

AN INTRODUCTION TO INVARIANTS
AND MODULI

SHIGERU MUKAI

Translated by W. M. Oxbury



PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa
<http://www.cambridge.org>

© Cambridge University Press 2003

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2003

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 10/13 pt. *System* L^AT_EX 2_ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data

Mukai, Shigeru, 1953–
[Mojurai riron. English]

An introduction to invariants and moduli / S. Mukai; translated by W.M. Oxbury.

p. cm. – (Cambridge studies in advanced mathematics)

Includes bibliographical references and index.

ISBN 0-521-80906-1

1. Invariants. 2. Moduli theory. I. Title. II. Series.

QA244 .M8413 2003

512.5–dc21

2002023422

ISBN 0 521 80906 1 hardback

Contents

Preface	<i>page xi</i>
Acknowledgements	xiii
Introduction	xv
(a) What is a moduli space?	xv
(b) Algebraic varieties and quotients of algebraic varieties	xvi
(c) Moduli of bundles on a curve	xix
1 Invariants and moduli	1
1.1 A parameter space for plane conics	1
1.2 Invariants of groups	9
(a) Hilbert series	9
(b) Molien's formula	13
(c) Polyhedral groups	15
1.3 Classical binary invariants	19
(a) Resultants and discriminants	19
(b) Binary quartics	26
1.4 Plane curves	32
(a) Affine plane curves	32
(b) Projective plane curves	35
1.5 Period parallelograms and cubic curves	41
(a) Invariants of a lattice	41
(b) The Weierstrass \wp function	44
(c) The \wp function and cubic curves	47
2 Rings and polynomials	51
2.1 Hilbert's Basis Theorem	51
2.2 Unique factorisation rings	55
2.3 Finitely generated rings	58

2.4	Valuation rings	61
	(a) Power series rings	61
	(b) Valuation rings	63
2.5	A diversion: rings of invariants which are not finitely generated	68
	(a) Graded rings	69
	(b) Nagata's trick	70
	(c) An application of Liouville's Theorem	73
3	Algebraic varieties	77
3.1	Affine varieties	78
	(a) Affine space	78
	(b) The spectrum	81
	(c) Some important notions	86
	<i>Morphisms</i>	86
	<i>Products</i>	87
	<i>General spectra and nilpotents</i>	88
	<i>Dominant morphisms</i>	89
	<i>Open immersions</i>	90
	<i>Local properties</i>	91
3.2	Algebraic varieties	91
	(a) Gluing affine varieties	91
	(b) Projective varieties	95
3.3	Functors and algebraic groups	98
	(a) A variety as a functor from algebras to sets	98
	(b) Algebraic groups	100
3.4	Completeness and toric varieties	103
	(a) Complete varieties	103
	(b) Toric varieties	107
	(c) Approximation of valuations	111
4	Algebraic groups and rings of invariants	116
4.1	Representations of algebraic groups	117
4.2	Algebraic groups and their Lie spaces	122
	(a) Local distributions	122
	(b) The distribution algebra	124
	(c) The Casimir operator	128
4.3	Hilbert's Theorem	130
	(a) Linear reductivity	130
	(b) Finite generation	135
4.4	The Cayley-Sylvester Counting Theorem	137
	(a) $SL(2)$	137
	(b) The dimension formula for $SL(2)$	140

(c)	A digression: Weyl measure	142
(d)	The Cayley-Sylvester Formula	143
(e)	Some computational examples	148
4.5	Geometric reductivity of $SL(2)$	152
5	The construction of quotient varieties	158
5.1	Affine quotients	159
(a)	Separation of orbits	159
(b)	Surjectivity of the affine quotient map	163
(c)	Stability	165
5.2	Classical invariants and the moduli of smooth hypersurfaces in \mathbb{P}^n	167
(a)	Classical invariants and discriminants	167
(b)	Stability of smooth hypersurfaces	171
(c)	A moduli space for hypersurfaces in \mathbb{P}^n	174
(d)	Nullforms and the projective quotient map	175
6	The projective quotient	181
6.1	Extending the idea of a quotient: from values to ratios	182
(a)	The projective spectrum	186
(b)	The Proj quotient	189
(c)	The Proj quotient by a $GL(n)$ action of ray type	195
6.2	Linearisation and Proj quotients	197
6.3	Moving quotients	201
(a)	Flops	201
(b)	Toric varieties as quotient varieties	205
(c)	Moment maps	208
7	The numerical criterion and some applications	211
7.1	The numerical criterion	212
(a)	1-parameter subgroups	212
(b)	The proof	213
7.2	Examples and applications	219
(a)	Stability of projective hypersurfaces	219
(b)	Cubic surfaces	224
(c)	Finite point sets in projective space	230
8	Grassmannians and vector bundles	234
8.1	Grassmannians as quotient varieties	235
(a)	Hilbert series	237
(b)	Standard monomials and the ring of invariants	239
(c)	Young tableaux and the Plücker relations	241
(d)	Grassmannians as projective varieties	245
(e)	A digression: the degree of the Grassmannian	247

