

Hans Havlicek

Divisible Designs, Laguerre Geometry, and Beyond

Summer School on Combinatorial Geometry and Optimisation 2004

“Giuseppe Tallini”

Brescia, Italy, July 4th–10th, 2004

Author's address:

Institut für Diskrete Mathematik und Geometrie

Technische Universität Wien

Wiedner Hauptstraße 8–10

A-1040 Wien

Austria

havlicek@geometrie.tuwien.ac.at

Final version, layout for two-sided printing using A4 paper (December 2004).

Corrected version (February 2006).

Copyright © 2004–2006 by Hans Havlicek. All rights reserved.

Preface

These notes are based upon a series of lectures given at the *Summer School on Combinatorial Geometry and Optimisation 2004 "Giuseppe Tallini"*. It took place at the *Catholic University of Brescia*, Italy, from June 4th until June 10th, 2004, within the *MIUR COFIN 2004* research project *Strutture Geometriche, Combinatoria e loro Applicazioni*, coordinated by GUGLIELMO LUNARDON, and supported by *Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni*. A preliminary version was used during the lectures. In its final form, several remarks, suggestions for further reading, and additional references have been added to the text.

It was wonderful to speak and discuss with so many participants of the summer school. Their feedback, questions, and criticism helped substantially to improve the final text.

Also, I am very grateful to ANDREA BLUNCK (Hamburg) and RALPH-HARDO SCHULZ (Berlin) for providing a lot of material, making so many suggestions, updating the list of references, and adding valuable remarks. It is impossible to thank them enough.

JOHANNES GMAINER (Vienna) deserves special mention for his careful proofreading. It allowed to eliminate a lot of errors.

Last, but not least, I would like to express my great appreciation to the local organizers: My thanks go to (in alphabetical order) MARIO MARCHI, SILVIA PIANTA, and ELENA ZIZIOLI, for their great efforts in organizing this summer school, their valuable assistance in many respects, their enthusiasm, their patience, their invitation to teach at this meeting, and their overwhelming hospitality.

HANS HAVLICEK

Vienna, December 2004

Contents

Preface	i
1 Introduction	1
2 Divisible Designs	3
2.1 Basic concepts and first examples	3
2.2 Group actions	11
2.3 A theorem of SPERA	13
2.4 Divisible designs and constant weight codes	16
2.5 Notes and further references	17
3 Laguerre Geometry	19
3.1 Real Laguerre geometry	19
3.2 The affine and the projective line over a ring	20
3.3 The distant relation	26
3.4 Chain geometries	30
3.5 Local rings, local algebras, and Laguerre algebras	34
3.6 Notes and further references	40
4 Divisible Designs via GL_2-Actions	41
4.1 How to choose a base block	41
4.2 Transversal divisible designs from Laguerre algebras	42
4.3 Divisible designs from local algebras	43
4.4 Other kinds of blocks	47
4.5 Notes and further references	49

5	An Outlook: Finite Chain Geometries	50
5.1	A parallelism based upon the Jacobson radical	50
5.2	Counting the point set	51
5.3	Divisible designs vs. finite chain geometries	52
	Bibliography	54
	Index	59

Chapter 1

Introduction

In these lecture notes we aim at bringing together design theory and projective geometry over a ring. Both disciplines are well established, but the results on the interaction between them seem to be rare and scattered over the literature. Thus our main goal is to present the basics from either side and to develop, or at least sketch, the principal connections between them.

In Chapter 2 we start from the scratch with divisible designs. Loosely speaking, a divisible design is a finite set of points which is endowed with an equivalence relation and a family of distinguished subsets, called blocks, such that no two distinct points of a block are equivalent. Furthermore, there have to be several constants, called the parameters of the divisible design, as they govern the basic combinatorial properties of such a structure. Our exposition includes a lot of simple examples. Also, we collect some facts about group actions. This leads us to a general construction principle for divisible designs, due to SPERA. This will be our main tool in the subsequent chapters.

Next, in Chapter 3 we take a big step by looking at the classical Laguerre geometry over the reals. This part of the text is intended mainly as a motivation and an invitation for further reading. Then we introduce our essential geometric concept, the projective line over a ring. Although we shall be interested in finite rings only, we do not exclude the infinite case. In fact, a restriction to finite rings would hardly simplify our exposition. From a ring containing a field, as a subring, we obtain a chain geometry. Again, we take a very short look at some classical examples, like Möbius geometries. Up to this point the connections with divisible designs may seem vague. However, if we restrict ourselves to finite local rings then all the prerequisites needed for constructing a divisible design are suddenly available, due to the presence of a unique maximal ideal in a local ring.

Chapter 4 is entirely devoted to the construction of a divisible design from the projective line over a finite local ring. The particular case of a local algebra is discussed in detail, but little seems to be known about the case of an arbitrary finite local ring, even though

such rings are ubiquitous. It is worth noting that the isomorphisms between certain divisible design can be described in terms of Jordan isomorphisms of rings and projectivities; strictly speaking this applies to divisible designs which stem from chain geometries over local algebras with sufficiently large ground fields. Geometric mappings arising from Jordan homomorphisms are rather involved, and the related proofs have the tendency to be very technical; we therefore present this material without giving a proof.

Chapter 5 can be considered as an outlook combined with an invitation for further research. We sketch how one can obtain an equivalence relation on the projective line over any ring via the Jacobson radical of the ring. Recall that such an equivalence relation is one of the ingredients for a divisible design. The maximal ideal of a local ring is its Jacobson radical, so that we can generalize some of our results from a local to an arbitrary ring. It remains open, however, if this equivalence relation could be used to construct successfully a divisible design even when the ring is not local. Finally, we collect some facts about finite chain geometries. Their combinatorial properties are—in a certain sense—almost those of divisible designs, but no systematic treatment seems to be known.

Chapter 2

Divisible Designs

2.1 Basic concepts and first examples

2.1.1 Suppose that a tournament is to take place with v participants coming from various teams, each team having the same number of members, say s . In order to avoid trivialities, we assume $v > 0$ and $s > 0$. So there are v/s teams. The tournament consists of a number of games. In any game $k \geq 2$ participants from different teams play against each other. Of course, there should be at least two teams, i.e., $2 \leq v/s$.

The problem is to organize this tournament in such a way that all participants are “treated equally”. Strictly speaking, the objective is as follows:

The number of games in which any two members from different teams play against each other has to be a constant value, say λ_2 .

In this way it is impossible that one participant would have the advantage of playing over and over again against a small number of members from other teams, whereas others would face many different counterparts during the games.

In the terminology to be introduced below, this problem amounts to constructing a 2 - (s, k, λ_2) -divisible design with v elements. The points of the divisible design are the participants, the point classes are the teams, and the blocks correspond to the games. Many of our examples will give solutions to this problem for certain values of s , k , λ_2 , and v .

2.1.2 Throughout this chapter we adopt the following assumptions: X is a finite set with an equivalence relation $\mathcal{R} \subset X \times X$. We denote by $[x]$ the \mathcal{R} -equivalence class of $x \in X$ and define

$$\mathcal{S} := \{[x] \mid x \in X\}. \quad (2.1)$$

A subset Y of X is called \mathcal{R} -*transversal* if $\#(Y \cap [x]) \leq 1$ for all $x \in X$. Observe that here the word “transversal” appears in a rather unusual context, since it is not demanded

that Y meets *all* equivalence classes in precisely one element. Cf., however, the definition of a transversal divisible design in 2.1.5.

Definition 2.1.3 A triple $\mathcal{D} = (X, \mathcal{B}, \mathcal{S})$ is called a t - (s, k, λ_t) -divisible design if there exist positive integers t, s, k, λ_t such that the following axioms hold:

- (A) \mathcal{B} is a set of \mathcal{R} -transversal subsets of X with $\#B = k$ for all $B \in \mathcal{B}$.
- (B) $\#[x] = s$ for all $x \in X$.
- (C) For each \mathcal{R} -transversal t -subset $Y \subset X$ there exist exactly λ_t elements of \mathcal{B} containing Y .
- (D) $t \leq \frac{v}{s}$, where $v := \#X$.

The elements of X are called *points*, those of \mathcal{B} *blocks*, and the elements of \mathcal{S} *point classes*.

We shall frequently use the shorthand “DD” for “divisible design”. Sometimes we shall speak of a t -DD without explicitly mentioning the remaining *parameters* s, k , and λ_t . According to our definition, a block is merely a subset of X . Hence the DDs which we are going to discuss are *simple*, i.e., we do not take into account the possibility of “repeated blocks”. Cf. [12, p. 2] for that concept.

Since \mathcal{S} is determined by \mathcal{R} and vice versa, we shall sometimes also write a divisible design in the form $(X, \mathcal{B}, \mathcal{R})$ rather than $(X, \mathcal{B}, \mathcal{S})$.

2.1.4 Let us write down some basic properties of a t - (s, k, λ_t) -DD. Since $s, t \geq 1$, axiom (D) implies that

$$\#X = v \geq st \geq 1 \quad (2.2)$$

or, said differently, that $X \neq \emptyset$. From this and (B) we infer that

$$\#\mathcal{S} = \frac{v}{s} \geq 1. \quad (2.3)$$

Hence, by (D) and (B), there exists at least one \mathcal{R} -transversal t -subset of X , say Y_0 . By virtue of (C), this Y_0 is contained in $\lambda_t \geq 1$ blocks so that

$$\#\mathcal{B} =: b \geq 1. \quad (2.4)$$

So, since $\mathcal{B} \neq \emptyset$, we can derive from axiom (A) and (2.3) the inequality

$$\#B = k \leq \frac{v}{s} \text{ for all } B \in \mathcal{B}. \quad (2.5)$$

2.1.5 A divisible design is called *transversal* if each block meets all point classes, otherwise it is called *regular*. Hence a t - (s, k, λ_t) -DD is transversal if, and only if equality holds in (2.5).

During the last decades there has been a change of terminology. Originally, the point classes of a DD were called *point groups* and DDs carried the name *group-divisible designs*. In order to avoid confusion with the algebraic term “group”, in [11] this name was changed to read *group-divisible designs*. We shall not use any of these phrases.

2.1.6 Let us add in passing that some authors use slightly different axioms for a DD in order to exclude certain cases that do not deserve interest. For example, according to our definition $s = v$ is allowed, but this forces $t = k = 1$.

On the other hand, our axiom (D) is essential in order to rule out trivial cases which would cause a lot of trouble. If we would allow $t > \frac{v}{s}$ then there would not be any \mathcal{R} -transversal t -subset of X , and (C) would hold in a trivial manner. Such a value for t would therefore have no meaning at all for a structure $\mathcal{D} = (X, \mathcal{B}, \mathcal{S})$.

Examples 2.1.7 We present some examples of DDs.

- (a) We consider the *Pappos configuration* in the real projective plane which is formed by 9 points and 9 lines according to Figure 2.1. We obtain a 2- $(3, 3, 1)$ -DD, say \mathcal{D} ,

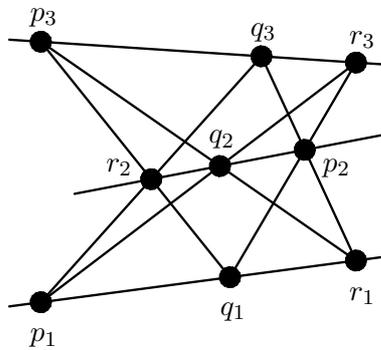


Figure 2.1: Pappos configuration

as follows: Let

$$X := \{p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3\},$$

i.e., $v = 9$. The blocks are, by definition, the 3-subsets of collinear points in X , so that $k = 3$. We define three point classes, namely $\{p_1, p_2, p_3\}$, $\{q_1, q_2, q_3\}$, and $\{r_1, r_2, r_3\}$, each with $s = 3$ elements. Then for any two points from distinct point classes there is a unique block containing them. So $t = 2$ and $\lambda_2 = 1$. This DD is transversal.

- (b) Let us take a *regular octahedron* in the Euclidean 3-space (Figure 2.2), and let us turn it into a DD as follows: Denote by X the set of all $v = 6$ vertices of the

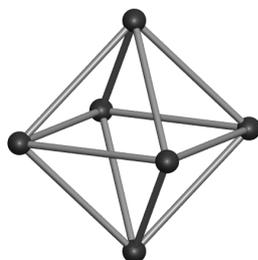


Figure 2.2: Octahedron

octahedron. For all $p, q \in X$ we put $p \mathcal{R} q$ if, and only if, p and q are opposite vertices. Hence $s = 2$. The blocks are defined as the triangular faces, whence $k = 3$. So we get a transversal 3 -($2, 3, 1$)-divisible design.

- (c) Our next example is the *projective plane* of order three which is depicted on the left hand side of Figure 2.3. It is a 2 -($1, 4, 1$)-DD with $v = 13$ points. There are 13 blocks; they are given by those subsets of the point set which consist of $k = 4$ points on a common curve. (Some of these curves are segments, others are not.) There are 13 point classes, because $s = 1$ means that all point classes are singletons.

We shall not need the definition of a finite projective plane and refer to [12, p. 6]. Let us add, however, that in the theory of projective planes one speaks of *lines* rather than blocks. The *order* of a projective plane is defined to be $k - 1$ if there are k points on one (or, equivalently, on every) line.

Let us remove one point from the point set of this projective plane. Also, let us redefine the point classes as the four truncated lines (illustrated by thick segments and a thick circular arc), the other nine lines remain as blocks. This yields a 2 -($3, 4, 1$)-DD.

If we delete one line and all its points from the projective plane of order three then we obtain the *affine plane* of order three. Each of the twelve remaining lines gives rise to a block with three points, the point classes are defined as singletons. As before, one speaks of (affine) lines rather than blocks in the context of affine planes. Observe that the *order* of an affine plane is just the number of points on one (or, equivalently, on every) line. See [12, p. 8] for further details.

This affine plane is a 2 -($1, 3, 1$)-DD with $v = 9$ points and, as before, all point classes are singletons. See the third picture in Figure 2.3. Two lines of an affine plane are called *parallel* if they are identical or if they have no point in common.

Finally, we change the set of lines and the set of point classes of this affine plane as follows: We exclude three mutually parallel lines from the line set, turn them into point classes, and disregard the one-element point classes of the underlying affine plane. The remaining nine lines are considered as blocks. In this way a 2-(3, 3, 1)-DD with $v = 9$ points is obtained. On the right hand side of Figure 2.3 the bold vertical segments represent the point classes.

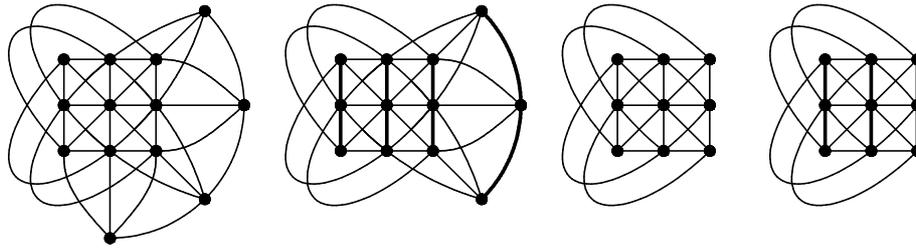


Figure 2.3: DDs from the projective plane of order 3

- (d) We proceed as in the previous example, but starting with the projective plane of order two which is a 2-(1, 3, 1)-DD with $v = 7$ points. In this way we obtain a 2-(2, 3, 1)-DD with $v = 6$ points, a 2-(1, 2, 1)-DD with $v = 4$ points (the affine plane of order 2), and a 2-(2, 2, 1)-DD with $v = 4$ points. See Figure 2.4.

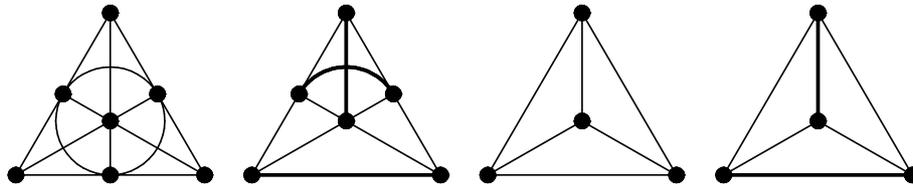


Figure 2.4: DDs from the projective plane of order 2

It is easy to check that the 3-DD from Example (b) is also a 2-DD; likewise all our 2-DDs are at the same time 1-DDs. Thus the previous examples illustrate the following result:

Theorem 2.1.8 *Let \mathcal{D} be a t -(s, k, λ_t)-DD with $t \geq 2$ and let i be an integer such that $1 \leq i \leq t$. Then \mathcal{D} is also an i -(s, k, λ_i)-DD with*

$$\lambda_i = \lambda_t \frac{\binom{vs^{-1} - i}{t - i} s^{t-i}}{\binom{k - i}{t - i}}. \quad (2.6)$$

Proof. We fix one transversal i -subset I . The proof will be accomplished by counting in two ways the number of pairs (Y, B) , where Y is a $(t - i)$ -subset of X such that $I \cup Y$ is a transversal t -subset, and where B is a block containing $I \cup Y$.

On the one hand, let us single out one of the λ_i blocks containing I . Then there are

$$\binom{k - i}{t - i}$$

possibilities to choose a Y within that particular block.

On the other hand, to select an arbitrary Y amounts to the following: First choose $t - i$ point classes out of the $vs^{-1} - i$ point classes that are disjoint from I (cf. (2.3)), and then choose in each of these point classes a single point (out of s). Hence there are precisely

$$\binom{vs^{-1} - i}{t - i} s^{t-i}$$

ways to find such a Y . For every Y there are λ_t pairs (Y, B) with the required property.

Altogether we obtain

$$\lambda_i \binom{k - i}{t - i} = \lambda_t \binom{vs^{-1} - i}{t - i} s^{t-i} \quad (2.7)$$

which completes the proof. \square

2.1.9 Theorem 2.1.8 enables us to calculate several other *parameters* of a t -(s, k, λ_t)-DD. Letting $i = 0$ in formula (2.6) provides the number of blocks, i.e.

$$b := \#\mathcal{B} = \lambda_t \frac{\binom{vs^{-1}}{t} s^t}{\binom{k}{t}}. \quad (2.8)$$

Likewise, for $i = 1$ we obtain the number

$$r := \lambda_1 \quad (2.9)$$

of blocks through a point which is therefore a constant. Provided that $i = t - 1$ formula (2.6) reads

$$\lambda_{t-1} = \lambda_t \frac{v - st + s}{k - t + 1}. \quad (2.10)$$

By Theorem 2.1.8, formula (2.10) remains valid if t is replaced with an integer t' , subject to the condition $1 \leq t' \leq t$. Hence we infer the equation

$$bk = rv \quad (2.11)$$

by letting $t' = 1$. For $t \geq 2$ we may let $t' = 2$ which gives

$$r(k - 1) = \lambda_2(v - s). \quad (2.12)$$

The last two equations are just particular cases of formula (2.7).

2.1.10 A divisible design with $s = 1$ is called a *design*; we refer to [67], or the two volumes [12] and [13]. In design theory the parameter s is not taken into account, and a t -(1, k , λ_t)-DD with v points is often called a t -(v , k , λ_t)-design. Of course, this is a *different notation* and we urge the reader not to draw the erroneous conclusion “ $v = s$ ” when comparing these lecture notes with a book on design theory.

We have already met examples of designs in Examples 2.1.7 (c) and (d), namely the projective and affine planes of orders three and two. However, designs are not the topic of this course. Instead, we shall focus our attention on the case when $s > 1$.

