DIVISIBLE DESIGNS, LAGUERRE GEOMETRY, AND BEYOND

H. Havlýček

UDC 512.55

Abstract. In this paper, we bring together design theory and projective geometry over a ring. Both disciplines are well established, but the results on the interaction between them are rare and are scattered over the literature. Our main goal is to present the basics from either side, to develop, or at least sketch, the principal connections between them, and to make recommendations for further reading.

CONTENTS

Chapter 1. Introduction ....................................... 883
Chapter 2. Divisible Designs ................................. 883
  2.1. Basic Concepts and First Examples ..................... 884
  2.2. Group Actions ........................................ 890
  2.3. Spera’s Theorem ...................................... 891
  2.4. Divisible Designs and Constant Weight Codes .......... 894
  2.5. Notes and Further References ........................ 895
Chapter 3. Laguerre Geometry ............................... 896
  3.1. Real Laguerre Geometry ............................. 896
  3.2. Affine and Projective Line over a Ring ................. 897
  3.3. Distant Relation .................................... 902
  3.4. Chain Geometries .................................. 904
  3.5. Local Rings, Local Algebras, and Laguerre Algebras .... 907
  3.6. Notes and Further References ........................ 912
Chapter 4. Divisible Designs via \( \text{GL}_2 \)-Actions .......... 912
  4.1. How to Choose a Base Block .......................... 912
  4.2. Transversal Divisible Designs from Laguerre Algebras ... 913
  4.3. Divisible Designs from Local Algebras ................. 914
  4.4. Other Kinds of Blocks ................................ 916
  4.5. Notes and Further References ........................ 918
Chapter 5. An Outlook: Finite Chain Geometries ............. 918
  5.1. Parallelism Based on the Jacobson Radical ............. 919
  5.2. Counting the Point Set ............................. 920
  5.3. Divisible Designs versus Finite Chain Geometries ...... 921
    References ........................................... 921

Translated from Sovremennaya Matematika i Ee Prilozheniya (Contemporary Mathematics and Its Applications), Vol. 75, Algebra and Geometry, 2011.

1072–3374/12/1866–0882 © 2012 Springer Science+Business Media New York
Chapter 1

INTRODUCTION

This is a revised and updated version of our lectures notes [60] from the Summer School on Combinatorial Geometry and Optimization 2004 “Giuseppe Tallini,” which took place at the Catholic University of Brescia, Italy.

In these 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, to develop, or at least sketch, the principal connections between them, and to make recommendations for further reading. There is no attempt to provide encyclopedic coverage with expansive notes and references.

In Chap. 2, we start from 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 Chap. 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 only in finite rings, 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.** Assume 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 that \( v > 0 \) and \( s > 0 \), so that 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 \( \lambda_2 \).

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 \( 2-(s,k,\lambda_2) \)-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 \( s, k, \lambda_2, \) and \( v \).

**2.1.2.** Throughout this chapter, we assume that \( X \) is a finite set with an equivalence relation \( R \subset X \times X \). We denote by \([x]\) the \( R \)-equivalence class of \( x \in X \) and define

\[
S := \{ [x] | x \in X \}.
\]  

(2.1.1)

A subset \( Y \) of \( X \) is called \( R \)-transversal if

\[
\#(Y \cap [x]) \leq 1 \quad \forall x \in X.
\]

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 Sec. 2.1.5).

**2.1.3. Definition.** A triple \( D = (X, B, S) \) is called a \( t-(s,k,\lambda_t) \)-divisible design if there exist positive integers \( t, s, k, \) and \( \lambda_t \) such that the following axioms hold:

(A) \( B \) is a set of \( R \)-transversal subsets of \( X \) with \( \#B = k \) for all \( B \in B \);

(B) \( \# [x] = s \) for all \( x \in X \);

(C) for each \( R \)-transversal \( t \)-subset \( Y \subset X \), there exist exactly \( \lambda_t \) elements of \( B \) containing \( Y \);

(D) \( t \leq v/s \), where \( v := \#X \).

Elements of \( X \) are called **points**, elements of \( B \) are called **blocks**, and elements of \( S \) are called **point classes**.

We will frequently use the abbreviation “DD” for “divisible design.” Sometimes, we will speak of a \( t \)-DD without explicitly mentioning the remaining parameters \( s, k, \) and \( \lambda_t \). According to our definition, a block is merely a subset of \( X \). Hence DDs that will be discussed are simple, i.e., we do not take into account the possibility of “repeated blocks” (cf. [14, p. 2] for that concept).
Since \( S \) is determined by \( R \) and vice versa, we sometimes also write a divisible design in the form \((X, B, R)\) rather than \((X, B, S)\).

\[ 2.1.4. \quad \text{Let us write down some basic properties of a } t-(s, k, \lambda t)-\text{DD. Since } s, t \geq 1, \text{ axiom (D) implies that} \]
\[ \#X = v \geq st \geq 1 \quad (2.1.2) \]
\[ \text{or, stated differently, that } X \neq \emptyset. \text{ From this and (B) we conclude that} \]
\[ \#S = \frac{v}{s} \geq 1. \quad (2.1.3) \]

Hence, by (D) and (B), there exists at least one \( R \)-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
\[ \#B =: b \geq 1. \quad (2.1.4) \]

So, since \( B \neq \emptyset \), we can derive from axiom (A) and (2.1.3) the inequality
\[ \#B = k \leq \frac{v}{s} \quad \text{for all } B \in \mathcal{B}. \quad (2.1.5) \]

\[ 2.1.5. \quad \text{A divisible design is said to be transversal if each block meets all point classes; otherwise it is called \textit{regular}. Hence a } t-(s, k, \lambda t)-\text{DD is transversal if and only if the equality holds in (2.1.5).} \]

During the last decades, there has been a change in terminology. Originally, the point classes of a DD were called \textit{point groups} and DDs carried the name \textit{group-divisible designs}. In order to avoid confusion with the algebraic term “group,” in [13] this name was changed to read \textit{group-divisible designs}. We shall not use any of these phrases.

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

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 \( R \)-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 \( \mathcal{D} = (X, B, S) \).

\[ 2.1.7. \quad \text{Examples. We present some examples of DDs.} \]

\( a \) We consider the \textit{Pappos configuration} in the real projective plane which is formed by 9 points and 9 lines according to Fig. 1. We obtain a \( 2-(3,3,1) \)-DD, say \( \mathcal{D} \), as follows. Let
\[ X := \{p_1, p_2, p_3, q_1, q_2, q_3, r_1, r_2, r_3\}, \]
i.e., \( v = 9 \). By definition, blocks are 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 exists a unique block containing them. So \( t = 2 \) and \( \lambda_2 = 1 \). This DD is transversal.

\( b \) Let us take a \textit{regular octahedron} in the Euclidean 3-space (Fig. 2), and let us turn it into a DD as follows. Denote by \( X \) the set of all \( v = 6 \) vertices of the octahedron. For all \( p, q \in X \), we set \( p \ R q \) if and only if \( p \) and \( q \) are opposite vertices. Hence \( s = 2 \). The blocks are defined as the triangular faces, whence \( k = 3 \). Thus, we obtain a transversal \( 3-(2,3,1) \)-divisible design.

885
(c) Our next example is the projective plane of order 3, which is depicted in Fig. 3 (left). It is a 2-(1, 4, 1)-DD with \( v = 13 \) points. There are 13 blocks; they are given by subsets of the point set that consist of \( k = 4 \) points on a common curve. (Some of these curves are segments, others are not.) There are 13 point classes since \( s = 1 \) means that all point classes are singletons.

We shall not need the definition of a finite projective plane and refer to [14, p. 6]. However, let us add 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 3, then we obtain the affine plane of order 3. 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 [14, 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 Fig. 3(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 Fig. 3, bold vertical segments represent the point classes.

(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 Fig. 4).

It is easy to verify that the 3-DD from Example 2.1.7(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.
2.1.8. Theorem. Let $\mathcal{D}$ be a $t-(s, k, \lambda_t)$-DD with $t \geq 2$ and $i$ be an integer such that $1 \leq i \leq t$. Then $\mathcal{D}$ is also an $i-(s, k, \lambda_i)$-DD with

$$
\lambda_i = \lambda_t \cdot \frac{{vs^{-1} - i \choose t - i} s^{t-i}}{{k - i \choose t - i}}.
$$

(2.1.6)

Proof. We fix a 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 one hand, let us single out one of the $\lambda_i$ blocks containing $I$. Then there are

$$
{vs^{-1} - i \choose t - i}
$$

possibilities to choose a $Y$ within that particular block.

On the other hand, we select an arbitrary $Y$ amount as follows. First, we choose $t - i$ point classes out of the $vs^{-1} - i$ point classes that are disjoint from $I$ (cf. (2.1.3)), and then choose in each of these point classes a single point (out of $s$). Hence there are precisely

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

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

Altogether, we obtain

$$
\lambda_i \cdot {k - i \choose t - i} = \lambda_t \cdot {vs^{-1} - i \choose t - i} s^{t-i},
$$

(2.1.7)

which completes the proof.
2.1.9. Theorem 2.1.8 enables us to calculate several other parameters of a \( t-(s,k,\lambda_t) \)-DD. Letting \( i = 0 \) in formula (2.1.6) provides the number of blocks, i.e.,

\[
b := \# B = \lambda_t \left( \frac{v{s^{-1}}}{t} \right)^s t.
\] (2.1.8)

Likewise, for \( i = 1 \) we obtain the number

\[
r := \lambda_1
\] (2.1.9)

of blocks through a point, which is therefore a constant. Provided that \( i = t - 1 \), formula (2.1.6) reads

\[
\lambda_{t-1} = \lambda_t \frac{v - st + s}{k - t + 1}.
\] (2.1.10)

By Theorem 2.1.8, formula (2.1.10) remains valid if \( t \) is replaced by an integer \( t' \), subject to the condition \( 1 \leq t' \leq t \). Hence we infer the equation

\[
bp = rv
\] (2.1.11)

by setting \( t' = 1 \). For \( t \geq 2 \) we may let \( t' = 2 \), which gives

\[
r(k - 1) = \lambda_2 (v - s).
\] (2.1.12)

The last two equations are just particular cases of formula (2.1.7).

2.1.10. A divisible design with \( s = 1 \) is called a design (we refer the reader to [14, 15, 48, 80, 95]. In design theory, the parameter \( s \) is not taken into account, and a \( t-(1,k,\lambda_t) \)-DD with \( v \) points is often called a \( t-(v,k,\lambda_t) \)-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 3 and 2. 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 \( D = (X,B,S) \) is a \( t-(s,k,\lambda_t) \)-DD and \( D' = (X',B',S') \) is a \( t'-(s',k',\lambda_{t'}) \)-DD, then an isomorphism is a bijection

\[
\varphi : X \rightarrow X' : p \mapsto p^\varphi
\]

such that

\[
B \in B \iff B^\varphi \in B',
\] (2.1.13)

\[
S \in S \iff S^\varphi \in S'.
\] (2.1.14)

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

$$v = v',\quad s = s',\quad k = k'.$$

However, in view of Theorem 2.1.8, we have $t \neq t'$. Thus, we impose the additional 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,

$$t = t',\quad \lambda_t = \lambda_{t'}.$$

2.1.13. Condition (2.1.14) in the definition of an isomorphism can be replaced by the seemingly weaker but nevertheless equivalent condition

$$(2.1.15) \quad S \in \mathcal{S} \quad \Rightarrow \quad S^\varphi \in \mathcal{S}'.$$

Assume that a bijection $\varphi : X \rightarrow X'$ satisfying (2.1.15) is given. If $S^\varphi \in \mathcal{S}'$ for some subset $S$ of $X$, then there is $x \in S$. Hence $x^\varphi \in S^\varphi \cap [x]^\varphi$ with $[x]^\varphi \in \mathcal{S}'$ by (2.1.15). Since two equivalence classes with a common element are identical, we obtain $S^\varphi = [x]^\varphi$ and, finally, $S = [x] \in \mathcal{S}$. In contrast to this result, the equivalence sign in (2.1.13) is essential (cf. Example 2.1.14 below).