8.2	Modules over a ring	251
	(a) Localisation	251
	(b) Local versus global	254
	(c) Free modules	257
	(d) Tensor products and flat modules	259
8.3	Locally free modules and flatness	262
	(a) Locally free modules	262
	(b) Exact sequences and flatness	264
8.4	The Picard group	268
	(a) Algebraic number fields	268
	(b) Two quadratic examples	271
8.5	Vector bundles	276
	(a) Elementary sheaves of modules	277
	(b) Line bundles and vector bundles	279
	(c) The Grassmann functor	282
	(d) The tangent space of the functor	284
9	Curves and their Jacobians	287
9.1	Riemann's inequality for an algebraic curve	288
	(a) Prologue: gap values and the genus	290
	(b) Divisors and the genus	292
	(c) Divisor classes and vanishing index of speciality	294
9.2	Cohomology spaces and the genus	297
	(a) Cousin's problem	297
	(b) Finiteness of the genus	301
	(c) Line bundles and their cohomology	304
	(d) Generation by global sections	307
9.3	Nonsingularity of quotient spaces	309
	(a) Differentials and differential modules	309
	(b) Nonsingularity	311
	(c) Free closed orbits	313
9.4	An algebraic variety with the Picard group as its set of points	316
	(a) Some preliminaries	316
	(b) The construction	319
	(c) Tangent spaces and smoothness	323
9.5	Duality	327
	(a) Dualising line bundles	327
	(b) The canonical line bundle	330
	(c) De Rham cohomology	332

9.6	The Jacobian as a complex manifold	334
(a)	Compact Riemann surfaces	335
(b)	The comparison theorem and the Jacobian	337
(c)	Abel's Theorem	342
10	Stable vector bundles on curves	348
10.1	Some general theory	349
(a)	Subbundles and quotient bundles	350
(b)	The Riemann-Roch formula	352
(c)	Indecomposable bundles and stable bundles	355
(d)	Grothendieck's Theorem	359
(e)	Extensions of vector bundles	361
10.2	Rank 2 vector bundles	365
(a)	Maximal line subbundles	365
(b)	Nonstable vector bundles	366
(c)	Vector bundles on an elliptic curve	369
10.3	Stable bundles and Pfaffian semiinvariants	371
(a)	Skew-symmetric matrices and Pfaffians	371
	<i>Even skew-symmetric matrices</i>	372
	<i>Odd skew-symmetric matrices</i>	374
	<i>Skew-symmetric matrices of rank 2</i>	375
(b)	Gieseker points	376
(c)	Semistability of Gieseker points	379
10.4	An algebraic variety with $SU_C(2, L)$ as its set of points	386
(a)	Tangent vectors and smoothness	387
(b)	Proof of Theorem 10.1	391
(c)	Remarks on higher rank vector bundles	394
11	Moduli functors	398
11.1	The Picard functor	400
(a)	Fine moduli and coarse moduli	400
(b)	Cohomology modules and direct images	403
(c)	Families of line bundles and the Picard functor	407
(d)	Poincaré line bundles	410
11.2	The moduli functor for vector bundles	413
(a)	Rank 2 vector bundles of odd degree	416
(b)	Irreducibility and rationality	418
(c)	Rank 2 vector bundles of even degree	419
11.3	Examples	422
(a)	The Jacobian of a plane quartic	422
(b)	The affine Jacobian of a spectral curve	424

