Universität Zürich[UZH]

Institut für Mathematik

Master Thesis

Classical Circle Theorems in Miquelian Möbius Planes

Author:
Vanessa Loureiro

Supervisors:
Prof. Dr. Norbert Hungerbühler (ETH Zürich)
PD Dr. Lorenz Halbeisen (ETH Zürich)

Co-Supervisor:
Prof. Dr. Andrew Kresch (Universität Zürich)

June 24, 2021

Abstract

Finite Miquelian Möbius planes may be explicitly constructed over the pair of finite fields $\mathrm{GF}(p^n)$ and $\mathrm{GF}(p^{2n})$, where p is a prime number and n a positive integer. With thereby resulting properties, we prove that the *five circles theorem* and *Miquel's pentagon theorem* both hold true in these planes. The key roles in the proofs are the introduction of the reflection at a block and the cross-ratio.

The abstract definition of Miquelian Möbius planes considered as an incidence structure involves four axioms. We prove that these axioms imply *Clifford's first and second circle theorems*, resulting in their validity in Miquelian Möbius planes. Moreover, we show that the latter two theorems are in turn equivalent to *Miquel's pentagon theorem* and *Steiner's quadrilateral theorem*, respectively.

Acknowledgements

First of all, I would like to express my sincere gratitude to my primary supervisor Prof. Dr. Norbert Hungerbühler, who introduced me to this topic and guided me throughout this thesis. Further, I would like to extend my sincere thanks to PD Dr. Lorenz Halbeisen for his dedicated support. I am extremely grateful for the valuable and encouraging meetings they provided me.

I would also like to thank Prof. Dr. Andrew Kresch for enabling the realization of this thesis as my co-supervisor on the part of the University of Zurich.

Contents

Abstract **iii**

Acknowledgements **v**

1 Introduction **1**

2 Preliminaries **5**
2.1 Finite Fields 5
2.1.1 Characterization 5
2.1.2 Automorphisms 7
2.1.3 Quadratic Field Extensions 8
2.2 Incidence Structures 11

3 Introduction to Miquelian Möbius Planes **13**
3.1 The Möbius Plane 13
3.2 Miquel's Theorem 17
3.3 Finite Miquelian Möbius Planes 18
3.3.1 Construction 18
3.3.2 Intersection Points of Two Blocks 31
3.3.3 The Plane $\mathcal{M}_{11}$ 36

4 Circle Theorems in Finite Miquelian Möbius Planes **39**
4.1 The Five Circles Theorem 39
4.1.1 Verification in $\mathcal{M}_{11}$ 39
4.1.2 The General Case 43
4.2 Miquel's Pentagon Theorem 54

5 A Connection to Clifford's Circle Theorems **59**
5.1 Clifford's First and Second Circle Theorems 60
5.2 Miquel-Clifford Configurations 65
5.2.1 Steiner's Quadrilateral Theorem 65
5.2.2 Miquel's Pentagon Theorem 66
5.3 Summary Diagram 69

A Code for Calculations in $\mathcal{M}_{11}$ **70**

B Computations in Mathematica **76**
B.1 The Five Circles Theorem 76

B.2 Miquel's Pentagon Theorem 78

C An Open Question **82**

Bibliography **86**

Chapter 1

Introduction

Auguste Miquel was born in 1816 in southern France. He was only 18 years old when he published beautiful geometric discoveries concerning the intersection of lines and circles in the newly founded journal of Joseph Liouville[1]. The first of these results indeed became the most famous one and is known as Miquel's theorem (or Miquel's triangle theorem). According to its original version, the theorem states the following.

Miquel's Theorem. Let k_1, k_2, and k_3 be three circles through a point I and otherwise in general position. Let P_{ij} be the second intersection point of the circles k_i and k_j for $i, j \in \{1, 2, 3\}$ with $i < j$, and let A be an arbitrary point on k_1 distinct from I, P_{12}, and P_{13}. Now let B be the second intersection point of the line $\overrightarrow{A\,P_{12}}$ and k_2, and let C be the second intersection point of the line $\overrightarrow{A\,P_{13}}$ and k_3. Then the points B, C, and P_{23} are collinear.

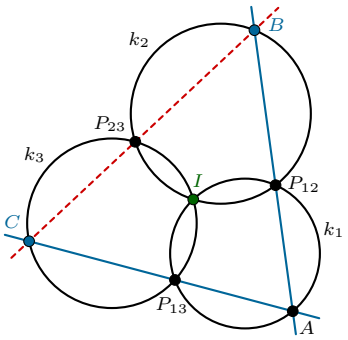


FIGURE 1.1: Miquel's theorem.

The proof is indeed elementary as the theorem follows directly from the properties of cyclic quadrilaterals (cf. [Miq36]). Also Miquel considered this result only as a stepping stone to prove his pentagon theorem and a theorem proposed in 1827/28 by the Swiss mathematician Jakob Steiner[2]. In fact, the latter two theorems can both

[1] Journal de mathématiques pures et appliquées [Miq36].
[2] "Questions proposées. Théorème sur le quadrilatère complet" [Ste28].

be proved with the repeated application of Miquel's theorem (cf. [Miq36] or [Var18]). Let us now also introduce these two theorems.

Steiner's Quadrilateral Theorem. The circumcircles of all four triangles of a complete quadrilateral are concurrent in a point M called the *Miquel point*.

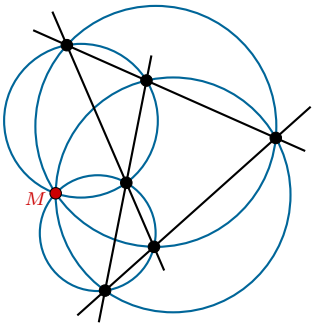


FIGURE 1.2: Steiner's quadrilateral theorem.

Miquel's Pentagon Theorem. Let $ABCDE$ be a convex pentagon, and let F, G, H, I, and J be the intersection points of the extended sides of the pentagon. Consider the circumcircles of the five triangles AFB, BGC, CHD, DIE, and EJA. Then the second intersection points of the circumcircles are concyclic.

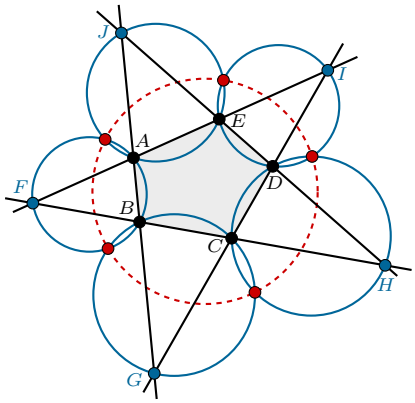


FIGURE 1.3: Miquel's pentagon theorem.

