7

More on Bracket Algebra

Algebra is generous; she often gives more than is asked of her.

D'Alembert (1717–1783)

The last chapter demonstrated that determinants (and in particular multihomogeneous bracket polynomials) are of fundamental importance in expressing projectively invariant properties. In this chapter we will alter our point of view. What if our "first-class citizens" were not the points of a projective plane but the values of determinants generated by them? We will see that with the use of Grassmann-Plücker relations we will be able to recover a projective configuration from its values of determinants.

We will start our treatment by considering vectors in $\mathbb{R}^3$ rather than considering homogeneous coordinates of points in $\mathbb{RP}^2$. This has the advantage that we can neglect the (only technical) difficulty that the determinant values vary when the coordinates of a point are multiplied by a scalar.

While reading this chapter the reader should constantly bear in mind that all concepts presented in this chapter generalize to arbitrary dimensions. Still we will concentrate on the case of vectors in $\mathbb{R}^2$ and in $\mathbb{R}^3$ to keep things conceptually as simple as possible.

7.1 From Points to Determinants ...

Assume that we are given a configuration of n vectors in $\mathbb{R}^3$ arranged in a matrix:

$$P = \begin{pmatrix} | & | & | & \dots & | \\ p_1 & p_2 & p_3 & \dots & p_n \\ | & | & | & \dots & | \end{pmatrix}.$$

Later on we will consider these vectors as homogeneous coordinates of a point configuration in the projective plane. The matrix P may be considered an element in $\mathbb{R}^{3\cdot n}$. There is an overall number of $\binom{n}{3}$ possible 3×3 matrix minors that could be formed from this matrix, since there are as many ways to select three points from the configuration. If we know the value of the corresponding determinants we can reconstruct the value of any bracket using permutations of the points and applying the appropriate sign changes, since we have

$$[a,b,c] = [b,c,a] = [c,a,b] = -[b,a,c] = -[a,c,b] = -[c,b,a].$$

We consider the index set E for the points in P by

$$E = \{1, 2, \ldots, n\}$$

and a corresponding index set for the index triples

$$\Lambda(n,3) := \{(i,j,k) \in \mathbb{E}^3 \mid i < j < k\}.$$

Calculating the determinants for our vector configuration can now be considered as a map

$$\begin{aligned} \Gamma\colon \mathbb{R}^{3\cdot n} &\to \mathbb{R}^{\binom{n}{3}}, \\ P &\mapsto ([p_1,p_2,p_3],[p_1,p_2,p_4],\ldots,[p_{n-2},p_{n-1},p_n]). \end{aligned}$$

We can consider the vector of determinants $\Gamma(P)$ itself as a map that assigns to each element $(i,j,k) \in \Lambda(n,3)$ the value of the corresponding determinant $[p_i,p_j,p_k]$. By applying the alternating rule, the values of all brackets can be recovered from the values of $\Gamma(P)$. In order to avoid all the information about a bracket being captured by the subscripts, we make the following typographical convention. If P is a matrix consisting of columns $p_1, p_2, \ldots, p_n$, then we may also write $[i,j,k]_P$ instead of $[p_i,p_j,p_k]$.

The reader should not be scared of the high dimension of the spaces involved. This high dimensionality comes from the fact that we consider an entire collection of n vectors now as a *single* object in $\mathbb{R}^{n\cdot 3}$. Similarly, an element in the space $\mathbb{R}^{\binom{n}{3}}$ may be considered a single object that carries the values of all determinants simultaneously. It will be our aim to show that both spaces carry in principle the same information if we are concerned with projective properties.

One of the fundamental relations between P and $\Gamma(P)$ is given by the following lemma:

Lemma 7.1. *Let $P \in (\mathbb{R}^3)^n$ be a configuration of n vectors in $\mathbb{R}^3$ and let T be an invertible 3×3 matrix. Then $\Gamma(T \cdot P) = \lambda \cdot \Gamma(P)$ for a suitable $\lambda \neq 0$.*

Proof. Let $(i,j,k) \in \Lambda(n,3)$: Then we have $\det(T \cdot p_i, T \cdot p_j, T \cdot p_k) = \det(T) \cdot [p_i,p_j,p_k]$. Thus we have $\Gamma(T \cdot P) = \det(T) \cdot \Gamma(P)$. □

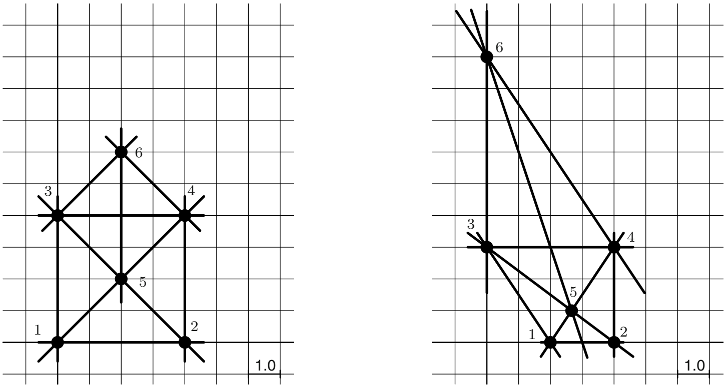

Fig. 7.1 A configuration and a projective image of it.