We may even drop condition (2.1.14) 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 (2.1.13) 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 $x, y \in X$.

2.1.14. Example. 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 (see Fig. 5). For both DDs, the point classes are 2-sets of opposite vertices. However, the blocks are different. First, we take all 8 triangular faces as blocks (Fig. 5, left). This gives a 2-(2,3,2)-DD which is also a 3-DD (cf. Example 2.1.7(b)). Second, only four triangular faces (given by the shaded triangles in Fig. 5, right) are considered as blocks, so that a 2-(2,3,1)-DD is obtained.

![Fig. 5. Two nonisomorphic 2DDs from an octahedron](image)

Observe that the identity mapping $\text{id}_X$ 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.

2.1.15. Exercise. Which of the DDs from Examples 2.1.7 and 2.1.14 are isomorphic?
2.2. Group Actions

2.2.1. Recall that all bijections (or permutations) of a finite set $X$ form the symmetric group $S_X$. If $G$ is an arbitrary group, then a homomorphism

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

is called a permutation representation of $G$. In this case, we say that the group $G$ acts on $X$ via $\alpha$. In fact, each $g \in G$ yields the bijection $g^\alpha : X \to X : x \mapsto x(g^\alpha)$.

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

$$x^{(gh)} = (x^g)^h \quad \forall x \in X, \quad \forall g, h \in G.$$

Provided that $\alpha$ is injective, the representation is called faithful. So for a faithful representation, we have $\ker \alpha = \{1_G\}$ as its kernel, and we can identify $G$ with its image $G^\alpha$. 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 assume that $G$ acts on $X$ (via $\alpha$).

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 act 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 strictly transitive. If $G$ acts 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 $G$ also acts in a natural way on certain other sets which are associated with $X$. For example, for every nonnegative integer $t$, the group $G$ acts on the $t$-fold product $X^t$ by

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

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

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

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

If this action is transitive, then the group $G$ is said to act $t$-homogeneously on $X$.

Similarly, $G$ acts on the power set of $X$.

In the sequel, we consider $t$-homogeneous and $t$-transitive group actions. Thus the following result deserves our interest, even though we are not going to use it.

2.2.3. Theorem (D. Livingstone and A. Wagner, [96]). Assume 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 [134] for a short proof, [50, p. 92], and [97, Sec. 16].

\[^1\]Most of the results from this section remain valid for an infinite set $X$. 

890
2.2.4. An equivalence relation $\mathcal{R}$ on $X$ is said to be $G$-invariant if
\[ x \mathcal{R} y \Rightarrow x^g \mathcal{R} y^g \quad \forall x, y \in X, \quad \forall g \in G. \tag{2.2.1} \]

Then
\[ x \mathcal{R} y \iff x^g \mathcal{R} y^g \quad \forall x, y \in X, \quad \forall g \in G \tag{2.2.2} \]
follows immediately by applying (2.2.1) to $x^g \mathcal{R} y^g$ and $g^{-1}$. Obviously, the finest and coarsest equivalence relations on $X$, i.e., the diagonal
\[ \text{diag}(X \times X) = \{(x, x) \mid x \in X\} \]
and $X \times X$, are $G$-invariant equivalence relations on $X$.

Now we assume 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.

Assume that $G$ acts imprimitively on $X$. A subset $S \subseteq X$ 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 $Y \subseteq X$, the set-wise stabilizer of $Y$ in $G$ is the set $G_Y$ of all $g \in G$ satisfying $Y^g = Y$. This stabilizer is a subgroup of $G$. The pointwise stabilizer of $Y \subseteq X$ 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 set-wise 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
\[ \#y^G = \frac{\#G}{\#G_y}. \tag{2.2.3} \]
It links the 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 the reader to [82, pp. 71–79] for a more systematic account on group actions.

2.3. Spera’s Theorem

2.3.1. The possibility of constructing divisible designs is given by the following theorem, which is due to A. G. Spera (see [124, Proposition 3.2]). For a similar construction for designs, see [14, 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) $B_0$. Its orbit under the action of $G$ will be our set of blocks.

2.3.2. Theorem. Let $X$ be a finite set endowed with an equivalence relation $\mathcal{R}$; the corresponding partition is denoted by $\mathcal{S}$. Moreover, assume 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 $s$;
(c) the group $G$ acts transitively on the set of $\mathcal{R}$-transversal $t$-subsets of $X$ for some positive integer $t \leq \#\mathcal{S}$. 

891
Finally, let $B_0$ be a $R$-transversal $k$-subset of $X$ with $t \leq k$. Then

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

is a $t$-$(s, k, \lambda_t)$-divisible design, where

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

(2.3.1)

and $G_{B_0} \subset G$ denotes the set-wise stabilizer of $B_0$.

**Proof.** First, let $\#X = v$. Since $B_0$ is $R$-transversal, we have

$$0 < t \leq k = \#B_0 \leq \#S = \frac{v}{s}$$

so that axiom (D) in the definition of a DD is satisfied. Also, we obtain $s, k > 0$.

Since $B_0$ is an $R$-transversal $k$-set, so is every element of $B_0^G$ defined by (2.2.2). 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 owing to our assumption $t \leq k$. Let $\lambda_t > 0$ be the number of blocks containing $Y$. Given an arbitrary $R$-transversal $t$-subset $Y' \subset X$, there is $g \in G$ with $Y' = Y^g$, since $Y \subset B_0$ is $R$-transversal. This $g$ takes the $\lambda_t$ distinct blocks through $Y$ to $\lambda_t$ distinct blocks through $Y'$. Similarly, the action of $g^{-1}$ shows that there cannot be more than $\lambda_t$ blocks containing $Y'$.

Altogether, we have verified the axioms of a divisible design. Yet, it remains to calculate the parameter $\lambda_t$. By definition, the group $G$ acts transitively on the set $B$ of blocks. By Eq. (2.2.3), the number of blocks is

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

whence, by (2.1.8), we obtain

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

which proves (2.3.1).

Note that in [124] our condition (b) is missing. On the other hand it is very easy to show that (b) cannot be dropped without affecting the assertion of the following theorem.

**2.3.3. Example.** Let $X = \{1, 2, 3\}$, $S = \{\{1\}, \{2, 3\}\}$, and let $G$ be the subgroup of the symmetric group $S_3$ 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 \((x_1, x_2, \ldots, x_t) \in X^t\) is called \(R\)-transversal if its entries belong to \(t\) distinct point classes.

2.3.5. Corollary. Theorem 2.3.2 remains true, mutatis mutandis, if assumption (b) is dropped and assumption (c) is replaced by the following:

\[(c_1)\] the group \(G\) acts transitively on the set of \(R\)-transversal \(t\)-tuples of \(X\) for some positive integer \(t \leq \#S\).

Proof. We observe that each \(R\)-transversal \(t\)-subset \(Y\) gives rise to \(t!\) mutually distinct \(R\)-transversal \(t\)-tuples with entries from \(Y\). Since \(0 < t \leq \#S\), it is obvious from \((c_1)\) that \(G\) acts transitively on the set of \(R\)-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 \(R\) are of the same size, we prove that \(G\) acts transitively on \(S\). Since assumption (a) remained unchanged, formula (2.2.2) can be shown as before. This implies that, for all \(S \in S\) and all \(g \in G\), the image \(S^g\) is an equivalence class; hence \(G\) acts on \(S\). For this action to be transitive, it suffices to establish that \(G\) acts transitively on \(X\). So let \(x_1\) and \(x'_1\) be arbitrary elements of \(X\). We infer from \(0 < t \leq \#S\) that there exist \(R\)-transversal \(t\)-tuples \((x_1, x_2, \ldots, x_t)\) and \((x'_1, x'_2, \ldots, x'_t)\). By \((c_1)\), there is at least one \(g \in G\) which takes the first to the second \(t\)-tuple. Therefore, \(x'_1 = x_1\).

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

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

\[(b_1)\] \(G\) acts transitively on \(S\).

Another possibility to alter the conditions in Theorem 2.3.2 is as follows (see [117, Remark 2.1]). Suppose that condition (b) is dropped and (c) is replaced by the following condition:

\[(c_2)\] the group \(G\) acts transitively on the set of \(R\)-transversal \(t\)-subsets of \(X\) for some positive integer \(t < \#S\).

In this case, let \(y_1, y_2, \ldots, y_w\), where \(w = \#S\), be a system of representatives for the equivalence classes of \(R\) such that

\[#y_1 \leq #y_2 \leq \cdots \leq #y_w\].

We claim that \((c_2)\) implies

\[#y_1 = #y_2 = \cdots = #y_w\],

which in turn is equivalent to \((b)\). By \((c_2)\), we have \(0 < t < w\) so that

\(Y := \{y_1, y_2, \ldots, y_t\}, \quad Y' := \{y_2, y_3, \ldots, y_t, y_w\}\)

are \(R\)-transversal \(t\)-subsets of \(X\). By the action of \(G\) on \(S\), the \(t\)-tuple

\(#y_2, #y_3, \ldots, #y_t, #y_w\)

arises from

\(#y_1, #y_2, \ldots, #y_t\)

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 \( S \).

### 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, e.g., [75] for an introduction to this subject). Let us write

\[
Z_m := \{0, 1, \ldots, m\} \subset \mathbb{Z}, \quad \text{where } m \geq 1.
\]

Let \( n \) be a positive integer. The **Hamming distance** of \( x = (x_1, x_2, \ldots, x_n) \) and \( y = (y_1, y_2, \ldots, y_n) \in Z_m^n \) is defined as the number of indices \( i \in \{1, 2, \ldots, n\} \) such that \( x_i \neq y_i \). It turns \( Z_m^n \) into a metric space. The **Hamming weight** of an element \( x \in Z_m^n \) is its Hamming distance from \((0, 0, \ldots, 0)\) or, stated differently, the number of its nonzero entries.\(^3\)

For our purposes, we define an **automorphism** of \( Z_m^n \) as a product of any two mappings of the following form. First we apply the bijection \( Z_m^n \to Z_m^n : (x_1, x_2, \ldots, x_n) \mapsto (x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \) where each \( \alpha_i \) is a permutation of \( Z_m \), and then the bijection \( Z_m^n \to Z_m^n : (x_1, x_2, \ldots, x_n) \mapsto (x_1^{\alpha}, x_2^{\alpha}, \ldots, x_n^{\alpha}), \) where \( \alpha \) is a permutation of \( \{1, 2, \ldots, n\} \). All such automorphisms form a group under the composition of mappings. Every automorphism preserves the Hamming distance. The Hamming weight is preserved if and only if \((0, 0, \ldots, 0)\) remains fixed.

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

Let \( C_1, C_2 \subset Z_m^n \) be codes. An **isomorphism** is an automorphism of \( Z_m^n \) taking \( C_1 \) to \( C_2 \). An **automorphism** of a code is defined similarly.