Around 50 years later, in 1882, the English mathematician William K. Clifford gave a different proof for Miquel's pentagon theorem using parabolas. In this way, Clifford generalized Miquel's results in the sense that he progressively increased the number of lines and circles involved (cf. [Cli82], p.51–52):

"$2n$ *lines determine* $2n$ *circles all meeting in a point;*
and for $2n+1$ *lines the* $2n+1$ *points so found lie on the same circle."*

Evidently, we obtain for $n = 2$ precisely Steiner's quadrilateral theorem and Miquel's pentagon theorem.

Thus Clifford obtained a sequence of increasing complexity each building on the previous. It was then found that the $2n$ and $2n + 1$ lines can be replaced by concurrent circles, which results in a more symmetric configuration. This step leads us to Clifford's circle theorems (cf. [Cox61], p.262).

Clifford's First Circle Theorem. Let $k_1, \ldots, k_4$ be four circles through a point P and otherwise in general position. Let P_{ij} be the second intersection point of the circles k_i and k_j for $i, j \in \{1, \ldots, 4\}$ with $i < j$, and let k_{ijl} denote the circle through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \ldots, 4\}$. Then the four circles $k_{123}, k_{124}, k_{134}$, and k_{234} all pass through one point P_{1234}.

Clifford's Second Circle Theorem. Let k_5 be a fifth circle through P. Then the five points $P_{1234}, P_{1235}, P_{1245}, P_{1345}$, and P_{2345} determined by Clifford's first circle theorem all lie on one circle k_{12345}.

Clifford's Third Circle Theorem. Let k_6 be a sixth circle through P. Then the six circles $k_{12345}, k_{12346}, k_{12356}, k_{12456}$, k_{13456}, and k_{23456} determined by Clifford's second circle theorem all pass through one point P_{123456}.

And so the chain continues with the closure alternately on a point or on a circle.

In 1907, a further theorem connected to Miquel's pentagon theorem was given by the English mathematician Frank Morley. He reversed the statement of Miquel's pentagon theorem and obtained the following.

The Five Circles Theorem. Given five circles centered on a sixth circle k and intersecting each other chainwise on k, then the lines joining their second intersection points form a pentagram whose points lie on the circles themselves.

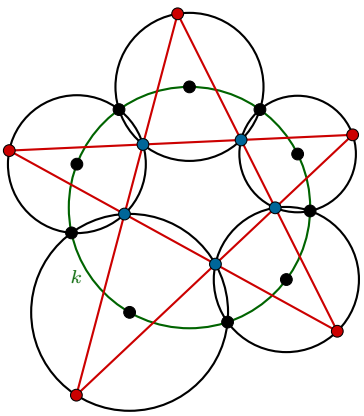


FIGURE 1.4: The five circles theorem.

A proof of this theorem that is based on simple properties of the Euclidean plane can be found in [Dan16].

All of the stated classical circle theorems were thoroughly studied in the Euclidean plane. However, the just mentioned transition from Miquel's pentagon theorem to Clifford's second circle theorem suggests that we consider the theorems in Möbius planes in which lines and circles are merged to a set of blocks. An accordingly adapted version of Miquel's theorem has already been rigorously investigated in Möbius planes and even became *the* classifying result for a certain class of Möbius planes, namely Miquelian Möbius planes (cf. [WS35] and [Che70]).

We consider the five circles theorem and Miquel‘s pentagon theorem in Miquelian Möbius planes of order q, where q is a prime power. Consequently, we also adapt the theorems using the notions of Möbius planes. This results in a case distinction for the five circles theorem and a generalization for Miquel‘s pentagon theorem in these planes. Clifford's circle theorems, on the other hand, can be stated analogously in Möbius planes. We consider Clifford's first and second circle theorems in Miquelian Möbius planes with a possibly infinite number of points. As introduced before, the connections between Steiner's quadrilateral theorem, Miquel's pentagon theorem, and Clifford's circle theorems are well-known, but we examine their dependence in Miquelian Möbius planes.

We start with some background on finite fields in chapter 2. In chapter 3, we introduce Miquelian Möbius planes and construct finite Miquelian Möbius planes over the pair of finite fields $\mathrm{GF}(q)$ and $\mathrm{GF}(q^2)$, where q is a prime power. With this, we prove in chapter 4 that the five circles theorem and Miquel's pentagon theorem are true in finite Miquelian Möbius planes of order q. In chapter 5, we prove Clifford‘s first and second circle theorems using only the three axioms of Möbius planes and Miquel's theorem. Moreover, we show that Clifford's first circle theorem is equivalent to Steiner's quadrilateral theorem and that Clifford's second circle theorem is equivalent to Miquel's pentagon theorem in Miquelian Möbius planes.

Chapter 2

Preliminaries

We begin by recalling some basics about finite fields since we are working later on in finite Miquelian Möbius planes that are constructed over the pair of finite fields $GF(p^n)$ and $GF(p^{2n})$, where p is a prime and n a positive integer. Therefore, we investigate in section 2.1 the existence of fields with p^n elements, consider automorphisms of finite fields, and examine $\mathrm{GF}(p^{2n})$ as the quadratic extension field of $\mathrm{GF}(p^n)$. In section 2.2, we recall the definition of an incidence structure, which we will need for the definition of Möbius planes.

This chapter is mainly based on [Hun17] and [Hun18], but the definitions and results can also be found in lots of algebra books, such as [LN96]. For results that are not proved in these background sections, a reference is always provided.

2.1 Finite Fields

2.1.1 Characterization

We immediately start with an important classification result due to E. H. Moore from 1893/94 [Moo94]:

Theorem 2.1.1. Every finite field is of order p^m for some prime number p and some positive integer m. Conversely, if p is a prime number and m a positive integer, then there are fields of order p^m and they are all isomorphic.

We can thus identify finite fields with the same number of elements. The concept of finite fields was introduced in 1830 by Évariste Galois, and for this reason, finite fields are also called *Galois fields*. Accordingly, we use the following notation.

Notation. $\mathrm{GF}(p^m)$ is the (up to isomorphsims) unique field with p^m elements for a prime number p and a positive integer m.

Firstly, let us take a look at the case $m = 1$ of theorem 2.1.1: A finite field of order p (with p prime) may be constructed as the integers modulo p. The p elements of $\mathrm{GF}(p)$ are then represented by $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}$, where $\overline{a} := a + p\mathbb{Z}$ for $a \in \mathbb{Z}$. The operations

are defined through the usual addition and multiplication on the ring $(\mathbb{Z}, +, \cdot)$ by

$$\overline{a} \oplus \overline{b} := \overline{a + b} \text{ and } \overline{a} \odot \overline{b} := \overline{a \cdot b}.$$

Then $\big(\mathrm{GF}(p), \oplus, \odot\big)$ is a field of order p (cf. [LN96], theorem 1.38).