The previous lemma states that up to a scalar multiple the vector $\Gamma(P)$ is invariant under linear transformations. On the level of point configurations in the projective plane this means that if two configurations of points are projectively equivalent, we can assign matrices of homogeneous coordinates P and Q to them such that $\Gamma(P) = \Gamma(Q)$. A little care has to be taken. Since the homogeneous coordinates of each point are determined only up to a scalar factor, we have to adjust these factors in the right way to get the above relation. We can get rid of the λ in Lemma 7.1 by an overall scaling applied to all homogeneous coordinates.

Example 7.1. Consider the two pictures in Figure 7.1. They are related by a projective transformation. We get homogeneous coordinates of the points by simply extending the Euclidean coordinates by a 1. The two coordinate matrices are

$$P = \begin{pmatrix} 0 & 4 & 0 & 4 & 2 & 2 \\ 0 & 0 & 4 & 4 & 2 & 6 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad Q = \begin{pmatrix} 2 & 4 & 0 & 4 & \frac{8}{3} & 0 \\ 0 & 0 & 3 & 3 & 1 & 9 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

For P the corresponding determinants indexed by $\Lambda(6,3)$ are

$[1,2,3]_P = 16$	$[1,3,5]_P = -8$	$[2,3,4]_P = -16$	$[2,5,6]_P = -8$
$[1,2,4]_P = 16$	$[1,3,6]_P = -8$	$[2,3,5]_P = 0$	$[3,4,5]_P = -8$
$[1,2,5]_P = 8$	$[1,4,5]_P = 0$	$[2,3,6]_P = -16$	$[3,4,6]_P = 8$
$[1,2,6]_P = 24$	$[1,4,6]_P = 16$	$[2,4,5]_P = 8$	$[3,5,6]_P = 8$
$[1,3,4]_P = -16$	$[1,5,6]_P = 8$	$[2,4,5]_P = 8$	$[4,5,6]_P = -8.$

The corresponding values for Q are

$[1,2,3]_Q = 6$	$[1,3,5]_Q = -4$	$[2,3,4]_Q = -16$	$[2,5,6]_Q = -8$
$[1,2,4]_Q = 6$	$[1,3,6]_Q = -12$	$[2,3,5]_Q = 0$	$[3,4,5]_Q = -8$
$[1,2,5]_Q = 2$	$[1,4,5]_Q = 0$	$[2,3,6]_Q = -24$	$[3,4,6]_Q = 24$
$[1,2,6]_Q = 18$	$[1,4,6]_Q = 24$	$[2,4,5]_Q = 4$	$[3,5,6]_Q = 16$
$[1,3,4]_Q = -12$	$[1,5,6]_Q = 8$	$[2,4,5]_Q = 12$	$[4,5,6]_Q = -16.$

At first sight these two collections of values seem not to be very related. However, if we simply choose different homogeneous coordinates for the point in the second picture, such as

$$r_1 = 4 \cdot q_1, \quad r_2 = 4 \cdot q_2, \quad r_3 = 2 \cdot q_3, \quad r_4 = 2 \cdot q_4, \quad r_5 = 3 \cdot q_5, \quad r_6 = 1 \cdot q_6,$$

we get

$[1,2,3]_R = 192$	$[1,3,5]_R = -96$	$[2,3,4]_R = -192$	$[2,5,6]_R = -96$
$[1,2,4]_R = 192$	$[1,3,6]_R = -96$	$[2,3,5]_R = 0$	$[3,4,5]_R = -96$
$[1,2,5]_R = 96$	$[1,4,5]_R = 0$	$[2,3,6]_R = -192$	$[3,4,6]_R = 96$
$[1,2,6]_R = 288$	$[1,4,6]_R = 192$	$[2,4,5]_R = 96$	$[3,5,6]_R = 96$
$[1,3,4]_R = -192$	$[1,5,6]_R = 96$	$[2,4,5]_R = 96$	$[4,5,6]_R = -96.$

This is exactly 12 times the values of the determinants obtained from P. It is also instructive to check the Grassmann-Plücker relations for a few special cases. For instance, we should have

$$[1,2,3]_P[4,5,6]_P - [1,2,4]_P[3,5,6]_P + [1,2,5]_P[3,4,6]_P - [1,2,6]_P[3,4,5]_P = 0.$$

This can easily be verified:

$$16 \cdot (-8) - 16 \cdot 8 + 8 \cdot 8 - 24 \cdot (-8) = -128 - 128 + 64 + 192 = 0.$$

7.2 ... and Back

We will now focus on the other direction. To what extent do the values of $\Gamma(P)$ already determine the entries of P? Let us first start with two observations.