2.1.11 If $\mathcal{D} = (X, \mathcal{B}, \mathcal{S})$ is a t -(s , k , λ_t)-DD and $\mathcal{D}' = (X', \mathcal{B}', \mathcal{S}')$ is a t' -(s' , k' , $\lambda_{t'}$)-DD then an *isomorphism* is a bijection

$$\varphi : X \rightarrow X' : p \mapsto p^\varphi$$

such that

$$B \in \mathcal{B} \Leftrightarrow B^\varphi \in \mathcal{B}' \quad (2.13)$$

$$S \in \mathcal{S} \Leftrightarrow S^\varphi \in \mathcal{S}'. \quad (2.14)$$

Clearly, the inverse mapping of an isomorphism is again an isomorphism. If the product of two isomorphisms is defined (as a mapping) then it is an isomorphism. The set of all isomorphisms of a DD onto itself, i.e. the set of all *automorphisms*, is a group under composition of mappings.

2.1.12 Suppose that there exists an isomorphism of a t -(s , k , λ_t)-DD \mathcal{D} onto a t' -(s' , k' , $\lambda_{t'}$)-DD \mathcal{D}' . Such DDs are said to be *isomorphic*. Then

$$v = v', \quad s = s', \quad \text{and} \quad k = k'.$$

However, in view of Theorem 2.1.8 we may have $t \neq t'$. Thus we impose the extra condition that the parameters t and t' are maximal, i.e., \mathcal{D} is a t -DD but not a $(t + 1)$ -DD, and likewise for \mathcal{D}' . Then, clearly,

$$t = t' \quad \text{and} \quad \lambda_t = \lambda_{t'}.$$

2.1.13 Condition (2.14) in the definition of an isomorphism can be replaced with the seemingly weaker but nevertheless equivalent condition

$$S \in \mathcal{S} \Rightarrow S^\varphi \in \mathcal{S}' \quad (2.15)$$

Suppose that we are given a bijection $\varphi : X \rightarrow X'$ satisfying (2.15). If $S^\varphi \in \mathcal{S}'$ for some subset S of X then there is an $x \in S$. Hence $x^\varphi \in S^\varphi \cap [x]^\varphi$ with $[x]^\varphi \in \mathcal{S}'$ by (2.15). Since two equivalence classes with a common element are identical, we get $S^\varphi = [x]^\varphi$ and, finally, $S = [x] \in \mathcal{S}$. In sharp contrast to this result, the equivalence sign in (2.13) is essential. Cf. Example 2.1.14 below.

We may even drop condition (2.14) in the following particular situation: Let $\varphi : X \rightarrow X'$ be a bijection of a 2-DD \mathcal{D} onto a 2-DD \mathcal{D}' such that (2.13) holds. Then, for all $x, y \in X$ with $x \neq y$ we have $x \mathcal{R} y$ if, and only if, there exists a block containing x and y . The same kind of characterization applies to \mathcal{D}' . Hence $x \mathcal{R} y$ is equivalent to $x^\varphi \mathcal{R}' y^\varphi$ for all $x, y \in X$.

Example 2.1.14 Let us consider once more a *regular octahedron* in the Euclidean 3-space. We turn the set of its vertices into a 2-DD with 6 points in two different ways (Figure 2.5): For both DDs the point classes are the 2-sets of opposite vertices. However, the blocks are different. Firstly, we take *all* 8 triangular faces as blocks (left image). This gives a 2-(2, 3, 2)-DD which is also a 3-DD. Cf. Example 2.1.7 (b). Secondly, only 4 triangular faces (given by the shaded triangles in the right image) are considered as blocks, so that a 2-(2, 3, 1)-DD is obtained.

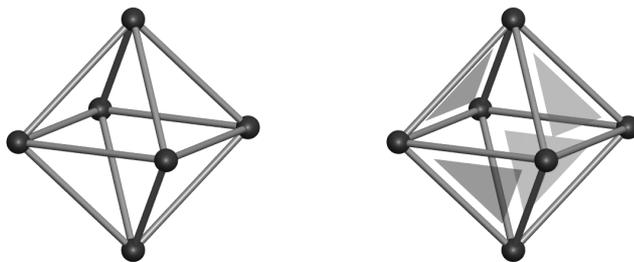


Figure 2.5: Two non-isomorphic 2-DDs from an octahedron

Observe that the identity mapping id_X maps every block of the second design onto a block of the first design, but not vice versa. Hence a bijection between the point sets of DDs which preserves point classes in both directions and blocks in one direction only, need not be an isomorphism.

Exercise 2.1.15 Which of the DDs from Examples 2.1.7 and 2.1.14 are isomorphic?

2.2 Group actions

2.2.1 Let us recall that all bijections (or *permutations*) of a finite set¹ X form the *symmetric group* S_X . If G is any group then a homomorphism

$$\alpha : G \rightarrow S_X : g \mapsto g^\alpha$$

is called a *permutation representation* of G . In this case the group G is also said to *operate* or *act* on X via α . In fact, each $g \in G$ yields the bijection

$$g^\alpha : X \rightarrow X : x \mapsto x^{(g^\alpha)}.$$

Whenever α is clear from the context, then we shall write x^g for the image of x under the permutation g^α . Thus, if the composition in G is written multiplicatively, we obtain

$$x^{(gh)} = (x^g)^h \text{ for all } x \in X \text{ and all } g, h \in G.$$

Provided that α is injective the representation is called *faithful*. So for a faithful representation we have $\ker \alpha = \{1_G\}$ as is kernel, and we can identify G with its image G^α . However, in most of our examples the representation will not be faithful, i.e., there will be distinct elements of G which yield the same permutation on X .

2.2.2 For the remaining part of this section we suppose that G acts on X (via α).

For each $x \in X$ we write $x^G := \{x^g \mid g \in G\}$ for the *orbit* of x under G . The set of all such orbits is a partition of X . If X itself is an orbit then G is said to operate *transitively* on X . This means that for any two elements $x, y \in X$ there is at least one $g \in G$ with $x^g = y$. If, moreover, this g is always uniquely determined then the action of G is called *regular* or *sharply transitive*. If G operates regularly on X then the representation is necessarily faithful, since every $g \in \ker \alpha$ has the property $x^g = x$ for all $x \in X$, whence $g = 1_G$.

The given group G acts also in a natural way on certain other sets which are associated with X . E.g., for every non-negative integer t , the group G acts on the t -fold product X^t by

$$(x_1, x_2, \dots, x_t)^g := (x_1^g, x_2^g, \dots, x_t^g).$$

If this is a transitive action on the subset of t -tuples with *distinct entries* from X then one says that G acts *t -transitively* on X .

Moreover, for $t \leq \#X$, the group G acts on the (non empty) set $\binom{X}{t}$ of all t -subsets of X by

$$\{x_1, x_2, \dots, x_t\}^g := \{x_1^g, x_2^g, \dots, x_t^g\}.$$

¹Most of the results from this section remain true for an infinite set X .

In case that this is a transitive action, the group G is said to act t -homogeneously on X . Similarly, G acts on the power set of X .

Later, we shall be concerned with t -homogeneous and t -transitive group actions. Thus the following result, due to DONALD LIVINGSTONE and ASCHER WAGNER [76], deserves our interest, even though we are not going to use it.

Theorem 2.2.3 *Suppose that the action of a group G on a finite set X is t -homogeneous, where $4 \leq 2t \leq \#X$. Then G acts $(t - 1)$ -transitively on X . If, moreover, $t > 4$ then G even acts t -transitively on X .*

See also [109] for a short proof, [43, p. 92], and [77, § 16].

2.2.4 An equivalence relation \mathcal{R} on X is called G -invariant if

$$x \mathcal{R} y \Rightarrow x^g \mathcal{R} y^g \text{ for all } x, y \in X \text{ and all } g \in G. \quad (2.16)$$

Then

$$x \mathcal{R} y \Leftrightarrow x^g \mathcal{R} y^g \text{ for all } x, y \in X \text{ and all } g \in G \quad (2.17)$$

follows immediately, by applying (2.16) to $x^g \mathcal{R} y^g$ and g^{-1} . The finest and the coarsest equivalence relation on X , i.e. the diagonal $\text{diag}(X \times X) = \{(x, x) \mid x \in X\}$ and $X \times X$, obviously are G -invariant equivalence relations on X .

Suppose now that G acts transitively on X . If $\text{diag}(X \times X)$ and $X \times X$ are the only G -invariant equivalence relations on X then the action of G is said to be *primitive*; otherwise the action of G is called *imprimitive*.

Suppose that G acts imprimitively on X . A subset $S \subset X$ is called a *block of imprimitivity* if it is an equivalence class of a G -invariant equivalence relation, say \mathcal{R} , which is neither $\text{diag}(X \times X)$ nor $X \times X$. Thus a block of imprimitivity is a subset S of X such that $\#S > 1$, $S \neq X$, and for all $g \in G$ we have either $S^g = S$ or $S^g \cap S = \emptyset$.

2.2.5 Given a subset $Y \subset X$ the *setwise stabilizer* of Y in G is the set G_Y , say, of all $g \in G$ satisfying $Y^g = Y$. This stabilizer is a subgroup of G . The *pointwise stabilizer* of $Y \subset X$ in G is the set of all $g \in G$ such that $y^g = y$ for all $y \in Y$. This pointwise stabilizer is also a subgroup of G and, clearly, it is a normal subgroup of the setwise stabilizer G_Y .

If $y \in X$ then we simply write G_y instead of $G_{\{y\}}$. With this convention, the mapping $y^g \mapsto G_y g$ is a bijection of the orbit y^G onto the set of right cosets of G_y in G , whence we obtain the fundamental formula

$$\#y^G = \frac{\#G}{\#G_y}. \quad (2.18)$$

It links cardinality of the orbit y^G with the index of the stabilizer G_y in G , i.e. the number of right (or left) cosets of G_y in G .

We refer to [69, pp. 71–79] for a more systematic account on group actions.

2.3 A theorem of SPERA

2.3.1 One possibility to construct divisible designs is given by the following Theorem which is due to ANTONINO GIORGIO SPERA [101, Proposition 3.2]. A similar construction for designs can be found in [12, Proposition 4.6].

The ingredients for this construction are a finite set X with an equivalence relation \mathcal{R} on its elements, a finite group G acting on X , and a so-called *base block* (or *starter block*) B_0 , say. Its orbit under the action of G will then be our set of blocks. More precisely, we can show the following:

Theorem 2.3.2 *Let X be a finite set which is endowed with an equivalence relation \mathcal{R} ; the corresponding partition is denoted by \mathcal{S} . Suppose, moreover, that G is a group acting on X , and assume that the following properties hold:*

- (a) *The equivalence relation \mathcal{R} is G -invariant.*
- (b) *All equivalence classes of \mathcal{R} have the same cardinality, say s .*
- (c) *The group G acts transitively on the set of \mathcal{R} -transversal t -subsets of X for some positive integer $t \leq \#\mathcal{S}$.*

Finally, let B_0 be an \mathcal{R} -transversal k -subset of X with $t \leq k$. Then

$$(X, \mathcal{B}, \mathcal{S}) \text{ with } \mathcal{B} := B_0^G = \{B_0^g \mid g \in G\}$$

is a t - (s, k, λ_t) -divisible design, where

$$\lambda_t := \frac{\#G}{\#G_{B_0}} \frac{\binom{k}{t}}{\binom{vs^{-1}}{t} s^t}, \quad (2.19)$$

and where $G_{B_0} \subset G$ denotes the setwise stabilizer of B_0 .

Proof. Firstly, let $\#X =: v$. Since B_0 is \mathcal{R} -transversal, we have $0 < t \leq k = \#B_0 \leq \#\mathcal{S} = \frac{v}{s}$ so that axiom (D) in the definition of a DD is satisfied. Also, we obtain $s, k > 0$.

As B_0 is an \mathcal{R} -transversal k -set, so is every element of B_0^G by (2.17). This verifies axiom (A), whereas axiom (B) is trivially true due to assumption (b).

Next, to show axiom (C), we consider the base block B_0 and a t -subset $Y \subset B_0$ which exists due to our assumption $t \leq k$. Let $\lambda_t > 0$ be the number of blocks containing Y . Given an arbitrary \mathcal{R} -transversal t -subset $Y' \subset X$ there is a $g \in G$ with $Y' = Y^g$, since

$Y \subset B_0$ is \mathcal{R} -transversal. This g takes the λ_t distinct blocks through Y to λ_t distinct blocks through Y' . Similarly, the action of g^{-1} shows that there cannot be more than λ_t blocks containing Y' .

Altogether, we have verified the axioms of a divisible design. Yet, it remains to calculate the parameter λ_t . By definition, the group G acts transitively on the set \mathcal{B} of blocks. By equation (2.18), the number of blocks is

$$b = \frac{\#G}{\#G_{B_0}},$$

whence, by (2.8), we get

$$\lambda_t = b \frac{\binom{k}{t}}{\binom{vs^{-1}}{t} s^t} = \frac{\#G}{\#G_{B_0}} \frac{\binom{k}{t}}{\binom{vs^{-1}}{t} s^t}$$

which proves (2.19). □

Note that in [101] our condition (b) is missing. On the other hand it is very easy to show that (b) cannot be dropped without effecting the assertion of the theorem:

Example 2.3.3 Let $X = \{1, 2, 3\}$, $\mathcal{S} = \{\{1\}, \{2, 3\}\}$, and let G be that subgroup of the symmetric group S_3 which is formed by the identity id_X and the transposition that interchanges 2 with 3. Then, apart from (b), all other assumptions of Theorem 2.3.2 are satisfied if we define $t := 2$ and $B_0 := \{1, 2\}$. However, no 2-DD is obtained, since there are two blocks containing 1, but there exists only one block through the point 2.

2.3.4 In the subsequent chapters we shall mainly apply a slightly modified version of Theorem 2.3.2 which is based on the following concept. A t -tuple $(x_1, x_2, \dots, x_t) \in X^t$ is called \mathcal{R} -transversal if its entries belong to t distinct point classes.

Corollary 2.3.5 *Theorem 2.3.2 remains true, mutatis mutandis, if assumption (b) is dropped and assumption (c) is replaced with*

(c₁) *The group G acts transitively on the set of \mathcal{R} -transversal t -tuples of X for some positive integer $t \leq \#\mathcal{S}$.*

Proof. We observe that each \mathcal{R} -transversal t -subset Y gives rise to $t!$ mutually distinct \mathcal{R} -transversal t -tuples with entries from Y . As $0 < t \leq \#\mathcal{S}$, it is obvious from (c₁) that G acts transitively on the set of \mathcal{R} -transversal t -subsets of X , i.e., condition (c) from Theorem 2.3.2 is satisfied.

In order to show that all equivalence classes of \mathcal{R} are of the same size, we prove that G acts transitively on \mathcal{S} . Since assumption (a) remained unchanged, formula (2.17) can be shown as before. This implies that, for all $S \in \mathcal{S}$ and all $g \in G$, the image S^g is an equivalence class; hence G acts on \mathcal{S} . For this action to be transitive it suffices to establish that G operates transitively on X . So let x_1 and x'_1 be arbitrary elements of X . We infer from $0 < t \leq \#\mathcal{S}$ that there exist \mathcal{R} -transversal t -tuples (x_1, x_2, \dots, x_t) and $(x'_1, x'_2, \dots, x'_t)$. By (c₁), there is at least one $g \in G$ which takes the first to the second t -tuple. Therefore $x_1^g = x'_1$. \square

2.3.6 Suppose that a divisible design \mathcal{D} is defined according to Theorem 2.3.2 or Corollary 2.3.5. Then the action of G on \mathcal{S} is t -homogeneous or t -transitive, respectively. In both cases the group G acts on X as an automorphism group of \mathcal{D} which, by the definition of \mathcal{B} , operates transitively on the set of blocks.

2.3.7 Clearly, Theorem 2.3.2 remains valid if we replace assumption (b) with the following:

(b₁) G acts transitively on \mathcal{S} .

Another possibility to alter the conditions in Theorem 2.3.2 is as follows [94, Remark 2.1]: Suppose that condition (b) is dropped and that (c) is replaced with

(c₂) *The group G acts transitively on the set of \mathcal{R} -transversal t -subsets of X for some positive integer $t < \#\mathcal{S}$.*

In this case, let y_1, y_2, \dots, y_w , where $w = \#\mathcal{S}$, be a system of representatives for the equivalence classes of \mathcal{R} such that $\#[y_1] \leq \#[y_2] \leq \dots \leq \#[y_w]$. We claim that (c₂) implies

$$\#[y_1] = \#[y_2] = \dots = \#[y_w]$$

which in turn is equivalent to (b). By (c₂), we have $0 < t < w$ so that

$$Y := \{y_1, y_2, \dots, y_t\} \text{ and } Y' := \{y_2, y_3, \dots, y_t, y_w\}$$

are \mathcal{R} -transversal t -subsets of X . By the action of G on \mathcal{S} , the t -tuple

$$(\#[y_2], \#[y_3], \dots, \#[y_t], \#[y_w])$$

arises from

$$(\#[y_1], \#[y_2], \dots, \#[y_t])$$

by re-arranging its entries. Therefore we obtain $\#[y_1] = \#[y_w]$, as required.

Finally, we may even just drop assumption (b) if the integer t admits the application of Theorem 2.2.3 which in turn will ensure that G acts transitively on \mathcal{S} .

2.4 Divisible designs and constant weight codes

2.4.1 There is a close relationship between DDs and certain codes which will be sketched in this section.

First, we collect some basic notions from coding theory. See, among others, the book [63] for an introduction to this subject. Let us write²

$$\mathbb{Z}_m := \{0, 1, \dots, m\} \subset \mathbb{Z}, \text{ where } m \geq 1.$$

Also let n be a positive integer. The *Hamming distance* of $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{Z}_m^n$ is defined as the number of indices $i \in \{1, 2, \dots, n\}$ such that $x_i \neq y_i$. It turns \mathbb{Z}_m^n into a metric space. The *Hamming weight* of an element $\mathbf{x} \in \mathbb{Z}_m^n$ is its Hamming distance from $(0, 0, \dots, 0)$ or, said differently, the number of its non-zero entries. This terminology is in honour of RICHARD WESLEY HAMMING (1915–1998), whose fundamental paper on error-detecting and error-correcting codes appeared in 1950.

For our purposes it will be adequate to define an *automorphism* of \mathbb{Z}_m^n as a product of any two mappings of the following form: First we apply a bijection

$$\mathbb{Z}_m^n \rightarrow \mathbb{Z}_m^n : (x_1, x_2, \dots, x_n) \mapsto (x_1^{\alpha_1}, x_2^{\alpha_2}, \dots, x_n^{\alpha_n}),$$

where each α_i is a permutation of \mathbb{Z}_m , and then a bijection

$$\mathbb{Z}_m^n \rightarrow \mathbb{Z}_m^n : (x_1, x_2, \dots, x_n) \mapsto (x_{1^\alpha}, x_{2^\alpha}, \dots, x_{n^\alpha}),$$

where α is a permutation of $\{1, 2, \dots, n\}$. All such automorphisms form a group under composition of mappings. Every automorphism preserves the Hamming distance. The Hamming weight is preserved if, and only if, $(0, 0, \dots, 0)$ remains fixed.

An m -ary code of length n is just a given subset $\mathcal{C} \subset \mathbb{Z}_m^n$. Its elements are called *codewords*. The set \mathbb{Z}_m is called the underlying *alphabet* of the code \mathcal{C} . A code is called a *constant weight code* if all codewords have the same (constant) Hamming weight.

Let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{Z}_m^n$ be codes. An *isomorphism* is an automorphism of \mathbb{Z}_m^n taking \mathcal{C}_1 to \mathcal{C}_2 . An *automorphism* of a code is defined similarly.