Secondly, we consider the case $m > 1$ of theorem 2.1.1: A finite field of order p^m (with p prime and $m \in \mathbb{N}_{>1}$) may be constructed as the polynomials with coefficients in $\mathrm{GF}(p)$ modulo an irreducible polynomial of degree m. So let us recall the definition of irreducible polynomials.

Definition 2.1.2. Let K be a field and $K[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid n \in \mathbb{N}_0, a_i \in K\}$ the set of polynomials in x with coefficients in K. Let $\alpha \in K[x] \backslash K$. If it holds that

$$\forall \mu, \nu \in K[x] \big(\alpha = \mu \cdot \nu \longrightarrow \mu \in K \vee \nu \in K\big),$$

then α is called an *irreducible polynomial* over $K[x]$.

Now let φ be an irreducible polynomial of degree m over $\mathrm{GF}(p)[x]$. The following lemma assures that we can always find such a polynomial (cf. [Neu08], corollary 6.14).

Lemma 2.1.3. For every $m \in \mathbb{N}$, there exists an irreducible polynomial φ of degree m over $\mathrm{GF}(p)[x]$.

The elements of $\mathrm{GF}(p^m)$ are then represented as polynomials $\alpha = \overline{a_{m-1}} x^{m-1} + \cdots + \overline{a_1} x + \overline{a_0}$ with $\overline{a_i} \in \mathrm{GF}(p)$ for $i \in \{0, \ldots, m-1\}$, which evidently gives us exactly p^m elements as needed. The operations are defined through the usual addition and multiplication on the polynomial ring $\big(\mathrm{GF}(p)[x], +, \cdot\big)$ by

$$\alpha \boxplus \beta := \alpha + \beta \text{ and } \alpha \boxdot \beta := \alpha \cdot \beta \pmod{\varphi}.$$

Then $\big(\mathrm{GF}(p^m), \boxplus, \boxdot\big)$ is a field of order p^m (cf. [LN96], theorem 1.61).

Convention. From now on, we omit the overline in the notation of the elements of $\mathrm{GF}(p)$. The line above an element will denote the conjugate element in the following (q.v. definition 2.1.17).

Example 2.1.4. We consider now the finite field $\mathrm{GF}(11^2)$, which we will later use again as an example for the construction of the Miquelian Möbius plane of order 11. To construct $\mathrm{GF}(11^2)$, we need an irreducible polynomial of degree 2 over $\mathrm{GF}(11)[x]$.

Claim. The polynomial $\varphi(x) = x^2 + 1$ is irreducible over $\mathrm{GF}(11)[x]$.

Proof. $\mathrm{GF}(11)[x]$ is a factorial ring (cf. [LN96], theorem 1.59). That is to say that every polynomial (except the zero polynomial) has a unique factorization into irreducible polynomials (up to order). Thus if φ were not irreducible, we could write φ as a product of linear factors $x - r$ that correspond to roots $r \in \mathrm{GF}(11)$ of φ. Such a root r would have the property that $r^2 = -1$, which implies that $r \neq 1$ and $r \neq -1$. Therefore, $r^3 = -r \neq 1$ and $r^4 = 1$. This means that the order of r in the

multiplicative group of GF(11) is 4. Lagrange's theorem tells us that every element of the group divides the order of the group. Since the order of the multiplicative group of GF(11) is 10 and $4 \nmid 10$, we conclude that there is no such element r. Thus φ is irreducible over GF(11)$[x]$. □

As mentioned, we can represent the elements of $\mathrm{GF}(11^2)$ as polynomials

$$a + bx, \text{ where } a, b \in \mathrm{GF}(11).$$

For $\alpha, \beta \in \mathrm{GF}(11^2)$ with $\alpha = a_1 + a_2 x$ and $\beta = b_1 + b_2 x$, we set

$$\alpha \boxplus \beta = (a_1 + b_1) + (a_2 + b_2)x \text{ and } \alpha \boxdot \beta = (a_1 + a_2 x) \cdot (b_1 + b_2 x) \pmod{x^2 + 1}.$$

With this, the field $\mathrm{GF}(11^2)$ is explicitly constructed.

The question now arises how two different fields $\mathrm{GF}(p^m)$ and $\mathrm{GF}(p^n)$ with $m < n \in \mathbb{N}$ are connected. In fact, there is a simple way to check whether $\mathrm{GF}(p^n)$ contains $\mathrm{GF}(p^m)$ (cf. [Neu08], theorem 6.7):

Theorem 2.1.5. $\mathrm{GF}(p^m)$ is a subfield of $\mathrm{GF}(p^n)$ if and only if $m \mid n$.

The smallest subfield of $\mathrm{GF}(p^m)$ is thus $\mathrm{GF}(p)$. We call $\mathrm{GF}(p)$ the *prime field* of $\mathrm{GF}(p^m)$.

2.1.2 Automorphisms

Let us first recall the binomial theorem in finite fields (cf. [LN96], theorem 1.46).

Lemma 2.1.6. Let $\alpha, \beta \in \mathrm{GF}(p^m)$. Then the following holds:

- $(\alpha + \beta)^p = \alpha^p + \beta^p$,
- $(\alpha - \beta)^p = \alpha^p - \beta^p$,
- $(\alpha \cdot \beta)^p = \alpha^p \cdot \beta^p$.

These identities suggest that we consider the map

$$F_p \colon \mathrm{GF}(p^m) \longrightarrow GF(p^m); \ \alpha \longmapsto \alpha^p.$$

And indeed, we can show with lemma 2.1.6 that F_p is in fact an automorphism of $\mathrm{GF}(p^m)$ in the following way:

- *F_p is bijective:* Let $\alpha, \beta \in \mathrm{GF}(p^m)$ and suppose that $F_p(\alpha) = F_p(\beta)$. Then

  $$0 = \alpha^p - \beta^p \iff 0 = (\alpha - \beta)^p \iff \alpha = \beta.$$

  So F_p is injective. As the field $\mathrm{GF}(p^m)$ is finite, it follows that F_p is surjective as well.

- *F_p is a field homomorphism:* Let $\alpha, \beta \in \mathrm{GF}(p^m)$. Then:

  (i) $F_p(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = F_p(\alpha) + F_p(\beta)$.

(ii) $F_p(\alpha \cdot \beta) = (\alpha \cdot \beta)^p = \alpha^p \cdot \beta^p = F_p(\alpha) \cdot F_p(\beta)$.