> **Observation 1:** *The elements in $\Gamma(P)$ are not independent of each other.* This comes from the fact that the entries at least have to satisfy the Grassmann-Plücker relations.
> **Observation 2:** *The elements in $\Gamma(P)$ can determine P only up to a linear transformation.* This is the statement of Lemma 7.1.

These two observations extract the essence of the relation between $\Gamma(P)$ and P. We will prove that for every $\Gamma \in \mathbb{R}^{\binom{n}{3}} - \{\mathbf{0}\}$ that satisfies the Grassmann-Plücker relations there is a $P \in \mathbb{R}^{3\cdot n}$ such that $\Gamma = \Gamma(P)$. This P is uniquely determined up to a linear transformation.

We again consider Γ as a map $\Lambda(n,3) \to \mathbb{R}$. For the rest of this chapter we will denote the value $\Gamma((i,j,k))$ by $[i,j,k]$. Thus the problem of finding a suitable P can be restated in the following way:

Find a P such that $[i,j,k] = [i,j,k]_P$ for all $(i,j,k) \in \Lambda(n,3)$.

If Γ is not the zero vector $\mathbf{0}$, then we may without loss of generality assume that $[1,2,3] = 1$ (otherwise we simply have to permute the indices in a suitable way, and scale Γ by a suitable factor). If we find any suitable matrix P with $\Gamma(P) = \Gamma$, then the first three vectors form an invertible matrix

$$M = \begin{pmatrix} | & | & | \\ p_1 & p_2 & p_3 \\ | & | & | \end{pmatrix}.$$

If we replace P by $P' := \det M \cdot M^{-1} \cdot P$, we still have $\Gamma(P') = \Gamma$ but in addition the first three vectors became unit vectors. The matrix P' has the shape

$$P' = \begin{pmatrix} 1 & 0 & 0 & p_{41} & p_{51} & \dots & p_{n1} \\ 0 & 1 & 0 & p_{42} & p_{52} & \dots & p_{n2} \\ 0 & 0 & 1 & p_{43} & p_{53} & \dots & p_{n3} \end{pmatrix}.$$

The key observation now is that each entry in the matrix corresponds to the value of a suitable bracket. For instance, we have

$$p_{43} = [1,2,4]; \quad p_{42} = -[1,3,4]; \quad p_{41} = [2,3,4].$$

Thus if our matrix P' exists, we can immediately fill in all the other entries if we know the values of Γ. We get

$$P' = \begin{pmatrix} 1 & 0 & 0 & [2,3,4] & [2,3,5] & \dots & [2,3,n] \\ 0 & 1 & 0 & -[1,3,4] & -[1,3,5] & \dots & -[1,3,n] \\ 0 & 0 & 1 & [1,2,4] & [1,2,5] & \dots & [1,2,n] \end{pmatrix}.$$

So far we have only made sure that brackets of the forms $[1,2,3]$, $[1,2,i]$, $[1,3,i]$, and $[2,3,i]$, $i = 4,\dots,n$, get the right value. How about all the remaining brackets (which are the vast majority)? This is the point where the Grassmann-Plücker relations come into play. If Γ satisfies all identities required by the Grassmann-Plücker relations, then all other bracket values will fit automatically. We can prove this by successively showing that (under the hypothesis that the Grassmann-Plücker relations hold) the values of the brackets are uniquely determined after fixing the brackets of the above form. Let us take the bracket $[1,4,5]$ for instance. By our assumptions on Γ we know that the relation

$$[1,2,3][1,4,5] - [1,2,4][1,3,5] + [1,2,5][1,3,4] = 0$$

must hold. Except for the value of the bracket $[1,4,5]$, all other bracket values are already fixed. Since $[1,2,3] \neq 0$, the value of $[1,4,5]$ is determined uniquely. Similarly, we can show that all values of the brackets of the forms $[1,i,j]$, $[2,i,j]$, and $[3,i,j]$ are uniquely determined. It remains to show that brackets that do not contain any of the indices 1, 2, 3 are also already fixed. As an example we take the bracket $[4,5,6]$. The following relation must hold:

$$[1,2,3][4,5,6] - [1,2,4][3,5,6] + [1,2,5][3,4,6] - [1,2,6][3,4,5] = 0.$$

Again all values except $[4,5,6]$ are already determined by our previous considerations. Hence the above expression fixes the value of $[4,5,6]$. We may argue similarly for any bracket $[i,j,k]$. We have finished the essential parts of the proof of the following theorem:

