Construction of a field

Renáta Ševčíková

Based on material from

General Lattice Theory by G. Graetzer

Geometric Algebra by E. Artin

INTRODUCTION

Suppose there is a geometry whose objects are elements of two sets (set of points $\mathcal{P}$, set of lines $\mathcal{L}$) and assume that certain axioms are true. Is it possible to find a field $\mathcal{K}$, s.t. the points of our geometry can be described by coordinates from $\mathcal{K}$ and the lines by linear equations over $\mathcal{K}$?

NEEDED FACTS

- canonical way how to extend affine plane to projective plane

Needed facts

- canonical way how to extend affine plane to projective plane
- one-to-one correspondence between projective spaces and projective geometry

NEEDED FACTS

- canonical way how to extend affine plane to projective plane
- one-to-one correspondence between projective spaces and projective geometry
- important properties of a geometry associated with modular geometric lattice are formulated only with points and lines

Needed facts

- canonical way how to extend affine plane to projective plane
- one-to-one correspondence between projective spaces and projective geometry
- important properties of a geometry associated with modular geometric lattice are formulated only with points and lines
- geometry with "good" properties (DA, PT)

Needed facts

- canonical way how to extend affine plane to projective plane
- one-to-one correspondence between projective spaces and projective geometry
- important properties of a geometry associated with modular geometric lattice are formulated only with points and lines
- geometry with "good" properties (DA, PT)
- existence of a (not necessarily) commutative field

First three axioms

- 1, Axiom: Given two distinct points P, Q, then there exists a unique line l, s.t. $P \in l$ & $Q \in l$. $(l = P + Q)$

First three axioms

- 1, Axiom: Given two distinct points P, Q, then there exists a unique line l, s.t. $P \in l$ & $Q \in l$. ($l = P + Q$)
- 2, Axiom: Given a point P and a line l, there exists exactly one line m, s.t. $P \in m$ & $m||l$ (m, l are parallel).

First three axioms

- 1, Axiom: Given two distinct points P, Q, then there exists a unique line l, s.t. $P \in l$ & $Q \in l$. ($l = P + Q$)
- 2, Axiom: Given a point P and a line l, there exists exactly one line m, s.t. $P \in m$ & $m||l$ (m, l are parallel).
- 3, Axiom: There exist three distinct points A, B, C, s.t. $C \notin A + B$; noncollinear points.

First three axioms

- 1, Axiom: Given two distinct points P, Q, then there exists a unique line l, s.t. $P \in l$ & $Q \in l$. ($l = P + Q$)
- 2, Axiom: Given a point P and a line l, there exists exactly one line m, s.t. $P \in m$ & $m || l$ (m, l are parallel).
- 3, Axiom: There exist three distinct points A, B, C, s.t. $C \notin A + B$; noncollinear points.

The property of some lines to be *parallel* is an equivalence. An equivalence class of parallel lines is called *pencil of parallel lines*.

Dilatation and Translation

Definition (Dilatation and trace)

The map $\sigma : P \to P$ is called *dilatation* if it has the following property:

Let us have two distinct points P and Q, s.t. $\sigma(P) = P'$ and $\sigma(Q) = Q'$ If there is some line $l' || P + Q$ and $P' \in l'$ then also $Q' \in l'$. We call a dilatation σ *degenerate* if it maps all points onto one given point.

Let σ be non-degenerate dilatation and P point on line l, s.t. $\sigma(P) \in l$. If $P \neq \sigma(P)$ then we call the line l the *trace* of σ; $l = P + \sigma(P)$.

Dilatation and Translation

Theorem

Dilatation σ is uniquely determined by the images of points P and Q.

Dilatation and Translation

Theorem

Dilatation σ is uniquely determined by the images of points P and Q.

Definition (Translation and direction)

A non-degenerate dilatation τ is called the *translation* if $\tau = 1$ (identity) or has no fixed point. In this case the trace are called the *direction*.

Dilatation and Translation

Theorem

Dilatation σ is uniquely determined by the images of points P and Q.

Definition (Translation and direction)

A non-degenerate dilatation τ is called the *translation* if $\tau = 1$ (identity) or has no fixed point. In this case the trace are called the *direction*.

Theorem

Translation τ is uniquely determined by the images of one point P.