2.4.2 We now present the essential construction: Suppose that $\mathcal{D} = (X, \mathcal{B}, \mathcal{S})$ is a t - (s, k, λ_t) -DD with $n := \frac{v}{s}$ point classes. Also let $m := s + 1$. We augment n ideal points to X , thus obtaining a set \tilde{X} with

$$\#\tilde{X} = v + n = mn.$$

To each point class we add precisely one ideal point in such a way that distinct point classes are extended by distinct ideal points. Given a point class $S \in \mathcal{S}$ we write \tilde{S} for the

²In Chapter 3 we shall use this symbol to denote the ring of integers modulo m .

corresponding *extended point class*. Any block $B \in \mathcal{B}$ has $k \leq s$ points. We turn it into an *extended block*, say \tilde{B} , by adding to B the $n - k$ ideal points of those extended point classes \tilde{S} which have empty intersection with B . Hence \tilde{B} meets every extended point class at precisely one point.

By the above, there exists a bijection

$$\psi : \tilde{X} \rightarrow \{1, 2, \dots, n\} \times \mathbb{Z}_m$$

such that for each point class $S \in \mathcal{S}$ there is an index $i \in \{1, 2, \dots, n\}$ with

$$S^\psi = \{i\} \times (\mathbb{Z}_m \setminus \{0\}) \text{ and } \tilde{S}^\psi = \{i\} \times \mathbb{Z}_m.$$

This means that under ψ the set $\tilde{X} \setminus X$ of ideal points goes over to $\{(i, 0) \mid i \in \{1, 2, \dots, n\}\}$. Furthermore, two points of \tilde{X} are in the same extended point class if, and only if, the first entries of their ψ -images coincide.

We are now in a position to define the *code of \mathcal{D}* (with respect to ψ) as the subset

$$\mathcal{C}(\mathcal{D}) = \{(j_1, j_2, \dots, j_n) \mid \exists B \in \mathcal{B} : \tilde{B}^\psi = \{(1, j_1), (2, j_2), \dots, (n, j_n)\}\} \subset \mathbb{Z}_m^n.$$

According to our construction, all codewords have weight k , whence $\mathcal{C}(\mathcal{D})$ is in fact a constant weight code.

In general, ψ can be chosen in different ways. However, this will yield isomorphic codes. So the actual choice of ψ turns out to be immaterial. In [96] the codes arising in this way are characterized. Also, it is shown that the entire construction can be reversed, i.e., one can go back from certain codes to divisible designs.

2.4.3 A neat connection exists between the automorphism group of a DD and the automorphism group of its constant weight code. Up to the exceptional case when $t = 2$ and $v = 2k$, the two groups are isomorphic [96, Theorem 3.1]. Also, if the automorphism group of \mathcal{D} is “large” then its corresponding code is well understood. See [44], [92], and [96] for a detailed discussion.

2.5 Notes and further references

2.5.1 There is a widespread literature on divisible designs, and some particular classes of DDs have been thoroughly investigated and characterized.

Among them are *translation divisible designs*, i.e. 2-DDs with a group T of automorphisms which acts sharply transitive on X (see 2.2.2) such that the following holds: For all blocks $B \in \mathcal{B}$ and all $g \in T$ there is either $B^g = B$ or $B^g \cap B = \emptyset$. The name of these

structures is due to the fact the same properties hold, *mutatis mutandis*, for the action of the group of translations on the set of points and lines of the Euclidean plane. We refer to [14], [62], [70], [86], [87], [88], [89], [90], [91], [98], [99], and the references given there. The more general class of “ $(s, k, \lambda_1, \lambda_2)$ -translation DDs” is considered in [93] and [100]. Another construction of these more general DDs uses a *Singer group* with a *relative difference set* [71]. As a general theme, each of the preceding constructions is based upon a group which acts as a group of automorphisms of the DD.

2.5.2 While Theorem 2.3.2 and Corollary 2.3.5 pave the way to constructing DDs, the actual choice of X , \mathcal{R} , G , and a base block B_0 is a subtler question. We collect here some results:

In [101] the following case is considered: X is the projective line over a finite local K -algebra R , and G is the general linear group $\text{GL}_2(R)$ in two variables over R . All this is part of our exposition in Chapters 3 and 4. In this way one obtains 3-divisible designs.

A higher-dimensional analogue, based upon the projective space over a finite local algebra can be found in [102]; here, in general, only 2-DDs are obtained.

Another approach uses as the set X the set of (affine) lines of a finite translation plane, \mathcal{R} is chosen to be the usual parallelism of lines, and G is a group of affine collineations which acts 2-transitively on the line at infinity and contains all translations. Apart from the finite Desarguesian planes this leads to Lüneburg planes and Suzuki groups; see [95] and [104]. A more general setting, where G acts 2-transitively on a subset of the line at infinity can be found in the papers [37], [40], and [94].

A class of DDs, where G is an orthogonal group or a unitary group, is determined in [39]. It was pointed out in [46] that one particular case of this construction is—up to isomorphism—a Laguerre geometry (see 3.5.13) which, by a completely different approach, appears already in [101].

In [38] the group G is chosen to be the classical group $\text{GL}_3(q)$ (the general linear group in 3 variables over the field with q elements) in order to obtain divisible designs.

Finally, we refer to [103] for a discussion of transitive extensions of imprimitive groups.

Chapter 3

Laguerre Geometry

3.1 Real Laguerre geometry

3.1.1 The classical *Laguerre geometry* is the geometry of spears and cycles in the Euclidean plane. A *spear* is an oriented line and a *cycle* is either an oriented circle or a point (a “circle with radius zero”). There is a *tangency relation* between spears and cycles; see the first two images in Figure 3.1. Furthermore, there exists a *parallelism* (written as \parallel) on the set of spears which is depicted in the third image. We shall not give formal definitions of these relations.

For our purposes it is more appropriate to identify a cycle with the set of all its tangent spears. Then it is intuitively obvious that any cycle contains precisely one spear from every parallel class, i.e., it is a “ \parallel -transversal set”. Also, given any three non-parallel spears there is a unique cycle containing them. All this reminds us of a divisible design, even though the set of spears is infinite.

This geometry is named after the French mathematician EDMOND NICOLAS LAGUERRE (1834–1886) who used it to solve a famous problem due to APOLLONIUS OF PERGA (262?–190? BC): Find all circles that touch three given circles (without orientation). See, for example, [82] and [83].

3.1.2 It was in the year of 1910 that WILHELM BLASCHKE (1885–1962) showed that the set of spears is in one-one correspondence with the points of a circular cylinder of the Euclidean 3-space [15], now called the *Blaschke cylinder*¹. Under this mapping the cycles correspond to the ellipses on the cylinder and two spears are parallel if, and only if, their images are on a common generator of the cylinder. Blaschke also showed that the real

¹From the point of view of projective geometry this is a quadratic cone without its vertex, whence it is also called the *Blaschke cone*.

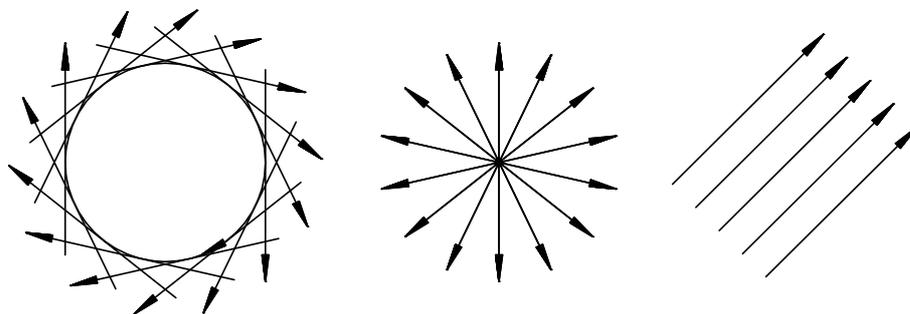


Figure 3.1: Two cycles with tangent spears, and a family of parallel spears

Laguerre geometry can be represented in terms of *dual numbers* $x + y\varepsilon$, where $x, y \in \mathbb{R}$, $\varepsilon \notin \mathbb{R}$, and $\varepsilon^2 = 0$; see Example 3.5.4 (b) for a concise definition.

3.1.3 There is a wealth of literature on the classical Laguerre geometry. We refer to [5, Chapter 1, § 2], [6, Chapter 4], [45, Chapter 15 A], [85], [110], [111], and the survey article [55]. Note that in [110] the term *inversive Galileian plane*—named after GALILEO GALILEI (1564–1642)—is used instead.

3.1.4 Our construction of divisible designs in Chapter 4 can be seen as a generalization of the classical Laguerre geometry, where a finite local ring takes over the role of the ring of dual numbers over the reals.

3.2 The affine and the projective line over a ring

All our rings are associative with a unit element (usually denoted by 1), which is inherited by subrings and acts unitaly on modules. The trivial case $1 = 0$ is excluded.

3.2.1 Let R be a ring. Given an element $s \in R$ there are various possibilities:

If there is an $l \in R$ with $ls = 1$ then s is called *left invertible*. Such an element l is said to be a *left inverse* of s . *Right invertible* elements and *right inverses* are defined analogously.

If s has both a left inverse l and a right inverse r then

$$l = l1 = l(sr) = (ls)r = 1r = r. \quad (3.1)$$

In this case, the element s is said to be *invertible*. Moreover, by the above, all left (right) inverses of s are equal to r (l) so that it is unambiguous to call $l = r =: s^{-1}$ the *inverse*

of s . The (multiplicative) group of invertible elements (*units*) of a ring R will be denoted by R^* . Clearly, 0 is neither left nor right invertible.

If $s \neq 0$ then s is called a *left zero divisor* if there exists a non-zero element $r \in R$ such that $sr = 0$. Such an s has no left inverse, since $ls = 1$ would imply $r = (ls)r = l(sr) = 0$. However, an element without a left inverse is in general not a left zero divisor. *Right zero divisors* are defined similarly.

Of course the distinction between “left” and “right” is superfluous if R is a commutative ring.

3.2.2 Suppose that we are given elements $a, b \in R$ with $ab = 1$. Hence $y = y1 = (ya)b$ for all $y \in R$. This implies that the *right translation* $\rho_b : R \rightarrow R : x \mapsto xb$ is surjective. Moreover, $(ba - 1)b = b1 - b = 0$. Thus, whenever we are able to show that ρ_b is injective we obtain $ba - 1 = 0$, i.e., $ba = 1$. This conclusion can be applied, for example, if R is a finite ring or a subring of the endomorphism ring of a finite-dimensional vector space.

Rings with the property that, for all $a, b \in R$, $ab = 1$ implies $ba = 1$ are called *Dedekind-finite* (see e.g. [73]). In fact, in most of our examples this condition will be satisfied. It carries the name of RICHARD DEDEKIND (1831–1916).

Exercise 3.2.3 Show that the endomorphism ring of an infinite dimensional vector space is not Dedekind-finite.

3.2.4 Let R be a ring. Then it is fairly obvious how to define the *affine line* over R . It is simply the set R , but—as in real or complex analysis—we adopt a geometric point of view by using the term *point* for the elements of R . We shall meet again this affine line as a subset of the projective line over R . However, to define something like a “projective line” over a ring R is a subtle task. As a matter of fact, various definitions have been used in the literature during the last decades. Some of those definitions are equivalent, some are equivalent only for certain classes of rings. A short survey on this topic is included in [75].

3.2.5 Of course, a definition of a projective line over a ring has to include, as a particular case, the projective line over a *field* F . Observe that we use the term “field” for what other authors call a *skew field* or a *division ring*. Thus multiplication in a field need not be commutative.

A particular case is well known from complex analysis: The *complex projective line* can be introduced as $\mathbb{C} \cup \{\infty\}$, where ∞ is an arbitrary new element. Intuitively, we think of ∞ as being $\frac{a}{0}$, where $a \in \mathbb{C}$ is non-zero. For all $a \in \mathbb{C}$, we have $\frac{a}{1} = \frac{xa}{x}$, $x \neq 0$. Thus every fraction $\frac{a}{b}$ other than “ $\frac{0}{0}$ ” determines an element of $\mathbb{C} \cup \{\infty\}$.

It is immediate to carry this over to an arbitrary field F . However, one has to be careful when using fractions in case that F is non-commutative, since $\frac{a}{b}$ could mean ab^{-1} or $b^{-1}a$.

We avoid ambiguity by representing the elements of the *projective line over an arbitrary field* F via

$$\begin{aligned} a &\leftrightarrow F(a, 1) = \{x(a, 1) \mid x \in F\} \text{ for all } a \in F, \\ \infty &\leftrightarrow F(1, 0). \end{aligned} \quad (3.2)$$

More formally, the projective line over F appears as the set of one-dimensional subspaces of the *left* vector space F^2 . Every non-zero vector in F^2 is a representative of a point. In terms of the projective line the zero vector $(0, 0) \in F^2$ has no meaning. Of course, we could also consider F^2 as a *right* vector space in order to describe this projective line. The choice of “left” or “right” is just a matter of taste.

3.2.6 Now let us turn to an arbitrary ring R . We consider a (unitary) left module M over R . A family $(\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$ of *vectors* in M is called a *basis* provided that the mapping

$$R^n \rightarrow M : (x_1, x_2, \dots, x_n) \mapsto \sum_{i=1}^n x_i \mathbf{b}_i \quad (3.3)$$

is a bijection. In this case M is called *free of rank* n . It is important to notice that this rank n is in general *not* uniquely determined by M . See, for example, [74, Example 1.4]

In order to define the projective line over a ring R we start with a module M over R which is free of rank 2. By virtue of the bijection given in (3.3), we replace M with R^2 . Of course, the left R -module R^2 is free of rank 2; this is immediate by considering the *standard basis* $((1, 0), (0, 1))$ of R^2 .

It is tempting to define the projective line over a ring just in same way as we did for a field in (3.2). However, this would not give “enough points”, since we would not get any “point” of the form $R(1, s)$, where $s \neq 0$ has no left inverse. Nevertheless, $R(s, 1)$ would be a point, i.e., we would not have symmetry with respect to the order of coordinates. At the other extreme one could say, as in the case of a field, that *every* pair $(a, b) \in R^2$, $(a, b) \neq (0, 0)$ should be a representative of some point. Yet, also here a problem arises: In general, we would get “far too much points” for our purposes. Cf., e.g., [36, p. 1128], where a distinction between “points” and “free points” is made.

It turned out that a “good” definition of the projective line over a ring R is as follows: A submodule $R(a, b) \subset R^2$ is a point if (a, b) is an element of a basis with two elements. As in the case of a vector space, the *general linear group* $\text{GL}_2(R)$ of invertible 2×2 -matrices with entries in R acts regularly on the set of those ordered bases of R^2 which consist of two vectors. Therefore, starting at the canonical basis we are lead to the following strict definition:

Definition 3.2.7 The *projective line over* R is the orbit

$$\mathbb{P}(R) := (R(1, 0))^{\text{GL}_2(R)}$$

of $R(1, 0)$ under the natural action of $\mathrm{GL}_2(R)$ on the subsets of R^2 . Its elements are called *points*.

We refer to [55, Definition 1.2.1] for an equivalent definition which avoids using coordinates. Cf. also [32] for the *dual* of a *projective line*.

3.2.8 Let us describe $\mathbb{P}(R)$ in different words: A pair $(a, b) \in R^2$ is called *admissible* (over R) if there exist $c, d \in R$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R)$. So we have

$$\mathbb{P}(R) = \{R(a, b) \subset R^2 \mid (a, b) \text{ admissible}\}. \quad (3.4)$$

Thus our definition of the projective line relies on admissible pairs. However, there may also be non-admissible pairs $(a, b) \in R^2$ such that $R(a, b) \in \mathbb{P}(R)$. Strictly speaking, this phenomenon occurs precisely when R is not Dedekind-finite (see 3.2.2). We refer to [29], Propositions 2.1 and 2.2, for further details. We therefore adopt the following convention:

Points of $\mathbb{P}(R)$ are represented by admissible pairs only.

This brings us in a natural way to the next result:

Theorem 3.2.9 *Let $(a, b) \in R^2$ and (a', b') be admissible pairs. Then $R(a, b) = R(a', b')$ if, and only if, there exists an element $u \in R^*$ with $(a', b') = u(a, b)$.*

Proof. Let $R(a, b) = R(a', b')$. By our assumption, there is a matrix $\gamma \in \mathrm{GL}_2(R)$ with first row (a, b) . Thus

$$(a, b) \cdot \gamma^{-1} = (1, 0), \quad (a', b') \cdot \gamma^{-1} =: (u, v), \quad \text{and} \quad R(1, 0) = R(u, v).$$

As (a', b') is admissible, so is (u, v) . Now $(u, v) \in R(1, 0)$ implies $x(1, 0) = (u, v)$ for some $x \in R$, whence $v = 0$. Similarly, we obtain $y(u, v) = (yu, 0) = (1, 0)$ for some $y \in R$. This means that y is a left inverse of u . By the above, $(u, v) = (u, 0)$ is admissible. Hence there exists an invertible matrix δ , say, with first row $(u, 0)$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} u & 0 \\ * & * \end{pmatrix}}_{\delta} \cdot \underbrace{\begin{pmatrix} z & * \\ * & * \end{pmatrix}}_{\delta^{-1}} = \begin{pmatrix} uz & * \\ * & * \end{pmatrix}$$

shows that z , i.e. the north-west entry of δ^{-1} , is a right inverse of u . Therefore

$$(a', b') = u((1, 0) \cdot \gamma) = u(a, b) \text{ with } u \in R^*,$$

as required.

Conversely, if u is a unit with $(a', b') = u(a, b)$ then $R = Ru$, whence $R(a, b) = R(ua, ub) = R(a', b')$. \square

3.2.10 We note that, for all $x \in R$,

$$\begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -x \end{pmatrix}^{-1} \in \mathrm{GL}_2(R), \quad \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}^{-1} \in \mathrm{GL}_2(R). \quad (3.5)$$

Hence the projective line over R contains all points $R(x, 1)$ with $x \in R$. If $x, y \in R$ are different then $R(x, 1) \neq R(y, 1)$. Analogous results hold for $R(1, x) \in \mathbb{P}(R)$ for all $x \in R$. However, if $x \in R^*$ then $R(1, x) = R(x^{-1}, 1)$, i.e., this point is taken into account for a second time. This shows that we can restrict ourselves to points $R(1, x)$ with $x \in R \setminus R^*$, and it establishes the estimate

$$\#\mathbb{P}(R) \geq \#R + \#(R \setminus R^*). \quad (3.6)$$

We shall see below that for certain rings the projective line contains even more points. Cf. however Theorem 3.5.5 and Corollary 3.5.6.

Example 3.2.11 Let $\mathbb{Z}/(6\mathbb{Z}) =: \mathbb{Z}_6$ be the (commutative) ring of integers modulo 6. We have $\mathbb{Z}_6^* = \{1, 5\}$, where $5 \equiv -1 \pmod{6}$; the ideals of \mathbb{Z}_6 are $\{0\}$, $2\mathbb{Z}_6 = 4\mathbb{Z}_6$, $3\mathbb{Z}_6$, and \mathbb{Z}_6 . Cf. [69, 2.6] for further details.