Theorem 7.1. *Let $\Gamma \in \mathbb{R}^{\binom{n}{3}}, \Gamma \neq \mathbf{0}$, be an assignment of bracket values that satisfies all Grassmann-Plücker relations. Then there exists a vector configuration $P \in \mathbb{R}^{3 \cdot n}$ with $\Gamma = \Gamma(P)$.*

Proof. For the proof we just summarize what we have done so far. With the above notation we may without loss of generality assume that $[1,2,3] = 1$. As above, set

$$P = \begin{pmatrix} 1 & 0 & 0 & [2,3,4] & [2,3,5] & \dots & [2,3,n] \\ 0 & 1 & 0 & -[1,3,4] & -[1,3,5] & \dots & -[1,3,n] \\ 0 & 0 & 1 & [1,2,4] & [1,2,5] & \dots & [1,2,n] \end{pmatrix}.$$

In particular, by this choice we have

$$[1,2,3] = [1,2,3]_P, \ [1,2,i] = [1,2,i]_P, \ [1,3,i] = [1,3,i]_P, \ [2,3,i] = [2,3,i]_P,$$

for any $i \in \{4,\dots,n\}$. Since P is a point configuration, it satisfies all Grassmann-Plücker relations. Since if the Grassmann-Plücker relations are satisfied the values of all brackets are determined uniquely if the above bracket values are fixed, we must have $\Gamma = \Gamma(P)$. □

Example 7.2. Assume that we are looking for a vector configuration that gives us the following bracket values (they have been chosen carefully to satisfy all Grassmann-Plücker relations, check it):

$[\mathbf{1},\mathbf{2},\mathbf{3}] = 1$	$[\mathbf{1},\mathbf{3},\mathbf{5}] = -1/2$	$[\mathbf{2},\mathbf{3},\mathbf{4}] = -1$	$[2,5,6] = -1/2$
$[\mathbf{1},\mathbf{2},\mathbf{4}] = 1$	$[\mathbf{1},\mathbf{3},\mathbf{6}] = -1/2$	$[\mathbf{2},\mathbf{3},\mathbf{5}] = 0$	$[3,4,5] = -1/2$
$[\mathbf{1},\mathbf{2},\mathbf{5}] = 1/2$	$[1,4,5] = 0$	$[\mathbf{2},\mathbf{3},\mathbf{6}] = -1$	$[3,4,6] = 1/2$
$[\mathbf{1},\mathbf{2},\mathbf{6}] = 3/2$	$[1,4,6] = 1$	$[2,4,5] = 1/2$	$[3,5,6] = 1/2$
$[\mathbf{1},\mathbf{3},\mathbf{4}] = -1$	$[1,5,6] = 1/2$	$[2,4,5] = 1/2$	$[4,5,6] = -1/2.$

The brackets that are emphasized by bold letters are those we can directly use to obtain the entries in our matrix

$$P = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & 1 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 1 & \frac{1}{2} & \frac{3}{2} \end{pmatrix}.$$

It is easy to check that the other bracket values are satisfied automatically. The careful reader may have recognized that the brackets were chosen such in a way that they again produce a projectively equivalent copy of the drawing in Figure 7.1.

7.3 A Glimpse of Invariant Theory

The essence of the last two chapters can be stated in the following way: *The determinants $\Gamma(P)$ of a vector configuration P carry essentially the same information as the configuration itself.* In principle, we can perform all operations of projective geometry entirely on the level of determinants.

There are several ways to exploit this fact, and we want to mention at least a few of them. In this section we want to review a few facts that belong to the context of *classical invariant theory* (see for instance [98, 131]). This theory originated precisely in the efforts of the classical geometers to understand how geometry and algebra are related. Besides a purely theoretical interest there were also very practical motivations for considering this topic: People in the nineteenth century did not have computers. All calculations had to be done by hand. For dealing with geometric constructions of nontrivial size it was absolutely necessary to have advanced algebraic techniques that reduced the amount of hand calculations to a minimum. Plücker, who was (as we already have seen) one of the pioneers in this field, once said (according to Klein) that *one has to read in equations.* This means to draw far-reaching conclusions from simple algebraic facts. Striving for powerful algebraic techniques that are as close to geometry as possible first led to the development of homogeneous coordinates, later to the recognition of the importance of determinants and still later to the development of invariant theory.