Dilatation and Translation

Lemma (3)

In given geometry all dilatations form a group $\mathcal{D}$ and all translations form its sub-group $\mathcal{T}$. If σ is a dilatation and $\tau \neq 1$ a translation, then τ and $\sigma\tau\sigma^{-1}$ have the same direction. If the translations are of different directions, then $\mathcal{T}$ is commutative group.

Trace preserving homomorphism

Definition (Trace-preserving homomorphism)

A map $\alpha : \mathcal{T} \to \mathcal{T}$ is called the *trace-preserving homomorphism* if

- α is a homomorphism: $\alpha(\tau_1 \cdot \tau_2) = \alpha(\tau_1) \cdot \alpha(\tau_2)$
- α *preserves* traces; i.e. either $\alpha(\tau) = 1$ or τ and $\alpha(\tau)$ have the same direction.

Trace preserving homomorphism

Definition (Trace-preserving homomorphism)

A map $\alpha : \mathcal{T} \to \mathcal{T}$ is called the *trace-preserving homomorphism* if

- α is a homomorphism: $\alpha(\tau_1 \cdot \tau_2) = \alpha(\tau_1) \cdot \alpha(\tau_2)$
- α *preserves* traces; i.e. either $\alpha(\tau) = 1$ or τ and $\alpha(\tau)$ have the same direction.

The set of all α will be denoted by $\mathcal{K}$.

Trace preserving homomorphism

Definition (Trace-preserving homomorphism)

A map $\alpha : \mathcal{T} \to \mathcal{T}$ is called the *trace-preserving homomorphism* if

- α is a homomorphism: $\alpha(\tau_1 \cdot \tau_2) = \alpha(\tau_1) \cdot \alpha(\tau_2)$
- α *preserves* traces; i.e. either $\alpha(\tau) = 1$ or τ and $\alpha(\tau)$ have the same direction.

The set of all α will be denoted by $\mathcal{K}$.

Examples: $0 : \tau \to 1, \quad 1 : \tau \to \tau, \quad \alpha : \tau \to \tau^{-1}, \quad \alpha : \tau \to \sigma\tau\sigma^{-1}$

Axioms of "symmetry"

- 4, Axiom: Given any two points P, Q, there exists a translation

  $\tau_{PQ} : \tau_{PQ}(P) = Q$.

AXIOMS OF "SYMMETRY"

- 4, Axiom: Given any two points P, Q, there exists a translation $\tau_{PQ} : \tau_{PQ}(P) = Q$.
- 5, Axiom: If τ_1 and τ_2 are translations with the same direction and if $\tau_1 \neq 1$, $\tau_2 \neq 1$, $\tau_1 \neq \tau_2$, then there exists unique $\alpha \in \mathcal{K}$: $\tau_2 = \alpha(\tau_1)$

Axioms of "symmetry"

- 4, Axiom: Given any two points P, Q, there exists a translation $\tau_{PQ} : \tau_{PQ}(P) = Q$.
- 5, Axiom: If τ_1 and τ_2 are translations with the same direction and if $\tau_1 \neq 1$, $\tau_2 \neq 1$, $\tau_1 \neq \tau_2$, then there exists unique $\alpha \in \mathcal{K}$: $\tau_2 = \alpha(\tau_1)$
- 5P, Axiom: For a given point P: Given points Q, R, s.t. P, Q, R are distinct but line on a line, then there exists a dilatation σ: $\sigma(P) = P$ & $\sigma(Q) = R$.

Construction of a ring

Definition

Let α and $\beta \in \mathcal{K}$. We construct maps $\alpha + \beta$ and $\alpha \cdot \beta$:

$$\alpha + \beta : \tau \rightarrow \alpha(\tau) \cdot \beta(\tau)$$

$$\alpha \cdot \beta : \tau \rightarrow \alpha(\beta(\tau))$$

Theorem (Construction of a ring,6)

If α and $\beta \in \mathcal{K}$, then $\alpha + \beta$ and $\alpha \cdot \beta \in \mathcal{K}$. Under this definition the set $\mathcal{K}$ becomes an associative ring with unit element 1 (identity).

Proof

Proof.