As x varies in \mathbb{Z}_6 , we obtain from the first matrix in (3.5) six points

$$\mathbb{Z}_6(0, 1), \mathbb{Z}_6(1, 1), \dots, \mathbb{Z}_6(5, 1),$$

and, for $x \in \mathbb{Z}_6 \setminus \mathbb{Z}_6^*$ from the second part of (3.5) four more points

$$\mathbb{Z}_6(1, 0), \mathbb{Z}_6(1, 2), \mathbb{Z}_6(1, 3), \mathbb{Z}_6(1, 4).$$

In this way we reach all points $\mathbb{Z}_6(a, b)$ where a or b is a unit. Therefore it remains to find out if there exist elements $a, b \in \mathbb{Z}_6 \setminus \mathbb{Z}_6^*$ and $c, d \in \mathbb{Z}_6$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_6)$$

which in turn is equivalent to

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in \mathbb{Z}_6^*.$$

This means that the ideal generated by a and b has to be the entire ring \mathbb{Z}_6 . Consequently,

$$(a, b) \in \{(2, 3), (4, 3), (3, 2), (3, 4)\}.$$

Thus the only remaining points in the projective line over \mathbb{Z}_6 are

$$\mathbb{Z}_6(2, 3), \mathbb{Z}_6(3, 2).$$

Therefore $\#\mathbb{P}(\mathbb{Z}_6) = 12$. Altogether, we see that among the 36 elements of \mathbb{Z}_6^2 there are 24 admissible and 12 non-admissible pairs.

3.2.12 A pair $(a, b) \in R^2$ is called *unimodular* (over R) if there exist $x, y \in R$ with

$$ax + by = 1.$$

This is equivalent to saying that the right ideal generated by a and b is the entire ring R .

Let (a, b) be the first row of a matrix $\gamma \in \mathrm{GL}_2(R)$ and suppose that the first column of γ^{-1} reads $(x, y)^T$. We read off from $\gamma\gamma^{-1} = 1$, where 1 denotes the identity matrix in $\mathrm{GL}_2(R)$, that every admissible pair is unimodular. We remark that

$$(a, b) \in R^2 \text{ unimodular over } R \Rightarrow (a, b) \text{ admissible over } R \quad (3.7)$$

is satisfied, in particular, for all *commutative* rings, since $ax + by = 1$ can be interpreted as the determinant of an invertible matrix with first row (a, b) and second row $(-y, x)$. WALTER BENZ in his famous book [5] considers only commutative rings and defines the projective line using unimodular pairs.

In fact (3.7) holds also for certain non-commutative rings [55, Proposition 1.4.2], namely for rings of *stable rank 2*, but we shall not give a definition of this concept here. It was the late Dutch geometer FERDINAND D. VELDKAMP (1931–1999) who first pointed out the significance for geometry of the stable rank of a ring. We refer to [106, § 2] and [108] for excellent surveys on this topic. Let us remark, however, that all finite rings are of stable rank 2.

An example of a ring R , where (3.7) is not true, can be found in [31, Remark 5.1].

3.2.13 As the concept of an admissible pair depends on the invertibility of square matrices over a ring R , one may ask for a criterion which allows to decide whether or not such a square matrix is invertible. In the general case, something like this does not seem to exist. Nevertheless, there are particular cases where we can not only decide invertibility but also explicitly describe the inverse, as we already did in 3.2.10. Some of the subsequent examples come from the *elementary subgroup* of $\mathrm{GL}_2(R)$, i.e. the subgroup generated by elementary matrices; see [41] for the algebraic background, and [31] for the geometry behind.

Examples 3.2.14 Let γ be a 2×2 matrix over R .

- (a) If all entries of γ commute with each other then we can calculate the determinant $\det \gamma$ in the usual way. The given matrix is invertible if, and only if, $\det \gamma \in R^*$. In this case γ^{-1} can be described in terms of $\det \gamma$ and the cofactor matrix of γ as in the case of a commutative field.
- (b) A diagonal matrix $\gamma = \mathrm{diag}(a, b)$ is invertible if, and only if a and b are units.

(c) If we are given a lower triangular 2×2 matrix γ then

$$\gamma =: \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}}_{\in \text{GL}_2(R)} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}. \quad (3.8)$$

We know from (3.5) that the second matrix on the right hand side is invertible.

Suppose now that a or d is a unit. By (b) and (3.8), γ is invertible if, and only if, a and d are units. In this case

$$\gamma^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -d^{-1}ca^{-1} & d^{-1} \end{pmatrix}. \quad (3.9)$$

Of course, there is a similar formula for the inverse of an upper triangular matrix with invertible entries in the main diagonal.

(d) Suppose that $a \in R$ is right invertible so that $ab = 1$ for some $b \in R$. A straightforward verification shows that

$$\gamma := \begin{pmatrix} a & 0 \\ 1 - ba & b \end{pmatrix} \in \text{GL}_2(R), \text{ with } \gamma^{-1} = \begin{pmatrix} b & 1 - ba \\ 0 & a \end{pmatrix}.$$

This means that for rings which are not Dedekind-finite there are invertible *lower* triangular matrices with *both* diagonal entries not in R^* . Also, somewhat surprisingly, the inverse of such a matrix is *upper* triangular.

3.3 The distant relation

3.3.1 The point set $\mathbb{P}(R)$ is endowed with a relation *distant* (\triangle) which is defined via the action of $\text{GL}_2(R)$ on the set of pairs of points by

$$\triangle := (R(1, 0), R(0, 1))^{\text{GL}_2(R)}.$$

Letting $p = R(a, b)$ and $q = R(c, d)$ and taking into account Theorem 3.2.9 gives then

$$p \triangle q \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(R). \quad (3.10)$$

The distant relation is symmetric, since exchanging two rows in an invertible matrix does not influence its invertibility. In addition, \triangle is anti-reflexive, because $R(1, 0) \neq R(0, 1)$

implies that distant points are distinct². However, in general distinct points need not be distant. Cf. Theorem 3.3.7 below.

Non-distant points ($\not\sim$) are also called *neighbouring* or *parallel*; see, for example, [5], [55], [108]. However, in these lectures we shall use the term “parallel” in a different meaning which will be explained in 5.1.1. The two notions “parallel” and “neighbouring” coincide precisely when R is a local ring. See Theorem 5.1.4 and our preliminary definition in 3.5.8.

A crucial property of the distant relation is stated in the following result on the action of $\mathrm{GL}_2(R)$ on the projective line.

Theorem 3.3.2 *The group $\mathrm{GL}_2(R)$ acts 3- Δ -transitively on $\mathbb{P}(R)$, i.e. transitively on the set of triples of mutually distant points.*

Proof. (a) We consider the points $R(1, 0)$, $R(0, 1)$, and $R(1, 1)$. They are mutually distant by (3.5). Also, let $R(a, b)$ be a point which is distant to $R(1, 0)$ and $R(0, 1)$. Consequently,

$$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \in \mathrm{GL}_2(R) \text{ and } \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(R).$$

Hence $a, b \in R^*$ by Example 3.2.14 (c). But this means that the matrix $\mathrm{diag}(a, b) \in \mathrm{GL}_2(R)$ takes $R(1, 1)$ to $R(a, b)$, whereas $R(1, 0)$ and $R(0, 1)$ remain unchanged.

(b) Given three mutually distant points $p, q, r \in \mathbb{P}(R)$ there is, by the definition of the distant relation, a matrix $\gamma \in \mathrm{GL}_2(R)$ which takes the pair of points (p, q) to $(R(1, 0), R(0, 1))$. Then, according to (a), there is also an invertible matrix which takes r^γ to $R(1, 1)$, while $R(1, 0)$ and $R(0, 1)$ remain invariant. Since this property holds for every triple of mutually distant points, the assertion follows. \square

3.3.3 Let us determine the pointwise stabilizer Ω , say, of $\{R(1, 0), R(0, 1), R(1, 1)\}$ under the action of $\mathrm{GL}_2(R)$ on the projective line $\mathbb{P}(R)$. If γ is in this stabilizer then $\gamma = \mathrm{diag}(a, b)$, because each of $R(1, 0)$ and $R(0, 1)$ has to coincide with its image. By Example 3.2.14 (b), a and b are units in R . Moreover, we infer from $R(1, 1)^\gamma = R(a, b) = R(1, 1)$ that $a = b$. These two conditions are also sufficient. Therefore

$$\Omega = \{\mathrm{diag}(a, a) \mid a \in R^*\}. \quad (3.11)$$

Now we ask for the kernel of the action of $\mathrm{GL}_2(R)$ on the projective line $\mathbb{P}(R)$ which clearly is contained in Ω . If $\gamma = \mathrm{diag}(a, a) \in \Omega$ is in this kernel then

$$R(1, x)^\gamma = R(a, xa) = R(1, a^{-1}xa) \text{ for all } x \in R.$$

²This is one of the rare occasions where we need that $0 \neq 1$ in R . Over the zero ring $R = \{0\}$ (which is excluded from our exposition) we have $0 = 1$. Therefore, by defining the projective line as above, we obtain $R(0, 0) = R(1, 0) = R(0, 1)$. This means that $R(0, 0)$ is the only point of this projective line, and that $R(0, 0)$ is distant to itself.

Recall that

$$Z(R) := \{a \in R \mid ax = xa \text{ for all } x \in R\}$$

is the *centre* of R ; it is a subring of R . Therefore a has to be unit in the centre of R . Conversely, every matrix $\text{diag}(a, a)$ with $a \in Z(R)^*$ fixes $\mathbb{P}(R)$ pointwise. It is easy to show (as in elementary linear algebra) that the kernel of our group action is equal to the *centre* of $\text{GL}_2(R)$, viz.

$$\begin{aligned} Z(\text{GL}_2(R)) &= \{\beta \in \text{GL}_2(R) \mid \beta\xi = \xi\beta \text{ for all } \xi \in \text{GL}_2(R)\} \\ &= \{\text{diag}(a, a) \mid a \in Z(R)^*\}. \end{aligned} \quad (3.12)$$

As usual, the factor group $\text{GL}_2(R)/Z(\text{GL}_2(R)) =: \text{PGL}_2(R)$ is called a *projective linear group*; its elements are called *projectivities* and can be considered as permutations of $\mathbb{P}(R)$.

Theorem 3.3.4 *The following statements are equivalent.*

- (a) $\text{PGL}_2(R)$ acts sharply transitively on the set of triples of mutually distant points.
- (b) The group R^* of units in R is contained in the centre $Z(R)$.

Proof. The result is an immediate consequence of (3.11) and (3.12). □

The interested reader should also compare this result with the characterizations given in [55, Proposition 1.3.4].

3.3.5 Given a point $p \in \mathbb{P}(R)$ let

$$\Delta(p) := \{x \in \mathbb{P}(R) \mid x \Delta p\}.$$

If we consider $\mathbb{P}(R)$ as the set of vertices of the *distant graph*, i.e. the unordered graph of the symmetric relation Δ , then $\Delta(p)$ is just the *neighbourhood* of p in this graph. Once a point p has been chosen, the points of $\mathbb{P}(R)$ fall into two classes: The points of $\Delta(p)$ are called *proper* (with respect to p), the remaining points are called *improper* (with respect to p).

As $\text{GL}_2(R)$ acts transitively on $\mathbb{P}(R)$ it suffices to describe the neighbourhood of $R(1, 0)$, a point which is also denoted by the symbol ∞ . By Example 3.2.14 (c), a point $R(a, b)$ is in $\Delta(\infty)$ precisely when $b \in R^*$. But then we may assume w.l.o.g. that $b = 1$, because $R(a, b) = R(b^{-1}a, 1)$. The *embedding*

$$R \rightarrow \mathbb{P}(R) : a \mapsto R(a, 1) \quad (3.13)$$

maps the affine line over R injectively onto the subset $\Delta(\infty)$ of the projective line over R . We already met this embedding in 3.2.10. It shows that the neighbourhood of any point has $\#R$ elements.

By virtue of (3.13), we may even identify the affine line over the ring R with the subset $\Delta(\infty)$. From

$$\underbrace{\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}}_{\in \text{GL}_2(R)} \begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ b & 1 \end{pmatrix}$$

follows that—in affine terms—two points $a, b \in R$ are distant, precisely when $a - b$ is a unit.

Example 3.3.6 We continue the investigation of the projective line $\mathbb{P}(\mathbb{Z}_6)$; see Example 3.2.11. In Figure 3.2 each point of $\mathbb{P}(\mathbb{Z}_6)$ is labelled by one of its admissible pairs.

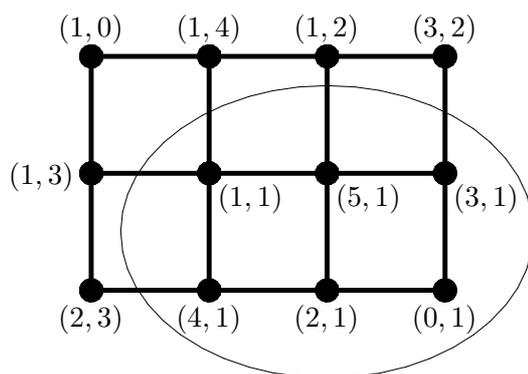


Figure 3.2: The distant relation on $\mathbb{P}(\mathbb{Z}_6)$

The distant relation on $\mathbb{P}(\mathbb{Z}_6)$ is illustrated in the following way: Two distinct points are distant if they are *not* on a common line. The six points inside the ellipse comprise the neighbourhood of $\infty = \mathbb{Z}_6(1, 0)$ in the distant graph.

As a general theme, one aims at characterizing algebraic properties of a ring R in terms of the distant relation on the associated projective line. Here is a first result in this direction.

Theorem 3.3.7 *A ring R is a field if, and only if, any two distinct points of the projective line $\mathbb{P}(R)$ are distant.*

Proof. (a) Let R be a field. Given distinct points $p = R(a, b)$ and $q = R(c, d)$ of $\mathbb{P}(R)$ we obtain $(0, 0) \neq (a, b) \notin R(c, d)$ and $(0, 0) \neq (c, d) \notin R(a, b)$, since a one-dimensional

vector space is spanned by each of its non-zero vectors. This means that (a, b) and (c, d) are linearly independent vectors of the left vector space R^2 , whence $p \triangle q$ follows from (3.10).

(b) Conversely, the point $R(1, 0)$ is distinct from each point $R(1, x)$, where x varies in $R \setminus \{0\}$. By Example 3.2.14 (c), we obtain that every non-zero element of R is invertible or, said differently, that R is a field. \square

3.4 Chain geometries

3.4.1 The only structure on the projective line over a ring we have encountered so far is the distant relation. Suppose now that a field K is contained in R , as a subring. Thus $1 \in K$ is the identity element of R , and R can be considered as a left or a right vector space over K . The ring R is, by definition, a K -algebra precisely when the field K belongs to the centre of R .

Lemma 3.4.2 *The mapping*

$$\mathbb{P}(K) \rightarrow \mathbb{P}(R) : K(k, l) \mapsto R(k, l) \quad (3.14)$$

is well defined. It takes distinct points of $\mathbb{P}(K)$ to distant points of $\mathbb{P}(R)$.

Proof. The assertions are immediate from $\mathrm{GL}_2(K) \subset \mathrm{GL}_2(R)$. \square

The following definition is taken from a paper by CLAUDIO BARTOLONE [2]. For a systematic account see [28], and for the particular case when R is an algebra over K the reader should compare with [5] and [55].

Definition 3.4.3 Let R be a ring containing a field K , as a subring. Also, let C_0 be the image of the projective line $\mathbb{P}(K)$ under the embedding (3.14). A subset of $\mathbb{P}(R)$ is called a K -chain (or shortly a *chain*, K being understood) if it belongs to set

$$\mathcal{C}(K, R) := C_0^{\mathrm{GL}_2(R)}.$$

The *chain geometry* over (K, R) is the structure

$$\Sigma(K, R) := (\mathbb{P}(R), \mathcal{C}(K, R)).$$

By definition, all chains arise from the *standard chain* C_0 under the action of the group $\mathrm{GL}_2(R)$. Observe that we refrain from excluding the trivial case when $R = K$.

3.4.4 If $\Sigma(K, R)$ and $\Sigma(K', R')$ are chain geometries then an *isomorphism* is a bijection $\varphi : \mathbb{P}(R) \rightarrow \mathbb{P}(R')$ preserving chains in both directions. By definition, the group $\text{PGL}_2(R)$ is a group of automorphisms of $\Sigma(K, R)$.

Our first observation is a characterization of the distant relation \triangle of $\mathbb{P}(R)$ in terms of a chain geometry $\Sigma(K, R)$ (see [55, 2.4.2] for the case of algebras):

Theorem 3.4.5 *Let $p, q \in \mathbb{P}(R)$ be distinct points of $\Sigma(K, R)$. Then $p \triangle q$ holds if, and only if, there is a chain $D \in \mathcal{C}(K, R)$ joining p and q .*

Proof. By the definition of the distant relation in 3.3.1, we know that $p \triangle q$ implies $p = R(1, 0)^\gamma$, $q = R(0, 1)^\gamma$ for some $\gamma \in \text{GL}_2(R)$. Hence in this case $p, q \in C_0^\gamma \in \mathcal{C}(K, R)$.

Conversely, if $p, q \in C_0^\gamma \in \mathcal{C}(K, R)$, with $\gamma \in \text{GL}_2(R)$, then $p^{\gamma^{-1}}$ and $q^{\gamma^{-1}}$ are distinct points of the standard chain $C_0 = \mathbb{P}(K)$. By Lemma 3.4.2, we have $p^{\gamma^{-1}} \triangle q^{\gamma^{-1}}$. Since γ preserves \triangle , this proves the assertion. \square

Given three mutually distant points we now want to determine the chains through them. Note that, by Theorem 3.4.5, any two distinct points on a chain are distant.

Theorem 3.4.6 *Let the points $p, q, r \in \mathbb{P}(R)$ be mutually distant. Then there is at least one chain $D \in \mathcal{C}(K, R)$ containing p, q , and r .*

Proof. As the group $\text{GL}_2(R)$ acts 3- \triangle -transitively on $\mathbb{P}(R)$ by Theorem 3.3.2, there exists a $\gamma \in \text{GL}_2(R)$ with $p = R(1, 0)^\gamma$, $q = R(0, 1)^\gamma$, and $r = R(1, 1)^\gamma$. Obviously, $D := C_0^\gamma$ is a chain through p, q , and r . \square

The essential result on the group action of $\text{GL}_2(R)$ on $\Sigma(K, R)$ is as follows:

Theorem 3.4.7 *Let $D, D' \in \mathcal{C}(K, R)$ be chains. Suppose, furthermore, that $p, q, r \in D$ and $p', q', r' \in D'$ are, respectively, three mutually distinct points. Then there exists a matrix $\gamma \in \text{GL}_2(R)$ such that $p^\gamma = p'$, $q^\gamma = q'$, $r^\gamma = r'$, and $D^\gamma = D'$.*

Proof. There exists a matrix $\gamma_1 \in \text{GL}_2(R)$ mapping D to the standard chain C_0 . Put $p_1 := p^{\gamma_1}$, $q_1 := q^{\gamma_1}$, $r_1 := r^{\gamma_1}$. The group $\text{GL}_2(K) \subset \text{GL}_2(R)$ leaves C_0 invariant and acts 3-fold transitively on C_0 . Hence there is a $\gamma_2 \in \text{GL}_2(K)$ with $p_1^{\gamma_2} = R(1, 0)$, $q_1^{\gamma_2} = R(0, 1)$, $r_1^{\gamma_2} = R(1, 1)$. Then, we also have $C_0^{\gamma_2} = C_0$.