(c)	The Jacobian of a curve of genus 1	425
(d)	Vector bundles on a spectral curve	431
(e)	Vector bundles on a curve of genus 2	433
12	Intersection numbers and the Verlinde formula	437
12.1	Sums of inverse powers of trigonometric functions	439
(a)	Sine sums	439
(b)	Variations	441
(c)	Tangent numbers and secant numbers	444
12.2	Riemann-Roch theorems	447
(a)	Some preliminaries	448
(b)	Hirzebruch-Riemann-Roch	450
(c)	Grothendieck-Riemann-Roch for curves	453
(d)	Riemann-Roch with involution	455
12.3	The standard line bundle and the Mumford relations	457
(a)	The standard line bundle	457
(b)	The Newstead classes	461
(c)	The Mumford relations	463
12.4	From the Mumford relations to the Verlinde formula	465
(a)	Warming up: secant rings	466
(b)	The proof of formulae (12.2) and (12.4)	470
12.5	An excursion: the Verlinde formula for quasiparabolic bundles	476
(a)	Quasiparabolic vector bundles	476
(b)	A proof of (12.6) using Riemann-Roch and the Mumford relations	480
(c)	Birational geometry	483
	Bibliography	487
	Index	495

1

Invariants and moduli

This chapter explores some examples of parameter spaces which can be constructed by elementary means and with little previous knowledge as an introduction to the general theory developed from Chapter 3 onwards. To begin, we consider equivalence classes of plane conics under Euclidean transformations and use invariants to construct a parameter space which essentially corresponds to the eccentricity of a conic.

This example already illustrates several essential features of the construction of moduli spaces. In addition we shall look carefully at some cases of finite group actions, and in particular at the question of how to determine the ring of invariants, the fundamental tool of the theory. We prove Molien's Formula, which gives the Hilbert series for the ring of invariants when a finite group acts linearly on a polynomial ring.

In Section 1.3, as an example of an action of an algebraic group, we use classical invariants to construct a parameter space for $GL(2)$ -orbits of binary quartics.

In Section 1.4 we review plane curves as examples of algebraic varieties. A plane curve without singularities is a Riemann surface, and in the particular case of a plane cubic this can be seen explicitly by means of doubly periodic complex functions. This leads to another example of a quotient by a discrete group action, in this case parametrising lattices in the complex plane. The group here is the modular group $SL(2, \mathbb{Z})$ (neither finite nor connected), and the Eisenstein series are invariants. Among them one can use two, g_2 and g_3 , to decide when two lattices are isomorphic.

1.1 A parameter space for plane conics

Consider the curve of degree 2 in the (real or complex) (x, y) plane

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0. \quad (1.1)$$

If the left-hand side factorises as a product of linear forms, then the curve is a union of two lines; otherwise we say that it is *nondegenerate* (Figure 1.1).

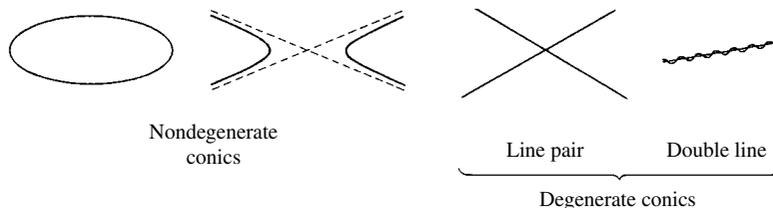


Figure 1.1

Let us consider the classification of such curves of degree 2, up to Euclidean transformations, from the point of view of their invariants. The Euclidean transformation group G contains the set of translations

$$x \mapsto x + l, \quad y \mapsto y + m$$

as a normal subgroup and is generated by these and the rotations. Alternatively, G can be viewed as the group of matrices

$$X = \begin{pmatrix} p & q & l \\ -q & p & m \\ 0 & 0 & 1 \end{pmatrix}, \quad p^2 + q^2 = 1. \quad (1.2)$$

Curves of degree 2 correspond to symmetric 3×3 matrices by writing the equation (1.1) as

$$(x, y, 1) \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = 0,$$

and then under the Euclidean transformation (1.2) the symmetric matrix of the curve transforms by

$$\begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \mapsto X^t \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} X.$$

In other words, the 6-dimensional vector space V of symmetric 3×3 matrices is a representation of the Euclidean transformation group G (see Section 1.21.10). Now, geometry studies properties which are invariant under groups of transformations, so let us look for invariants under this group action, in the form of polynomials $F(a, b, \dots, f)$.