Assume we have translations τ_1, τ_2 and α, β, $\gamma \in K$, then

- $(\alpha + \beta)(\tau_1 \cdot \tau_2) = (\alpha + \beta)(\tau_1) \cdot (\alpha + \beta)(\tau_2)$
- $(\alpha \cdot \beta)(\tau_1 \cdot \tau_2) = (\alpha \cdot \beta)(\tau_1) \cdot (\alpha \cdot \beta)(\tau_2)$
- $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
- $\alpha + \beta = \beta + \alpha$
- $0 + \alpha = \alpha, \alpha + (-1) \cdot \alpha = 0 \ldots (\mathcal{K}, +)$ commutative group
- $(\beta + \gamma) \cdot \alpha = \beta \cdot \alpha + \gamma \cdot \alpha, \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$
- $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$
- $1 \cdot \alpha = \alpha; \alpha \cdot 1 = \alpha$

$\square$

"$\mathcal{K}$ IS A FIELD"

Theorem

Let $\alpha \in \mathcal{K}$, $\alpha \neq 0$ and P a point. There exist a unique dilatation σ which has P as fixed point and such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in \mathcal{T}$.

"$\mathcal{K}$ IS A FIELD"

Theorem

Let $\alpha \in \mathcal{K}$, $\alpha \neq 0$ and P a point. There exist a unique dilatation σ which has P as fixed point and such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in \mathcal{T}$.

Theorem

$\mathcal{K}$ is a field (possibly not commutative under multiplication).

"$\mathcal{K}$ IS A FIELD"

Theorem

Let $\alpha \in \mathcal{K}$, $\alpha \neq 0$ and P a point. There exist a unique dilatation σ which has P as fixed point and such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in \mathcal{T}$.

Theorem

$\mathcal{K}$ is a field (possibly not commutative under multiplication).

Proof

Proof.

Let $\alpha \neq 0 \in \mathcal{K}$. Find a dilatation σ such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$.

Proof

Proof.

Let $\alpha \neq 0 \in \mathcal{K}$. Find a dilatation σ such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$. The map which sends τ into $\sigma^{-1}\tau\sigma$, denoted α^{-1} is also in $\mathcal{K}$.

Proof

Proof.

Let $\alpha \neq 0 \in \mathcal{K}$. Find a dilatation σ such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$. The map which sends τ into $\sigma^{-1}\tau\sigma$, denoted α^{-1} is also in $\mathcal{K}$.Thus using the notation τ^{α} instead of $\alpha(\tau)$ we have

$$\tau^{\alpha\cdot\alpha^{-1}} = (\tau^{\alpha^{-1}})^{\alpha} = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1} = \tau^{1}$$

$$\tau^{\alpha^{-1}\cdot\alpha} = (\tau^{\alpha})^{\alpha^{-1}} = \sigma^{-1}(\sigma\tau\sigma^{-1})\sigma = \tau^{1}$$

Proof

Proof.

Let $\alpha \neq 0 \in \mathcal{K}$. Find a dilatation σ such that $\alpha(\tau) = \sigma\tau\sigma^{-1}$. The map which sends τ into $\sigma^{-1}\tau\sigma$, denoted α^{-1} is also in $\mathcal{K}$.Thus using the notation τ^{α} instead of $\alpha(\tau)$ we have

$$\tau^{\alpha\cdot\alpha^{-1}} = (\tau^{\alpha^{-1}})^{\alpha} = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1} = \tau^{1}$$

$$\tau^{\alpha^{-1}\cdot\alpha} = (\tau^{\alpha})^{\alpha^{-1}} = \sigma^{-1}(\sigma\tau\sigma^{-1})\sigma = \tau^{1}$$

This shows that $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$ and establishes an existence of an inverse. $\square$

INTRODUCTION TO COORDINATES

Theorem

Let $\tau_1 \neq 1$, $\tau_2 \neq 1$ *and* $\tau_1 \neq \tau_2$ *be translations with different directions. To any translation* $\tau \in \mathcal{T}$ *there exist unique* $\alpha, \beta \in \mathcal{K}$, *s.t.*

$\tau = \alpha(\tau_1) \cdot \beta(\tau_2) = \beta(\tau_2) \cdot \alpha(\tau_1)$.

Introduction to coordinates

Theorem

Let $\tau_1 \neq 1$, $\tau_2 \neq 1$ and $\tau_1 \neq \tau_2$ be translations with different directions. To any translation $\tau \in \mathcal{T}$ there exist unique α, $\beta \in \mathcal{K}$, s.t.