#### 2.4.2. Now we present the essential construction. Assume that \( D = (X, B, S) \) is a \( t-(s, k, \lambda_1) \)-DD with \( n := v/s \) 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 \( S \in S \) we write \( \tilde{S} \) for the corresponding **extended point class**. Any block \( B \in B \) has \( k \leq s \) points. We turn it into an **extended block** \( \tilde{B} \) 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

\[
\psi : \tilde{X} \to \{1, 2, \ldots, n\} \times Z_m
\]

such that for each point class \( S \in S \), there exists an index \( i \in \{1, 2, \ldots, n\} \) with

\[
S^{\psi} = \{i\} \times (Z_m \setminus \{0\}), \quad \tilde{S}^{\psi} = \{i\} \times Z_m.
\]

---

\(^2\)In Chap. 3, we use this symbol to denote the ring of integers modulo \( m \).

\(^3\)This terminology is in honor of R. W. Hamming whose fundamental paper on error-detecting and error-correcting codes appeared in 1950.
This means that under \( \psi \), the set \( \tilde{X} \setminus X \) of ideal points goes over to
\[
\{(i,0) \mid i \in \{1,2,\ldots,n\}\}.
\]
Furthermore, two points of \( \tilde{X} \) are in the same extended point class if and only if the first entries of their \( \psi \)-images coincide.

Now we are in a position to define the code of \( D \) (with respect to \( \psi \)) as the subset of \( \mathbb{Z}_m^n \) given by
\[
C(D) := \left\{(j_1,j_2,\ldots,j_n) \mid \exists B \in \mathcal{B} : \tilde{B}^\psi = \{(1,j_1),(2,j_2),\ldots,(n,j_n)\}\right\}.
\]
According to our construction, all codewords have weight \( k \), whence \( C(D) \) is in fact a constant weight code.

In general, \( \psi \) can be chosen in different ways. However, this will yield isomorphic codes. So the actual choice of \( \psi \) turns out to be immaterial. In [119], 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 where \( t = 2 \) and \( v = 2k \), the two groups are isomorphic [119, Theorem 3.1]. Also, if the automorphism group of \( D \) is “large,” then its corresponding code is well understood (see [51, 115, 119] 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 strictly transitive on \( X \) (see Sec. 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 [16, 74, 83, 109–114, 121, 122], and the references therein.

The more general class of “\((s,k,\lambda_1,\lambda_2)\)-translation DDs” is considered in [116, 123].

Another construction of these more general DDs uses a Singer group with a relative difference set (see [84]). 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 [124], 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 Chaps. 3 and 4. In this way, one obtains 3-divisible designs.

A higher-dimensional analog based on the projective space over a finite local algebra can be found in [125]; 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 L"uneburg planes and Suzuki groups (see [118, 127]). A more general setting, where \( G \) acts 2-transitively on a subset of the line at infinity, can be found in [43, 46, 117].
A class of DDs, where $G$ is an orthogonal group or a unitary group, is determined in [45]. It was pointed out in [55] that one particular case of this construction is—up to an isomorphism—a Laguerre geometry (see Sec. 3.5.13) which, by a completely different approach, appears already in [124].

In [44], 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.

Also, we refer to [126] for a discussion of transitive extensions of imprimitive groups. A generalization of Spera’s construction was exhibited in [54, 56]. It was put into a more general context in [38] as follows. Let a group $G$ act on some set $X$ and a starter $t$-\emph{DD} in $X$ be given. Then, under certain technical conditions, a new $t$-DD can be obtained via the action of $G$ on $X$.

**Chapter 3**

**LAGUERRE GEOMETRY**

3.1. Real Laguerre Geometry

3.1.1. The classical \emph{Laguerre geometry} is the geometry of spears and cycles in the Euclidean plane. A \emph{spear} is an oriented line and a \emph{cycle} is either an oriented circle or a point (a “circle with radius zero”). There is a \emph{tangency relation} between spears and cycles (see Fig. 6). Furthermore, there exists a \emph{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 nonparallel 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 E. N. Laguerre who used it to solve the following famous problem of Apollonius of Perga: Find all circles that touch three given circles without orientation (see, e.g., [102, 103]).

![Fig. 6. Two cycles with tangent spears, and a family of parallel spears](image)

3.1.2. In 1910, W. Blaschke showed that the set of spears is in one-one correspondence with the points of a circular cylinder of the Euclidean 3-space [17], now called the \emph{Blaschke cylinder}.\footnote{From the point of view of projective geometry, this is a quadratic cone without its vertex, whence it is also called the \emph{Blaschke cone}.} 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
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, Chap. 1,
Sec. 2], [6, Chap. 4], [53, Chap. 15A], [67, 105, 108, 135, 136]. Note that in [135] the term inversive
Galileian plane is used instead.

3.1.4. Our construction of divisible designs in Chap. 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 (see [7] for a different generalisation of Laguerre geometry).

3.2. Affine and 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 unitally 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 \( l \in R \) with \( ls = 1 \), then \( s \) is said to be left invertible and \( l \) is called a left inverse of \( s \).
Right invertible elements and right inverses are defined similarly.

If \( s \) has both a left inverse \( l \) and a right inverse \( r \), then

\[
  l = l1 = l(sr) = (ls)r = 1r = r. \tag{3.2.1}
\]

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 nonzero element \( r \in R \) such that \( sr = 0 \).
Such \( s \) 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. Assume that elements \( a, b \in R \) with \( ab = 1 \) are given. Hence

\[
  y = y1 = (ya)b \quad \forall y \in R.
\]

This implies that the right translation \( \rho_b : R \to R : x \to xb \) is surjective. Moreover, \((ba - 1)b = \]
\( b1 - b = 0 \). Thus, whenever we are able to show that \( \rho_b \) 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., [87]). In fact, in most of our examples this condition will be satisfied.

3.2.3. Exercise. 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, and some are equivalent only for certain classes of rings. A short survey on this topic is included in [89].

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 $\infty$ is an arbitrary new element. Intuitively, we think of $\infty$ as being $\frac{a}{1}$, where $a \in \mathbb{C}$ is nonzero. For all $a \in \mathbb{C}$, we have $\frac{a}{1} = \frac{ax}{x}$, $x \neq 0$. Thus every fraction $\frac{a}{b}$ other than “$0$” 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 the case where $F$ is noncommutative, 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

$$a \leftrightarrow F(a, 1) = \{x(a, 1) \mid x \in F\} \quad \forall a \in F, \quad \infty \leftrightarrow F(1, 0). \quad (3.2.2)$$

More formally, the projective line over $F$ appears as the set of one-dimensional subspaces of the left vector space $F^2$. Every nonzero 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 $(b_1, b_2, \ldots, b_n)$ of vectors in $M$ is called a basis provided that the mapping

$$R^n \to M : (x_1, x_2, \ldots, x_n) \mapsto \sum_{i=1}^{n} x_i b_i \quad (3.2.3)$$

is a bijection. In this case, $M$ is called free of rank $n$. It is important to note that this rank $n$ is in general not uniquely determined by $M$ (see, e.g., [88, 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 (3.2.3), we replace $M$ by $R^2$. 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 the same way as we did for a field in (3.2.2). 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. This point of view is adopted, for example, in [42, p. 1128], where a distinction between “points” and “free points” is made, and in [52]. Yet, also here a problem arises: By following this approach we would get, in general, “far too much points” for our purposes.

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 $GL_2(R)$ of invertible $2 \times 2$-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 led to the following strict definition.

**3.2.7. Definition.** The projective line over \( R \) is the orbit

\[
P(R) := \left( R(1, 0) \right)^{\text{GL}_2(R)}
\]

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

We refer to [40, 1.3] and [67, Definition 1.2.1] for an equivalent definition which avoids using coordinates (cf. also [34] 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 said to be admissible (over \( R \)) if there exist \( c, d \in R \) such that \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(R) \). So we have

\[
\mathbb{P}(R) = \{ R(a, b) \subset R^2 \mid (a, b) \text{ admissible} \}.
\] (3.2.4)

Thus, our definition of the projective line relies on admissible pairs. However, there may also be nonadmissible 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 Sec. 3.2.2). We refer to [31], 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.

**3.2.9. Theorem.** 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 \( \gamma \in \text{GL}_2(R) \) with first row \( (a, b) \). Thus,

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

Since \( (a', b') \) 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 \( y(u, 0) = (1, 0) \) 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 \( \delta \), say, with first row \((u, 0)\). Then

\[
\begin{pmatrix}
1 & 0 \\
0 & 1 \\
\end{pmatrix} =
\begin{pmatrix}
u & 0 \\
* & *
\end{pmatrix}
\begin{pmatrix}
z & * \\
* & *
\end{pmatrix} =
\begin{pmatrix}
uz & * \\
* & *
\end{pmatrix}
\delta^{-1}
\]

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

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

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 \( x \in R \),
\[
\begin{pmatrix}
  x & 1 \\
  1 & 0
\end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -x \end{pmatrix} \quad \in \text{GL}_2(R),
\begin{pmatrix}
  1 & x \\
  0 & 1
\end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(R).
\] (3.2.5)

Hence the projective line over \( R \) contains all points \( R(x,1) \) with \( x \in R \). If \( x, y \in R \) are different, then \( R(x,1) \neq R(y,1) \). Similar 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
\[
\# \mathbb{P}(R) \geq \# R + \# (R \setminus R^*).
\] (3.2.6)

We see below that for certain rings the projective line contains even more points (cf. Theorem 3.5.5 and Corollary 3.5.6).

3.2.11. Example. 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 \( \{0\}, 2\mathbb{Z}_6, 3\mathbb{Z}_6, \) and \( \mathbb{Z}_6 \) (cf. [82, 2.6] for further details).

As \( x \) varies in \( \mathbb{Z}_6 \), from the first matrix in (3.2.5) we obtain six points
\[
\mathbb{Z}_6(0,1), \mathbb{Z}_6(1,1), \ldots, \mathbb{Z}_6(5,1),
\]
and, for \( x \in \mathbb{Z}_6 \setminus \mathbb{Z}_6^* \), from the second part of (3.2.5), 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
\[
\begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \in \text{GL}_2(\mathbb{Z}_6),
\]
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 nonadmissible pairs.

3.2.12. A pair \((a,b) \in R^2\) is said to be 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 \( \gamma \in \text{GL}_2(\mathbb{R}) \) and assume that the first column of \( \gamma^{-1} \) reads (\( x,y \)). We read off from \( \gamma \gamma^{-1} = 1 \), where \( 1 \) denotes the identity matrix in \( \text{GL}_2(\mathbb{R}) \), that every admissible pair is unimodular. We note that
\[
(a,b) \in R^2 \text{ is unimodular over } R \quad \Rightarrow \quad (a,b) \text{ is admissible over } R
\] (3.2.7)
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 \((-y, x)\). Benz [5] considers only commutative rings and defines the projective line using unimodular pairs.

In fact, (3.2.7) also holds for certain noncommutative rings [67, Proposition 1.4.2], namely for rings of stable rank 2, but we shall not give a definition of this concept here. The Dutch geometer F. D. Veldkamp pointed out the significance for geometry of the stable rank of a ring. We refer to [129, 131] 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 (3.2.7) is not valid can be found in [33, 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 one 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 Sec. 3.2.10. Some of the subsequent examples come from the elementary subgroup of \(GL_2(R)\), i.e., the subgroup generated by elementary matrices (see [47] for the algebraic background and [33] for the geometry behind).

3.2.14. Examples. Let \(\gamma\) be a \((2 \times 2)\)-matrix over \(R\).

(a) If all entries of \(\gamma\) 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, \(\gamma^{-1}\) can be described in terms of \(\det \gamma\) and the cofactor matrix of \(\gamma\) as in the case of a commutative field.

(b) A diagonal matrix \(\gamma = \text{diag}(a, b)\) is invertible if and only if \(a\) and \(b\) are units.

(c) If a lower triangular \((2 \times 2)\)-matrix \(\gamma\) is given, then

\[
\gamma =: \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \quad \in GL_2(R)
\]

(3.2.8)

We know from (3.2.5) that the second matrix on the right-hand side is invertible.