Define γ'_1 and γ'_2 accordingly. Then $\gamma = \gamma_1 \gamma_2 \gamma_2'^{-1} \gamma_1'^{-1}$ has the required properties. \square

Now it is easy to determine the number of chains containing three mutually distant points:

Theorem 3.4.8 *Let*

$$N := \{n \in R^* \mid n^{-1}K^*n = K^*\}$$

be the normalizer of K^ in R^* . Then the following assertions hold:*

- (a) *The set of chains through any three mutually distant points of $\Sigma(K, R)$ is in 1-1-correspondence with the set*

$$\{Nr \mid r \in R^*\}$$

of right cosets of N in the multiplicative group R^ .*

- (b) *In $\Sigma(K, R)$ there exists exactly one chain through any three mutually distant points if, and only if, K^* is a normal subgroup of R^* .*

Proof. We recall from (3.11) that the subgroup

$$\Omega = \{\text{diag}(a, a) \mid a \in R^*\} \cong R^*$$

of $\text{GL}_2(R)$ is the pointwise stabilizer of the set $\{R(1, 0), R(0, 1), R(1, 1)\}$. So, by Theorem 3.4.7, the chains through $R(1, 0), R(0, 1), R(1, 1)$ are precisely the images C_0^ω , where ω ranges in Ω . Since

$$R(1, x)^\Omega = \{R(1, a^{-1}xa) \mid a \in R^*\}$$

holds, in particular, for all $x \in K^*$, the stabilizer of the standard chain C_0 in Ω is

$$\Omega_{C_0} = \{\text{diag}(n, n) \mid n \in N\} \cong N.$$

So, by (2.18), assertion (a) follows for the three given points and, by Theorem 3.4.7, for any three pairwise distant points.

Of course, the condition in (b) just means that $R^* = N$. □

Examples 3.4.9 In each of the following examples there is a unique chain through any three distinct points of $\Sigma(K, R)$:

- (a) Suppose that K belongs to the centre of R , i.e., R is a K -algebra. Then, since K^* is in the centre of R^* , its normalizer N coincides with R^* . Most of the examples which we shall encounter later on will be of this kind.
- (b) Let R be a commutative ring. Then the assumptions of Example (a) are satisfied without imposing a condition on K .
- (c) Suppose that $K^* = R^*$. Then $N = R^* = K^*$ is trivially true. Observe that $K^* = R^*$ does not mean that $K = R$; take, for example, a polynomial ring $K[T]$ over a commutative field K in an indeterminate T ; see also [28, Example 2.5 (a)].

- (d) Let $\mathbb{Z}_2 = \text{GF}(2)$ be the field with two elements. Also let $R = \mathbb{Z}_2^{2 \times 2}$ be the ring of 2×2 matrices over \mathbb{Z}_2 . There are six invertible elements in this ring, namely

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The centre of R is given by $Z(R) = \{\text{diag}(x, x) \mid x \in \mathbb{Z}_2\}$. We put

$$K := \left\{ \begin{pmatrix} x & y \\ y & x+y \end{pmatrix} \mid x, y \in \mathbb{Z}_2 \right\}.$$

It is easily seen that K is a subring of R which is isomorphic to $\text{GF}(4)$, i.e. the field with 4 elements. Of course, $K^* \not\subset Z(R)$. Since $\#R^* = 6$, the multiplicative group K^* has index 2 in R^* and therefore is normal.

We now determine the intersection of all chains through three mutually distant points of a chain geometry $\Sigma(K, R)$. To this end we introduce the field

$$F := \bigcap_{a \in R^*} a^{-1}Ka$$

which is a subring of R . Consequently, we can embed the projective line $\mathbb{P}(F)$ in $\mathbb{P}(R)$ and define a chain geometry $\Sigma(F, R)$ as above. Its chains will be called F -chains in order to distinguish them from the chains which arise from $\Sigma(K, R)$.

Theorem 3.4.10 *Let $p, q, r \in \mathbb{P}(R)$ be mutually distant points. Then the intersection of all chains of $\Sigma(K, R)$ through p, q, r is an F -chain.*

Proof. We consider w.l.o.g. the points $R(1, 0)$, $R(0, 1)$, and $R(1, 1)$. According to Theorem 3.4.7 the chains joining them are exactly the images C_0^ω , with $\omega \in \Omega$; compare (3.11). Given a matrix $\text{diag}(a, a) \in \Omega$ we compute

$$C_0^\omega = \{R(a, 0)\} \cup \{R(ka, a) \mid k \in K\} = \{R(1, 0)\} \cup \{R(a^{-1}ka, 1) \mid k \in K\}.$$

Therefore

$$\begin{aligned} \bigcap_{\omega \in \Omega} C_0^\omega &= \{R(1, 0)\} \cup \bigcap_{a \in R^*} \{R(a^{-1}ka, 1) \mid k \in K\} \\ &= \{R(1, 0)\} \cup \{R(f, 1) \mid f \in F\}, \end{aligned}$$

which equals $\mathbb{P}(F)$, considered as a subset of $\mathbb{P}(R)$. \square

3.5 Local rings, local algebras, and Laguerre algebras

3.5.1 Let R be a ring. The *Jacobson radical* of a ring R , named after NATHAN JACOBSON (1910–1999) and denoted by $\text{rad } R$, is the intersection of all maximal left (or right) ideals of R . It is a two sided ideal of R and its elements can be characterized as follows:

$$b \in \text{rad } R \Leftrightarrow 1 - ab \in R^* \text{ for all } a \in R \Leftrightarrow 1 - ba \in R^* \text{ for all } a \in R;$$

see [73, pp. 53–54].

Suppose that R is *left artinian*—after EMIL ARTIN (1898–1962)—i.e., there does not exist an infinite strictly descending chain of left ideals of R . then $\text{rad } R$ is the largest *nilpotent* left ideal, and it is also the largest nilpotent right ideal; this means that $(\text{rad } R)^n = 0$ for some positive integer n [73, Theorem 4.12]. Consequently, $\text{rad } R$ is actually a nilpotent ideal. All this holds, in particular, if R is a finite ring. See [72] for further references on nilpotent rings.

3.5.2 A ring R is called a *local ring* if $R \setminus R^*$ is an ideal³ of R . There are several equivalent definitions of a local ring and the interested reader should compare with [73, Theorem 19.1]. We just mention that a ring R is local if, and only if, it has an ideal $J \neq R$ containing all ideals other than R . This is equivalent to saying that R has a unique maximal ideal.

Let R be a local ring. Since $R \setminus R^*$ is the only maximal left ideal of R , we obtain

$$\text{rad } R = R \setminus R^*,$$

Since $\text{rad } R$ is an ideal, we can construct the factor ring $\overline{R} := R/\text{rad } R$ based upon the canonical epimorphism $R \rightarrow \overline{R} : a \mapsto \overline{a}$. If $\overline{a} \neq \overline{0}$ then $a \in R^*$, whence \overline{a} is a unit in \overline{R} . This means that \overline{R} is a field, and we have the property

$$a \in R^* \Leftrightarrow \overline{a} \in \overline{R}^*. \quad (3.15)$$

Given a matrix $\gamma = (\gamma_{ij})$ with entries in R we put $\overline{\gamma} := (\overline{\gamma_{ij}})$. Then one can show as above that

$$\gamma \in \text{GL}_m(R) \Leftrightarrow \overline{\gamma} \in \text{GL}_m(\overline{R}) \quad (3.16)$$

holds for all natural numbers $m \geq 1$.

³By an “ideal” we always mean a two-sided ideal. The term “local ring” comes from algebraic geometry: At any point p of an algebraic variety, the rational functions which are “locally” regular (i.e. regular in some neighbourhood of p) form a local ring. The non-units in this ring are those functions which vanish at p . Compare [97, p. 72].

3.5.3 A K -algebra R is said to be *local* if R is a local ring. Clearly, K and $\text{rad } R$ are subspaces of the vector space R (over K), and they meet at 0 only. If, moreover, the group $(R, +)$ is the direct sum of its subgroups K and $\text{rad } R$ then R is called a *Laguerre algebra* over K . Here it is important to emphasize the ground field. Each Laguerre algebra R over K is a local algebra over any *proper* subfield F of K . On the other hand, it is not a Laguerre algebra over F , because $F \oplus \text{rad } R$ (direct sum of additive groups) is a proper subgroup of $(R, +)$.

Examples 3.5.4 Here are some examples of local rings and local algebras:

- (a) A trivial example of a local ring is a field.
- (b) As has been noted before, the classical example of a local ring is the ring of *dual numbers* over the reals. There are several ways to define it. For example, we may start with the polynomial ring $\mathbb{R}[T]$ in the indeterminate T , consider the ideal (T^2) which is generated by T^2 , and define the real dual numbers as the quotient ring $\mathbb{R}[T]/(T^2)$. Letting $\varepsilon := T + (T^2)$ leads to the usual notation of a dual number in the form

$$a + b\varepsilon \text{ with } a, b \in \mathbb{R}, \text{ where } \varepsilon \notin \mathbb{R}, \text{ and } \varepsilon^2 = 0.$$

This example allows several generalizations which are discussed below.

- (c) In Example (b) we may replace \mathbb{R} with any commutative field K thus obtaining the ring of *dual numbers* over K . Such a ring of dual numbers will be denoted by $K[\varepsilon]$. It is a two-dimensional Laguerre algebra over K with $\text{rad } K[\varepsilon] = K\varepsilon$.

We may even allow K to be a (non-commutative) field if we require T to be a *central indeterminate*. This means that in the polynomial ring $K[T]$ the indeterminate T commutes with every element of K . Even though this ring of dual numbers is of the form $K \oplus K\varepsilon$, it is not an algebra over K , unless K is commutative.

- (d) Let $R = K[\varepsilon]$ be a ring of dual numbers as in (c) and let $\sigma \in \text{Aut}(K)$ be an automorphism of K other than the identity. We keep addition unaltered, but introduce a new multiplication (denoted by $*$) in $K[\varepsilon]$ as follows:

$$(a + b\varepsilon) * (c + d\varepsilon) := ac + (ad + bc^\sigma)\varepsilon \text{ for all } a, b, c, d \in K.$$

This gives a ring $K[\varepsilon; \sigma]$ of *twisted dual numbers* over K . It is a local ring with $K\varepsilon$ the ideal of all non-invertible elements. It cannot be an algebra over K , even if K is commutative, because K is not in the centre of $K[\varepsilon; \sigma]$.

- (e) An immediate generalization of (c) is to consider the factor ring $K[T]/(T^h)$ for some natural number $h \geq 1$. As before, we put $\varepsilon := T + (T^h)$, whence this ring is of the form

$$K[\varepsilon] := K \oplus \underbrace{K\varepsilon \oplus K\varepsilon^2 \oplus \dots \oplus K\varepsilon^{h-1}}_{=\text{rad } K[\varepsilon]}.$$

- (f) Let V be an n -dimensional vector space over a commutative field K . Then the exterior algebra

$$\bigwedge V = \underbrace{\bigwedge^0 V}_{=K} \oplus \underbrace{\bigwedge^1 V}_{=V} \oplus \cdots \oplus \bigwedge^n V \quad (3.17)$$

is a Laguerre algebra over K with dimension 2^n ; see, for example, [69, 7.2]. Multiplication in this algebra is usually denoted by the wedge sign (\wedge). If (b_1, b_2, \dots, b_n) is a basis of V then the family of vectors

$$b_{i_1} \wedge b_{i_2} \wedge \cdots \wedge b_{i_k}, \quad \text{where } 1 \leq i_1 < i_2 < \cdots < i_k \leq n \text{ and } k \in \{0, 1, \dots, n\}$$

is a basis of $\bigwedge V$. Of course, when $k = 0$ the corresponding empty product is defined to be $1 \in \bigwedge V$. The product of vectors is alternating and therefore skew symmetric. Thus we have $v \wedge v = 0$ and $v \wedge w = -w \wedge v$ for all $v, w \in V$.

In particular, for $V = K$ the exterior algebra $\bigwedge K$ is just the ring of dual numbers over K . Here some care has to be taken, since according to (3.17) we get two copies of K in $\bigwedge K$, namely $\bigwedge^0 K$ (a copy of the field K) and $\bigwedge^1 K$ (a copy of the vector space K), and they *must not be identified*.

- (g) Let \mathbb{Z} be the ring of integers and let $1 < q = p^h \in \mathbb{Z}$ be a power of a prime p . Then $\mathbb{Z}/(q\mathbb{Z}) =: \mathbb{Z}_q$ is a local ring. The ideal $\text{rad } \mathbb{Z}_q$ comprises the residue classes (modulo q) of all integers kp , where $k \in \mathbb{Z}$, so it is the zero ideal precisely when $h = 1$. The quotient field $\mathbb{Z}_q/\text{rad } R$ is the Galois field $\mathbb{Z}_p = \text{GF}(p)$ which carries the name of EVARISTE GALOIS (1811–1832).

If $h > 1$ then \mathbb{Z}_q is not an algebra over any field, because the smallest positive integer n satisfying $\sum_{i=1}^n 1 \equiv 0 \pmod{q}$ is $n = q$. However, the characteristic of a finite field is a prime, and an infinite field cannot be a subset of \mathbb{Z}_q .

While for an arbitrary ring it is difficult (or maybe even hopeless) to describe explicitly the associated projective line, for a local ring this is an easy task:

Theorem 3.5.5 *Let R be a local ring. Then*

$$\mathbb{P}(R) = \{R(x, 1) \mid x \in R\} \cup \{R(1, x) \mid x \in R \setminus R^*\}. \quad (3.18)$$

Proof. By 3.2.10, the elements of the sets on the right hand side of (3.18) are points of $\mathbb{P}(R)$. We infer from (3.16) that the mapping

$$\mathbb{P}(R) \rightarrow \mathbb{P}(\overline{R}) : R(a, b) \mapsto R(\overline{a}, \overline{b}) \quad (3.19)$$

is well-defined; moreover, it takes distant points of $\mathbb{P}(R)$ to distinct points of the projective line over the field \overline{R} . Cf. Theorem 3.3.7. So let $R(a, b)$ be a point of $\mathbb{P}(R)$. By (3.19), $\overline{R}(\overline{a}, \overline{b})$ is a point of $\mathbb{P}(\overline{R})$. Thus either $\overline{b} \neq \overline{0}$, whence $b \in R^*$ and $R(a, b) = R(b^{-1}a, 1)$; or $\overline{b} = \overline{0}$, whence $\overline{a} \neq \overline{0}$, $b \in R \setminus R^*$, $a \in R^*$, and $R(a, b) = R(1, a^{-1}b)$. \square

Corollary 3.5.6 *The projective line over a local ring R has cardinality*

$$\#\mathbb{P}(R) = \#R + \#\text{rad } R. \quad (3.20)$$

This improves formula (3.6) for local rings. The following characterization is essential:

Theorem 3.5.7 *A ring R is a local ring if, and only if, the relation “non-distant” ($\not\triangleleft$) on the projective line $\mathbb{P}(R)$ is an equivalence relation.*

Proof. (a) Over any ring R , the relation $\not\triangleleft$ on $\mathbb{P}(R)$ is reflexive and symmetric, since \triangleleft is anti-reflexive and symmetric according to 3.3.1.

(b) Suppose that R is local. By the action of $\text{GL}_2(R)$, it suffices to show that $p \not\triangleleft R(1, 0)$ and $R(1, 0) \not\triangleleft q$ implies $p \not\triangleleft q$ for all $p, q \in \mathbb{P}(R)$. With $p = R(a, b)$ and $q = R(c, d)$ we obtain

$$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \notin \text{GL}_2(R) \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} \notin \text{GL}_2(R).$$

Thus, by Example 3.2.14 (c), b and d are in $R \setminus R^* = \text{rad } R$. But then $xb + yd \in \text{rad } R$ for all $x, y \in R$, whence

$$\begin{pmatrix} * & * \\ x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} * & * \\ * & 1 \end{pmatrix} \quad \text{for all } x, y \in R.$$

This implies $p \not\triangleleft q$.

(c) Conversely, let $\not\triangleleft$ be an equivalence relation. We have to show that $J := R \setminus R^* \neq \emptyset$ is an ideal. Given $a, b \in J$ we infer from 3.3.5 that $R(1, a) \not\triangleleft R(1, 0) \not\triangleleft R(1, b)$. So, transitivity of $\not\triangleleft$ yields

$$\begin{pmatrix} 1 & a \\ 1 & b \end{pmatrix} \notin \text{GL}_2(R).$$

From

$$\begin{pmatrix} 1 & a \\ 1 & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & a - b \end{pmatrix} \underbrace{\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}}_{\in \text{GL}_2(R)} \notin \text{GL}_2(R)$$

we read off that the first matrix on the right hand side is not invertible, whence $a - b \in J$. Thus J is an additive subgroup of R .

Next, we show that $ab = u$, where $a, b \in R$ and $u \in R^*$, implies that a and b are units. It suffices to treat the case $u = 1$: By Example 3.2.14 (d), the matrix

$$\begin{pmatrix} a & 0 \\ 1 - ba & b \end{pmatrix}$$

has an inverse. Hence $R(a, 0)$ and $R(1 - ba, b)$ are points such that

$$R(1, 0) \not\sim R(a, 0) \triangle R(1 - ba, b).$$

As $R(a, 0)$ and $R(1 - ba, b)$ are in distinct equivalence classes, so are $R(1, 0)$ and $R(1 - ba, b)$. Therefore

$$\begin{pmatrix} 1 & 0 \\ 1 - ba & b \end{pmatrix} \in \text{GL}_2(R).$$

We deduce from Example 3.2.14 (c) that b is a unit. Thus, finally, $a = b^{-1}$ is a unit, too.

By the above, a product of two ring elements, with one factor in J , cannot be a unit. Altogether, this means that J is an ideal. \square

3.5.8 If R is a *local ring* then two points $p, q \in \mathbb{P}(R)$ are said to be *parallel*, in symbols $p \parallel q$, if they are non-distant. By the above this is an equivalence relation and the equivalence classes of $\mathbb{P}(R)$ are also called *parallel classes*. A definition of parallel points on the projective line over an *arbitrary ring* will be given in 5.1.1.

The following result is immediate from the proof of Theorem 3.5.7:

Corollary 3.5.9 *Let $\mathbb{P}(R)$ be the projective line over a local ring R . Then every parallel class of $\mathbb{P}(R)$ has $\# \text{rad } R$ elements.*

The relations “ \parallel ” and “ $=$ ” coincide precisely when R is a field; see Theorem 3.3.7. In this case we get the finest equivalence relation on $\mathbb{P}(R)$, i.e., parallel classes are singletons.

Our proof of Theorem 3.5.7 could be shortened by using the following characterization of local rings (see [73, Theorem 19.1]): A ring R is local if, and only if, $R \setminus R^*$ is a group under addition.

3.5.10 Suppose that L is a field and that $K \subset L$ is a proper subfield contained in the centre of L . Then the chain geometry $\Sigma(K, L)$ is called a *Möbius geometry* in honour of AUGUST FERDINAND MÖBIUS (1790–1868). Two points of $\Sigma(K, L)$ are distant precisely when they are distinct, since L is a local ring and $\text{rad } R = \{0\}$. Hence there is a unique chain through any three distinct points.

Observe that the terminology in the literature is varying. We follow [55] by assuming that K is in the centre of L . Some authors drop this condition and speak of a Möbius geometry $\Sigma(K, L)$ even if K is just a proper subfield of L . Also the term *geometry of a field extension* for such a chain geometry $\Sigma(K, L)$ is being used. However, because of our emphasis on the finite case, this more general point of view is irrelevant for our purposes. Cf. Theorem 3.5.12.

Examples 3.5.11 Here are some examples of Möbius geometries and their generalizations. The reader should consult [5] for further details.

- (a) The classical example of a Möbius geometry is based on the fields \mathbb{R} and $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ of real and complex numbers. In fact, $\Sigma(\mathbb{R}, \mathbb{C})$ can be seen as an algebraic model of the geometry of circles on a Euclidean 2-sphere. There is a unique chain (circle) through any three distinct points.
- (b) Let $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ denote the real quaternions. Then $\Sigma(\mathbb{R}, \mathbb{H})$ is a Möbius geometry which is isomorphic to the geometry of circles on the Euclidean 4-sphere. There is a unique chain (circle) through any three distinct points.
- (c) Another interesting classical example is $\Sigma(\mathbb{C}, \mathbb{H})$, where \mathbb{C} is identified with $\mathbb{R} \oplus \mathbb{R}i$. It is an algebraic model for the geometry of 2-spheres on a Euclidean 4-sphere. Here there is more than one chain through three distinct points. It is not a Möbius geometry according to our definition, because the centre of the real quaternions is \mathbb{R} .