The transformation matrix (1.2) has determinant 1, and so the first invariant polynomial we encounter is

$$D = \det \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}.$$

Here $D \neq 0$ exactly when the degree 2 curve is nondegenerate, and for this reason D is called the *discriminant* of the curve. Next we observe that the trace and determinant of the 2×2 submatrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ are also invariant; we will denote these by $T = a + c$ and $E = ac - b^2$. Moreover, any invariant polynomial can be (uniquely) expressed as a polynomial in D, T, E . In other words, the following is true.

Proposition 1.1. *The set of polynomials on V invariant under the action of G is a subring of $\mathbb{C}[a, b, c, d, e, f]$ and is generated by D, T, E . Moreover, these elements are algebraically independent; that is, the subring is $\mathbb{C}[D, T, E]$. \square*

Proof. Let $G_0 \subset G$ be the translation subgroup, with quotient $G/G_0 \cong O(2)$, the rotation group of the plane. We claim that it is enough to show that the subring of polynomials invariant under G_0 is

$$\mathbb{C}[a, b, c, d, e, f]^{G_0} = \mathbb{C}[a, b, c, D]. \quad (1.3)$$

This is because the polynomials in $\mathbb{C}[a, b, c]$ invariant under the rotation group $O(2)$ are generated by the trace T and discriminant E .

We also claim that if we consider polynomials in a, b, c, d, e, f and $1/E$, then

$$\mathbb{C}\left[a, b, c, d, e, f, \frac{1}{E}\right]^{G_0} = \mathbb{C}\left[a, b, c, D, \frac{1}{E}\right]. \quad (1.4)$$

It is clear that this implies (1.3), and so we are reduced to proving (1.4). The point here is that the determinant D can be written

$$D = Ef + (2bde - ae^2 - cd^2),$$

so that

$$f = \frac{D + ae^2 + cd^2 - 2bde}{E},$$

and hence

$$\mathbb{C}\left[a, b, c, d, e, f, \frac{1}{E}\right] = \mathbb{C}\left[a, b, c, d, e, D, \frac{1}{E}\right].$$

So a polynomial F in this ring (that is, a polynomial in a, b, c, d, e, f with coefficients which may involve powers of $1/E$) which is invariant under G_0 has to satisfy

$$F(a, b, c, d + al + bm, e + bl + cm, D) = F(a, b, c, d, e, D)$$

for arbitrary translations (l, m) . Taking $(l, m) = (-bt, at)$ shows that F cannot have terms involving e , while taking $(l, m) = (-ct, bt)$ shows that it cannot have terms involving d ; so we have shown (1.4). \square

Remark 1.2. One can see that Proposition 1.1 is consistent with a dimension count as follows. First, V has dimension 6. The Euclidean group G has dimension 3 (that is, Euclidean motions have 3 degrees of freedom). A general curve of degree 2 is preserved only by the finitely many elements of G (namely, 180° rotation about the centre and the trivial element), and hence we expect that ‘the quotient V/G has dimension 3’. Thus we may think of the three invariants D, T, E as three ‘coordinate functions on the quotient space’. \square

The space of all curves of degree 2 is $V \cong \mathbb{C}^6$, but here we are only concerned with polynomials, viewed as functions, on this space. Viewed in this sense the space is called an affine space and denoted \mathbb{A}^6 . (See Chapter 3.) We shall denote the subset corresponding to nondegenerate curves by $U \subset V$. This is an open set defined by the condition $D \neq 0$. The set of ‘regular functions’ on this open set is the set of rational functions on V whose denominator is a power of D , that is,

$$\mathbb{C} \left[a, b, c, d, e, f, \frac{1}{D} \right].$$

Up to now we have been thinking not in terms of curves but rather in terms of their defining equations of degree 2. In the following we shall want to think in terms of the curves themselves. Since two equations that differ only by a scalar multiple define the same curve, we need to consider functions that are invariant under the larger group \tilde{G} generated by G and the scalar matrices $X = rI$. The scalar matrix rI multiplies the three invariants D, E, T by r^6, r^4, r^2 , respectively. It follows that the set

$$\mathbb{C} \left[a, b, c, d, e, f, \frac{1}{D} \right]^{\tilde{G}}$$

of \tilde{G} -invariant polynomial functions on U is generated by

$$A = \frac{E^3}{D^2}, \quad B = \frac{T^3}{D}, \quad C = \frac{ET}{D}.$$

Among these three expressions there is a relation

$$AB - C^3 = 0,$$

so that:

a moduli space for nondegenerate curves of degree 2 in the Euclidean plane is the affine surface in \mathbb{A}^3 defined by the equation $xz - y^3 = 0$.