Now we assume that \(a\) or \(d\) is a unit. By (b) and (3.2.8), \(\gamma\) is invertible if and only if \(a\) and \(d\) are units. In this case,

\[
\gamma^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -d^{-1}ca^{-1} & d^{-1} \end{pmatrix}.
\]

(3.2.9)

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

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

\[
\gamma := \begin{pmatrix} a & 0 \\ 1-ba & b \end{pmatrix} \in GL_2(R), \quad \gamma^{-1} = \begin{pmatrix} b & 1-ba \\ 0 & a \end{pmatrix}.
\]

This means that for rings that 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. Distant Relation

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

\[
\triangle := \left( R(1, 0), R(0, 1) \right)^{\text{GL}_2(R)}.
\]

Setting \( p = R(a, b) \) and \( q = R(c, d) \) and taking into account Theorem 3.2.9, we have

\[
p \triangle q \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(R).
\]

(3.3.1) The distant relation is symmetric since exchanging two rows in an invertible matrix does not influence its invertibility. In addition, \( \triangle \) is anti-reflexive since \( R(1, 0) \neq R(0, 1) \) implies that distant points are distinct\(^5\). However, in general distinct points need not be distant (cf. Theorem 3.3.7 below).

Nondistant points (\( \not\triangle \)) are also called \( \text{neighboring} \) or \( \text{parallel} \) (see, e.g., [5, 67, 131]). However, in these lectures we shall use the term “parallel” in a different sense which will be explained in Sec. 5.1.1. The two notions “parallel” and “neighboring” coincide precisely when \( R \) is a local ring (see Theorem 5.1.4 and our preliminary definition in Sec. 3.5.8).

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

3.3.2. Theorem. The group \( \text{GL}_2(R) \) acts \( 3\triangle \)-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 (3.2.5). Also, let \( R(a, b) \) be a point which is distant to \( R(1, 0) \) and \( R(0, 1) \). Consequently,

\[
\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \in \text{GL}_2(R), \quad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(R).
\]

Hence \( a, b \in R^* \) by Example 3.2.14(c). But this means that the matrix \( \text{diag}(a, b) \in \text{GL}_2(R) \) 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 \( \gamma \in \text{GL}_2(R) \) 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 \( r^\gamma \) 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 \( \Omega \), say, of \( \{R(1, 0), R(0, 1), R(1, 1)\} \) under the action of \( \text{GL}_2(R) \) on the projective line \( \mathbb{P}(R) \). If \( \gamma \) lies in this stabilizer, then \( \gamma = \text{diag}(a, b) \) since each of \( R(1, 0) \) and \( R(0, 1) \) must coincide with its image. By Example 3.2.14(b), \( a \) and \( b \) are units in \( R \). Moreover, we conclude from \( R(1, 1)^\gamma = R(a, b) = R(1, 1) \) that \( a = b \). These two conditions are also sufficient. Therefore,

\[
\Omega = \{ \text{diag}(a, a) \mid a \in R^* \}.
\]

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

\[
R(1, x)^\gamma = R(a, xa) = R(1, a^{-1}xa) \quad \forall x \in R.
\]

\(^5\)This 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 
\[ Z(R) := \{ a \in R \mid ax = xa \ \forall x \in R \} \]
is the center of \( R \); it is a subring of \( R \). Therefore, \( a \) must be a unit in the center 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 center of \( \text{GL}_2(R) \), viz.
\[ Z(\text{GL}_2(R)) = \{ \beta \in \text{GL}_2(R) \mid \beta \xi = \xi \beta \ \forall \xi \in \text{GL}_2(R) \} = \{ \text{diag}(a, a) \mid a \in Z(R)^* \}. \] (3.3.3)

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 \( \mathbb{P}(R) \).

3.3.4. Theorem. The following statements are equivalent.
(a) \( \text{PGL}_2(R) \) acts strictly transitively on the set of triples of mutually distant points.
(b) The group \( R^* \) of units in \( R \) is contained in the center \( Z(R) \).

Proof. The result is an immediate consequence of (3.3.2) and (3.3.3).

The interested reader should also compare this result with the characterizations given in [67, Proposition 1.3.4].

3.3.5. Given a point \( p \in \mathbb{P}(R) \), let
\[ \triangle(p) := \{ x \in \mathbb{P}(R) \mid x \triangle p \}. \]
If we consider \( \mathbb{P}(R) \) as the set of vertices of the distant graph, i.e., the unordered graph of the symmetric relation \( \triangle \), then \( \triangle(p) \) is just the neighborhood 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 \( \triangle(p) \) 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 neighborhood of \( R(1, 0) \), a point which is also denoted by the symbol \( \infty \). By Example 3.2.14(c), a point \( R(a, b) \) is in \( \triangle(\infty) \) precisely when \( b \in R^* \). But then, without loss of generality, we may assume that \( b = 1 \) since
\[ R(a, b) = R(b^{-1}a, 1). \]
The embedding
\[ R \to \mathbb{P}(R) : a \mapsto R(a, 1) \] (3.3.4)
maps the affine line over \( R \) injectively onto the subset \( \triangle(\infty) \) of the projective line over \( R \). We already met this embedding in Sec. 3.2.10. It shows that the neighborhood of any point has \#R elements.

By virtue of (3.3.4), we may even identify the affine line over the ring \( R \) with the subset \( \triangle(\infty) \). From
\[ \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ b & 1 \end{pmatrix} \]
follows that—in affine terms—two points \( a, b \in R \) are distant precisely when \( a - b \) is a unit.

3.3.6. Example. We continue the investigation of the projective line \( \mathbb{P}(\mathbb{Z}_6) \) (see Example 3.2.11).

In Fig. 7, each point of \( \mathbb{P}(\mathbb{Z}_6) \) is labelled by one of its admissible pairs. 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 neighborhood 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.

**3.3.7. Theorem.** 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

$$(0, 0) \neq (a, b) \notin R(c, d), \quad (0, 0) \neq (c, d) \notin R(a, b)$$

since a one-dimensional vector space is spanned by each of its nonzero 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 (3.3.1).

(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 nonzero element of $R$ is invertible or, stated differently, that $R$ is a field. \hfill \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. Now assume 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 center of $R$.

**3.4.2. Lemma.** The mapping

$$\mathbb{P}(K) \to \mathbb{P}(R) : K(k, l) \mapsto R(k, l)$$

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

**Proof.** The assertions are immediate from $\text{GL}_2(K) \subseteq \text{GL}_2(R)$. \hfill \square

The following definition was introduced by Bartolone [2] (for a systematic account, see [30]; for the particular case where $R$ is an algebra over $K$, cf. [5, 40, 67]).

**3.4.3. Definition.** 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 (3.4.1). A subset of $\mathbb{P}(R)$ is called a $K$-chain (or, in
short, a chain, \( K \) being understood) if it belongs to the set
\[
\mathcal{C}(K, R) := C_0^{\text{GL}_2(R)}.
\]
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 \( \text{GL}_2(R) \). Observe that we refrain from excluding the trivial case where \( R = K \).

3.4.4. If \( \Sigma(K, R) \) and \( \Sigma(K', R') \) are chain geometries, then an isomorphism is a bijection \( \varphi : \mathbb{P}(R) \to \mathbb{P}(R') \) 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 [67, 2.4.2] for the case of algebras).

3.4.5. Theorem. 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 Sec. 3.3.1, we know that \( p \triangle q \) implies \( p = R(1, 0)^\gamma \) and \( q = R(0, 1)^\gamma \) for some \( \gamma \in \text{GL}_2(R) \). Hence in this case \( p, q \in C_0^\gamma \subset \mathcal{C}(K, R) \).

Conversely, if \( p, q \in C_0^\gamma \subset \mathcal{C}(K, R) \), where \( \gamma \in \text{GL}_2(R) \), 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 \( \gamma \) preserves \( \triangle \), this proves the assertion.

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.

3.4.6. Theorem. 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 \( \gamma \in \text{GL}_2(R) \) 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 \( r \).

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

3.4.7. Theorem. Let \( D, D' \in \mathcal{C}(K, R) \) be chains. Furthermore, assume that \( p, q, r \in D \) and \( p', q', r' \in D' \), respectively, are 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 \( C_0 \). We set
\[
p_1 := p^{\gamma_1}, \quad q_1 := q^{\gamma_1}, \quad r_1 := r^{\gamma_1}.
\]
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
\[
p_1^{\gamma_2} = R(1, 0), \quad q_1^{\gamma_2} = R(0, 1), \quad r_1^{\gamma_2} = R(1, 1).
\]
Then we also have \( C_0^{\gamma_2} = C_0 \).

Define \( \gamma'_1 \) and \( \gamma'_2 \) accordingly. Then
\[
\gamma = \gamma_1 \gamma_2 \gamma'_2 \gamma'^{-1} \gamma_1^{-1}
\]
has the required properties. \( \square \)
Now it is easy to determine the number of chains containing three mutually distant points.

**3.4.8. Theorem.** 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 (3.3.2) that the subgroup

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

of \( GL_2(R) \) 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 \( R(1, 0), R(0, 1), \) and \( R(1, 1) \) are precisely the images \( C_0^\omega \), where \( \omega \) ranges in \( \Omega \). 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 \( \Omega \) is

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

So, by (2.2.3), 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 \( R^* = N \).

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

(a) Assume that \( K \) belongs to the center of \( R \), i.e., \( R \) is a \( K \)-algebra. Then, since \( K^* \) is in the center 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 3.4.9(a) are satisfied without imposing a condition on \( K \).

(c) Assume 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 [30, 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 \( (2 \times 2) \)-matrices over \( \mathbb{Z}_2 \). There are six invertible elements in this ring, namely,

\[
\begin{bmatrix}
1 & 0 \\
0 & 1 
\end{bmatrix}, \quad \begin{bmatrix}
1 & 0 \\
0 & 1 
\end{bmatrix}, \quad \begin{bmatrix}
0 & 1 \\
1 & 0 
\end{bmatrix}, \quad \begin{bmatrix}
0 & 1 \\
1 & 1 
\end{bmatrix}, \quad \begin{bmatrix}
1 & 1 \\
1 & 0 
\end{bmatrix}, \quad \begin{bmatrix}
1 & 1 \\
0 & 1 
\end{bmatrix}.
\]

The center of \( R \) is given by

\[ Z(R) = \{ \text{diag}(x, x) \mid x \in \mathbb{Z}_2 \}. \]

We set

\[ K := \left\{ \begin{bmatrix} x & y \\ y & x + y \end{bmatrix} \mid x, y \in \mathbb{Z}_2 \right\}. \]
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, \( K^* \not\subseteq \mathbb{Z}(R) \). Since \( \# R^* = 6 \), the multiplicative group \( K^* \) has index 2 in \( R^* \) and therefore is normal.

Now we 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 \( \Sigma(K, R) \).

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

**Proof.** Without loss of generality, we consider 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 \( C_0^\omega \), with \( \omega \in \Omega \) (cf. (3.3.2)). Given a matrix \( \text{diag}(a, a) \in \Omega \), we have

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

Therefore,

\[
\bigcap_{\omega \in \Omega} C_0^\omega = \{R(1, 0)\} \cup \bigcap_{a \in R^*} \{R(a^{-1}ka, 1) \mid k \in K\} = \{R(1, 0)\} \cup \{R(f, 1) \mid f \in F\},
\]

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

3.5. **Local Rings, Local Algebras, and Laguerre Algebras**

3.5.1. Let \( R \) be a ring. The *Jacobson radical* \( \text{rad} R \) of a ring \( R \) is the intersection of all maximal left (or right) ideals of \( R \). It is a two-sided ideal of \( R \); its elements can be characterized as follows:

\[
b \in \text{rad} R \iff 1 - ab \in R^* \quad \forall a \in R \iff 1 - ba \in R^* \quad \forall a \in R
\]

(see [87, pp. 53–54]).