(iii) $F_p(0) = 0$ and $F_p(1) = 1$.

Definition 2.1.7. The map

$$\begin{aligned} F_p \colon \mathrm{GF}(p^m) &\longrightarrow GF(p^m), \\ \alpha &\longmapsto \alpha^p. \end{aligned}$$

is called *Frobenius automorphism*.

Since the composition of two automorphisms is again an automorphism, we immediately find that

$$F_p^{(k)} \colon \alpha \mapsto \alpha^{p^k} \text{ for } 0 < k < m$$

are automorphisms of $\mathrm{GF}(p^m)$ as well. Observe that $F_p^{(m)} = \mathrm{id}$, since Lagrange's theorem implies that $\alpha^{p^m} = \alpha$ for all $\alpha \in \mathrm{GF}(p^m)$.
It turns out that there are no other automorphisms of $\mathrm{GF}(p^m)$ (cf. [Neu08], theorem 10.8):

Theorem 2.1.8. The automorphisms of $\mathrm{GF}(p^m)$ are precisely the Frobenius automorphism F_p and its functional powers $F_p^{(k)} = \underbrace{F \circ F \circ \cdots \circ F}_{k \text{ times}}$.

Moreover, since $F_p(0) = 0$, $F_p(1) = 1$, $F_p(2) = F_p(1+1) = F_p(1) + F_p(1) = 2$, and so on, we obtain the following lemma.

Lemma 2.1.9. The Frobenius automorphism F_p of $\mathrm{GF}(p^m)$ keeps exactly the elements of the prime field $\mathrm{GF}(p)$ fixed.

2.1.3 Quadratic Field Extensions

We saw that $\mathrm{GF}(p^n)$ is a subfield of $\mathrm{GF}(p^{2n})$, since $n \mid 2n$ (q.v. theorem 2.1.5). In other words, $\mathrm{GF}(p^{2n})$ is an *extension field* of $\mathrm{GF}(p^n)$. A field can always be regarded as a vector space over any of its subfields (where the "vectors" are the field elements, and the "scalars" are the elements of the subfield). Therefore, we define the degree of a field extension as follows (cf. [LN96], definition 1.83).

Definition 2.1.10. Let L be an extension field of K. If L (considered as a vector space over K) is finite-dimensional, then L is called a *finite extension field* of K. The dimension d of the vector space L over K is called the *degree* of L over K. In symbols: $[L : K] = d$.

Example 2.1.11. Consider the field extension $\mathbb{R} \subseteq \mathbb{C}$. Since $\mathbb{C}$ is a vector space of dimension 2 over $\mathbb{R}$ (with basis $\{1, i\}$), it follows that $\mathbb{C}$ is an extension field of $\mathbb{R}$ of degree 2. As $[\mathbb{C} : \mathbb{R}] = 2$, we also say that $\mathbb{C}$ is a *quadratic* extension field of $\mathbb{R}$.

Example 2.1.12. Let K be a field with p elements, and let L be a finite extension field of K of degree m. Then L has p^m elements.

Proof. We consider L as a vector space over K. Since $[L : K] = m < \infty$, it follows that L has a basis over K consisting of m elements, say $b_1, \dots, b_m$. This means that every element of L has a unique representation given by $k_1 b_1 + \cdots + k_m b_m$ for some $k_i \in K$ with $i \in \{1, \dots, m\}$. Consequently, L has exactly p^m elements, as there are p possibilities for each $k_i \in K$. □

An important result to compute the degree of a field extension is given by the following theorem (cf. [LN96], theorem 1.84).

Theorem 2.1.13. Let L and M be finite extension fields of K and L, respectively. Then M is a finite extension field of K with degree

$$[M : K] = [M : L] \cdot [L : K].$$

With this, we can compute the degree of the field extension $\mathrm{GF}(p^n) \subseteq \mathrm{GF}(p^{2n})$:

$$[\mathrm{GF}(p^{2n}) : \mathrm{GF}(p^n)] = \frac{[\mathrm{GF}(p^{2n}) : \mathrm{GF}(p)]}{[\mathrm{GF}(p^n) : \mathrm{GF}(p)]} = \frac{2n}{n} = 2.$$

Observation 2.1.14. $\mathrm{GF}(p^{2n})$ is the quadratic extension field of $\mathrm{GF}(p^n)$.

We specifically consider now the automorphism $F_p^{(n)}$ of $\mathrm{GF}(p^{2n})$.

Proposition 2.1.15. The map

$$\begin{aligned} F_p^{(n)} \colon \mathrm{GF}(p^{2n}) &\longrightarrow GF(p^{2n}), \\ \alpha &\longmapsto \alpha^{p^n}. \end{aligned}$$

is an automorphism of $\mathrm{GF}(p^{2n})$ that keeps exactly the elements of $\mathrm{GF}(p^n)$ fixed.

Proof. From theorem 2.1.8, we know that $F_p^{(n)}$ is an automorphism of $\mathrm{GF}(p^{2n})$. Thus we are left to prove that $F_p^{(n)}(\alpha) = \alpha$ if and only if $\alpha \in \mathrm{GF}(p^n)$. For this, we consider the polynomial

$$\psi(x) := x^{p^n} - x \in \mathrm{GF}(p)[x].$$

From Lagrange's theorem we know that $x^{p^n} = x$ for all $x \in \mathrm{GF}(p^n)$. This means that all p^n elements of $\mathrm{GF}(p^n)$ are roots of ψ. But the polynomial ψ is of degree p^n and has therefore at most p^n roots over $\mathrm{GF}(p^{2n})$. Consequently, $F_p^{(n)}$ keeps exactly the elements of $\mathrm{GF}(p^n)$ fixed. □

Remark 2.1.16. Observe that the complex conjugation behaves in a similar way with respect to $\mathbb{C}$ and $\mathbb{R}$ (cf. [Ben73], chapter 1): The map

$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{C}, \\ x + iy &\longmapsto x - iy \ \text{ (with } x, y \in \mathbb{R}) \end{aligned}$$

is an automorphism of $\mathbb{C}$ that keeps exactly the elements of $\mathbb{R}$ fixed.

The analogy between the behaviour of $F_p^{(n)}$ with respect to $\mathrm{GF}(p^{2n})$ and $\mathrm{GF}(p^n)$ and the behaviour of the complex conjugation with respect to $\mathbb{C}$ and $\mathbb{R}$ gives reason for the following definition.

Definition 2.1.17. For $z \in \mathrm{GF}(p^{2n})$, we call

(i) $\overline{z} := F_p^{(n)}(z) = z^{p^n}$ the *conjugate element* of z over $\mathrm{GF}(p^n)$,

(ii) $\|z\| := z \cdot \overline{z}$ the *norm* of z over $\mathrm{GF}(p^n)$,

(iii) $\mathrm{Tr}(z) := z + \overline{z}$ the *trace* of z over $\mathrm{GF}(p^n)$.