(The origin is a singular point of this surface called a rational double point of type A_2 .)

One can also see this easily in the following way. By acting on the defining equation (1.1) of a nondegenerate degree 2 curve with a scalar matrix rI for a suitable $r \in \mathbb{C}$ we can assume that $D(a, b, \dots, f) = 1$. The set of curves normalised in this way is then an affine plane with coordinates T, E . Now, the ambiguity in choosing such a normalisation is just the action of ωI , where $\omega \in \mathbb{C}$ is an imaginary cube root of unity, and so the parameter space for nondegenerate degree 2 curves is the surface obtained by dividing out the (T, E) plane by the action of the cyclic group of order 3,

$$(T, E) \mapsto (\omega T, \omega^2 E).$$

The origin is a fixed point of this action, and so it becomes a quotient singularity in the parameter space.

Next, let us look at the situation over the real numbers \mathbb{R} . We note that here cube roots are uniquely determined, and so by taking that of the discriminant D of equation (1.1) we see that for real curves of degree 2 we can take as coordinates the numbers

$$\alpha = \frac{E}{\sqrt[3]{D^2}}, \quad \beta = \frac{T}{\sqrt[3]{D}}.$$

In this way the curves are parametrised simply by the real (α, β) plane:

- (i) Points in the (open) right-hand parabolic region $\beta^2 < 4\alpha$ and the (closed) 4th quadrant $\alpha \geq 0, \beta \leq 0$ do not correspond to any curves over the real numbers. (It is natural to refer to the union of these two sets as the ‘imaginary region’ of the (α, β) plane. See Figure 1.2.) The points of the parameter space are real, but the coefficients of the defining equation (1.1)

always require imaginary complex numbers. For example, the origin $(0, 0)$ corresponds to the curve

$$\sqrt{-1}(x^2 - y^2) + 2xy = 2x.$$

- (ii) Points of the parabola $\beta^2 = 4\alpha$ in the 1st quadrant correspond to circles of radius $\sqrt{2/\beta}$.
- (iii) Points of the open region $\beta^2 > 4\alpha > 0$ between the parabola and the β -axis parametrise ellipses.
- (iv) Points of the positive β -axis $\alpha = 0, \beta > 0$ parametrise parabolas.
- (v) Points in the left half-plane $\alpha < 0$ parametrise hyperbolas. Within this region, points along the negative α -axis parametrise rectangular hyperbolas (the graph of the reciprocal function), while points in the 2nd and 3rd quadrants correspond respectively to acute angled and obtuse angled hyperbolas.

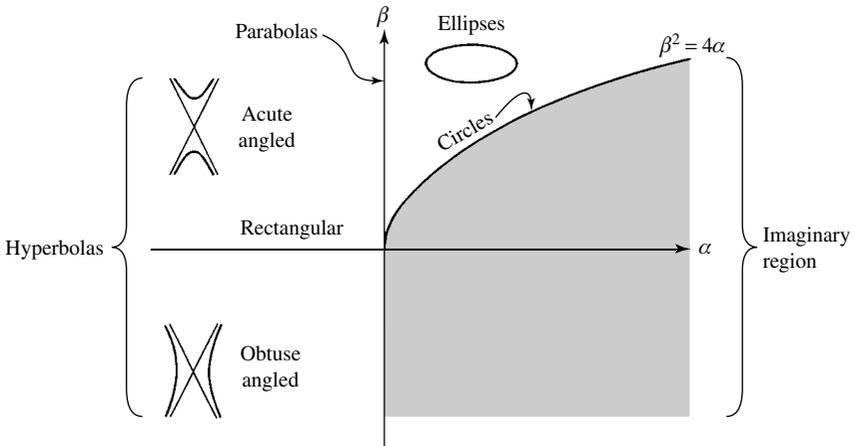


Figure 1.2: The parameter space of real curves of degree 2

Let us now follow a rotation of this figure in the positive direction about the origin.