One might be tempted to think that nowadays with the help of computers that can do all the “number crunching” it is no longer necessary to care about sophisticated algebraic techniques, since calculations on the coordinate level can be carried out automatically. In fact, exactly the opposite is the case. The rise of computational power has led to a considerable demand for sophisticated techniques for performing geometric calculations. There are several reasons for this (and we will list only a few of them):

- With computers it is possible to deal with really huge geometric situations that were not previously within reach. So still it is necessary to compute efficiently.
- Practical applications in computer-aided design, robotics, computer vision, and structural mechanics lead to problems that are at the core of projective geometry, and the algebraic techniques that are used there have to be appropriate for the problem. (For instance, consider an autonomous robot that has to use pictures taken by a video camera to obtain an inner model of the environment. This corresponds to the problem of lifting a two-dimensional projective scene to a three-dimensional one.)
- Symbolic calculations on the coordinate level very soon lead to a combinatorial explosion, since usually every single multiplication of two polynomials doubles the number of summands involved.
- The rise of computers opened the new discipline of "automatic deduction in geometry" (see [45, 115, 133, 60, 17]). There one is, for instance, interested in automatically generating proofs for geometric theorems. In order to be able to retranslate the automatically generated proof into geometric statements one has finally to reinterpret algebraic terms geometrically. This is much easier if the algebraic statements are "close" to geometry.

Our investigations of the last two sections showed that brackets form a *functional basis* for projective invariants. To make this notion a bit more precise, we first slightly broaden the scope of Definition 6.1, in which we introduced projectively invariant properties. To avoid technical difficulties that arise from configurations that do not have full rank, we call a configuration of points given by homogeneous coordinates $P \in \mathbb{R}^{3 \cdot n}$ *proper* if P has rank 3. If P is not proper, then all points of P lie on a line, or even collapse to a single point.

Definition 7.1. Let M be an arbitrary set. A *projective invariant* of n points in the real projective plane is a map $f\colon \mathbb{R}^{3 \cdot n} \to M$ such that for all invertible real 3×3 matrices $T \in \mathrm{GL}(\mathbb{R}, 3)$ and $n \times n$ invertible real diagonal matrices $D \in \mathrm{diag}(\mathbb{R}, n)$ and for any proper configuration P, we have

$$f(P) = f(T \cdot P \cdot D).$$

In this definition the image range M is taken to be an arbitrary set. If M is the set $\{\mathbf{true}, \mathbf{false}\}$, then f is a projectively invariant property as introduced in Definition 6.1. If $M = \mathbb{R} \cup \{\infty\}$, then f measures some number that is invariant under projective transformations (such as the cross-ratio, for instance). We now want to study under what circumstances one can generate one projective invariant from others. For this we introduce the concept of a functional basis.

Definition 7.2. A collection $f_i\colon \mathbb{R}^{3\cdot n} \to M_i,\ i = 1, \dots, k$, of functions is a *functional basis* of the set of all projective invariants if for every projective invariant $f\colon \mathbb{R}^{3\cdot n} \to M$, there is a function

$$m\colon M_1 \times \cdots \times M_k \to M$$

such that for all $X \in \mathbb{R}^{3\cdot n}$ we have

$$f(X) = m(f_1(X), \dots, f_k(X)).$$

In other words, if $f_1, \dots, f_k$ is a functional basis then it completely suffices to know the values of these functions to calculate the value of any other invariant. We can also understand the concept of functional basis on an algorithmic level. For every invariant f there exists an algorithm $\mathcal{A}$ that takes the values of $f_1, \dots, f_k$ as input and calculates the value of f. The last two sections essentially prove the following theorem:

Theorem 7.2. *The entries of the determinant vector $\Gamma(P)$ form a functional basis for all projective invariants.*

Proof (sketch). Let f be any invariant and let P be an arbitrary proper configuration of points. Since P is proper, at least one entry of $\Gamma := \Gamma(P)$ is nonzero (this means that at least one determinant does not vanish). Thus we can use the techniques of Section 7.2 to calculate a configuration $P' := P'(\Gamma)$ that is projectively equivalent to P. Thus we must have $f(P'(\Gamma)) = f(P)$, which proves the claim. □

This theorem is a weak version of a much deeper algebraic fact that is known as the *first fundamental theorem* of projective invariant theory (see [131, 126]). Theorem 7.2 states only that we can *compute* any invariant if we know the values of the brackets. It does not state that the algebraic structure of an invariant is preserved by any means. The first fundamental theorem in addition guarantees that the algebraic type of an invariant is essentially preserved.

Unfortunately, at this point we have to pay a price for calculating with homogeneous coordinates. Since we do not distinguish homogeneous coordinates that differ only by a scalar multiple, we have to take care of these equivalence classes in a corresponding algebraic setup. Any polynomial in the entries of the matrix $P \in \mathbb{R}^{3\cdot n}$ is thus not invariant under rescaling of the homogeneous coordinates. This implies that the category of *polynomials* is not the appropriate one for talking about projective invariants. There are essentially two ways out of this dilemma. Both involve quite a few technical difficulties. The first is to introduce the concept of a *relative invariant polynomial*. Such a polynomial $f(P)$ is not an invariant in the sense of Definition 7.1. Rather than being strictly invariant, one requires that the action of $T \in \mathrm{GL}(\mathbb{R},3)$ and $D \in \mathrm{diag}(\mathbb{R},n)$ change $f(T \cdot P \cdot D)$ in a very predictable way. If D has diagonal entries $\lambda_1, \dots, \lambda_k$, then f is called a relative invariant if there are exponents $\tau_1, \dots, \tau_n, \tau$ such that

$$f(T \cdot P \cdot D) = \det(T)^{\tau} \cdot \lambda_1^{\tau_1} \cdot \cdots \cdot \lambda_n^{\tau_n} \cdot f(P).$$

This means that rescaling and transforming only results in a controllable factor that essentially depends only on the number of times a point is involved in the function f.