Then, in accordance with the properties of the complex conjugation, we obtain the following results.

Lemma 2.1.18. For all $z \in \mathrm{GF}(p^{2n})$ it holds that:

(a) $\overline{\overline{z}} = z$,

(b) $\overline{\|z\|} = \|z\|$,

(c) $\overline{\mathrm{Tr}(z)} = \mathrm{Tr}(z)$.

Proof. (a) $\overline{\overline{z}} = \left(z^{p^n}\right)^{p^n} = z^{p^n p^n} = z^{p^{2n}}$. As the order of the multiplicative group of $\mathrm{GF}(p^{2n})$ is $p^{2n} - 1$, it follows from Lagrange's theorem that $z^{p^{2n}} = z$, and thus, $\overline{\overline{z}} = z$.

(b) $\overline{\|z\|} = \overline{z \cdot \overline{z}} = \overline{z} \cdot \overline{\overline{z}} \overset{\text{(a)}}{=} \overline{z} \cdot z = \|z\|$.

(c) $\overline{\mathrm{Tr}(z)} = \overline{z + \overline{z}} = \overline{z} + \overline{\overline{z}} \overset{\text{(a)}}{=} \overline{z} + z = \mathrm{Tr}(z)$.

□

Observation 2.1.19. Since the automorphism $F_p^{(n)}$ of $\mathrm{GF}(p^{2n})$ fixes exactly the elements of $\mathrm{GF}(p^n)$ (q.v. proposition 2.1.15), it follows that

$$z \in \mathrm{GF}(p^n) \iff z = \overline{z}.$$

Also, lemma 2.1.18 and observation 2.1.19 imply the following.

Corollary 2.1.20. For $z \in \mathrm{GF}(p^{2n})$ it holds that

$$\mathrm{Tr}(z) \in \mathrm{GF}(p^n) \quad \text{and} \quad \|z\| \in \mathrm{GF}(p^n).$$

We finish the preparatory work on finite fields by recalling squares in $\mathrm{GF}(p^m)$ (cf. [HK15]).

Definition 2.1.21. An element $s \in \mathrm{GF}(p^m)$ is called a *square* in $\mathrm{GF}(p^m)$ if there exists an element $r \in \mathrm{GF}(p^m)$ such that $s = r^2$. Otherwise, s is called a *nonsquare* in $\mathrm{GF}(p^m)$.

Note that the associated polynomial $\varphi(x) = x^2 - s$ is of degree 2 and has thus at most two roots over $\mathrm{GF}(p^m)$. If $r \in \mathrm{GF}(p^m)$ is a root, then $-r \in \mathrm{GF}(p^m)$ is a root as well.

Notation. If s is a square in $\mathrm{GF}(p^m)$, then $\sqrt{s}$ denotes any of the two roots of $\varphi(x) = x^2 - s$ over $\mathrm{GF}(p^m)$.

Since $\mathrm{GF}(p^{2n})$ is the quadratic field extension over $\mathrm{GF}(p^n)$, we obtain the following lemma (cf. [HK15]).

Lemma 2.1.22. Every element of $\mathrm{GF}(p^n)$ is a square in $\mathrm{GF}(p^{2n})$.

We can use lemma 2.1.22 and the properties of the automorphism $F_p^{(n)}$ to establish a condition that allows us to check more efficiently whether an element $s \in \mathrm{GF}(p^n)$ is also a square in $\mathrm{GF}(p^n)$:

Lemma 2.1.23. Let $s \in \mathrm{GF}(p^n)$. For $\sqrt{s} \in \mathrm{GF}(p^{2n})$ it holds that:

(i) If s is a square in $\mathrm{GF}(p^n)$, then $\overline{\sqrt{s}} = \sqrt{s}$.

(ii) If s is a nonsquare in $\mathrm{GF}(p^n)$, then $\overline{\sqrt{s}} = -\sqrt{s}$.

Proof. (i) Let $s \in \mathrm{GF}(p^n)$ be a square in $\mathrm{GF}(p^n)$. Then we obtain from lemma 2.1.22 that $\sqrt{s} \in \mathrm{GF}(p^n)$. Now observation 2.1.19 immediately implies that $\overline{\sqrt{s}} = \sqrt{s}$.

(ii) Let $s \in \mathrm{GF}(p^n)$ be a nonsquare in $\mathrm{GF}(p^n)$. Then according to lemma 2.1.22 we get that $\sqrt{s} \in \mathrm{GF}(p^{2n}) \backslash \mathrm{GF}(p^n)$. As $\sqrt{s}^2 = s \in \mathrm{GF}(p^n)$, observation 2.1.19 implies that $\overline{\sqrt{s}^2} = \sqrt{s}^2$. Using the fact that $F_p^{(n)}$ is an automorphism, we find that

$$\begin{aligned} \overline{\sqrt{s}^2} = \sqrt{s}^2 &\iff \left(\overline{\sqrt{s}}\right)^2 - \sqrt{s}^2 = 0 \\ &\iff \left(\overline{\sqrt{s}} - \sqrt{s}\right)\left(\overline{\sqrt{s}} + \sqrt{s}\right) = 0. \end{aligned} \tag{2.1}$$

Now since $\sqrt{s} \in \mathrm{GF}(p^{2n}) \backslash \mathrm{GF}(p^n)$, we know from observation 2.1.19 that $\overline{\sqrt{s}} \neq \sqrt{s}$. Therefore, equation (2.1) implies that $\overline{\sqrt{s}} + \sqrt{s} = 0$.

□

2.2 Incidence Structures

We will afterwards introduce Möbius planes as an incidence structure together with a set of axioms. The advantage of this approach lies in the fact that we thereby establish an axiomatic approach that makes our initial assumptions explicit. Let us now recall the definition of an incidence structure (cf. [Dem68]).

Definition 2.2.1. An *incidence structure* is a triple $(\mathbb{P}, \mathbb{B}, \mathbb{I})$, where $\mathbb{P}$, $\mathbb{B}$, and $\mathbb{I}$ are sets such that

$$\mathbb{P} \cap \mathbb{B} = \varnothing \quad \text{and} \quad \mathbb{I} \subseteq \mathbb{P} \times \mathbb{B}.$$

The elements of $\mathbb{P}$ are called *points*, those of $\mathbb{B}$ are called *lines*, *circles*, or *blocks*, and $\mathbb{I}$ is called the *incidence relation*. If $(P, g) \in \mathbb{I}$, then we say that "P lies on g", "g passes through P", or "P and g are incident".