Beginning with a circle (eccentricity $e = 0$), our curve grows into an ellipse through a parabolic phase ($e = 1$) before making a transition to a hyperbola. The angle between the asymptotes of this hyperbola is initially close to zero and gradually grows to 180° , at which point ($e = \infty$) the curve enters the imaginary region. After passing through this region it turns once again into a circle. (This is Kepler's Principle.)

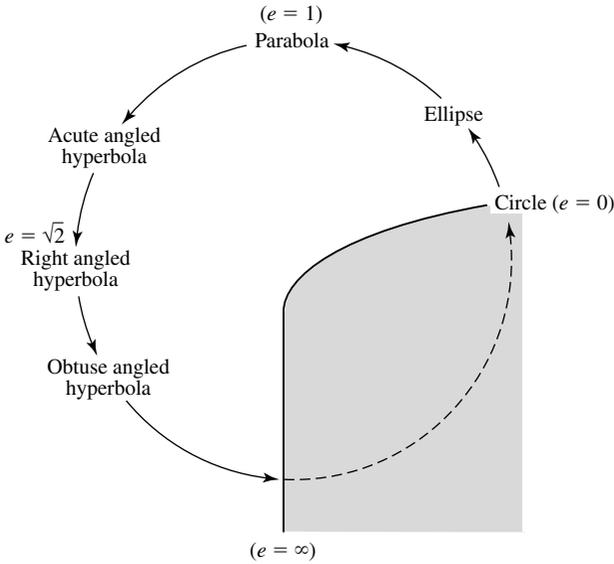


Figure 1.3: Transmigration of a conic

Remark 1.3. In the case of an ellipse, our curve has a (Euclidean invariant) area which is equal to $\pi/\sqrt{\alpha}$. In particular, this area increases as the curve approaches the β -axis, and one may think of a parabola, corresponding to a point on the axis, as having infinite area. Taking this point of view a step further, one may think of a hyperbola as having imaginary area. \square

We have thus established a correspondence between real curves of degree 2 up to Euclidean transformations and points of the (α, β) plane. The group G does not have the best properties (it is not linearly reductive – this will be explained in Chapter 4), but nevertheless in this example we are lucky and every point of the (α, β) plane corresponds to some curve.

Plane curves of degree 2 are also called *conics*, as they are the curves obtained by taking plane cross sections of a circular cone (an observation which goes back to Apollonius and Pappus). From this point of view, the eccentricity e of the curve is determined by the angle of the plane (Figure 1.4).

To be precise, let ϕ be the angle between the axis of the cone and the circular base, and let ψ be the angle between the axis and the plane of the conic. If we now let

$$e = \frac{\sin \psi}{\sin \phi},$$

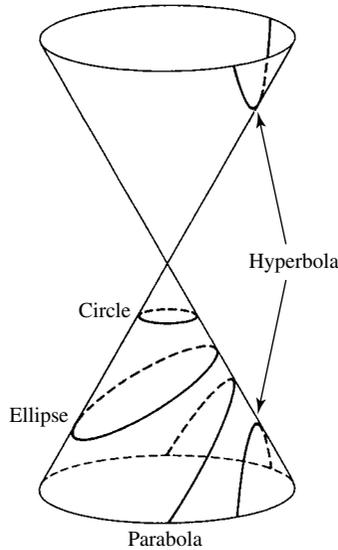


Figure 1.4: Plane sections of a cone

then for $e < 1$, $e = 1$ and $e > 1$, respectively, the conic section is an ellipse, a parabola or a hyperbola. As is well known, the eccentricity can also be expressed as

$$e = \frac{\text{distance from the focus}}{\text{distance to the directrix}}.$$

(For a curve with equation $(x/a)^2 \pm (y/b)^2 = 1$, where $a \leq b$, we find that $e = \sqrt{1 \mp (a/b)^2}$.) This is not an invariant polynomial function, but it satisfies an algebraic equation whose coefficients are invariants. Namely, it is the invariant multivalued function satisfying the quartic equation

$$(e^2 - 1) + \frac{1}{e^2 - 1} = 2 - \frac{T^2}{2E}.$$

Although e is properly speaking multivalued, we can take advantage of the fact that we are considering conics over the real numbers. In this case it is possible to choose a branch so that the function is single-valued for conics with real coefficients.