The other way out is to change the category of functions under consideration and not consider polynomials as the important functions. The simplest category of functions in which projective invariants arise is that of *rational functions* that are quotients of polynomials. We already have encountered such types of invariants. The cross-ratio is the simplest instance of such an invariant. We will follow this path a little later.

For now we want to state at least one version of the first fundamental theorem that avoids all these technical difficulties for the price of not directly making a statement about projective geometry [131]. Our version of the first fundamental theorem is formulated on the level of *vector configurations*. Thus this time we distinguish vectors that differ by scalar multiples. Furthermore, we have to restrict the set of allowed transformations to those that have determinant one (this means we have to study group actions of $SL(\mathbb{R},3)$; this still includes all projective transformations).

Theorem 7.3. *Let $f\colon \mathbb{R}^{3 \cdot n} \to \mathbb{R}$ be a polynomial with the property that for every $T \in \mathrm{SL}(\mathbb{R},3)$ and every $P \in \mathbb{R}^{3 \cdot n}$ we have*

$$f(P) = f(T \cdot P).$$

Then f can be expressed as a polynomial in the 3×3 sub-determinants of P.

So, the first fundamental theorem does not state that every invariant can be expressed in terms of the determinants. It states that every *polynomial* invariant can be expressed as a *polynomial* in the determinants. To understand the power of this statement we want to emphasize that by this theorem, usually rather long and involved formulas on the level of coordinates (i.e., the entries of P) will factor into small and geometrically understandable polynomials on the level of brackets. We will not prove the first fundamental theorem here since the proof requires some nontrivial and extensive technical machinery. (A proof of this classical theorem may be found, for instance, in [131], in [33], or in [126].) However, we at least want to give an example that demonstrates the power of the statement.

Example 7.3. We want to analyze the condition that six points $1, 2, 3, 4, 5, 6$ lie on a common quadratic curve (a conic). Algebraically this can be stated in the following way. Assume that the points $1, \ldots, 6$ have homogeneous coordinates $(x_1, y_1, z_1), \ldots, (x_6, y_6, z_6)$. If all points are on a common quadratic curve, there are parameters a, b, c, d, e, f such that the quadratic equations

$$a \cdot x_i^2 + b \cdot y_i^2 + c \cdot z_i^2 + d \cdot x_i \cdot y_i + e \cdot x_i \cdot z_i + d \cdot y_i \cdot z_i = 0$$

for $i = 1, \ldots, 6$ hold (and at least one of the parameters does not vanish). This defines a system of linear equations

$$\begin{pmatrix} x_1^2 & y_1^2 & z_1^2 & x_1y_1 & x_1z_1 & y_1z_1 \\ x_2^2 & y_2^2 & z_2^2 & x_2y_2 & x_2z_2 & y_2z_2 \\ x_3^2 & y_3^2 & z_3^2 & x_3y_3 & x_3z_3 & y_3z_3 \\ x_4^2 & y_4^2 & z_4^2 & x_4y_4 & x_4z_4 & y_4z_4 \\ x_5^2 & y_5^2 & z_5^2 & x_5y_5 & x_5z_5 & y_5z_5 \\ x_6^2 & y_6^2 & z_6^2 & x_6y_6 & x_6z_6 & y_6z_6 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

This system has a nontrivial solution if and only if the determinant of this matrix does not vanish. Expanding this determinant produces a polynomial $f(x_1, x_2, , \ldots, z_6)$ in 18 variables with 720 summands each of degree 12. The polynomial must be a projective invariant, since the condition of six points being on a conic is invariant under projective transformations. The first fundamental theorem tells us that this polynomial must be expressible in terms of determinants. In fact, on the level of determinants the polynomial simplifies to the following form:

$$[1,2,3][1,5,6][4,2,6][4,5,3] - [4,5,6][4,2,3][1,5,3][1,2,6] = 0.$$

This condition can be easily checked by a computer algebra system. One generates the polynomial f by expanding the above determinant and then applies to f an operation like `simplify(f)`. If the computer algebra system is clever enough, it will find a form that resembles the above bracket expression.

If one takes a closer look at the above bracket expression one observes that after expansion back to the coordinate level each of the two summands produces many summands. Each bracket is a determinant with 6 summands, and thus each summand produces $6^4 = 1296$ summands on the level of coordinates. Altogether we have 2592 summands, and 1872 of these summands cancel pairwise.