Now we turn to the finite case. Finite fields are commutative by a famous theorem due to JOSEPH HENRY MCLAGAN-WEDDERBURN (1882–1948) for which ERNST WITT (1911–1991) has given an elegant short proof; cf. [1]. Since finite commutative fields are precisely the well known Galois fields, the finite Möbius geometries are easily described.

Theorem 3.5.12

- (a) *Each finite Möbius geometry is of the form $\Sigma(\text{GF}(q), \text{GF}(q^h))$, where $q \geq 2$ is a power of a prime and $h \geq 2$ is an integer.*
- (b) *Let $q \geq 2$ be a power of a prime and let $h \geq 1$ be an integer. Then the chain geometry $\Sigma(\text{GF}(q), \text{GF}(q^h))$ is a 3-design if its chains are considered as “blocks”. The parameters of this design are*

$$v = q^h + 1, \quad k = q + 1, \quad \text{and} \quad \lambda_3 = 1.$$

Proof. (a) If K is a proper subfield of a finite field L then $K = \text{GF}(q)$, where $q \geq 2$ is a power of a prime, $L = \text{GF}(q^h)$, and $h \geq 2$ equals the dimension of L over K , as a vector space⁴.

(b) We have $\#\mathbb{P}(\text{GF}(q^h)) = q^h + 1$ according to (3.18). By their definition, all chains have $\#\mathbb{P}(\text{GF}(q)) = q + 1$ elements. Since L is commutative, every multiplicative subgroup of L^* is normal. Thus, by Theorem 3.4.8 (b) applied to K^* and L^* , there is a unique chain through any three distinct points. \square

In part (b) of the preceding Theorem we did not exclude the trivial case $h = 1$, even though it does not deserve our attention.

⁴It is worth noting here that $L = \text{GF}(q^h)$ contains a unique subfield with q elements.

3.5.13 Suppose that R is Laguerre algebra over K . Then $\Sigma(K, R)$ is called a *Laguerre geometry*. If, moreover, R is finite then the chain geometry $\Sigma(K, R)$ gives rise to a transversal divisible 3-design; it will be discussed in detail in Section 4.2.

3.6 Notes and further references

3.6.1 There are several surveys on chain geometries and related concepts. The publications [4], [5], [7], [8], [9], and [55], together with the references given there, cover these topics from the very beginning up to the year 1992. Below we restrict our attention to recent publications.

3.6.2 Various approaches have been made to axiomatize chain geometries, certain classes of chain geometries, or structures sharing some properties with a specific type of chain geometry.

This has led to concepts like *Benz planes* (see [42, Section 5]), *weak chain spaces*, *chain spaces*, *contact spaces* (cf. [55, Section 3], [80]), and *circle planes* [25]. However, in general those structures are much more general than chain geometries. Nevertheless they can sometimes be described algebraically in terms of a ring containing a subfield if some extra assumptions are made. See [20], [24], [58], [59], and [61].

The investigation of *topological circle planes* is part of the book [84]. It contains a wealth of bibliographical data.

Characterizations of projective groups $\text{PGL}_2(R)$, where R is a ring, are given in [21], [26] and [57].

3.6.3 On the other hand, it is possible to consider structures being more general than associative algebras (e.g. *alternative algebras* or *Jordan systems*) in order to obtain a kind of “chain geometry”. We refer to [10], [16], [17], [18], [19], [26], [35], and [56].

3.6.4 Other papers related with certain chain geometries are [23], [27], [47], [48], [49], [50], [53], and [54]. Every chain geometry gives rise to *partial affine spaces*. Such spaces are investigated in [60], [79], and [81].

Chapter 4

Divisible Designs via GL_2 -Actions

4.1 How to choose a base block

4.1.1 Let R be a finite local ring. As before, we write $\text{rad } R := R \setminus R^*$ for its Jacobson radical. According to Theorem 3.5.7 and by the definition in 3.5.8, the relation “parallel” (\parallel) is an equivalence relation on the projective line $\mathbb{P}(R)$. Also, $\text{GL}_2(R)$ is a group acting on $\mathbb{P}(R)$. In fact, we are in a position to apply Theorem 2.3.2:

Theorem 4.1.2 *Let R be a finite local ring, and let B_0 be a \parallel -transversal subset of the projective line $\mathbb{P}(R)$ with $k \geq 3$ points. Then*

$$(\mathbb{P}(R), \mathcal{B}, \parallel) \text{ with } \mathcal{B} := B_0^{\text{GL}_2(R)}$$

is a 3 -(s, k, λ_3)-divisible design with $v = \#R + \#\text{rad } R$ points, and $s = \#\text{rad } R$.

Proof. By Corollary 3.5.6, the projective line over R has finite cardinality $\#R + \#\text{rad } R$. It was shown in Corollary 3.5.9 that all parallel-classes have $\#\text{rad } R$ elements. According to its definition, the relation \triangle is a $\text{GL}_2(R)$ -invariant notion. Recall that, by the definition in 3.5.8, the relations \parallel and $\not\parallel$ coincide for a local ring. Therefore, also the equivalence relation \parallel is $\text{GL}_2(R)$ -invariant. Hence the assertion follows from Theorem 2.3.2. \square

4.1.3 While Theorem 4.1.2 shows that we can construct a wealth of DDs from the projective line over a finite local ring, one essential problem remains open:

What is the number of blocks containing a \parallel -transversal 3-set?

Or, said differently:

What is the value of the parameter λ_3 ?

We read off from (2.19) that to answer this question amounts to finding two non-negative integers: Firstly, $\#\text{GL}_2(R)$ and, secondly, the cardinality of the setwise stabilizer of the base block B_0 under the action of the general linear group $\text{GL}_2(R)$. It is easy to determine the order of the group $\text{GL}_2(R)$; see the exercise below. However, it seems impossible to state any result about the size of setwise stabilizer of B_0 without any further information concerning B_0 .

Exercise 4.1.4 Show that

$$\#\text{GL}_2(\text{GF}(q)) = (q^2 - 1)(q^2 - q). \quad (4.1)$$

Given a finite local ring R with $R/\text{rad } R \cong \text{GF}(q)$ verify that

$$\#\text{GL}_2(R) = (\#\text{rad } R)^4 (q^2 - 1)(q^2 - q). \quad (4.2)$$

4.1.5 If R is a finite local ring, but *not* a local algebra (e.g. $R = \mathbb{Z}_4$), then the divisible designs which arise from $\mathbb{P}(R)$ seem to be unknown. We therefore have to exclude them from our discussion in the next section.

It would be interesting learn more about the DDs which are based upon the projective line over such a ring. However, it seems to the author as if there would not exist a “natural” choice for a base block.

4.2 Transversal divisible designs from Laguerre algebras

4.2.1 In applying Theorem 4.1.2, we start with the easiest case, viz. the 3-divisible designs defined by Laguerre geometries. Recall that for a field K which is contained in a ring R , as a subring, we write $\mathcal{C}(K, R)$ for the set of K -chains of the projective line $\mathbb{P}(R)$.

Theorem 4.2.2 *Let R be an h -dimensional Laguerre algebra over $\text{GF}(q)$, $1 \leq h < \infty$. Then*

$$(\mathbb{P}(R), \mathcal{C}(\text{GF}(q), R), \parallel)$$

is a transversal 3- $(s, k, 1)$ -divisible design with $v = q^h + q^{h-1}$ points, $s = q^{h-1}$, and $k = q + 1$.

Proof. The assertions on v and s follow immediately from Theorem 4.1.2, $\#R = q^h$, and $\#\text{rad } R = q^{h-1}$. Also, we have $k = \#\mathbb{P}(\text{GF}(q)) = q + 1 = \frac{v}{s}$. Finally, since $\text{GF}(q)$ is in the centre of R , we obtain $\lambda_3 = 1$ by Example 3.4.9 (a). \square

As an immediate consequence we can show that there exist a lot of mutually non-isomorphic transversal divisible designs:

Theorem 4.2.3 *Let $q \geq 2$ be a power of a prime and let $h \geq 1$ be a natural number. Then there is at least one h -dimensional Laguerre algebra over $\text{GF}(q)$. Therefore at least one transversal 3 -($s, k, 1$)-DD with parameters as in Theorem 4.2.2 exists.*

Proof. The assertion follows from Example 3.5.4 (e), by letting $K := \text{GF}(q)$. □

Exercise 4.2.4 Determine the parameters λ_2 , λ_1 , and λ_0 (the number of chains) of the DDs from Theorem 4.2.2.

4.3 Divisible designs from local algebras

4.3.1 We shall frequently make use of the following result from algebra. It is known as the *Wedderburn principal theorem*:

Theorem 4.3.2 *Let R be a finite local algebra over $K = \text{GF}(q)$. Then there is a $\text{GF}(q)$ -subalgebra L of R which is isomorphic to the field $R/\text{rad } R$ such that $R = \text{rad } R \oplus L$.*

We refer to [78, Theorem VIII.28] for a proof.

4.3.3 Given a finite-dimensional local algebra R over $K = \text{GF}(q)$ we have the associated field $R/\text{rad } R = \overline{R}$. The canonical epimorphism $R \rightarrow \overline{R}$ takes K to an isomorphic field which is a subring of \overline{R} . So we obtain that

$$\overline{R} \cong \text{GF}(q^m) \text{ for some natural number } m \geq 1.$$

This implies

$$\dim_K R = m + \dim_K(\text{rad } R).$$

By the above and Theorem 4.3.2, there is a field L which is isomorphic to $\overline{R} \cong \text{GF}(q^m)$ such that $K \subset L \subset R$, whence R is a left vector space over L . We let

$$h := \dim_L R \geq 1.$$

Hence

$$\dim_K R = (\dim_L R)(\dim_K L) = hm \tag{4.3}$$

and

$$\dim_K(\text{rad } R) = (h - 1)m. \tag{4.4}$$

The next theorem is taken from [101, Example 2.5]. It is a generalization of Theorem 4.2.2 which, of course, is included as a particular case for $m = 1$.

Theorem 4.3.4 *Let R be an finite-dimensional local algebra over $K = GF(q)$, with $R/\text{rad } R \cong GF(q^m)$, whence $\dim_K R = hm$ for some positive integer h . Then*

$$(\mathbb{P}(R), \mathcal{C}(GF(q), R), \parallel)$$

is a 3 - $(s, k, 1)$ -divisible design with $v = q^{hm} + q^{(h-1)m}$ points, $s = q^{(h-1)m}$ and $k = q + 1$.

Proof. It suffices to repeat the proof of Theorem 4.2.2, taking into account that now $\#\text{rad } R = q^{(h-1)m}$ by virtue of (4.4). \square

Next, we apply this result to construct DDs:

Theorem 4.3.5 *Let $q \geq 2$ be a power of a prime. Also, let h and m be a positive integers. Then there is at least one hm -dimensional local algebra R over $GF(q)$ with $R/\text{rad } R \cong GF(q^m)$. Therefore at least one 3 - $(s, k, 1)$ -divisible design with parameters as in Theorem 4.3.4 exists.*

Proof. We infer from Theorem 4.2.3 that there is an h -dimensional Laguerre algebra R over $GF(q^m)$. Therefore $R/\text{rad } R$ is isomorphic to $GF(q^m)$. This R is an hm -dimensional local algebra over $GF(q) \subset GF(q^m)$. \square

Observe that for $h > 1$ non-transversal DDs are obtained in this way.

4.3.6 By the definition of an (arbitrary) chain geometry $\Sigma(K, R)$, the group $GL_2(R)$ acts on $\mathbb{P}(R)$ as a group of automorphisms of $\Sigma(K, R)$ or, said differently, of the corresponding divisible design. Recall that $PGL_2(R)$ denotes the transformation group on $\mathbb{P}(R)$ which is induced by $GL_2(R)$. However, in general this group is only a subgroup of the full automorphism group.

We shall describe below the full automorphism group of certain chain geometries and hence of the corresponding DDs. In order to do so we need the following concept carrying the name of the German physicist PASCUAL JORDAN (1902–1980), who should not be confused with the French mathematician CAMILLE JORDAN (1839–1922).

4.3.7 Let R and R' be rings. A mapping $\sigma : R \rightarrow R'$ is called *Jordan homomorphism* if

$$(a + b)^\sigma = a^\sigma + b^\sigma, \quad 1^\sigma = 1 \ (\in R'), \quad (aba)^\sigma = a^\sigma b^\sigma a^\sigma \quad \text{for all } a, b \in R. \quad (4.5)$$

See, among others, [68, p. 2] or [55, p. 832]. For such a mapping σ and any element $a \in R^*$ the equation

$$1^\sigma = (aa^{-2}a)^\sigma = a^\sigma(a^{-2})^\sigma a^\sigma \quad (4.6)$$

shows that a^σ has a left and a right inverse, whence a^σ is a unit in R' . Also,

$$a^\sigma = (aa^{-1}a)^\sigma = a^\sigma(a^{-1})^\sigma a^\sigma \quad (4.7)$$

implies

$$(a^{-1})^\sigma = (a^\sigma)^{-1} \text{ for all } a \in R^*. \quad (4.8)$$

As usual, a bijective Jordan homomorphism is called a *Jordan isomorphism*; its inverse mapping is also a Jordan isomorphism.

4.3.8 Let $\sigma : R \rightarrow R'$ be a mapping. If σ is a homomorphism of rings then it is also a Jordan homomorphism. This remains true if $\sigma : R \rightarrow R'$ is an *antihomomorphism*; this means that σ is a homomorphism of the additive groups, sends $1 \in R$ to $1 \in R'$, whereas $(ab)^\sigma = b^\sigma a^\sigma$ for all $a, b \in R$. Of course, this antihomomorphism σ is at the same time a homomorphism if R^σ is a commutative subring of R' .

Let $\sigma : R \rightarrow R'$ be a Jordan homomorphism of rings. If R and R' are commutative and if $1 + 1 \in R^*$ then σ is a homomorphism. If R' has no left or right zero divisors then σ is a homomorphism or an antihomomorphism. See, among others, [3], [51], and [69, p. 114]. Thus under certain circumstances there will be no *proper* Jordan homomorphisms for two given rings, i.e. Jordan homomorphisms that are neither a homomorphism nor an antihomomorphism.

Examples 4.3.9 We present some Jordan homomorphisms other than homomorphisms.

- (a) A well known example of an antiautomorphism (a bijective antihomomorphism of a ring onto itself) is as follows: Let R commutative ring (or even a commutative field) and let $R^{m \times m}$ be the ring of $m \times m$ matrices with entries from R with $m \geq 2$. The transposition of matrices is an antiautomorphism $R^{m \times m} \rightarrow R^{m \times m}$.
- (b) Suppose that $R = \prod_{j \in J} R_j$ is the direct product of rings R_j . Similarly, let $R' = \prod_{j \in J} R'_j$. Assume, furthermore, that $\sigma_j : R_j \rightarrow R'_j$ is a family of mappings, where each σ_j is a homomorphism or an antihomomorphism. Then

$$\sigma := \prod_{j \in J} \sigma_j : R \rightarrow R' : (x_j)_{j \in J} \mapsto (x_j^{\sigma_j})_{j \in J}$$

is Jordan homomorphism.

If among the mappings σ_j there is a homomorphism, other than an antihomomorphism, and an antihomomorphism, other than a homomorphism, then σ will be a proper Jordan homomorphism. Thus proper Jordan homomorphisms can easily be found.

- (c) Let V be a two-dimensional vector space over a commutative field K and let b_1, b_2 be a basis. Then $(1, b_1, b_2, b_1 \wedge b_2)$ is a basis of the exterior algebra $\bigwedge V$; see [69, Section 7.2]. Hence there exists a unique K -linear bijection $\sigma : \bigwedge V \rightarrow \bigwedge V$ with the following properties: σ interchanges b_2 with $b_1 \wedge b_2$ and fixes the remaining basis elements 1 and b_1 . In order to show that σ is a Jordan isomorphism, it suffices to verify the last condition in (4.5) for the elements of the given basis. As a matter of fact, that condition is satisfied in a trivial way: Clearly, it is true if $a = 1$ or $b = 1$, otherwise it follows from $v_1 \wedge v_2 \wedge v_3 = 0$ for all $v_1, v_2, v_3 \in V$. Because of

$$(b_1 \wedge b_2)^\sigma = b_2 \neq 0, \quad \text{and} \quad b_1^\sigma \wedge b_2^\sigma = b_1 \wedge b_1 \wedge b_2 = 0,$$

the Jordan isomorphism σ is proper.

4.3.10 If a Jordan homomorphism of K -algebras is at the same time a K -linear mapping then it is called a *K -Jordan homomorphism*. The importance of K -Jordan isomorphisms is illustrated by the following result, due to ARMIN HERZER, which is presented without proof. See [55, Theorem 9.2.1], [2], and [33] for generalizations, and compare with Proposition 2.3 and Proposition 3.6 in the article [52].

Theorem 4.3.11 *Let R and R' be a local algebras over K . Then the following assertions hold:*

- (a) *If $\sigma : R \rightarrow R'$ is a K -Jordan isomorphism then the mapping*

$$\mathbb{P}(R) \rightarrow \mathbb{P}(R') : \begin{cases} R(1, a) \mapsto R'(1^\sigma, a^\sigma), \\ R(a, 1) \mapsto R'(a^\sigma, 1^\sigma), \end{cases}$$

is a well defined isomorphism of chain geometries.

- (b) *If, moreover, $\#K \geq 3$ then every isomorphism of $\Sigma(K, R)$ onto $\Sigma(K, R')$ is the product of a mapping as in (a) and a projectivity of $\mathbb{P}(R')$.*

4.3.12 By the above, we know not only all automorphisms of the DDs from Theorem 4.3.4, but also all isomorphisms between such DDs, provided that $\#K \geq 3$. Of course, “to know” means that the problem is reduced to finding all K -Jordan isomorphisms between the underlying K -algebras.

According to [52, Remark 4.3.2], there exist non-isomorphic Laguerre algebras which give rise to isomorphic chain geometries and therefore, by Theorem 4.2.2, to isomorphic divisible designs. However, those Laguerre algebras are Jordan isomorphic.

4.4 Other kinds of blocks

4.4.1 The construction of a DD from a chain geometry over a finite local algebra, as described in Theorem 4.3.4, can be generalized by modifying the set of blocks as follows.

Theorem 4.4.2 *Let R be an finite-dimensional local algebra over $K = \text{GF}(q)$, with $R/\text{rad } R \cong \text{GF}(q^m)$, whence $\dim_K R = hm$ for some positive integer h . Furthermore, let C_0 be the standard chain of the chain geometry $\Sigma(K, R)$, and suppose the base block B_0 to be chosen as follows:*

- (a) $B_0 := C_0 \setminus \{R(1, 0)\}$, for $q > 2$.
- (b) $B_0 := C_0 \setminus \{R(1, 0), R(0, 1)\}$, for $q > 3$.
- (c) $B_0 := C_0 \setminus \{R(1, 0), R(0, 1), R(1, 1)\}$, for $q > 4$.

This gives, according to Theorem 4.1.2, a 3 -(s, k, λ_3)-divisible design with

$$v = q^{hm} + q^{(h-1)m} \text{ and } s = q^{(h-1)m}.$$

The remaining parameters k and λ_3 are

$$\begin{aligned} k = q, \quad \lambda_3 = q - 2, & \quad \text{in case (a),} \\ k = q - 1, \quad \lambda_3 = \frac{1}{2}(q - 2)(q - 3), & \quad \text{in case (b),} \\ k = q - 2, \quad \lambda_3 = \frac{1}{6}(q - 2)(q - 3)(q - 4), & \quad \text{in case (c).} \end{aligned}$$

Proof. Firstly, we observe that $\#C_0 = q + 1$ and that C_0 is a \parallel -transversal subset. So the assumptions on the cardinality of q guarantee that B_0 has at least three points.