Assume that \( R \) is *left Artinian*, 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 \( n \) (see [87, Theorem 4.12]). Consequently, \( \text{rad} R \) is actually a nilpotent ideal. This holds, in particular, if \( R \) is a finite ring (see [85] for further references on nilpotent rings).

3.5.2. A ring \( R \) is called a *local ring* if \( R \setminus R^* \) is an ideal\(^6\) of \( R \). There are several equivalent definitions of a local ring (cf. [87, 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 unique maximal left ideal of \( R \), we obtain

\[
\text{rad} R = R \setminus R^*.
\]

\(^6\)By 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 neighborhood of \( p \)) form a local ring. The nonunits in this ring are functions that vanish at \( p \) (cf. [120, p. 72]).
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
\[
a \in R^* \iff \overline{a} \in \overline{R}^*.
\]
(3.5.1)

Given a matrix \( \gamma = (\gamma_{ij}) \) with entries in \( R \), we put \( \overline{\gamma} := (\overline{\gamma_{ij}}) \). Then one can show as above that \( \gamma \in \text{GL}_m(R) \iff \overline{\gamma} \in \text{GL}_m(\overline{R}) \) (3.5.2)

holds for all natural numbers \( m \geq 1 \).

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 only at 0. 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 \( F \) since \( F \oplus \text{rad}\, R \) (the direct sum of additive groups) is a proper subgroup of \( (R,+) \).

3.5.4. Examples. We present several examples of local rings and local algebras.

(a) A trivial example of a local ring is a field.

(b) As was noted above, the classical example of a local ring is the ring of dual numbers over the field of real numbers. There are several ways to define it. For example, we may start from the polynomial ring \( \mathbb{R}[T] \) in the indeterminate \( T \). Consider the ideal \( (T^2) \) generated by \( T^2 \) and define the ring of 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
\[
a + b\varepsilon \quad \text{with} \quad a, b \in \mathbb{R}, \quad \text{where} \quad \varepsilon \notin \mathbb{R} \text{ and } \varepsilon^2 = 0.
\]

This example allows several generalizations that are discussed below.

(c) In Example (b) we may replace \( \mathbb{R} \) by any commutative field \( K \) and obtain 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 (noncommutative) 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:
\[
(a + b\varepsilon) * (c + d\varepsilon) := ac + (ad + bc\sigma)\varepsilon \quad \forall a, b, c, d \in K.
\]

This yields the ring \( K[\varepsilon;\sigma] \) of twisted dual numbers over \( K \). It is a local ring with \( K\varepsilon \) the ideal of all noninvertible elements. It cannot be an algebra over \( K \) even if \( K \) is commutative since \( K \) is not in the center 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 above, we set \( \varepsilon := T + (T^h) \), whence this ring is of the form
\[
K[\varepsilon] := K \oplus K\varepsilon \oplus K\varepsilon^2 \oplus \cdots \oplus K\varepsilon^{h-1} = \text{rad}\, K[\varepsilon].
\]
(f) Let $V$ be an $n$-dimensional vector space over a commutative field $K$. Then the exterior algebra

$$\bigwedge V = \bigoplus_{k=0}^{n} V^{k}$$

is a Laguerre algebra over $K$ of dimension $2^n$ (see, e.g., [82, 7.2]). Multiplication in this algebra is usually denoted by the wedge sign ($\wedge$). If $(b_1, b_2, \ldots, b_n)$ is a basis of $V$, then the family of vectors

$$b_{i_1} \wedge b_{i_2} \wedge \cdots \wedge b_{i_k},$$

where $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ and $k \in \{0, 1, \ldots, n\}$, is a basis of $\bigwedge V$. Of course, if $k = 0$, the corresponding empty product is defined to be $1 \in \bigwedge V$. The product of vectors is alternating and hence skew symmetric. Thus we have

$$v \wedge v = 0, \quad v \wedge w = -w \wedge v, \quad v, w \in V.$$ 

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 (3.5.3) 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 $Z$ be the ring of integers and let $1 < q = p^h \in Z$ be a power of a prime $p$. Then $Z/(qZ) =: Z_q$ is a local ring. The ideal $\text{rad } Z_q$ comprises the residue classes (modulo $q$) of all integers $kp$, where $k \in Z$, so it is the zero ideal precisely when $h = 1$. The quotient field $Z_q/\text{rad } R$ is the Galois field $Z_{p^h} = GF(p)$.

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

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.

### 3.5.5. Theorem

Let $R$ be a local ring. Then

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

(3.5.4)

Proof. By Sec. 3.2.10, the elements of the sets on the right-hand side of (3.5.4) are points of $\mathbb{P}(R)$. We conclude from (3.5.2) that the mapping

$$\mathbb{P}(R) \to \mathbb{P}(\overline{R}) : (a, b) \mapsto (\overline{a}, \overline{b})$$

(3.5.5)

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 (3.5.5), $\overline{R}(\overline{a}, \overline{b})$ is a point of $\mathbb{P}(\overline{R})$. Thus either $\overline{b} \neq 0$ (whence $b \in R^*$ and $R(a, b) = R(b^{-1}a, 1)$) or $\overline{b} = 0$ (whence $\overline{a} \neq 0$, $b \in R \setminus R^*$, $a \in R^*$, and $R(a, b) = R(1, a^{-1}b)$).

$$\square$$

### 3.5.6. Corollary

The projective line over a local ring $R$ has cardinality

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

(3.5.6)

This improves formula (3.2.6) for local rings. The following characterization is essential.

### 3.5.7. Theorem

A ring $R$ is a local ring if and only if the relation “nondistant” ($\not\Delta$) on the projective line $\mathbb{P}(R)$ is an equivalence relation.
Proof. (a) Over any ring $R$, the relation $\not\triangle$ on $\mathbb{P}(R)$ is reflexive and symmetric since $\triangle$ is anti-reflexive and symmetric according to Sec. 3.3.1.

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

$$
\begin{pmatrix}
1 & 0 \\
\alpha & \beta
\end{pmatrix} \not\in \text{GL}_2(R), \\
\begin{pmatrix}
1 & 0 \\
\gamma & \delta
\end{pmatrix} \not\in \text{GL}_2(R).
$$

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

$$
\begin{pmatrix}
* & * \\
x & y
\end{pmatrix} \begin{pmatrix}
a & b \\
c & d
\end{pmatrix} \neq \begin{pmatrix}
* & * \\
0 & 1
\end{pmatrix} \quad \forall x, y \in R.
$$

This implies $p \not\triangle q$.

(c) Conversely, let $\not\triangle$ be an equivalence relation. We must prove that $J := R \setminus R^* \neq \emptyset$ is an ideal. Given $a, b \in J$ we conclude from Sec. 3.3.5 that $R(1, a) \not\triangle R(1, 0) \not\triangle R(1, b)$. The transitivity of $\not\triangle$ yields

$$
\begin{pmatrix}
1 & a \\
1 & b
\end{pmatrix} \not\in \text{GL}_2(R).
$$

From

$$
\begin{pmatrix}
1 & a \\
1 & b
\end{pmatrix} = \begin{pmatrix}
1 & 0 \\
1 & a-b
\end{pmatrix} \begin{pmatrix}
1 & a \\
0 & -1
\end{pmatrix} \not\in \text{GL}_2(R)
$$

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 consider 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

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

Since $R(a, 0)$ 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 also a unit.

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.

\begin{flushright}
\hfill $\Box$
\end{flushright}

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 nondistant. 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 Sec. 5.1.1.

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

3.5.9. Corollary. 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 “∥” and “=” coincide precisely when \( R \) is a field (see Theorem 3.3.7). In this case, we obtain 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 [87, Theorem 19.1]): a ring \( R \) is local if and only if \( R \setminus R^* \) is a group under addition.

3.5.10. Assume that \( L \) is a field and that \( K \subset L \) is a proper subfield contained in the center of \( L \). Then the chain geometry \( \Sigma(K, L) \) is called a Möbius geometry. 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 [67] by assuming that \( K \) is in the center 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).

3.5.11. Examples. Here are some examples of Möbius geometries and their generalizations. The reader should consult [5, 40] 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 center of the real quaternions is \( \mathbb{R} \).

Now we turn to the finite case. Finite fields are commutative by a famous theorem due to Mclagan-Wedderburn, for which Witt suggested an elegant short proof (cf. [1]). Since finite commutative fields are precisely the well-known Galois fields, the finite Möbius geometries are easily described.

3.5.12. Theorem.

(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

\[
v = q^h + 1, \quad k = q + 1, \quad \lambda_3 = 1.
\]

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 \( h \geq 2 \) is equal to the dimension of \( L \) over \( K \), as a vector space.\(^7\)

(b) We have \( \#\mathbb{P}(\text{GF}(q^h)) = q^h + 1 \) according to (3.5.4). 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.

\( \square \)

\(^7\)It is worth noting here that \( L = \text{GF}(q^h) \) contains a unique subfield with \( q \) elements.
In part (b) of the preceding theorem we did not exclude the trivial case $h = 1$, even though it does not deserve our attention.

3.5.13. Assume 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 Sec. 4.2.

3.6. Notes and Further References

3.6.1. There are several books and surveys on chain geometries and related concepts. The publications [4, 5, 8–10, 40, 61, 67] (see also the references therein) cover these topics from the very beginning up to 2006. Below we restrict our attention to some 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 [49, Sec. 5]), weak chain spaces, chain spaces, contact spaces (cf. [67, Sec. 3], [100]), and circle planes [27]. 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 [22, 26, 70, 71, 73]).

The investigation of topological circle planes is part of the book [104]. It contains a wealth of bibliographical data. Characterizations of projective groups $\text{PGL}_2(R)$, where $R$ is a ring, are given in [23, 28, 69] (see also [40, Chap. 6]). Properties of projective lines over “small” rings are reviewed in [106, 107].

3.6.3. On the other hand, it is possible to consider structures that are more general than associative algebras (e.g., alternative algebras or Jordan systems) in order to obtain a kind of “chain geometry.” We refer the reader to [11, 12, 18–21, 28, 41, 68], and [40, Chap. 3],

3.6.4. Other papers related to certain chain geometries are [25, 29, 57–59, 62, 65, 66]. Every chain geometry gives rise to partial affine spaces. Such spaces are investigated in [72, 99, 101].

CHAPTER 4

DIVISIBLE DESIGNS VIA $\text{GL}_2$-ACTIONS

4.1. How to Choose a Base Block

4.1.1. Let $R$ be a finite local ring. As above, we write $\text{rad } R := R \setminus R^*$ for its Jacobson radical. According to Theorem 3.5.7 and by the definition in Sec. 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.

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

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

is a $3$-$(s, k, \lambda_3)$-divisible design with $v = \#R + \#\text{rad } R$ points, and $s = \#\text{rad } R$. 

912
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 Sec. 3.5.8, the relations \( \| \) and \( \not\triangle \) coincide for a local ring. Therefore, also the equivalence relation \( \| \) 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 \( \| \)-transversal 3-set?**

Or, said differently:

**What is the value of the parameter \( \lambda_3 \)?**

We read off from (2.3.1) that answering this question amounts to finding two nonnegative integers: first, \( \# \text{GL}_2(R) \) and, second, the cardinality of the set-wise 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 set-wise stabilizer of \( B_0 \) without any further information concerning \( B_0 \).