Notation. Let $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ be an incidence structure, $P \in \mathbb{P}$, and $g \in \mathbb{B}$. Then $P \,\mathrm{I}\, g$ denotes that $(P, g) \in \mathbb{I}$.

Chapter 3

Introduction to Miquelian Möbius Planes

Möbius planes are one of the three classes of Benz planes[1] and are named after the German mathematician August Ferdinand Möbius, who laid the foundations of the theory of circles. An important example of a Möbius plane is the *classical Möbius plane*, which is based on the geometry of lines and circles in the Euclidean plane. Therefore, we introduce in section 3.1 first the classical Möbius plane and then go over to the axiomatic definition of Möbius planes. In section 3.2, we consider Miquel's theorem, which geometrically characterizes *Miquelian* Möbius planes. Then in section 3.3, we use the classical Möbius plane to construct and examine *finite* Miquelian Möbius planes.

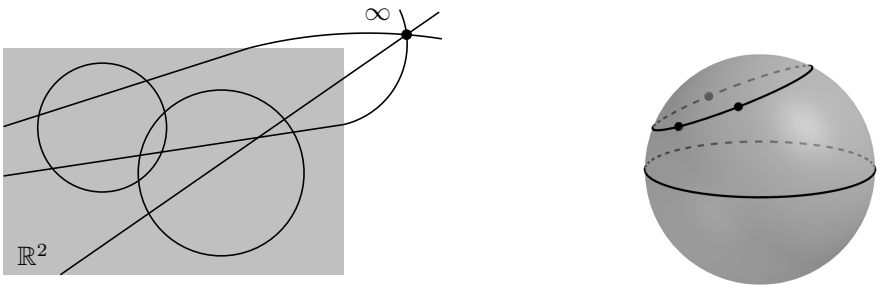
This chapter is mainly based on [Hun18] and [Har04]. Especially the construction of finite Miquelian Möbius planes follows [Hun18].

3.1 The Möbius Plane

We start from the Euclidean plane with the point set $\mathbb{R}^2$ and consider lines and circles. If we are given two different points, then there is of course exactly one line passing through them. Similarly, a circle is uniquely defined by three different points. However, if these three points are collinear, then we obtain a line again. In this light, the notions of circles and lines connect. With this in mind, let us merge the set of lines together with the set of circles to a set of blocks. This idea, however, leads us to a rather inhomogeneous incidence structure since two points determine one line and plenty of circles. But there is a way around this problem: we add a point at infinity, denoted as ∞, to every line (figure 3.1 (a)). And now, every block is determined by exactly three points. This resulting geometry is called *classical Möbius plane* (cf. [Har04], chapter 0).

[1] Benz planes split into three families, namely Möbius planes, Laguerre planes, and Minkowski planes.

The points in the classical Möbius plane are thus elements of the set $\mathbb{R}^2 \cup \{\infty\}$. Since the sets $\mathbb{R}^2 \cup \{\infty\}$ and $\mathbb{C} \cup \{\infty\}$ are isomorphic, we also obtain a three-dimensional model of the classical Möbius plane, namely the Riemann sphere (figure 3.1 (b)).



(a) Two-dimensional model of the classical Möbius plane.

(b) Three-dimensional model of the classical Möbius plane.

FIGURE 3.1: Models of the classical Möbius plane.

There are many Möbius planes that are different from the classical one. Let us thus consider the abstract definition of Möbius planes (cf. [Hun18]).

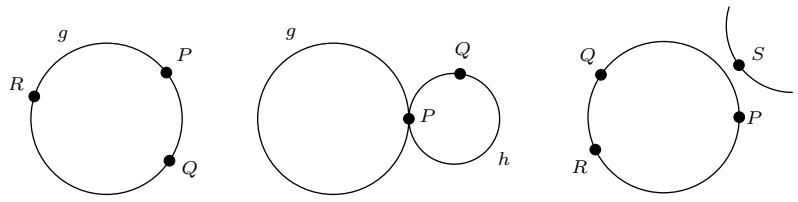
Definition 3.1.1. An incidence structure $\mathcal{M} = (\mathbb{P}, \mathbb{B}, \mathbb{I})$ with point set $\mathbb{P}$ and set of blocks $\mathbb{B}$ is called *Möbius plane* if the following three axioms hold:

(A1) For any three different points $P, Q, R \in \mathbb{P}$, there exists a unique block $g \in \mathbb{B}$ such that $P \,\mathrm{I}\, g$, $Q \,\mathrm{I}\, g$, and $R \,\mathrm{I}\, g$.

(A2) For any block $g \in \mathbb{B}$ and any two points $P, Q \in \mathbb{P}$ with $P \,\mathrm{I}\, g$ and $\neg(Q \,\mathrm{I}\, g)$, there exists a unique block $h \in \mathbb{B}$ such that

$$P \,\mathrm{I}\, h,\ Q \,\mathrm{I}\, h,\ \text{and } \forall R \in \mathbb{P},\ R \neq P : R \,\mathrm{I}\, g \implies \neg(R \,\mathrm{I}\, h).$$

(A3) There are four different points $P, Q, R, S \in \mathbb{P}$ that are not all incident with one block. Moreover, every block is incident with at least one point.



(A1) (A2) (A3)

FIGURE 3.2: Axioms of the Möbius plane.

Notation. Let $P, Q, R \in \mathbb{P}$. We denote the unique block passing through P, Q, and R by $\overrightarrow{P\,Q\,R}$.

The existence of a concrete model proves the consistency of an axiomatic system. As introduced above, the Riemann sphere (as a model of the extended complex plane $\mathbb{C} \cup \{\infty\}$) is a model of a Möbius plane, where

$$\mathbb{P} := \text{the set of points on the sphere}, \quad \mathbb{B} := \text{the set of circles on the sphere},$$
$$\mathbb{I} \subseteq \mathbb{P} \times \mathbb{B} : \; P \,\mathrm{I}\, g \;:\Longleftrightarrow\; P \in g.$$

Using the complex plane (where the complex number $z = x + iy$ is represented by the point $(x, y) \in \mathbb{R}^2$, and $\overline{z} = x - iy$ is the complex conjugate of z), we can also describe the set of points and the set of blocks in the following way (cf. [Har04], chapter 3):

$$\mathbb{P} := \mathbb{C} \cup \{\infty\}, \infty \notin \mathbb{C} \text{ and} \tag{3.1}$$
$$\mathbb{B} := \left\{ \{z \in \mathbb{C} \mid \overline{a}z + a\overline{z} = b\} \cup \{\infty\} \,\middle|\, a \in \mathbb{C}\backslash\{0\}, b \in \mathbb{R} \right\}$$
$$\cup \left\{ \{z \in \mathbb{C} \mid (z-c)\overline{(z-c)} = r\} \,\middle|\, c \in \mathbb{C}, r \in \mathbb{R}_{>0} \right\}, \tag{3.2}$$

where the solution sets of the equations $\overline{a}z + a\overline{z} = b$ and $(z-c)\overline{(z-c)} = r$ over $\mathbb{C}$ form a line and a circle, respectively.