Next, since $\text{GL}_2(R)$ acts 3 - Δ -transitively on $\mathbb{P}(R)$, it suffices to determine the number of blocks through $M := \{R(1, 0), R(0, 1), R(1, 1)\}$. By Theorem 4.2.2, the standard chain C_0 is the only chain containing M . Henceforth any block containing M has to be a subset of C_0 . There are $\binom{q-2}{j}$ possibilities to choose a j -set W in $C_0 \setminus M$, where $j \in \{1, 2, 3\}$. We infer from Theorem 3.4.7 that each such $C_0 \setminus W$ is a chain. This proves the assertions on λ_3 . The rest is clear from Theorem 4.3.4. \square

4.4.3 The previous theorem is taken from [46]. It suggests to remove four or even more points from the standard chain in order to obtain a base block for a 3-DD. It is possible to treat the case for four points by considering the number of *cross ratios* that arise if those points are written in any order. In general, four distinct points determine six cross ratios, but for a *harmonic*, *equianharmonic*, or *superharmonic* tetrad there are less than six values; cf. [65, Section 6.1]. Thus several cases have to be treated separately. We refer

to [46], and note that the results from there carry over immediately to our slightly more general setting of a local algebra. Also, the “complementary” setting where a 4-subset of the standard chain is chosen to be the base block is described in [46]. As before, cross ratios are the key to calculating the parameter λ_3 .

4.4.4 Yet another “natural choice” of a base block is the projective line over such a field $L \subset R$ which meets the requirements of the Wedderburn principle theorem (see 4.3.2). A general treatment of these DDs seems to be missing in the literature, but we are in a position to present at least one example. It is based on [78, Exercise XIX.1]:

Example 4.4.5 Let $L := GF(4) = \{0, 1, \tau, \tau^2\}$ be the field with four elements. Its multiplicative group is cyclic of order three. Addition in L is subject to $x + x = 0$ for all $x \in L$, and $1 + \tau = \tau^2$. The mapping $\sigma : L \rightarrow L : x \mapsto x^2$ is easily seen to be an automorphism of order two.

We consider the local ring $R := GF(4)[\varepsilon; \sigma]$ of twisted dual numbers over L . Thus

$$\varepsilon^2 = 0 \text{ and } \varepsilon x = x^\sigma \varepsilon = x^2 \varepsilon \text{ for all } x \in L;$$

cf. Example 3.5.4 (d). R is a local algebra over $K := GF(2) \subset L$, but not an algebra over L , because τ is not in the centre of R . The radical of R is $\text{rad } R = L\varepsilon = \varepsilon L$. An isomorphism $R/\text{rad } R \rightarrow L$ is given by $(x + y\varepsilon) + \text{rad } R \mapsto x$ for all $x, y \in L$.

Following Theorem 3.4.8 we determine the normalizer of L^* in R^* . The units in R^* have the form

$$n = x + y\varepsilon \text{ with } x \in L^* \text{ and } y \in L.$$

Given such an n we clearly have $n^{-1}1n = 1$. By $n^{-1}\tau^2n = (n^{-1}\tau n)^2$, it remains to calculate $n^{-1}\tau n$. We obtain

$$\begin{aligned} n^{-1}\tau n &= (x + y\varepsilon)^{-1}\tau(x + y\varepsilon) \\ &= (x^{-1} - y\varepsilon)\tau(x + y\varepsilon) \\ &= \tau + x^{-1}\tau y\varepsilon - y\varepsilon\tau x - y\varepsilon\tau y\varepsilon \\ &= \tau + x^{-1}\tau y\varepsilon - x^2y\tau^2\varepsilon - y^3\tau^2\varepsilon^2 \\ &= \tau(1 + x^2y(1 - \tau)\varepsilon). \end{aligned}$$

As x^2y can assume all values in L , there are four possibilities, viz.

$$\begin{aligned} x^2y = 0 & : n^{-1}\tau n = \tau \in L^*, \\ x^2y = 1 & : n^{-1}\tau n = \tau + \varepsilon \notin L^*, \\ x^2y = \tau & : n^{-1}\tau n = \tau + \tau\varepsilon \notin L^*, \\ x^2y = \tau^2 & : n^{-1}\tau n = \tau + \tau^2\varepsilon \notin L^*. \end{aligned}$$

We infer that $n = x + y\varepsilon$ is in the normalizer of L^* in R^* if, and only if, $y = 0$. Consequently, this normalizer coincides with L^* . By $\#L^* = 3$ and $\#R^* = 16 - 4 = 12$, there

are four chains through any three mutually distant points. Summing up, we have shown that

$$(\mathbb{P}(\mathrm{GF}(4)[\varepsilon; \sigma]), \mathcal{C}(\mathrm{GF}(4), \mathrm{GF}(4)[\varepsilon; \sigma]), \parallel)$$

is a transversal 3-(4, 5, 4)-DD with $v = 20$ points and $b = 256$ blocks. As a matter of fact, we actually have a 4-(4, 5, 1)-DD: Given any \mathcal{R} -transversal 4-set, say $\{p_0, p_1, p_2, p_3\}$, precisely one of the four blocks through p_0, p_1, p_2 will contain p_3 .

4.5 Notes and further references

4.5.1 All finite chain geometries (not only Laguerre geometries) have nice point models in finite projective spaces, and models in terms of finite Grassmannians. See the many references in [55, p. 812], [29], and [30]. Thus, many DDs from this chapter allow—up to isomorphism—other descriptions from which their connection with finite local algebras may not be immediate.

For example, the DD which belongs to the algebra of dual numbers over $\mathrm{GF}(q)$ arises also as follows:

- (a) The points of the DD are the points of a quadratic cone without its vertex in the three-dimensional projective space over $\mathrm{GF}(q)$. The blocks are the non-degenerate conic sections of this cone. The point classes are the generators of this cone, the vertex being removed from them. This is the finite analogue of the Blaschke cone.
- (b) The points of the DD are the lines of a parabolic linear congruence without its axis in the three-dimensional projective space over $\mathrm{GF}(q)$. The blocks are the reguli which are entirely contained in this congruence. The point classes are the pencils of lines which are entirely contained in this congruence, the axis being removed from them.

The *Klein mapping*—carrying the name of FELIX KLEIN (1849–1925)—is a one-one correspondence between the set of lines of the three-dimensional projective space over a commutative field K and the set of points of a certain quadric in a five-dimensional projective space over K ; it is called the *Klein quadric*. A reader who is familiar with this mapping will notice immediately that the Klein image of the model in (b) is just the model described in (a). However, the ambient space of the cone now is a three-dimensional tangent space of the Klein quadric. Cf. [64, 15.4].

Chapter 5

An Outlook: Finite Chain Geometries

5.1 A parallelism based upon the Jacobson radical

5.1.1 Now we turn our attention to the projective line over an arbitrary ring R , as we present the announced definition of parallel points in the general case. It is taken from [34], where the term “radical parallelism” is used instead: A point $p \in \mathbb{P}(R)$ is called *parallel* to a point $q \in \mathbb{P}(R)$ if

$$x \triangle p \Rightarrow x \triangle q$$

holds for all $x \in \mathbb{P}(R)$. In this case we write $p \parallel q$. By definition, the distant relation on $\mathbb{P}(R)$ is a $\text{GL}_2(R)$ -invariant notion. Hence

$$p \parallel q \Leftrightarrow p^\gamma \parallel q^\gamma \tag{5.1}$$

holds for all $p, q \in \mathbb{P}(R)$ and all $\gamma \in \text{GL}_2(R)$.

Clearly, the relation \parallel is reflexive and transitive. We shall see below that \parallel is in fact an equivalence relation; also it will become clear that our previous definition of parallel points (R a local ring) is a particular case of the definition from the above.

5.1.2 The connection between the parallelism on $\mathbb{P}(R)$ and the Jacobson radical of R (cf. 3.5.1) is as follows: We consider the factor ring $R/\text{rad } R =: \overline{R}$ and the canonical epimorphism $R \rightarrow \overline{R} : a \mapsto a + \text{rad } R =: \overline{a}$. It has the crucial property

$$a \in R^* \Leftrightarrow \overline{a} \in \overline{R}^* \tag{5.2}$$

for all $a \in R$; cf. [73, Proposition 4.8]. The Jacobson radical of the factor ring $R/\text{rad } R$ is zero [73, Proposition 4.6].

In geometric terms we obtain a mapping

$$\mathbb{P}(R) \rightarrow \mathbb{P}(\overline{R}) : p = R(a, b) \mapsto \overline{R}(\overline{a}, \overline{b}) =: \overline{p} \tag{5.3}$$

which is well defined and surjective [29, Proposition 3.5]. Furthermore, as a geometric counterpart of (5.2) we have

$$p \triangle q \Leftrightarrow \bar{p} \triangle \bar{q} \quad (5.4)$$

for all $p, q \in \mathbb{P}(R)$, where we use the same symbol to denote the distant relations on $\mathbb{P}(R)$ and on $\mathbb{P}(\bar{R})$, respectively. See Propositions 3.1 and 3.2 in [29]. Of course, all this is a generalization of the mapping given in (3.19), where R was supposed to be local.

The following is taken from Theorem 2.2 and Corollary 2.3 in [34]:

Theorem 5.1.3 *The mapping given by (5.3) has the property*

$$p \parallel q \Leftrightarrow \bar{p} = \bar{q} \quad (5.5)$$

for all $p, q \in \mathbb{P}(R)$. Consequently, the parallelism (\parallel) on the projective line over a ring is an equivalence relation.

Let us write $[p]$ for the *parallel class* of $p \in \mathbb{P}(R)$. It can be derived from (5.5) that

$$\#[p] = \#\text{rad } R \quad (5.6)$$

for all $p \in \mathbb{P}(R)$. Thus the cardinality of $\text{rad } R$ can be recovered from the $\mathbb{P}(R)$ as the cardinality of an arbitrarily chosen class of parallel points. In particular, \parallel is the equality relation if, and only if, $\text{rad } R = \{0\}$.

An easy consequence of (5.4) and Theorem 5.1.3 is

$$p \parallel q \Leftrightarrow \bar{p} = \bar{q} \Rightarrow \bar{p} \not\triangle \bar{q} \Leftrightarrow p \not\triangle q \quad (5.7)$$

for all $p, q \in \mathbb{P}(R)$. In general, however, the converse of (5.7) is not true:

Theorem 5.1.4 *Let R be an arbitrary ring. The relations “parallel” (\parallel) and “non-distant” ($\not\triangle$) on $\mathbb{P}(R)$ coincide if, and only if, R is a local ring.*

For a proof we refer to [34, Theorem 2.5]. By the above, our two definitions of parallel points in 3.5.8 and 5.1.1 coincide in case of a local ring.

5.2 Counting the point set

5.2.1 Let R be a finite ring. The problem to determine the number of points of the projective line over R is intricate. Our approach follows [107, Section 10] and it uses the following famous theorem on the structure of semisimple rings due to JOSEPH HENRY MACLAGAN–WEDDERBURN and EMIL ARTIN; cf. [73, Theorem 3.5]. We state it only for the particular case of a finite ring:

Theorem 5.2.2 *Let R be a finite ring such that $\text{rad } R$ is zero. Then R is isomorphic to a direct product $R_1 \times R_2 \times \cdots \times R_n$, where each R_i is a full matrix ring $\text{GF}(q_i)^{m_i \times m_i}$. The number n is uniquely determined, as are the pairs (m_i, q_i) for $i \in \{1, 2, \dots, n\}$.*

5.2.3 It is possible to count the number of points of the projective line over the ring of $m \times m$ matrices with entries from $\text{GF}(q)$, because there exists a bijection from this projective line onto the set of m -dimensional subspaces of a $2m$ -dimensional vector space over the same field. This result is due to XAVIER HUBAUT [66, p. 500], who proved it for an arbitrary commutative field K instead of $\text{GF}(q)$. This powerful tool was generalized by ANDREA BLUNCK [22, Theorem 2.1] to the ring of endomorphisms of a vector space, without any restriction on its dimension or the ground field.

By virtue of this bijection and by a result of JOSEPH ADOLPHE THAS [105, 3.3], we obtain

$$\#(\mathbb{P}(\text{GF}(q)^{m \times m})) = \prod_{i=0}^{m-1} \frac{q^{2m-i} - 1}{q^{m-i} - 1}. \quad (5.8)$$

See also [65, Theorem 3.1].

Next, it is easy to see that the projective line over a direct product of rings, say

$$R_1 \times R_2 \times \cdots \times R_n,$$

is in one-one correspondence with the cartesian product¹

$$\mathbb{P}(R_1) \times \mathbb{P}(R_2) \times \cdots \times \mathbb{P}(R_n).$$

Hence the Wedderburn–Artin Theorem 5.2.2 and formula (5.8) provide the number of points on the projective line over a direct product of matrix rings.

Finally, given any finite ring R we infer from (5.6) that

$$\#\mathbb{P}(R) = (\#\text{rad } R) (\#\mathbb{P}(\overline{R})), \quad (5.9)$$

where $\overline{R} = R/\text{rad } R$. Since $\text{rad } \overline{R} = 0$, we can apply our result from the above to count the number of points on $\mathbb{P}(\overline{R})$, thus obtaining a formula for the number of points of the projective line $\mathbb{P}(R)$.

5.3 Divisible designs vs. finite chain geometries

5.3.1 To end this series of lectures, let us compare the definition of a divisible design from 2.1.3 with properties of a chain geometry $\Sigma(K, R)$, where R is a finite ring. Given $\Sigma(K, R)$ we can associate with it the positive integers

$$v := \#\mathbb{P}(R), \quad t := 3, \quad s_1 := \#\text{rad } R, \quad s_2 := v - \#R, \quad k := \#K + 1, \quad \text{and } \lambda_t, \quad (5.10)$$

¹The case $\mathbb{Z}_6 \cong \text{GF}(2) \times \text{GF}(3)$ is illustrated in Figure 3.2.

where λ_t is the constant number of blocks through any $t = 3$ mutually distant points. As we saw, λ_t depends on “how” the field K is embedded in R , whence we cannot not state a precise value. We remark that $v \geq \#R + \# \text{rad } R$ implies the inequality

$$s_2 \geq \#R + \# \text{rad } R - \#R = \# \text{rad } R.$$

5.3.2 Given a finite chain geometry the following assertions hold, where we use the constants introduced in (5.10):

- (A₁) $\#[x] = s_1$ for all $x \in \mathbb{P}(R)$.
- (A₂) $\#\{y \in \mathbb{P}(R) \mid y \not\sim x\} = s_2$ for all $x \in \mathbb{P}(R)$.
- (B₁) $\mathcal{C}(K, R)$ is a set of subsets of $\mathbb{P}(R)$ with $\#C = k$ for all chains $C \in \mathcal{C}(K, R)$. The points of any chain are mutually distant.
- (C₁) For each t -subset $Y \subset \mathbb{P}(R)$ of mutually distant points there exist a exactly λ_t chains of $\mathcal{C}(K, R)$ containing Y .
- (D₁) $t \leq \frac{v}{s_1}$.

Thus any finite chain geometries is “almost” a 3-divisible design. However, unless R is a local ring, a \parallel -transversal 3-subset of $\mathbb{P}(R)$ need not be a subset of any chain, and the parameter s_1 need not coincide with s_2 .

On the other hand, the preceding conditions (A₁)–(D₁) could serve as a starting point for the investigation of “divisible design-like structures” in the future.

Bibliography

- [1] M. Aigner and G. M. Ziegler. *Proofs from The Book*. Springer Verlag, Berlin, third edition, 2004.
- [2] C. Bartolone. Jordan homomorphisms, chain geometries and the fundamental theorem. *Abh. Math. Sem. Univ. Hamburg*, 59:93–99, 1989.
- [3] C. Bartolone and F. Bartolozzi. Topics in geometric algebra over rings. In R. Kaya, P. Plaumann, and K. Strambach, editors, *Rings and Geometry*, pages 353–389. Reidel, Dordrecht, 1985.
- [4] W. Benz. Über Möbiusebenen. *Jber. Deutsch. Math. Verein.*, 63:1–27, 1960.
- [5] W. Benz. *Vorlesungen über Geometrie der Algebren*. Springer, Berlin, 1973.
- [6] W. Benz. *Geometrische Transformationen*. BI-Wissenschaftsverlag, Mannheim, 1992.
- [7] W. Benz, W. Leissner, and H. Schaeffer. Kreise, Zykel, Ketten. Zur Geometrie der Algebren. Ein Bericht. *Jber. Deutsch. Math. Verein.*, 74:107–122, 1972.
- [8] W. Benz and H. Mäurer. Über die Grundlagen der Laguerre-Geometrie. Ein Bericht. *Jber. Deutsch. Math. Verein.*, 67:14–42, 1964.
- [9] W. Benz, H.-J. Samaga, and H. Schaeffer. Cross ratios and a unifying treatment of von Staudt's notion of reeller Zug. In P. Plaumann and K. Strambach, editors, *Geometry – von Staudt's Point of View*, pages 127–150. Reidel, Dordrecht, 1981.
- [10] W. Bertram and K.-H. Neeb. Projective completions of Jordan pairs. I. The generalized projective geometry of a Lie algebra. *J. Algebra*, 277:474–519, 2004.
- [11] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. BI-Wissenschaftsverlag, Mannheim, 1985.
- [12] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory I*. Cambridge University Press., Cambridge, 1999.
- [13] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory II*. Cambridge University Press., Cambridge, 1999.
- [14] M. Biliotti and G. Micelli. On translation transversal designs. *Rend. Sem. Mat. Univ. Padova*, 73:217–229, 1985.
- [15] W. Blaschke. Über die Laguerresche Geometrie der Speere in der Euklidischen Ebene. *Mh. Math. Phys.*, 21:3–60, 1910.

- [16] A. Blunck. Chain geometries over local alternative algebras. *J. Geom.*, 44:33–44, 1992.
- [17] A. Blunck. Chain spaces over Jordan systems. *Abh. Math. Sem. Univ. Hamburg*, 64:33–49, 1994.
- [18] A. Blunck. A quadric model for Klingenberg chain spaces. *Geom. Dedicata*, 55:237–246, 1995.
- [19] A. Blunck. Generalized affine chain geometries. *J. Geom.*, 56:9–17, 1996.
- [20] A. Blunck. Chain spaces via Clifford algebras. *Monatsh. Math.*, 123:98–107, 1997.
- [21] A. Blunck. *Geometries for certain linear groups over rings — construction and coordinatization*. Habilitationsschrift, Technische Universität Darmstadt, 1997.
- [22] A. Blunck. Regular spreads and chain geometries. *Bull. Belg. Math. Soc. Simon Stevin*, 6:589–603, 1999.
- [23] A. Blunck. Reguli and chains over skew fields. *Beiträge Algebra Geom.*, 41:7–21, 2000.
- [24] A. Blunck. Chain spaces with many reflections. *J. Geom.*, 72:18–26, 2001.
- [25] A. Blunck. Finite circle planes. In R. Camina and L. Fajstrup, editors, *Proceedings of the Ninth International Meeting of European Women in Mathematics*, pages 155–159. Hindawi, Stony Brook, 2001.
- [26] A. Blunck. Projective groups over rings. *J. Algebra*, 249:266–290, 2002.
- [27] A. Blunck. The cross ratio for quadruples of subspaces. *Mitt. Math. Ges. Hamburg*, 22:81–97, 2003.
- [28] A. Blunck and H. Havlicek. Extending the concept of chain geometry. *Geom. Dedicata*, 83:119–130, 2000.
- [29] A. Blunck and H. Havlicek. Projective representations I. Projective lines over rings. *Abh. Math. Sem. Univ. Hamburg*, 70:287–299, 2000.
- [30] A. Blunck and H. Havlicek. Projective representations II. Generalized chain geometries. *Abh. Math. Sem. Univ. Hamburg*, 70:301–313, 2000.
- [31] A. Blunck and H. Havlicek. The connected components of the projective line over a ring. *Adv. Geom.*, 1:107–117, 2001.
- [32] A. Blunck and H. Havlicek. The dual of a chain geometry. *J. Geom.*, 72:27–36, 2001.
- [33] A. Blunck and H. Havlicek. Jordan homomorphisms and harmonic mappings. *Monatsh. Math.*, 139:111–127, 2003.
- [34] A. Blunck and H. Havlicek. Radical parallelism on projective lines and non-linear models of affine spaces. *Math. Pannonica*, 14:113–127, 2003.
- [35] A. Blunck and M. Stroppel. Klingenberg chain spaces. *Abh. Math. Sem. Univ. Hamburg*, 65:225–238, 1995.
- [36] U. Brehm, M. Greferath, and S. E. Schmidt. Projective geometry on modular lattices. In F. Buekenhout, editor, *Handbook of Incidence Geometry*. Elsevier, Amsterdam, 1995.
- [37] C. Cerroni. Divisible designs from semifield planes. *Discrete Math.*, 255:47–54, 2002. Combinatorics '98 (Palermo).