4.1.4. Exercise. Show that

\[
\# \text{GL}_2(\text{GF}(q)) = (q^2 - 1)(q^2 - q). \tag{4.1.1}
\]

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

\[
\# \text{GL}_2(R) = (\# \text{rad} R)^4(q^2 - 1)(q^2 - q). \tag{4.1.2}
\]

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 to learn more about the DDs which are based upon the projective line over such a ring, for example the projective line over a Galois ring (see [133]). However, it seems to the author that a “natural” choice for a base block does not exist.

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 \( C(K, R) \) for the set of \( K \)-chains of the projective line \( \mathbb{P}(R) \).

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

\[
(\mathbb{P}(R), C(\text{GF}(q), R), \|)
\]

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 center 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 nonisomorphic transversal divisible designs.
4.2.3. Theorem. 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 \( K := \text{GF}(q) \).

4.2.4. Exercise. Determine the parameters \( \lambda_2, \lambda_1, \) and \( \lambda_0 \) (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.

4.3.2. Theorem (Wedderburn principal theorem). 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 [98, 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 \( R \to \overline{R} \) takes \( K \) to an isomorphic field which is a subring of \( \overline{R} \). So we obtain that

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

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 set

\[
h := \dim_L R \geq 1.
\]

Hence

\[
\dim_K R = (\dim_L R)(\dim_K L) = hm \quad (4.3.1)
\]

and

\[
\dim_K (\text{rad} R) = (h - 1)m. \quad (4.3.2)
\]

The next theorem is taken from [124, Example 2.5]. It is a generalization of Theorem 4.2.2 which, of course, is included as a particular case for \( m = 1 \).

4.3.4. Theorem. 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 \( h \). Then

\[
(P(R), C(\text{GF}(q), R), ||)
\]

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 (4.3.2).

Next, we apply this result to construct DDs.

4.3.5. Theorem. 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 \( \text{GF}(q) \) with \( R/\text{rad} R \cong \text{GF}(q^m) \). Therefore, at least one \( 3-(s,k,1) \)-divisible design with parameters as in Theorem 4.3.4 exists.
Proof. We conclude from Theorem 4.2.3 that there is an \( h \)-dimensional Laguerre algebra \( R \) over \( \text{GF}(q^m) \). Therefore, \( R/\text{rad} R \) is isomorphic to \( \text{GF}(q^m) \). This \( R \) is an \( hm \)-dimensional local algebra over \( \text{GF}(q) \subset \text{GF}(q^m) \). ∎

Observe that for \( h > 1 \) nontransversal DDs are obtained in this way.

4.3.6. By the definition of an (arbitrary) chain geometry \( \Sigma(K,R) \), the group \( \text{GL}_2(R) \) acts on \( \mathbb{P}(R) \) as a group of automorphisms of \( \Sigma(K,R) \) or, said differently, of the corresponding divisible design. Recall that \( \text{PGL}_2(R) \) denotes the transformation group on \( \mathbb{P}(R) \), which is induced by \( \text{GL}_2(R) \). 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 \( \sigma : R \to R' \) is called a Jordan homomorphism if

\[
(a + b)^\sigma = a^\sigma + b^\sigma, \quad 1^\sigma = 1 (\in R'), \quad (aba)^\sigma = a^\sigma b^\sigma a^\sigma \quad \text{for all } a, b \in R \tag{4.3.3}
\]

(see, e.g., [81, p. 2] or [67, p. 832]). For such a mapping \( \sigma \) and any element \( a \in R^* \), the equation

\[
1^\sigma = (aa^{-2})^\sigma = a^\sigma(a^{-2})^\sigma a^\sigma \tag{4.3.4}
\]

shows that \( a^\sigma \) has a left and a right inverse, whence \( a^\sigma \) is a unit in \( R' \). Also,

\[
a^\sigma = (aa^{-1})^\sigma = a^\sigma(a^{-1})^\sigma a^\sigma \tag{4.3.5}
\]

implies

\[
(a^{-1})^\sigma = (a^\sigma)^{-1} \quad \text{for all } a \in R^*. \tag{4.3.6}
\]

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

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

Let \( \sigma : R \to R' \) be a Jordan homomorphism of rings. If \( R \) and \( R' \) are commutative and \( 1+1 \in R^* \), then \( \sigma \) is a homomorphism. If \( R' \) has no left or right zero divisors, then \( \sigma \) is a homomorphism or an anti-homomorphism (see, e.g., [3, 63] and [82, 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 anti-homomorphism.

4.3.9. Examples. We present some Jordan homomorphisms other than homomorphisms.

(a) A well known example of an anti-automorphism (a bijective anti-homomorphism of a ring onto itself) is as follows. Let \( R \) be a commutative ring (or even a commutative field) and \( R^{m \times m} \) be the ring of \( (m \times m) \)-matrices with entries from \( R \) with \( m \geq 2 \). The transposition of matrices is an anti-automorphism \( R^{m \times m} \to R^{m \times m} \).

915
(b) Assume that \( R = \prod_{j \in J} R_j \) is the direct product of rings \( R_j \). Similarly, let \( R' = \prod_{j \in J} R'_j \). Furthermore, assume that \( \sigma_j : R_j \rightarrow R'_j \) is a family of mappings, where each \( \sigma_j \) is a homomorphism or an anti-homomorphism. Then

\[
\sigma := \prod_{j \in J} \sigma_j : R \rightarrow R' : (x_j)_{j \in J} \mapsto \left( x'_j \right)_{j \in J}
\]

is a Jordan homomorphism.

If among the mappings \( \sigma_j \), there is a homomorphism other than an anti-homomorphism and an antihomomorphism other than a homomorphism, then \( \sigma \) 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 \( \wedge V \) (see \[82, Sec. 7.2\]). Hence, there exists a unique \( K \)-linear bijection \( \sigma : \wedge V \rightarrow \wedge V \) with the following properties: \( \sigma \) interchanges \( b_2 \) with \( b_1 \wedge b_2 \) and fixes the remaining basis elements 1 and \( b_1 \). In order to show that \( \sigma \) is a Jordan isomorphism, it suffices to verify the last condition in (4.3.3) for the elements of the given basis. As a matter of fact, that condition is satisfied trivially. Clearly, it is valid 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

\[
(b_1 \wedge b_2)^\sigma = b_2 \neq 0, \quad b_1^\sigma \wedge b_2^\sigma = b_1 \wedge b_1 \wedge b_2 = 0,
\]

the Jordan isomorphism \( \sigma \) 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 Herzer, which is presented without proof (see \[67, Theorem 9.2.1\], \[40, Chap. 4\], and \[2, 35\] for generalizations and also cf. \[64, Propositions 2.3 and 3.6\]).

4.3.11. Theorem. 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 \[64, Remark 4.3.2\], there exist nonisomorphic 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.
4.4.2. Theorem. Let $R$ be an finite-dimensional local algebra over $K = \text{GF}(q)$, with $R/\text{rad} \cong \text{GF}(q^m)$, 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 $3$-$(s, k, \lambda_3)$-divisible design with

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

The remaining parameters $k$ and $\lambda_3$ are

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

Proof. First, we observe that $\#C_0 = q + 1$ and $C_0$ is a $||$-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 $3\Delta$-transitively on $\mathcal{P}(R)$, 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 $M$ must 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 obtain from Theorem 3.4.7 that each such $C_0 \setminus W$ is a chain. This proves the assertions on $\lambda_3$. The rest is clear from Theorem 4.3.4. \qed

4.4.3. The previous theorem is taken from [55]. 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. [77, Sec. 6.1]). Thus several cases have to be treated separately. We refer to [55], 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 [55]. As before, cross ratios are the key to calculating the parameter $\lambda_3$.

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 Theorem 4.3.2). A general treatment of these DDs seems to be missing in the literature. We present here the following example which is based on [98, Exercise XIX.1] (see also [39] for a generalization).

4.4.5. Example. Let $L := \text{GF}(4) = \{0, 1, \tau, \tau^2\}$ be the field with four elements. Its multiplicative group is cyclic of order 3. Addition in $L$ is subject to $x + x = 0$ for all $x \in L$, and $1 + \tau = \tau^2$. The mapping $\sigma : L \to L : x \mapsto x^2$ is easily seen to be an automorphism of order 2.

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

$$\varepsilon^2 = 0, \quad \varepsilon x = x^2 \varepsilon = x^2 \varepsilon \quad \forall x \in L$$

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

917
Following Theorem 3.4.8, we determine the normalizer of $L^*$ in $R^*$. The units in $R^*$ have the form

$$n = x + ye, \quad x \in L^*, \ y \in L.$$  

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

$$n^{-1}\tau n = (x + ye)^{-1}\tau (x + ye) = (x^{-1} - ye)\tau (x + ye) = \tau + x^{-1}\tau ye - y\tau x - ye\tau e$$

$$= \tau + x^{-1}\tau ye - x^2y^2\tau^2 e - y^3\tau^2 e^2 = \tau(1 + x^2y(1 - \tau e)).$$

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

- $x^2y = 0$:
  $$n^{-1}\tau n = \tau \in L^*,$$

- $x^2y = 1$:
  $$n^{-1}\tau n = \tau + e \notin L^*,$$

- $x^2y = \tau$:
  $$n^{-1}\tau n = \tau + \tau e \notin L^*,$$

- $x^2y = \tau^2$:
  $$n^{-1}\tau n = \tau + \tau^2 e \notin L^*.$$

We see that $n = x + ye$ lies 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 obtain that

$$\left(\mathbb{P}(\text{GF}(4)[\varepsilon; \sigma]), \mathcal{C}(\text{GF}(4), \text{GF}(4)[\varepsilon; \sigma]), \mathcal{C}\right)$$

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 references in [31, 32], [40, Chap. 11], and [67, p. 812]). 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 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 GF($q$). The blocks are the nondegenerate 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 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** is a bijective 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 note 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. [76, 15.4]).
5.1. Parallelism Based on the Jacobson Radical

5.1.1. Now we consider projective lines over an arbitrary ring \( R \), as we present the announced definition of parallel points in the general case. It is taken from [36], 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

\[ p \parallel q \iff p^\gamma \parallel q^\gamma \quad (5.1.1) \]

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 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. Sec. 3.5.1) is as follows. We consider the factor ring \( R/\text{rad} \ R =: \overline{R} \) and the canonical epimorphism \( R \to \overline{R} : a \mapsto a + \text{rad} \ R =: \overline{a} \). It has the crucial property

\[ a \in R^* \iff \overline{a} \in \overline{R}^* \quad \forall a \in R \quad (5.1.2) \]

(cf. [87, Proposition 4.8]). The Jacobson radical of the factor ring \( R/\text{rad} \ R \) is zero [87, Proposition 4.6].

In geometric terms, we obtain a mapping

\[ \mathbb{P}(R) \to \mathbb{P}(\overline{R}) : p = R(a, b) \mapsto \overline{R}(\overline{a}, \overline{b}) =: \overline{p}, \quad (5.1.3) \]

which is well defined and surjective [31, Proposition 3.5]. Furthermore, as a geometric counterpart of (5.1.2) we have

\[ p \triangle q \iff \overline{p} \triangle \overline{q} \quad \forall p, q \in \mathbb{P}(R), \quad (5.1.4) \]

where we use the same symbol to denote the distant relations on \( \mathbb{P}(R) \) and on \( \mathbb{P}(\overline{R}) \), respectively (see [31, Propositions 3.1 and 3.2]). Of course, all this is a generalization of the mapping given in (3.5.5), where \( R \) was assumed to be local.

The following assertion follows from [36, Theorem 2.2, Corollary 2.3].