$\tau = \alpha(\tau_1) \cdot \beta(\tau_2) = \beta(\tau_2) \cdot \alpha(\tau_1)$.

Now select point $\mathcal{O}$ (origin) and translations τ_1, τ_2 like above. τ_1-trace and τ_2-trace trough $\mathcal{O}$ shall be coordinate axis and points $\tau_1(\mathcal{O})$, $\tau_2(\mathcal{O})$ shall be "unit points". Let now P be any point. we write the translation τ_{OP} in the form $\tau_{OP} = \alpha(\tau_1) \cdot \beta(\tau_2)$ with unique $\alpha, \beta \in \mathcal{K}$ and assign to P the pair (α, β) as *coordinates*.

DESAURUES' THEOREM

Theorem (Desaurgues' theorem,7)

Let l_1, l_2, l_3 be distinct lines, which are either parallel or meet in some point P. If $Q, Q' \in l_1$, $R, R' \in l_2$ and $S, S' \in l_3$ and we assume that $Q + R || Q' + R'$ and $Q + S || Q' + S'$ then also $S + R || S' + R'$.

DESAURUES' THEOREM

Theorem (Desaurgues' theorem,7)

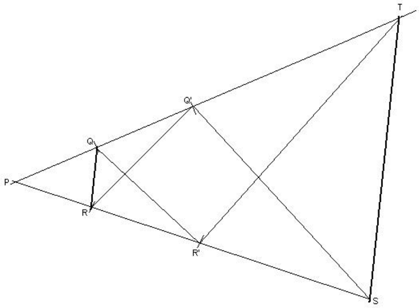
Let l_1, l_2, l_3 be distinct lines, which are either parallel or meet in some point P. If $Q, Q' \in l_1$, $R, R' \in l_2$ and $S, S' \in l_3$ and we assume that $Q + R || Q' + R'$ and $Q + S || Q' + S'$ then also $S + R || S' + R'$.

Theorem (8)

Desaurgues' theorem holds in projective geometry where all 5 axioms hold.

PAPPUS' THEOREM

The Pappus' theorem is the following configuration:



$Q+R'$ and $Q'+S$, $Q'+R$ and $R'+T$, $Q+R$ and $T+S$ are pairs of opposite sides of the hexagon. Now "if two of these pairs are parallel, so is the third" (PT).

Pappus' theorem

Select $P \in \mathcal{P}$, $\alpha \neq 0 \in \mathcal{K}$, by only one σ_α we can obtain $\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}$, also for β $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$.

PAPPUS' THEOREM

Select $P \in \mathcal{P}$, $\alpha \neq 0 \in \mathcal{K}$, by only one σ_α we can obtain $\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}$, also for β $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$.Then

$$\tau^{\alpha \cdot \beta} = (\tau^\beta)^\alpha = \sigma_\alpha \sigma_\beta \tau \sigma_\beta^{-1} \sigma_\alpha^{-1} = \sigma_\alpha \sigma_\beta \tau (\sigma_\alpha \sigma_\beta)^{-1}$$

Pappus' theorem

Select $P \in \mathcal{P}$, $\alpha \neq 0 \in \mathcal{K}$, by only one σ_α we can obtain $\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}$, also for β $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$.Then

$$\tau^{\alpha \cdot \beta} = (\tau^\beta)^\alpha = \sigma_\alpha \sigma_\beta \tau \sigma_\beta^{-1} \sigma_\alpha^{-1} = \sigma_\alpha \sigma_\beta \tau (\sigma_\alpha \sigma_\beta)^{-1}$$

$$\tau^{\alpha \cdot \beta} = \sigma_{\alpha \cdot \beta} \tau \sigma_{\alpha \cdot \beta}^{-1}$$

Pappus' theorem

Select $P \in \mathcal{P}$, $\alpha \neq 0 \in \mathcal{K}$, by only one σ_α we can obtain $\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}$, also for β $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$.Then

$$\tau^{\alpha \cdot \beta} = (\tau^\beta)^\alpha = \sigma_\alpha \sigma_\beta \tau \sigma_\beta^{-1} \sigma_\alpha^{-1} = \sigma_\alpha \sigma_\beta \tau (\sigma_\alpha \sigma_\beta)^{-1}$$

$$\tau^{\alpha \cdot \beta} = \sigma_{\alpha \cdot \beta} \tau \sigma_{\alpha \cdot \beta}^{-1}$$

$\Rightarrow \sigma_{\alpha \cdot \beta} = \sigma_\alpha \cdot \sigma_\beta$.