Observe that two distinct blocks g and h share at most two points, which holds true in every Möbius plane. For if g and h have three common points or more, then axiom (A1) ensures that $g = h$.

Definition 3.1.2. For two blocks $g, h \in \mathbb{B}$ with $g \neq h$, we say that:

- g and h are *disjoint*, if $\mathrm{card}(g \cap h) = 0$,
- g and h are *tangent* (or *touch*), if $\mathrm{card}(g \cap h) = 1$,
- g and h are *intersecting*, if $\mathrm{card}(g \cap h) = 2$.

Definition 3.1.3. Let $g, h \in \mathbb{B}$, and let $P \in \mathbb{P}$. If either $g = h$ or $g \cap h = \{P\}$, then we say that g and h are *P-parallel*, denoted by $g \parallel_P h$.

Axiom (A2) immediately implies the following.

Lemma 3.1.4. The relation *P-parallel* is an equivalence relation.

Proof. It is easy to see that the relation P-parallel is reflexive and symmetric. The transitivity can be seen as follows: Let $g, h, k \in \mathbb{B}$ with $g \parallel_P h$ and $h \parallel_P k$.

- If $g = h$ or $h = k$, then we trivially obtain that $g \parallel_P k$.
- Now let $g \neq h$ and $h \neq k$. Assume that $g \cap k = \{P, Q\}$ with $P \neq Q \in \mathbb{P}$. Then, since $\neg(Q \,\mathrm{I}\, h)$, $g \parallel_P h$, and $k \parallel_P h$, axiom (A2) implies that $g = k$. Hence $g \parallel_P k$.

□

Let us now consider a first example of a Möbius plane with a *finite* number of points. We define

$\mathbb{P} :=$ the set consisting of the four vertices of a regular tetrahedron and its geometric center,

$\mathbb{B} :=$ the set consisting of circles that pass precisely through three points,

$\mathbb{I} \subseteq \mathbb{P} \times \mathbb{B} : \; P \,\mathrm{I}\, g \;:\Longleftrightarrow\; P \in g.$

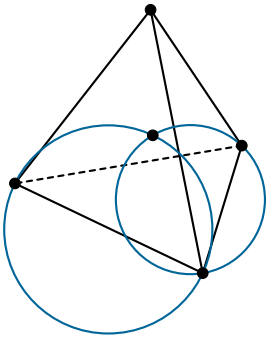


FIGURE 3.3: Minimal model of a Möbius plane (with two out of ten blocks shown).

This is indeed the minimal model of a Möbius plane, which is also known as the tetrahedron model due to the construction (figure 3.3). It consists of only five points and $\binom{5}{3} = 10$ blocks. Consequently, it is easy to verify that the axioms (A1)–(A3) are true.

Now, on the one hand, every block in this plane contains exactly three points by construction. On the other hand, through each point pass precisely $\binom{4}{2} = 6$ blocks. In fact, one can show that each block in a finite Möbius plane has the same number of points and through each point of the plane pass the same number of blocks (cf. [Har04], lemma 3.5). We can thus define the order of a finite Möbius plane as follows.

Definition 3.1.5. A Möbius plane $\mathcal{M} = (\mathbb{P}, \mathbb{B}, \mathbb{I})$, where $\mathbb{P}$ and $\mathbb{B}$ are finite sets, is called a *finite Möbius plane*. If $n+1$ points are incident with one block, then we call n the *order* of $\mathcal{M}$.

Notation. A finite Möbius plane $\mathcal{M}$ of order n is denoted by $\mathcal{M}_n$.

Example 3.1.6. The minimal model of a Möbius plane is of order 2, since there are 3 points on each block. Now we can also state the number of points and the number of blocks in terms of the order of the plane (cf. [Har04], lemma 3.6):

$$\mathrm{card}(\mathbb{P}) = 2^2 + 1 = 5, \quad \mathrm{card}(\mathbb{B}) = 2(2^2 + 1) = 10.$$

Moreover, through each point pass $2(2+1) = 6$ blocks.

3.2 Miquel's Theorem

The theorem of Miquel was stated and proved in the Euclidean geometry in 1838 by the French mathematician Auguste Miquel (q.v. chapter 1). Adjusted to the terminologies of Möbius planes, Miquel's theorem may be stated (and generalized) in the following way.

Theorem 3.2.1. Let $P_1, \dots, P_8 \in \mathbb{P}$ be eight different points. If it holds that

$$P_1 \in \overrightarrow{P_2\, P_3\, P_4}, \quad P_3 \in \overrightarrow{P_4\, P_5\, P_6},$$
$$P_5 \in \overrightarrow{P_6\, P_7\, P_8}, \quad P_7 \in \overrightarrow{P_8\, P_1\, P_2}, \quad \text{and} \quad P_1 \in \overrightarrow{P_3\, P_5\, P_7},$$

then the points P_2, P_4, P_6, and P_8 lie on a common block as well.

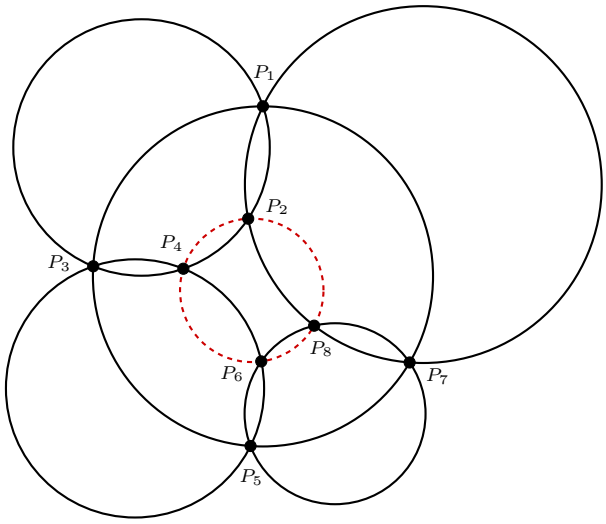


FIGURE 3.4: Miquel's theorem.

The question of validity of Miquel's theorem was of great interest in Möbius planes, since it only holds true in a particular class of Möbius planes (cf. [WS35] and [Che70]). Just as an affine plane is classified as Desarguesian if additionally the theorem of Desargues is true, a Möbius plane is classified as *Miquelian* if additionally the theorem of Miquel is true.