Since there are nontrivial dependencies among the determinants (such as Grassmann-Plücker relations), the bracket expression is far from unique. There are $\binom{6}{3}$ equivalent bracket expressions with 2 summands, and many more with more than two summands. Expanding any of these equivalent expressions to the coordinate level results in the same polynomial f.

The first fundamental theorem can be proved constructively by providing an explicit algorithm that takes a polynomial

$$f(P) \in \mathbb{R}[x_{1,1}, x_{1,2}, x_{1,3}, \ldots, x_{n,1}, x_{n,2}, x_{n,3}] =: \mathbb{R}[\mathbf{X}]$$

on the coordinate level as input and produces a polynomial in the brackets of the points $1, \ldots, n$ whenever f is an invariant. Here $\mathbf{X}$ abbreviates the collection of all indeterminates on the coordinate level. One strategy for this is to introduce a generic basis of three independent points e_1, e_2, e_3. Under the assumption of invariance of f one may without loss of generality assume that these three vectors are the three unit vectors. Thus each variable on the coordinate level can be expressed as a bracket that involves two unit vectors and one point of the configuration. So we can rewrite f as a polynomial $b(\ldots)$ in these brackets. Now the difficult part of the proof begins. One can show that using Grassmann-Plücker relations, b can be rewritten in the form

$$b = [e_1, e_2, e_3]^\tau \cdot b'(\ldots).$$

Here $b'(\ldots)$ is a bracket polynomial that involves only points $1, \ldots, n$. Since $[e_1, e_2, e_3]^\tau$ is constantly 1, the polynomial $b'(\ldots)$ must be the desired bracket polynomial. The reader interested in a formal proof that follows these lines is referred to [126].

A general problem in the translation of coordinate polynomials to bracket polynomials is that one has almost no control on the length of the resulting bracket polynomial. It is still a difficult open research problem to provide efficient algorithms that generate bracket expressions of provably short length.

7.4 Projectively Invariant Functions

In geometry one is often interested in measuring certain values of geometric configurations (lengths, angles, etc.). As we have seen, lengths and angles are not invariant under projective transformations. Thus they are not a reasonable measure within the framework of projective geometry. In contrast, it is appropriate to study functions $f\colon \mathbb{RP}^2 \to \mathbb{R} \cup \{\infty\}$ that are projectively invariant in the sense of Definition 7.1. Here we will focus on rational functions that are projectively invariant.

We have already met one of these functions: the cross-ratio. If we reconsider the proofs of Lemmas 4.4 (invariance under rescaling homogeneous coordinates) and 4.5 (invariance under projective transformations), we immediately see how to obtain other projectively invariant rational functions. The crucial property is that in the numerator and in the denominator we have multihomogeneous functions with the same degree for any letter. Under these conditions, rescaling factors of homogeneous coordinates and determinants of projective transformations will cancel perfectly.

We will see later on (in Part III of this book) how to express angles and distances as invariant functions that relate projective objects with special points or lines (such as the line at infinity).

Under mild nondegeneracy assumptions it can be shown that every rational projectively invariant function can be expressed as a rational function in cross-ratios. The proof of this fact essentially reconstructs the coordinates of the configuration (up to projective equivalence) from the cross-ratios (by techniques similar to those of Section 5.4). Then the invariant functions can simply be expanded in terms of cross-ratios. A formal proof may be found in [18].

7.5 The Bracket Algebra

In this section we want to change our point of view and again consider the brackets as “first-class citizens” in preference to coordinates. We have seen in Sections 7.1 and 7.2 that brackets carry all information that is necessary to reconstruct a configuration up to projective equivalence. Furthermore, Section 7.3 showed that as a consequence of this we can compute any projective invariant from the values of the brackets. In particular, Example 7.3 indicated that expressing projective invariants on the level of brackets leads to considerably shorter expressions compared to the coordinate level. Moreover, the bracket expressions are often much easier to interpret geometrically than the coordinate expression.

Taking all this into account, it would be a wise strategy to drop the coordinate level completely and model the entire setup of projective geometry over $\mathbb{R}$ on the level of brackets.

For this we will in this chapter consider the brackets $[a, b, c]$ themselves as indeterminates that may take any value in $\mathbb{R}$. The set of all brackets on n points is abbreviated

$$\mathbf{B} := \{[i, j, k] \mid i, j, k \in E\}, \quad E = \{1, \dots, n\}.$$

The polynomial ring $\mathbb{R}[\mathbf{B}]$ contains all polynomials that we can possibly write with those brackets (remember, the brackets are now variables, not determinants). If the brackets really came from the determinants of a vector configuration they would be far from independent. There would be many relations among them: a bracket that contains a repeated letter would have to be zero, the brackets would satisfy the alternating determinant rules, and, last but not least, the brackets would have to satisfy the Grassmann-Plücker relations.