Suppose we extend the Euclidean transformation group to include also similarities (dilations and contractions). Transforming a conic by a scale factor k multiplies α by $\sqrt[3]{k^2}$ and multiplies β by $\sqrt[3]{k}$. So the ‘moduli space’ is now the

(α, β) plane, minus the origin, divided out by the action of scalars

$$(\alpha, \beta) \mapsto (\sqrt[3]{k^2}\alpha, \sqrt[3]{k}\beta).$$

In other words, it is a projective line (more precisely, the weighted projective line $\mathbb{P}(1 : 2)$; see Example 3.46 in Chapter 3). The one dimensional parameter that we obtain in this way is essentially the eccentricity e .

The aim of the first part of this book is to generalise the construction of this sort of parameter space to equivalence classes of polynomials in several variables under the action of the general linear group. In geometric language, our aim is to construct parameter spaces for equivalence classes of general-dimensional projective hypersurfaces with respect to projective transformations.

1.2 Invariants of groups

To say that a polynomial $f(x_1, \dots, x_n)$ in n variables is an *invariant* with respect to an $n \times n$ matrix $A = (a_{ij})$ can have one of two meanings:

- (i) f is invariant under the coordinate transformation determined by A . That is, it satisfies

$$f(Ax) := f\left(\sum_i a_{1i}x_i, \dots, \sum_i a_{ni}x_i\right) = f(x). \quad (1.5)$$

- (ii) f is invariant under the derivation

$$\mathcal{D}_A = \sum_{i,j} a_{ij}x_i \frac{\partial}{\partial x_j}$$

determined by A . In other words, it satisfies

$$\mathcal{D}_A f = \sum_{i,j} a_{ij}x_i \frac{\partial f}{\partial x_j} = 0. \quad (1.6)$$

In both cases, the invariant polynomials under some fixed set of matrices form a subring of $\mathbb{C}[x_1, \dots, x_n]$. The idea of a Lie group and of a Lie algebra, respectively, arises in a natural way out of these two notions of invariants.

(a) Hilbert series

To begin, we review the first notion 1.2(i) of invariance. (The second will reappear in Chapter 4.) Given a set of nonsingular matrices $T \subset GL(n)$, we consider the set of all invariant polynomials

$$\{f \in \mathbb{C}[x_1, \dots, x_n] \mid f(Ax) = f(x) \text{ for all } A \in T\}.$$

Clearly this is a subring of $\mathbb{C}[x_1, \dots, x_n]$, called the *ring of invariants* of T . Notice that if $f(x)$ is an invariant under matrices A and B , then it is an invariant under the inverse A^{-1} and the product AB . It follows that in the definition of the ring of invariants we may assume without loss of generality that T is closed under taking products and inverses. This is just the definition of a group; moreover, in essence we have here the definition of a group representation.

Definition 1.4. Let $G \subset GL(n)$ be a subgroup. A polynomial $f \in \mathbb{C}[x_1, \dots, x_n]$ satisfying

$$f(Ax) = f(x) \text{ for all } A \in G$$

is called a G -invariant. □

We shall write $S = \mathbb{C}[x_1, \dots, x_n]$ for the polynomial ring and S^G for the ring of invariants of G . Let us examine some cases in which G is a finite group.

Example 1.5. Let G be the symmetric group consisting of all $n \times n$ permutation matrices – that is, having a single 1 in each row and column, and 0 elsewhere. The invariants of G in $\mathbb{C}[x_1, \dots, x_n]$ are just the symmetric polynomials. These form a subring which includes the n elementary symmetric polynomials

$$\begin{aligned} \sigma_1(x) &= \sum_i x_i \\ \sigma_2(x) &= \sum_{i < j} x_i x_j \\ &\dots \\ \sigma_n(x) &= x_1 \dots x_n, \end{aligned}$$

and it is well known that these generate the subring of all symmetric polynomials. □

Example 1.6. Suppose G is the alternating group consisting of all even permutation matrices (matrices as in the previous example, that is, with determinant +1). In this case a G -invariant polynomial can be uniquely expressed as the sum of a symmetric and an alternating polynomial:

$$\left\{ \begin{array}{l} \text{invariant} \\ \text{polynomials} \end{array} \right\} \cong \left\{ \begin{array}{l} \text{symmetric} \\ \text{polynomials} \end{array} \right\} \oplus \left\{ \begin{array}{l} \text{alternating} \\ \text{polynomials} \end{array} \right\}.$$