5.1.3. Theorem. The mapping given by (5.1.3) has the property

\[ p \parallel q \iff \overline{p} = \overline{q} \quad \forall p, q \in \mathbb{P}(R). \quad (5.1.5) \]

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 (5.1.5) that

\[ \#[p] = \# \text{rad} \ R \quad \forall p \in \mathbb{P}(R). \quad (5.1.6) \]

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 (5.1.4) and Theorem 5.1.3 is

\[ p \parallel q \iff \overline{p} = \overline{q} \Rightarrow p \neq q \iff p \neq q \quad \forall p, q \in \mathbb{P}(R). \quad (5.1.7) \]
In general, however, the converse of (5.1.7) is not valid.

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

For a proof, we refer the reader to [36, Theorem 2.5]. By the above, our two definitions of parallel points in Secs. 3.5.8 and 5.1.1 coincide in the case of a local ring.

5.2. Counting the Point Set

5.2.1. Let $R$ be a finite ring. The problem of determining the number of points of the projective line over $R$ is intricate. Our approach follows [130, Sec. 10] and it uses the following famous Wedderburn–Artin theorem on the structure of semisimple rings (cf. [87, Theorem 3.5]). We state it only for the particular case of a finite ring.

5.2.2. Theorem (Wedderburn–Artin theorem). 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 $i \in \{1, 2, \ldots, n\}$.

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 $\text{GF}(q)$, since 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 Hubaut [79, p. 500], who proved it for an arbitrary commutative field $K$ instead of $\text{GF}(q)$. This powerful tool was generalized by Blunck [24, Theorem 2.1] to the ring of endomorphisms of a vector space, without any restriction on its dimension or the ground field. We add in passing that the projective line over a matrix ring is essentially nothing else but a particular example of a projective space of matrices as considered in [132, p. 124] (see also [37, 78]).

By virtue of this bijection and by a result of Thas [128, 3.3], we obtain

$$\#(\mathbb{P}(\text{GF}(q)^{m \times m})) = \prod_{i=0}^{m-1} \frac{q^{2m-i} - 1}{q^{m-i} - 1} \quad (5.2.1)$$

(see also [77, 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 bijection correspondence with the Cartesian product

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

Hence the Wedderburn–Artin theorem 5.2.2 and formula (5.2.1) 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 (5.1.6) that

$$\#\mathbb{P}(R) = (\# \text{rad} \ R) (\#\mathbb{P}(\overline{R})), \quad (5.2.2)$$

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 $\mathbb{P}(R)$.

---

8The case $\mathbb{Z}_6 \cong \text{GF}(2) \times \text{GF}(3)$ is illustrated in Fig.7.
5.3. Divisible Designs versus Finite Chain Geometries

5.3.1. To complete this series of lectures, let us compare the definition of a divisible design from Definition 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

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

where \(\lambda_t\) is the constant number of blocks through any \(t = 3\) mutually distant points. As we saw, \(\lambda_t\) depends on “how” the field \(K\) is embedded in \(R\), whence we cannot 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 (5.3.1).

(A1) \(\#[x] = s_1\) for all \(x \in P(R)\).

(A2) \(\#\{y \in P(R) \mid y \neq x\} = s_2\) for all \(x \in P(R)\).

(B1) \(C(K, R)\) is a set of subsets of \(P(R)\) with \(\#C = k\) for all chains \(C \in C(K, R)\). The points of any chain are mutually distant.

(C1) For each \(t\)-subset \(Y \subset P(R)\) of mutually distant points, there exist exactly \(\lambda_t\) chains of \(C(K, R)\) containing \(Y\).

(D1) \(t \leq v/s_1\).

Thus, any finite chain geometry is “almost” a 3-divisible design. However, unless \(R\) is a local ring, a \(\parallel\)-transversal 3-subset of \(P(R)\) 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.

REFERENCES

1. M. Aigner and G. M. Ziegler, Proofs from the Book, Springer-Verlag, Berlin (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: Rings and Geometry (R. Kaya, P. Plaumann, and K. Strambach, eds.), Reidel, Dordrecht (1985), pp. 353–389.
4. W. Benz, “Über Möbiusebenen,” Jber. Deutsch. Math. Verein., 63, 1–27 (1960).
5. W. Benz, Vorlesungen über Geometrie der Algebren, Springer-Verlag, Berlin (1973).
6. W. Benz, Geometrische Transformationen, BI Wissenschaftsverlag, Mannheim (1992).
7. W. Benz, Classical Geometries in Modern Contexts, Birkhäuser, Basel (2007).
8. W. Benz, W. Leissner, and H. Schaeffer, “Kreise, Zykel, Ketten. Zur Geometrie der Algebren. Ein Bericht,” Jber. Deutsch. Math. Verein., 74, 107–122 (1972).
9. W. Benz and H. Mäurer, “Über die Grundlagen der Laguerre-Geometrie. Ein Bericht,” Jber. Deutsch. Math. Verein., 67, 14–42 (1964).
10. W. Benz, H.-J. Samaga, and H. Schaeffer, “Cross ratios and a unifying treatment of von Staudt’s notion of reeller Zug,” in: Geometry: von Staudt’s Point of View (P. Plaumann and K. Strambach, eds.), Reidel, Dordrecht (1981), pp. 127–150.
11. 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).
12. W. Bertram and K.-H. Neeb, “Projective completions of Jordan pairs, II. Manifold structures and symmetric spaces,” *Geom. Dedicata*, **112**, 73–113 (2005).

13. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, BI Wissenschaftsverlag, Mannheim (1985).

14. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory, I*, Cambridge Univ. Press, Cambridge (1999).

15. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory II*, Cambridge Univ. Press, Cambridge (1999).

16. M. Biliotti and G. Micelli, “On translation transversal designs,” *Rend. Sem. Mat. Univ. Padova*, **73**, 217–229 (1985).

17. W. Blaschke, “Über die Laguerresche Geometrie der Speere in der Euklidischen Ebene,” *Mh. Math. Phys.*, **21**, 3–60 (1910).

18. A. Blunck, “Chain geometries over local alternative algebras,” *J. Geom.*, **44**, 33–44 (1992).

19. A. Blunck, “Chain spaces over Jordan systems,” *Abh. Math. Sem. Univ. Hamburg*, **64**, 33–49 (1994).

20. A. Blunck, “A quadric model for Klingenberg chain spaces,” *Geom. Dedicata*, **55**, 237–246 (1995).

21. A. Blunck, “Generalized affine chain geometries,” *J. Geom.*, **56**, 9–17 (1996).

22. A. Blunck, “Chain spaces via Clifford algebras,” *Monatsh. Math.*, **123**, 98–107 (1997).

23. A. Blunck, *Geometries for Certain Linear Groups over Rings. Construction and Coordinatization*, Habilitationsschrift, Techn. Univ. Darmstadt (1997).

24. A. Blunck, “Regular spreads and chain geometries,” *Bull. Belg. Math. Soc. Simon Stevin*, **6**, 589–603 (1999).

25. A. Blunck, “Reguli and chains over skew fields,” *Beiträge Algebra Geom.*, **41**, 7–21 (2000).

26. A. Blunck, “Chain spaces with many reflections,” *J. Geom.*, **72**, 18–26 (2001).

27. A. Blunck, “Finite circle planes,” in: *Proc. Ninth Int. Meeting of European Women in Mathematics* (R. Camina and L. Fajstrup, eds.), Hindawi, Stony Brook (2001), pp. 155–159.

28. A. Blunck, “Projective groups over rings,” *J. Algebra*, **249**, 266–290 (2002).

29. A. Blunck, “The cross ratio for quadruples of subspaces,” *Mitt. Math. Ges. Hamburg*, **22**, 81–97 (2003).

30. A. Blunck and H. Havlicek, “Extending the concept of chain geometry,” *Geom. Dedicata*, **83**, 119–130 (2000).

31. A. Blunck and H. Havlicek, “Projective representations, I. Projective lines over rings,” *Abh. Math. Sem. Univ. Hamburg*, **70**, 287–299 (2000).

32. A. Blunck and H. Havlicek, “Projective representations, II. Generalized chain geometries,” *Abh. Math. Sem. Univ. Hamburg*, **70**, 301–313 (2000).

33. A. Blunck and H. Havlicek, “The connected components of the projective line over a ring,” *Adv. Geom.*, **1**, 107–117 (2001).

34. A. Blunck and H. Havlicek, “The dual of a chain geometry,” *J. Geom.*, **72**, 27–36 (2001).

35. A. Blunck and H. Havlicek, “Jordan homomorphisms and harmonic mappings,” *Monatsh. Math.*, **139**, 111–127 (2003).

36. A. Blunck and H. Havlicek, “Radical parallelism on projective lines and nonlinear models of affine spaces,” *Math. Pannonica*, **14**, 113–127 (2003).

37. A. Blunck and H. Havlicek, “On bijections that preserve complementarity of subspaces,” *Discr. Math.*, **301**, 46–56 (2005).