We can take these dependencies into account by factoring out the corresponding relations from the ring $\mathbb{R}[\mathbf{B}]$.

Definition 7.3. We define the following three ideals in the ring $\mathbb{R}[\mathbf{B}]$:

- $\mathbf{I}_{\text{repeat}} := \Big\langle \{[i,j,k] \in \mathbf{B} \mid i = j \quad \text{or} \quad i = k \quad \text{or} \quad j = k\} \Big\rangle$,
- $\mathbf{I}_{\text{altern}} := \Big\langle \{[\lambda_1, \lambda_2, \lambda_3] + \sigma(\pi)[\lambda_{\pi(1)}, \lambda_{\pi(2)}, \lambda_{\pi(3)}] \big| \lambda_1, \lambda_2, \lambda_3 \in E, \sigma \in S_3\} \Big\rangle$,
- $\mathbf{I}_{\text{GP}} := \Big\langle \{[a,b,c][d,e,f] - [a,b,d][c,e,f] + [a,b,e][c,d,f] - [a,b,f][c,d,e] \mid a,b,c,d,e,f \in E\} \Big\rangle$.

In this expression π is a permutation of three elements, and $\sigma(\pi)$ is its sign. The *bracket ring* **BR** is the ring $\mathbb{R}[\mathbf{B}]$ factored modulo these three ideals:

$$\mathbf{BR} := \mathbb{R}[\mathbf{B}] / \langle \mathbf{I}_{\text{repeat}} \cup \mathbf{I}_{\text{altern}} \cup \mathbf{I}_{\text{GP}} \rangle.$$

Thus the bracket ring is defined in a way that brackets with repeated letters are automatically zero (this is forced by $\mathbf{I}_{\text{repeat}}$). Furthermore, alternating determinant rules are forced by $\mathbf{I}_{\text{altern}}$, and finally, the Grassmann-Plücker relations are forced by $\mathbf{I}_{\text{GP}}$. See [132] for a more elaborate treatment of the bracket ring. Bracket polynomials that are identical in **BR** turn out to expand to the same expression when we replace the brackets by the corresponding determinants. In order to formulate this precisely, we introduce a ring homomorphism

$$\Phi\colon \mathbb{R}(\mathbf{B}) \to \mathbb{R}[\mathbf{X}]$$

that models the expansion of brackets. This homomorphism is uniquely determined by its action on the brackets

$$\Phi([i,j,k]) := \det(x_i, x_j, x_k).$$

We now can prove the following theorem:

Theorem 7.4. *Let f, g be two polynomials in $\mathbb{R}(\mathbf{B})$ such that $f \equiv g$ in the bracket ring. Then $\Phi(f) = \Phi(g)$.*

Proof. If $f \equiv g$ in the bracket ring, then there is a polynomial $h \in \langle \mathbf{I}_{\text{repeat}} \cup \mathbf{I}_{\text{altern}} \cup \mathbf{I}_{\text{GP}} \rangle$ such that $f = g + h$ in $\mathbb{R}[\mathbf{B}]$. Applying the operator Φ to both sides, we obtain

$$\Phi(f) = \Phi(g + h) = \Phi(g) + \Phi(h) = \Phi(g).$$

The last equation holds since every polynomial in the ideals $\mathbf{I}_{\text{repeat}}, \mathbf{I}_{\text{altern}}, \mathbf{I}_{\text{GP}}$ expands to zero under Φ by definition. □

The converse of the above theorem is true as well:

Theorem 7.5. *Let f, g be two polynomials in $\mathbb{R}(\mathbf{B})$ with $\Phi(f) = \Phi(g)$. Then $f - g \in \langle \mathbf{I}_{\text{repeat}} \cup \mathbf{I}_{\text{altern}} \cup \mathbf{I}_{\text{GP}} \rangle$.*

Equivalently, we can state this theorem also by saying that every bracket polynomial $f \in \mathbb{R}(\mathbf{B})$ with $\Phi(f) = 0$ is automatically in the ideal

$$\left\langle \mathbf{I}_{\text{repeat}} \cup \mathbf{I}_{\text{altern}} \cup \mathbf{I}_{\text{GP}} \right\rangle.$$

This theorem is also known as the *second fundamental theorem* of invariant theory: All bracket polynomials that are identical to zero for all point configurations are generated by our three ideals. If we, a little less formally, identify bracket symbols according to the rules

$$[i, j, k] = [j, k, i] = [k, i, j] = -[i, k, j] = -[k, j, i] = -[j, i, k],$$

we can also express this theorem by saying that every bracket expression $f(\mathbf{B})$ that vanishes on all configurations can be written as

$$f = \sum m_i \cdot \gamma_i,$$

where the γ_i are Grassmann-Plücker relations.