Moreover, the set of alternating polynomials is a free module over the ring of symmetric polynomials with the single generator

$$\Delta(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

□

Example 1.7. Let $G = \{\pm I_n\} \subset GL(n)$, the subgroup of order 2, where I_n is the identity matrix. This time the set of invariant polynomials is a vector space with basis consisting of all monomials of even degree. As a ring it is generated by the monomials of degree 2; in the case $n = 2$, for example, it is generated by x_1^2, x_1x_2, x_2^2 . □

Let $S = \mathbb{C}[x_1, \dots, x_n]$. Any polynomial $f(x) = f(x_1, \dots, x_n)$ can be written as a sum of homogeneous polynomials:

$$f(x) = f_0 + f_1(x) + f_2(x) + \dots + f_{\text{top}}(x) \quad \text{with } \deg f_i(x) = i.$$

Invariance of $f(x)$ is then equivalent to invariance of all the summands $f_i(x)$. Denoting by $S_d \subset S$ the subspace of homogeneous polynomials of degree d , it follows that there are direct sum decompositions

$$S = \bigoplus_{d \geq 0} S_d, \quad S^G = \bigoplus_{d \geq 0} S^G \cap S_d.$$

(S and S^G are *graded rings*. See Section 2.5(a).) We can introduce a generating function for the dimensions of the homogeneous components of S^G . This is the formal power series in an indeterminate t , called the *Hilbert series* (also called the Poincaré series, or the Molien series) of the graded ring S^G :

$$P(t) := \sum_{d \geq 0} (\dim S^G \cap S_d) t^d \in \mathbb{Z}[[t]].$$

Example 1.8. The Hilbert series of the matrix groups in Examples 1.5 and 1.6 are given, respectively, by the generating functions:

(i)
$$\frac{1}{(1-t)(1-t^2) \cdots (1-t^n)},$$

(ii)
$$\frac{1 + t^{n(n-1)/2}}{(1-t)(1-t^2) \cdots (1-t^n)}.$$

One sees this in the following way. First, if we expand the expression

$$\frac{1}{(1 - \sigma_1)(1 - \sigma_2) \cdots (1 - \sigma_n)}$$

as a formal series, the terms form a basis of the infinite-dimensional vector space of symmetric polynomials. So, substituting t^i for σ_i we obtain (i) for the Hilbert series of Example 1.5. For Example 1.6, a similar argument gives (ii) after noting that

$$S^G = \mathbb{C}[\sigma_1, \dots, \sigma_n] \oplus \mathbb{C}[\sigma_1, \dots, \sigma_n]\Delta,$$

where $\deg \Delta = n(n - 1)/2$. □

Note that by a similar argument the full polynomial ring $S = \bigoplus S_d$ has Hilbert series $P(t) = (1 - t)^{-n}$. In particular, this gives the familiar fact that $\dim S_d = \binom{n-1+d}{n-1}$. We will make more systematic use of this idea in the proof of Molien's Theorem below.

The Hilbert series is a very important invariant of the ring S^G which, as these examples illustrate, measures its 'size and shape':

Proposition 1.9. *If S^G is generated by homogeneous polynomials f_1, \dots, f_r of degrees d_1, \dots, d_r , then the Hilbert series of S^G is the power series expansion at $t = 0$ of a rational function*

$$P(t) = \frac{F(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_r})}$$

for some $F(t) \in \mathbb{Z}[t]$.

Proof. We use induction on r , observing that when $r = 1$ the ring S^G is just $\mathbb{C}[f_1]$ with the Hilbert series

$$P(t) = 1 + t^{d_1} + t^{2d_1} + \cdots = \frac{1}{1 - t^{d_1}}.$$

For $r > 1$ we consider the (injective complex linear) map $S^G \rightarrow S^G$ defined by $h \mapsto f - rh$. We denote the image by $R \subset S^G$ and consider the Hilbert series for the graded rings R and S^G/R . These satisfy

$$P_{S^G}(t) = P_R(t) + P_{S^G/R}(t).$$