Projective Geometries over Finite Fields

SECOND EDITION

J. W. P. Hirschfeld

School of Mathematical Sciences
University of Sussex

CLARENDON PRESS • OXFORD
1998

CONTENTS

I INTRODUCTION

1	**Finite fields**	3
1.1	Definitions and existence	3
1.2	Automorphisms	4
1.3	Functions	5
1.4	Quadratic equations	7
1.5	Roots of an element	9
1.6	Primitive and subprimitive polynomials	11
1.7	Notation for small finite fields	14
1.8	Invariants of polynomials	15
1.9	Some equations with few terms	18
1.10	Cubic equations	21
1.11	Quartic equations	24
1.12	Notes and references	29
2	**Projective spaces and algebraic varieties**	31
2.1	Projective space over a field	31
	2.1.1 Definition of the space and its automorphisms	31
	2.1.2 The Fundamental Theorem of Projective Geometry	32
	2.1.3 The Principle of Duality	33
	2.1.4 Coordinate frames	33
	2.1.5 Polarities	34
2.2	Affine space over a field	36
2.3	Incidence structures	38
2.4	Canonical forms for projectivities	41
2.5	Subprimitive characteristic polynomials	46
2.6	Orders of projectivities	47
2.7	Varieties	48
2.8	Plane curves	51
2.9	The number of points on an algebraic curve I: the Hasse–Weil theorem	55
2.10	Linear systems of primals	60
2.11	The number of points on an algebraic curve II: the Stöhr–Voloch theorem	61
2.12	A generalization of the theorem of Menelaus	64
2.13	Some results from group theory	69

2.14 Links with coding theory 72
2.14.1 Basic definitions 72
2.14.2 Projective systems and the weight hierarchy 73
2.14.3 Algebraic geometry codes 75
2.15 Notes and references 77

II Elementary General Properties

3 Subspaces 85
3.1 Numbers 85
3.2 Characterization of subspaces 87
3.3 Sets of subspaces 89
3.4 Notes and references 91

4 Partitions 93
4.1 Partitions by subspaces 93
4.2 Cyclic projectivities 95
4.3 Partitions by subgeometries 103
4.4 Notes and references 113

5 Canonical forms for varieties and polarities 115
5.1 Quadric and Hermitian varieties 115
5.2 Projective classification of quadrics 121
5.3 Polarities 126
5.4 Notes and references 131

III The Line and the Plane

6 The line 135
6.1 Harmonic tetrads 135
6.2 Quadric and Hermitian varieties 137
6.3 The projective group of the line 139
6.4 The line for small orders 143
6.5 Notes and references 151

7 First properties of the plane 153
7.1 Preliminaries 153
7.2 Conics 155
7.3 Hermitian curves 160
7.4 The projective group of the plane 162
7.5 Perspectivities 168
7.6 Pencils of quadrics 171
7.7 Notes and references 172

8 Ovals 176
8.1 Arcs 176
8.2 Ovals for fields of odd order 178
8.3 Polarities 180
8.4 Ovals in a plane of even order 184
8.5 Translation ovals 193
8.6 Almost ovals 197
8.7 Notes and references 198

9 Arithmetic of arcs of degree two 201
9.1 The basic equations 201
9.2 Small arcs 206
9.3 Examples of complete arcs 209
9.4 Notes and references 213

10 Arcs in ovals 216
10.1 The connection between arcs and curves 216
10.2 The number of points on an algebraic curve III: further results 218
10.3 Arcs in ovals in planes of even order 222
10.4 Arcs in ovals in planes of odd order 226
10.5 The second largest complete arc: further results 229
10.6 Arcs and Hermitian curves 233
10.7 Notes and references 234

11 Cubic curves 237
11.1 Configurations 237
11.2 Double points, points of inflexion, and the group law 240
11.3 Nuclei of a cubic in characteristic three 248
11.4 Classification of singular cubics 250
11.4.1 Cubics with a node: type I 250
11.4.2 Cubics with a cusp: type II 252
11.4.3 Cubics with an isolated double point: type III 254
11.5 Properties of non-singular cubics 262
11.6 Non-singular cubics with nine rational inflexions 267
11.7 Non-singular cubics with three rational inflexions 269
11.8 Non-singular cubics with one rational inflexion 270
11.9 Non-singular cubics with no rational inflexions 287
11.10 Number of rational points on a cubic 289
11.11 Classification of non-singular cubics 291
11.12 Notes and references 296

12 Arcs of higher degree 301
12.1 Definitions and basic consequences 301
12.2 Maximal arcs in planes of even order 304
12.3 Arcs with two intersection numbers 305

12.4 Arcs with small deficiency 312
12.5 Further upper bounds for the size of an arc 320
12.6 Arcs in small planes 321
12.7 Maximal arcs in planes of odd order 323
12.8 Arcs and algebraic curves 326
12.9 Notes and references 331

13 Blocking sets 334
13.1 Definitions and examples 334
13.2 Bounds on the size of blocking sets 338
13.3 Lacunary polynomials and lower bounds 341
13.4 Blocking sets of Rédei type 344
13.5 Blocking sets in small planes 345
13.6 Multiple blocking sets 349
13.7 Nuclei 354
13.8 Blocking and multiple blocking sets in affine planes 358
13.9 Notes and references 361

14 Small planes 364
14.1 The plane of order two 364
14.2 The plane of order three 366
14.3 The plane of order four 368
14.4 The plane of order five 372
14.5 The plane of order seven 373
14.6 The plane of order eight 376
14.7 The plane of order nine 379
14.8 The plane of order eleven 385
14.9 The plane of order thirteen 386
14.10 Notes and references 387

Appendix I. Orders of and isomorphisms among the semi-linear groups 390
AI.1 Definitions 390
AI.2 Isomorphisms proved in the text 391
AI.3 Table of group orders 391
AI.4 Notes and references 394

Appendix II. Errata for *General Galois Geometries* 395

Notation 397

References 404

Index 547