PAPPUS' THEOREM

Select $P \in \mathcal{P}$, $\alpha \neq 0 \in \mathcal{K}$, by only one σ_α we can obtain $\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}$, also for β $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$.Then

$$\tau^{\alpha\cdot\beta} = (\tau^\beta)^\alpha = \sigma_\alpha \sigma_\beta \tau \sigma_\beta^{-1} \sigma_\alpha^{-1} = \sigma_\alpha \sigma_\beta \tau (\sigma_\alpha \sigma_\beta)^{-1}$$

$$\tau^{\alpha\cdot\beta} = \sigma_{\alpha\cdot\beta} \tau \sigma_{\alpha\cdot\beta}^{-1}$$

$\Rightarrow \sigma_{\alpha\cdot\beta} = \sigma_\alpha \cdot \sigma_\beta$.

The mult. group of non-zero elements from $\mathcal{K} \sim$ group of dilatations which have P as fixed point. $\mathcal{K}$ commutative $\Leftrightarrow \mathcal{D}$ commutative.

Pappus' theorem

Now select $m \neq l \in \mathcal{L}$, $P \in l, m$, $Q \neq P$, $Q \in l$,$R \neq P$, $R \in m$.

σ_1 dilatation: $\sigma_1(P) = P$, $l = \sigma_1-$trace, $\sigma_1(Q) = Q' \neq P$ (A5).

σ_2 dilatation: $\sigma_2(P) = P$, $m = \sigma_2-$trace, $\sigma_2(R) = R' \neq P$ (A5).

Construct $S = \sigma_1\sigma_2(R) \in m$, $T = \sigma_2\sigma_1(Q) \in l$ - given by

$$Q + R' || \sigma_1(Q) + \sigma_1(R') || Q' + \sigma_1\sigma_2(R) = Q' + S$$

$$R + Q' || \sigma_2(R) + \sigma_2(Q') || R' + \sigma_2\sigma_1(Q) = R' + T$$

$\sigma_1\sigma_2 = \sigma_2\sigma_1 \Leftrightarrow \sigma_1\sigma_2(Q) = \sigma_2\sigma_1(Q)$ or $\sigma_1\sigma_2(Q) = T$. Since $\sigma_1\sigma_2(Q) \in l$ it is determined by $Q + R || \sigma_1\sigma_2(Q) + \sigma_1\sigma_2(R) = \sigma_1\sigma_2(Q) + S$ and set $Q + R || T + S$ - condition for commutativity.

Pappus' theorem and commutative law

Theorem (Artin E., Geometric algebra, 1964)

The field $\mathcal{K}$ is commutative iff in given geometry the Pappus' theorem holds.

Pappus' theorem and commutative law

Theorem (Artin E., Geometric algebra, 1964)

The field $\mathcal{K}$ is commutative iff in given geometry the Pappus' theorem holds.

Proof.

- relation between mult. group of non-zero elements of $\mathcal{K}$ and group of dilatations with same fixed point P
- application of σ_1, σ_2 on points defined in Pappus' theorem: Q, R; i.e. $\sigma_1(Q) = Q'$, $\sigma_2(R) = R'$ (construct $S = \sigma_1\sigma_2(R)$, $T = \sigma_2\sigma_1(Q)$)
- configuration of T and S determined by pairs of parallel lines

□

Wedderburns' theorem

Theorem (Wedderburns' theorem)

Every field with a finite number of elements is commutative.

WEDDERBURNS' THEOREM

Theorem (Wedderburns' theorem)

Every field with a finite number of elements is commutative.

According to this theorem there is a geometric application:

Lemma (10)

In a Desarguesian plane with only finite number of points the Pappus' theorem holds.

APPLICATION RESULTS ON LATTICES

- linear subspaces of projective space form a modular geometric lattice
- linear subspaces define the geometry whose subspaces are exactly the linear spaces (projective geometry)

Theorem (11)

Let L be modular geometric lattice. Then L satisfies the arguesian identity iff Desaurues' theorem holds in associate projective geometry and there exists a field $\mathcal{K}$ which elements are exactly the atoms in L.

THANK YOU FOR YOUR ATTENTION