- [38] C. Cerroni and R.-H. Schulz. Divisible designs admitting $GL(3, q)$ as an automorphism group. *Geom. Dedicata*, 83:343–350, 2000.
- [39] C. Cerroni and R.-H. Schulz. Divisible designs admitting, as an automorphism group, an orthogonal group or a unitary group. In Jungnickel D. and Niederreiter H., editors, *Finite fields and applications (Augsburg, 1999)*, pages 95–108. Springer, Berlin, 2001.
- [40] C. Cerroni and A. G. Spera. On divisible designs and twisted field planes. *J. Combin. Des.*, 7:453–464, 1999.
- [41] P. M. Cohn. On the structure of the GL_2 of a ring. *Inst. Hautes Etudes Sci. Publ. Math.*, 30:365–413, 1966.
- [42] A. Delandtsheer. Dimensional linear spaces. In F. Buekenhout, editor, *Handbook of Incidence Geometry*, pages 781–842. Elsevier, Amsterdam, 1995.
- [43] P. Dembowski. *Finite Geometries*. Classics in Mathematics. Springer, Berlin, 1997.
- [44] T. Etzion. Optimal constant weight codes over \mathbb{Z}_k and generalized designs. *Discrete Math.*, 169(1-3):55–82, 1997.
- [45] O. Giering. *Vorlesungen über höhere Geometrie*. Vieweg, Braunschweig, Wiesbaden, 1982.
- [46] S. Giese, H. Havlicek, and R.-H. Schulz. Some constructions of divisible designs from Laguerre geometries. *Discrete Math.*, 301:74–82, 2005.
- [47] H. Havlicek. On the geometry of field extensions. *Aequationes Math.*, 45:232–238, 1993.
- [48] H. Havlicek. Spheres of quadratic field extensions. *Abh. math. Sem. Univ. Hamburg*, 64:279–292, 1994.
- [49] H. Havlicek. Affine circle geometry over quaternion skew fields. *Discrete Math.*, 174:153–165, 1997.
- [50] H. Havlicek and K. List. A three-dimensional Laguerre geometry and its visualization. In G. Weiß, editor, *Proceedings—Dresden Symposium Geometry: constructive & kinematic (DSG.CK)*, pages 122–129. Institut für Geometrie, Technische Universität Dresden, Dresden, 2003.
- [51] I. N. Herstein. Jordan homomorphisms. *Trans. Amer. Math. Soc.*, 81:331–341, 1956.
- [52] A. Herzer. On isomorphisms of chain geometries. *Note Mat.*, 7:251–270, 1987.
- [53] A. Herzer. Der äquiforme Raum einer Algebra. *Mitt. Math. Ges. Hamburg*, 13:129–154, 1993.
- [54] A. Herzer. N -zyklische Algebren. *Mitt. Math. Ges. Hamburg*, 13:119–128, 1993.
- [55] A. Herzer. Chain geometries. In F. Buekenhout, editor, *Handbook of Incidence Geometry*, pages 781–842. Elsevier, Amsterdam, 1995.
- [56] A. Herzer. Affine Kettengeometrien über Jordanalgebren. *Geom. Dedicata*, 59:181–195, 1996.
- [57] A. Herzer. Der Satz von Tits für $PGL_2(R)$, R ein kommutativer Ring vom stabilen Rang 2. *Geom. Dedicata*, 62:167–178, 1996.

- [58] A. Herzer. Kennzeichnung von Berührstrukturen, die Kettengeometrien sind. *J. Geom.*, 62:166–175, 1998.
- [59] A. Herzer and B. Klos. Synthetische Konstruktion eines affinen Kettenraumes. *Mitt. Math. Ges. Hamburg*, 15:35–44, 1996.
- [60] A. Herzer and S. Meuren. Ein Axiomensystem für partielle affine Räume. *J. Geom.*, 50:124–142, 1995.
- [61] A. Herzer and H. Ramroth. Die projektive Gerade über einem Ring, der direktes Produkt kommutativer Körper ist. *J. Algebra*, 176:1–11, 1995.
- [62] A. Herzer and R.-H. Schulz. Some new (s, k, λ) -translation transversal designs with non-abelian translation group. *J. Geom.*, 35:87–96, 1989.
- [63] R. Hill. *A First Course in Coding Theory*. Oxford University Press, Oxford, 1986.
- [64] J. W. P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Oxford University Press, Oxford, 1985.
- [65] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Clarendon Press, Oxford, second edition, 1998.
- [66] X. Hubaut. Algèbres projectives. *Bull. Soc. Math. Belg.*, 17:495–502, 1965.
- [67] D. R. Hughes and F. C. Piper. *Design Theory*. Cambridge University Press, Cambridge, second edition, 1985.
- [68] N. Jacobson. *Structure and Representation of Jordan Algebras*. Amer. Math. Soc., Providence, 1968.
- [69] N. Jacobson. *Basic Algebra I*. Freeman, New York, 1989.
- [70] D. Jungnickel. Transversal designs associated with Frobenius groups. *J. Geom.*, 17:140–154, 1981.
- [71] D. Jungnickel. On automorphism groups of divisible designs. *Canad. J. Math.*, 34:257–297, 1982.
- [72] R. L. Kruse and D. T. Price. *Nilpotent Rings*. Gordon and Breach, New York, 1969.
- [73] T. Y. Lam. *A First Course in Noncommutative Rings*. Springer, New York, 1991.
- [74] T. Y. Lam. *Lectures on Modules and Rings*. Springer, New York, 1999.
- [75] A. Lashkhi. Harmonic maps over rings. *Georgian Math. J.*, 4:41–64, 1997.
- [76] D. Livingstone and A. Wagner. Transitivity of finite permutation groups on unordered sets. *Math. Z.*, 90:393–403, 1965.
- [77] H. Lüneburg. *Transitive Erweiterungen endlicher Permutationsgruppen*. Lecture Notes in Mathematics, No. 84. Springer, Berlin, 1969.
- [78] B. R. McDonald. *Finite Rings with Identity*. Dekker, New York, 1974.
- [79] St. Meuren. Partial affine spaces of dimension ≥ 3 . *J. Geom.*, 56:113–125, 1996.
- [80] M. Özcan and A. Herzer. Berührstrukturen, die keine Kettenräume sind. *Geom. Dedicata*, 78:241–251, 1999.

- [81] V. Pambuccian. Über das Reichhaltigkeitsaxiom für partielle affine Räume. *J. Geom.*, 55:139–140, 1996.
- [82] D. Pedoe. A forgotten geometrical transformation. *Enseignement Math. (2)*, 18:255–267, 1972.
- [83] D. Pedoe. Laguerre’s axial transformation. *Math. Mag.*, 48:23–30, 1975.
- [84] B. Polster and G. Steinke. *Geometry on Surfaces*. Cambridge University Press, Cambridge, 2001.
- [85] J. F. Rigby. The geometry of cycles, and generalized Laguerre inversion. In C. Davis, B. Grünbaum, and F. A. Sherk, editors, *The Geometric Vein*, pages 355–378. Springer, New York, 1981.
- [86] R.-H. Schulz. Transversal designs and Hughes-Thompson groups. *Mitt. Math. Sem. Giessen*, 165:185–197, 1984.
- [87] R.-H. Schulz. On the classification of translation group-divisible designs. *European J. Combin.*, 6:369–374, 1985.
- [88] R.-H. Schulz. Transversal designs and partitions associated with Frobenius groups. *J. Reine Angew. Math.*, 355:153–162, 1985.
- [89] R.-H. Schulz. On translation transversal designs with $\lambda > 1$. *Arch. Math. (Basel)*, 49:97–102, 1987.
- [90] R.-H. Schulz. Transversal designs with $\lambda > 1$ associated with Frobenius groups. *Results Math.*, 12:401–410, 1987.
- [91] R.-H. Schulz. On the existence of generalized triads related to transversal designs. *Ars Combin.*, 25(B):203–209, 1988. Eleventh British Combinatorial Conference (London, 1987).
- [92] R.-H. Schulz. Constant weight codes and divisible designs with large automorphism groups. *Rend. Circ. Mat. Palermo (2) Suppl.*, 53:173–188, 1998. Combinatorics ’98 (Mondello).
- [93] R.-H. Schulz and A. G. Spera. Divisible designs and groups. *Geom. Dedicata*, 44:147–157, 1992.
- [94] R.-H. Schulz and A. G. Spera. Construction of divisible designs from translation planes. *Europ. J. Combin.*, 19:479–486, 1998.
- [95] R.-H. Schulz and A. G. Spera. Divisible designs admitting a Suzuki group as an automorphism group. *Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat. (8)*, 1:705–714, 1998.
- [96] R.-H. Schulz and A. G. Spera. Automorphisms of constant weight codes and of divisible designs. *Des. Codes Cryptogr.*, 20:89–97, 2000.
- [97] I. R. Shafarevich. *Basic Algebraic Geometry*. Springer, Berlin Heidelberg New York, 1977.
- [98] A. G. Spera. Translation divisible designs. *Arch. Math. (Basel)*, 55:507–515, 1990.
- [99] A. G. Spera. On affine translation divisible designs. *J. Geom.*, 40:175–185, 1991.
- [100] A. G. Spera. Semi-regular divisible designs and Frobenius groups. *Geom. Dedicata*, 42:285–294, 1992.

-
- [101] A. G. Spera. t -Divisible designs from imprimitive permutation groups. *Europ. J. Combin.*, 13:409–417, 1992.
- [102] A. G. Spera. On divisible designs and local algebras. *J. Comb. Designs*, 3:203–212, 1995.
- [103] A. G. Spera. Transitive extensions of imprimitive groups. *Discrete Math.*, 155:233–241, 1996. *Combinatorics (Acireale, 1992)*.
- [104] A. G. Spera. Divisible designs associated with translation planes admitting a 2-transitive collineation group on the points at infinity. *Aequationes Math.*, 59:191–200, 2000.
- [105] J. A. Thas. The m -dimensional projective space $S_m(M_n(GF(q)))$ over the total matrix algebra $M_n(GF(q))$ of the $n \times n$ -matrices with elements in the Galois field $GF(q)$. *Rend. Mat. Roma (VI)*, 4:459–532, 1971.
- [106] F. D. Veldkamp. Projective ring planes and their homomorphisms. In R. Kaya, P. Plaumann, and K. Strambach, editors, *Rings and Geometry*. D. Reidel, Dordrecht, 1985.
- [107] F. D. Veldkamp. Projective geometry over finite rings. *Quaderni del Seminario di Geometrie Combinatorie*, 92:1–39, January 1989. Dipartimento di Matematica Istituto G. Castelnuovo, Università degli Studi di Roma.
- [108] F. D. Veldkamp. Geometry over rings. In F. Buekenhout, editor, *Handbook of Incidence Geometry*, pages 1033–1084. Elsevier, Amsterdam, 1995.
- [109] H. Wielandt. Endliche k -homogene Permutationsgruppen. *Math. Z.*, 101:142, 1967.
- [110] I. M. Yaglom. *A Simple Non-Euclidean Geometry and Its Physical Basis*. Springer, New York Heidelberg Berlin, 1979.
- [111] I. M. Yaglom. On the circular transformations of Möbius, Laguerre, and Lie. In C. Davis, B. Grünbaum, and F. A. Sherk, editors, *The Geometric Vein*, pages 345–353. Springer, New York, 1981.

Index

- admissible pair, 23
- affine line over a ring, 21
- affine plane, 6
 - order of an, 6
- algebra, 30
 - alternative, 40
 - exterior, 36
 - local, 35
- alphabet, 16
- antihomomorphism of rings, 45
- automorphism
 - of \mathbb{Z}_m^n , 16
 - of a code, 16
 - of a DD, 9
- base block, 13
- basis, 22
 - standard, 22
- Benz plane, 40
- Blaschke cone, 19, 49
- Blaschke cylinder, 19
- block, 4
 - extended, 17
 - of imprimitivity, 12
 - starter, 13
- central indeterminate, 35
- centre
 - of a group, 28
 - of a ring, 28
- chain, 30
 - standard, 30
- chain geometries
 - isomorphism of, 31
- chain geometry, 30
- chain space, 40
 - weak, 40
- circle plane, 40
 - topological, 40
- code
 - m -ary, 16
 - automorphism of, 16
 - code of a DD, 17
 - codeword, 16
 - complex projective line, 21
 - constant weight code, 16
 - contact space, 40
 - cross ratio, 47
 - cycle, 19
- DD, 4
 - automorphism of a, 9
 - code of a, 17
 - parameters of a, 4, 8
 - regular, 5
 - simple, 4
 - transversal, 5
- DDs
 - isomorphism of, 9
- Dedekind-finite ring, 21
- design, 9
 - divisible, 4
 - group-divisible, 5
 - group-divisible, 5
- difference set
 - relative, 18
- Δ -transitive group action, 27
- distant graph, 28
- distant points, 26
- division ring, 21
- dual numbers, 20, 35
- dual of a projective line, 23
- element
 - invertible, 20
 - left invertible, 20
 - right invertible, 20
- elementary subgroup, 25
- embedding, 28
- equianharmonic tetrad, 47

- extended block, 17
- extended point class, 17
- exterior algebra, 36
- faithful representation, 11
- field, 21
 - skew, 21
- field extension
 - geometry of a, 38
- free of rank n , 22
- Galileian plane
 - inversive, 20
- general linear group, 22
- geometry of a field extension, 38
- group-divisible design, 5
- group
 - centre of a, 28
 - general linear, 22
 - projective linear, 28
 - symmetric, 11
- group action, 11
 - Δ -transitive, 27
 - imprimitive, 12
 - primitive, 12
 - regular, 11
 - sharply transitive, 11
 - t -homogeneous, 12
 - t -transitive, 11
 - transitive, 11
- group operation, 11
- group-divisible design, 5
- Hamming distance, 16
- Hamming weight, 16
- harmonic tetrad, 47
- ideal
 - nilpotent left (right), 34
- ideal point, 16
- imprimitive group action, 12
- imprimitivity
 - block of, 12
- improper point, 28
- indeterminate
 - central, 35
- inverse, 20
 - left, 20
 - right, 20
- inversive Galileian plane, 20
- invertible element, 20
- isomorphism
 - of chain geometries, 31
 - of codes, 16
 - of DDs, 9
- Jacobson radical, 34
- Jordan homomorphism, 44
 - proper, 45
- Jordan isomorphism of rings, 45
- Jordan system, 40
- K -algebra, 30
- K -chain, 30
- K -Jordan homomorphism, 46
- Klein mapping, 49
- Klein quadric, 49
- Laguerre geometry, 19, 40
- left artinian ring, 34
- left inverse, 20
- left invertible, 20
- left invertible element, 20
- left zero divisor, 21
- length, 16
- line, 6
 - affine, over a ring, 21
 - complex projective, 21
 - dual of a projective, 23
 - projective, over a field, 22
 - projective, over a ring, 22
- lines
 - parallel, 6
- local algebra, 35
- local ring, 34
- m -ary code, 16
- module
 - free of rank n , 22
- Möbius geometry, 38
- neighbourhood, 28
- neighbouring points, 27
- nilpotent left (right) ideal, 34
- normalizer, 32
- numbers
 - dual, 20, 35
 - twisted dual, 35, 48
- octahedron

- regular, 6, 10
- orbit, 11
- order
 - of a projective plane, 6
 - of an affine plane, 6
- pair
 - admissible, 23
 - unimodular, 25
- Pappos configuration, 5
- parallel class, 51
- parallel lines, 6
- parallel points, 27, 38, 50
- parallel spears, 19
- parallelism, 19
- parameters of a DD, 4, 8
- partial affine space, 40
- permutation, 11
- permutation representation, 11
- plane
 - affine, 6
 - projective, 6
- point, 4, 21, 23
 - ideal, 16
 - improper, 28
 - proper, 28
- point class, 4
 - extended, 17
- point group, 5
- points
 - distant, 26
 - neighbouring, 27
 - parallel, 27, 38, 50
- pointwise stabilizer, 12
- primitive group action, 12
- projective line
 - complex, 21
 - dual of a, 23
 - over a field, 22
 - over a ring, 22
- projective linear group, 28
- projective plane, 6
 - order of a, 6
- projectivity, 28
- proper Jordan homomorphism, 45
- proper point, 28
- \mathcal{R} -transversal subset, 3
- \mathcal{R} -transversal t -tuple, 14
- regular DD, 5
- regular group action, 11
- regular octahedron, 6, 10
- relative difference set, 18
- representation, 11
 - faithful, 11
- right inverse, 20
- right invertible, 20
- right invertible element, 20
- right translation, 21
- right zero divisor, 21
- ring
 - centre of a, 28
 - Dedekind-finite, 21
 - left artinian, 34
 - local, 34
 - stable rank of a, 25
- rings
 - antihomomorphism of, 45
 - Jordan homomorphism of, 44
 - Jordan isomorphism of, 45
- setwise stabilizer, 12
- sharply transitive group action, 11
- simple DD, 4
- Singer group, 18
- skew field, 21
- space
 - partial affine, 40
- spear, 19
- spears
 - parallel, 19
- stabilizer
 - pointwise, 12
 - setwise, 12
- stable rank of a ring, 25
- standard basis, 22
- standard chain, 30
- starter block, 13
- subgroup
 - elementary, 25
- subset
 - \mathcal{R} -transversal, 3
- superharmonic tetrad, 47
- symmetric group, 11
- t -homogeneous group action, 12
- t -transitive group action, 11
- t -tuple

- \mathcal{R} -transversal, 14
- tangency relation, 19
- tetrad
 - equianharmonic, 47
 - harmonic, 47
 - superharmonic, 47
- theorem
 - of Wedderburn (on finite fields), 39
 - Wedderburn principal, 43
 - Wedderburn–Artin, 52
- topological circle plane, 40
- transitive group action, 11
- translation
 - right, 21
- translation DD, 17
- transversal DD, 5
- twisted dual numbers, 35, 48

- unimodular pair, 25
- unit, 21

- vector, 22

- weak chain space, 40
- Wedderburn principal theorem, 43
- Wedderburn theorem (on finite fields), 39
- Wedderburn–Artin theorem, 52

- zero divisor
 - left, 21
 - right, 21