curves with Suzuki automorphism group	564
12.3	Curves with unitary automorphism group	572
12.4	Curves with Ree automorphism group	575
12.5	A curve attaining the Serre Bound	585
12.6	Notes	587
Chapter 13. Applications: codes and arcs		590
13.1	Algebraic-geometry codes	590
13.2	Maximum distance separable codes	594
13.3	Arcs and ovals	599
13.4	Segre's generalisation of Menelaus' Theorem	603
13.5	The connection between arcs and curves	607
13.6	Arcs in ovals in planes of even order	611
13.7	Arcs in ovals in planes of odd order	612
13.8	The second largest complete arc	615
13.9	The third largest complete arc	623
13.10	Exercises	625
13.11	Notes	625
Appendix A. Background on field theory and group theory		627
A.1	Field theory	627
A.2	Galois theory	633
A.3	Norms and traces	635
A.4	Finite fields	636
A.5	Group theory	638
A.6	Notes	649
Appendix B. Notation		650
Bibliography		655
Index		689