38. A. Blunck, H. Havlicek, and C. Zanella, “Lifting of divisible designs,” *Des. Codes Cryptogr.*, **42**, No. 1, 1–14 (2007).
39. A. Blunck, H. Havlicek, and C. Zanella, “Divisible designs from twisted dual numbers,” Des. Codes Cryptogr., 47, Nos. 1–3, 11–20 (2008).
40. A. Blunck and A. Herzer, Kettengeometrien. Eine Einführung, Shaker-Verlag, Aachen (2005).
41. A. Blunck and M. Stroppel, “Klingenberg chain spaces,” Abh. Math. Sem. Univ. Hamburg, 65, 225–238 (1995).
42. U. Brehm, M. Greferath, and S. E. Schmidt, “Projective geometry on modular lattices,” in: Handbook of Incidence Geometry (F. Buekenhout, ed.), Elsevier, Amsterdam (1995).
43. C. Cerroni, “Divisible designs from semifield planes,” Discr. Math., 255, 47–54 (2002).
44. C. Cerroni and R.-H. Schulz, “Divisible designs admitting $GL(3,q)$ as an automorphism group,” Geom. Dedicata, 83, 343–350 (2000).
45. C. Cerroni and R.-H. Schulz, “Divisible designs admitting, as an automorphism group, an orthogonal group or a unitary group,” in: Finite Fields and Applications (Augsburg, 1999) (D. Jungnickel and H. Niederreiter, eds.), Springer-Verlag, Berlin (2001), pp. 95–108.
46. C. Cerroni and A. G. Spera, “On divisible designs and twisted field planes,” J. Combin. Des., 7, 453–464 (1999).
47. P. M. Cohn, “On the structure of the $GL_2$ of a ring,” Inst. Hautes Etudes Sci. Publ. Math., 30, 365–413 (1966).
48. Ch. J. Colbourn and J. H. Dinitz, eds. Handbook of Combinatorial Designs, Discr. Math. Appl., Boca Raton, FL (2007).
49. A. Delandtsheer, “Dimensional linear spaces,” in: Handbook of Incidence Geometry (F. Buekenhout, ed.), Elsevier, Amsterdam (1995), pp. 781–842.
50. P. Dembowski, Finite Geometries, Springer-Verlag, Berlin (1997).
51. T. Etzion, “Optimal constant weight codes over $Z_k$ and generalized designs,” Discr. Math., 169, Nos. 1–3, 55–82 (1997).
52. C.-A. Faure, “Morphisms of projective spaces over rings,” Adv. Geom., 4, No. 1, 19–31 (2004).
53. O. Giering, Vorlesungen über höhere Geometrie, Vieweg, Braunschweig, Wiesbaden (1982).
54. S. Giese, Block-zerlegbare divisible designs, Ph.D. thesis, Freie Universität, Berlin (2005); http://www.diss.fu-berlin.de/diss/receive/FUDISS_thesis_00000001833.
55. S. Giese, H. Havlicek, and R.-H. Schulz, “Some constructions of divisible designs from Laguerre geometries,” Discr. Math., 301, 74–82 (2005).
56. S. Giese and R.-H. Schulz, “Divisible designs with dual translation group,” Des. Codes Cryptogr., 43, No. 1, 41–45 (2007).
57. H. Havlicek, “On the geometry of field extensions,” Aequat. Math., 45, 232–238 (1993).
58. H. Havlicek, “Spheres of quadratic field extensions,” Abh. Math. Sem. Univ. Hamburg, 64, 279–292 (1994).
59. H. Havlicek, “Affine circle geometry over quaternion skew fields,” Discr. Math., 174, 153–165 (1997).
60. H. Havlicek, “Divisible designs, Laguerre geometry, and beyond,” Quaderni Sem. Mat. Brescia, 11 (2006); http://www.dmf.bs.unicatt.it/~semmat/preprints/2006.html.
61. H. Havlicek, “From pentacyclic coordinates to chain geometries, and back,” Mitt. Math. Ges. Hamburg, 26, 75–94 (2007).
62. H. Havlicek and K. List, “A three-dimensional Laguerre geometry and its visualization,” in: Proc. Dresden Symp. Geometry: Constructive and Kinematic (G. Weiβ, ed.), Inst. Geom., Techn. Univ. Dresden (2003), pp. 122–129.
63. I. N. Herstein, “Jordan homomorphisms,” Trans. Am. Math. Soc., 81, 331–341 (1956).
64. A. Herzer, “On isomorphisms of chain geometries,” Note Mat., 7, 251–270 (1987).
65. A. Herzer, “Der aquiforme Raum einer Algebra,” Mitt. Math. Ges. Hamburg, 13, 129–154 (1993).
66. A. Herzer, “N-zyklische Algebren,” Mitt. Math. Ges. Hamburg, 13, 119–128 (1993).
67. A. Herzer, “Chain geometries,” in: Handbook of Incidence Geometry (F. Buekenhout, ed.), Elsevier, Amsterdam (1995), pp. 781–842.
68. A. Herzer, “Affine Kettengeometrien über Jordanalgebren,” Geom. Dedicata, 59, 181–195 (1996).
69. A. Herzer, “Der Satz von Tits für PGL2(R), R ein kommutativer Ring vom stabilen Rang 2,” Geom. Dedicata, 62, 167–178 (1996).
70. A. Herzer, “Kennzeichnung von Berührungstrukturen, die Kettengeometrien sind,” J. Geom., 62, 166–175 (1998).
71. A. Herzer and B. Klos, “Synthetische Konstruktion eines affinen Kettenraumes,” Mitt. Math. Ges. Hamburg, 15, 35–44 (1996).
72. A. Herzer and S. Meuren, “Ein Axiomensystem für partielle affine Räume,” J. Geom., 50, 124–142 (1995).
73. A. Herzer and H. Ramroth, “Die projektive Gerade über einem Ring, der direktes Produkt kommutativer Körper ist,” J. Algebra, 176, 1–11 (1995).
74. A. Herzer and R.-H. Schulz, “Some new (s,k,λ)-translation transversal designs with nonabelian translation group,” J. Geom., 35, 87–96 (1989).
75. R. Hill, A First Course in Coding Theory, Oxford Univ. Press, Oxford (1986).
76. J. W. P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Oxford Univ. Press, Oxford (1985).
77. J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford (1998).
78. L.-P. Huang, Geometry of Matrices over Ring, Science Press, Beijing (2006).
79. X. Hubaut, “Algèbres projectives,” Bull. Soc. Math. Belg., 17, 495–502 (1965).
80. D. R. Hughes and F. C. Piper, Design Theory, Cambridge Univ. Press, Cambridge (1985).
81. N. Jacobson, Structure and Representation of Jordan Algebras, Am. Math. Soc., Providence, Rhode Island (1968).
82. N. Jacobson, Basic Algebra, I, Freeman, New York (1989).
83. D. Jungnickel, “Transversal designs associated with Frobenius groups,” J. Geom., 17, 140–154 (1981).
84. D. Jungnickel, “On automorphism groups of divisible designs,” Can. J. Math., 34, 257–297 (1982).
85. R. L. Kruse and D. T. Price, Nilpotent Rings, Gordon and Breach, New York (1969).
86. T. Kvirikashvili and A. Lashkhi, “On the fundamental theorem of geometric algebra over SF-rings,” Commun. Algebra, 36, No. 9, 3564–3573 (2008).
87. T. Y. Lam, A First Course in Noncommutative Rings, Springer-Verlag, New York (1991).
88. T. Y. Lam, Lectures on Modules and Rings, Springer-Verlag, New York (1999).
89. A. Lashkhi, “Harmonic maps over rings,” Georgian Math. J., 4, 41–64 (1997).
90. A. A. Lashkhi, “Harmonic maps of modules,” Mat. Zametki, 47, No. 1, 161–163 (1991).
91. A. A. Lashkhi and T. G. Kvirikashvili, “Perspective maps for modules,” Mat. Zametki, 77, No. 6, 946–947 (2005).
92. A. A. Lashkhi and T. G. Kvirikashvili, “Affine geometry of modules over a ring with an invariant basis number,” J. Math. Sci., 137, No. 5, 5161–5173 (2006).
93. A. A. Lashkhi and T. G. Kvirikashvili, “Perspective maps of modules,” J. Math. Sci., 155, No. 5, 789–795 (2008).
94. A. A. Lashkhi and T. G. Kvirikashvili, “Affine geometry of modules over a ring with invariant basis number,” Mat. Zametki, 82, No. 6, 838–849 (2007).
95. C. C. Lindner and C. A. Rodger, Design Theory, Discr. Math. Appl., Boca Raton, FL (2009).
96. D. Livingstone and A. Wagner, “Transitivity of finite permutation groups on unordered sets,” Math. Z., 90, 393–403 (1965).
97. H. Lüneburg, Transitive Erweiterungen endlicher Permutationsgruppen, Lect. Notes Math., 84, Springer-Verlag, Berlin (1969).
98. B. R. McDonald, Finite Rings with Identity, Marcel Dekker, New York (1974).
99. S. Meuren, “Partial affine spaces of dimension ≥3,” J. Geom., 56, 113–125 (1996).
100. M. Özcan and A. Herzer, “Berührungstrukturen, die keine Kettenräume sind,” Geom. Dedicata, 78, 241–251 (1999).
101. V. Pambuccian, “Über das Reichhaltigkeitsaxiom für partielle affine Räume,” J. Geom., 55, 139–140 (1996).
102. D. Pedoe, “A forgotten geometrical transformation,” Enseignement Math. (2), 18, 255–267 (1972).
103. D. Pedoe, “Laguerre’s axial transformation,” Math. Mag., 48, 23–30 (1975).
104. B. Polster and G. Steinke, Geometry on Surfaces, Cambridge Univ. Press, Cambridge (2001).
105. J. F. Rigby, “The geometry of cycles, and generalized Laguerre inversion,” in: The Geometric Vein (C. Davis, B. Grünbaum, and F. A. Sherk, eds.), Springer-Verlag, New York (1981), pp. 355–378.
106. M. Saniga, M. Planat, M. R. Kibler, and P. Pracna, “A classification of the projective lines over small rings,” Chaos Solitons Fractals, 33, No. 4, 1095–1102 (2007).
107. M. Saniga, M. Planat, and P. Pracna, “A classification of the projective lines over small rings, II. Noncommutative case,” http://arxiv.org/abs/math/0606500v1.
108. E. M. Schröder, “Metric geometry,” in: Handbook of Incidence Geometry (F. Buekenhout, ed.), Elsevier, Amsterdam (1995), pp. 945–1013.
109. R.-H. Schulz, “Transversal designs and Hughes–Thompson groups,” Mitt. Math. Sem. Giessen, 165, 185–197 (1984).
110. R.-H. Schulz, “On the classification of translation group-divisible designs,” Eur. J. Combin., 6, 369–374 (1985).
111. R.-H. Schulz, “Transversal designs and partitions associated with Frobenius groups,” J. Reine Angew. Math., 355, 153–162 (1985).
112. R.-H. Schulz, “On translation transversal designs with λ > 1,” Arch. Math. (Basel), 49, 97–102 (1987).
113. R.-H. Schulz, “Transversal designs with λ > 1 associated with Frobenius groups,” Res. Math., 12, 401–410 (1987).
114. R.-H. Schulz, “On the existence of generalized triads related to transversal designs,” Ars Combin., 25(B), 203–209 (1988).
115. R.-H. Schulz, “Constant weight codes and divisible designs with large automorphism groups,” Rend. Circ. Mat. Palermo (2) Suppl., 53, 173–188 (1998).
116. R.-H. Schulz and A. G. Spera, “Divisible designs and groups,” Geom. Dedicata, 44, 147–157 (1992).
117. R.-H. Schulz and A. G. Spera, “Construction of divisible designs from translation planes,” Eur. J. Combin., 19, 479–486 (1998).
118. 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).

119. R.-H. Schulz and A. G. Spera, “Automorphisms of constant weight codes and of divisible designs,” *Des. Codes Cryptogr.*, 20, 89–97 (2000).

120. I. R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, Berlin–Heidelberg–New York (1977).

121. A. G. Spera, “Translation divisible designs,” *Arch. Math. (Basel)*, 55, 507–515 (1990).

122. A. G. Spera, “On affine translation divisible designs,” *J. Geom.*, 40, 175–185 (1991).

123. A. G. Spera, “Semi-regular divisible designs and Frobenius groups,” *Geom. Dedicata*, 42, 285–294 (1992).

124. A. G. Spera, “$t$-Divisible designs from imprimitive permutation groups,” *Eur. J. Combin.*, 13, 409–417 (1992).

125. A. G. Spera, “On divisible designs and local algebras,” *J. Comb. Designs*, 3, 203–212 (1995).

126. A. G. Spera, “Transitive extensions of imprimitive groups,” *Discr. Math.*, 155, 233–241 (1996).

127. A. G. Spera, “Divisible designs associated with translation planes admitting a 2-transitive collineation group on the points at infinity,” *Aequat. Math.*, 59, 191–200 (2000).

128. 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* (6), 4, 459–532 (1971).

129. F. D. Veldkamp, “Projective ring planes and their homomorphisms,” in: *Rings and Geometry* (R. Kaya, P. Plaumann, and K. Strambach, eds.), Reidel, Dordrecht (1985), pp. 289–350.

130. F. D. Veldkamp, “Projective geometry over finite rings,” *Quaderni Semin. Geom. Combin.*, 92, 1–39 (1989).

131. F. D. Veldkamp, “Geometry over rings,” in: *Handbook of Incidence Geometry* (F. Buekenhout, ed.), Elsevier, Amsterdam (1995), pp. 1033–1084.

132. Z.-X. Wan, *Geometry of Matrices*, World Scientific, Singapore (1996).

133. Z.-X. Wan, *Lectures on Finite Fields and Galois rings*, World Scientific, River Edge, New Jersey (2003).

134. H. Wielandt, “Endliche $k$-homogene Permutationsgruppen,” *Math. Z.*, 101, 142 (1967).

135. I. M. Yaglom, *A Simple Non-Euclidean Geometry and Its Physical Basis*, Springer-Verlag, New York–Heidelberg–Berlin (1979).

136. I. M. Yaglom, “On the circular transformations of Möbius, Laguerre, and Lie,” in: *The Geometric Vein* (C. Davis, B. Grünbaum, and F. A. Sherk, eds.), Springer-Verlag, New York (1981), pp. 345–353.

Hans Havlicek
Institut für Diskrete Mathematik und Geometrie,
Technische Universität Wien, Austria
E-mail: havlicek@geometrie.tuwien.ac.at

926