Definition 3.2.2. A Möbius planes $\mathcal{M} = (\mathbb{P}, \mathbb{B}, \mathbb{I})$ is called *Miquelian Möbius plane* if Miquel's theorem holds true.

Remark 3.2.3. As Miquel's theorem is satisfied in the Euclidean plane, it follows that the classical Möbius plane is indeed Miquelian. Observe that if $\infty \in \{P_2, P_4, P_6, P_8\}$, then the resulting visualization of Miquel's theorem coincides with the one from the originally stated version by Miquel (figures 1.1 and 3.5).

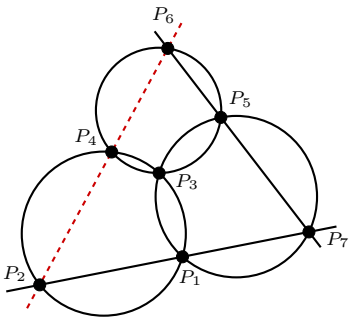


FIGURE 3.5: Miquel's theorem with $P_8 = \infty$.

3.3 Finite Miquelian Möbius Planes

Every Möbius plane is associated with an affine plane of the same order (cf. [Har04], theorem 3.2). However, the only known finite values for the order of an affine plane are prime powers, and consequently, the same holds true for a Möbius plane. We will now construct finite Möbius planes over the pair of finite fields $\mathrm{GF}(q^2)$ and $\mathrm{GF}(q)$, where q is a prime power, and show that they are indeed Miquelian.

3.3.1 Construction

The idea for the description of finite Miquelian Möbius planes is to adjust the construction of the classical Möbius plane. More specifically, we replace the Riemann sphere $\mathbb{C} \cup \{\infty\}$ by $\mathrm{GF}(p^{2n}) \cup \{\infty\}$, and the Frobenius automorphism $F_p^{(n)}$ of $\mathrm{GF}(p^{2n})$ will take over the part of the complex conjugation, which we use for the description of the set of blocks (q.v. definition in (3.2)). Recall that the complex conjugation and the Frobenius automorphism $F_p^{(n)}$ are automorphisms of $\mathbb{C}$ and $\mathrm{GF}(p^{2n})$, respectively, that keep the elements of $\mathbb{R}$ and $\mathrm{GF}(p^n)$, respectively, fixed (q.v. remark 2.1.16 and proposition 2.1.15). Accordingly, the role of $\mathrm{GF}(p^n)$ in finite Miquelian Möbius planes corresponds to the role of $\mathbb{R}$ in the classical Möbius plane.

Thus, in analogy to the description of the classical Möbius plane (q.v. definitions in (3.1) and (3.2)), we define

$$\mathbb{P} := \mathrm{GF}(p^{2n}) \cup \{\infty\}, \infty \notin \mathrm{GF}(p^{2n}), \tag{3.3}$$

$$\begin{aligned}\mathbb{B} := &\left\{ \{z \in \mathrm{GF}(p^{2n}) \mid \overline{a}z + a\overline{z} = b\} \cup \{\infty\} \,\middle|\, a \in \mathrm{GF}(p^{2n})\backslash\{0\}, b \in \mathrm{GF}(p^n) \right\} \\ &\cup \left\{ \{z \in \mathrm{GF}(p^{2n}) \mid (z-c)\overline{(z-c)} = r\} \,\middle|\, c \in \mathrm{GF}(p^{2n}), r \in \mathrm{GF}(p^n)\backslash\{0\} \right\},\end{aligned} \tag{3.4}$$

$$\mathbb{I} \subseteq \mathbb{P} \times \mathbb{B} : \; P \,\mathrm{I}\, g \;:\Longleftrightarrow\; P \in g, \tag{3.5}$$

where $\overline{z} = F_p^{(n)}(z)$ is the conjugate element of z over $\mathrm{GF}(p^n)$ (q.v. definition 2.1.17).

Observation 3.3.1. By the definitions of $\mathbb{P}$ and $\mathbb{B}$ in (3.3) and (3.4), respectively, we obtain:

- $\mathrm{card}(\mathbb{P}) = p^{2n} + 1$,
- $\mathrm{card}(\mathbb{B}) = \frac{p^{2n}-1}{p^n-1} \cdot p^n + p^{2n}(p^n - 1) = (p^n + 1) \cdot p^n + p^n(p^{2n} - p^n) = p^n(p^{2n} + 1)$.

Notice that we consider in (3.4) solutions of the equations $\|z - c\| = r$ and $\mathrm{Tr}(\overline{a}z) = b$. Moreover, we have two different types of blocks, which gives reason for the following definition.

Definition 3.3.2. (i) For $c \in \mathrm{GF}(p^{2n})$ and $r \in \mathrm{GF}(p^n)\backslash\{0\}$ the set

$$\{z \in \mathrm{GF}(p^{2n}) \mid (z-c)\overline{(z-c)} = r\}$$

forms a *block of the first type*, denoted by $\mathcal{B}^1_{(c,r)}$, that we henceforth call *circle*.

(ii) For $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$ and $b \in \mathrm{GF}(p^n)$ the set

$$\{z \in \mathrm{GF}(p^{2n}) \mid \overline{a}z + a\overline{z} = b\} \cup \{\infty\}$$

forms a *block of the second type*, denoted by $\mathcal{B}^2_{(a,b)}$, that we henceforth call *line*.

Before we verify that the incidence structure $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ defined in (3.3)–(3.5) is indeed a Miquelian Möbius plane, we determine the number of points on each block. For this, we consider the corresponding equations of $\mathcal{B}^1_{(c,r)}$ and $\mathcal{B}^2_{(a,b)}$ separately (cf. [Hun18]).

Proposition 3.3.3. (a) The equation $(z-c)\overline{(z-c)} = r$ for $c \in \mathrm{GF}(p^{2n})$ and $r \in \mathrm{GF}(p^n)\backslash\{0\}$ has exactly $p^n + 1$ solutions over $\mathrm{GF}(p^{2n})$.

(b) The equation $\overline{a}z + a\overline{z} = b$ for $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$ and $b \in \mathrm{GF}(p^n)$ has exactly p^n solutions over $\mathrm{GF}(p^{2n})$.

Proof. (a) Let $x = z - c \in \mathrm{GF}(p^{2n})$. Then the equation $(z-c)\overline{(z-c)} = r$ gets

$$x\overline{x} = r, \quad \text{where } r \in \mathrm{GF}(p^n)\backslash\{0\}.$$

Thus let $\varphi(x) = x\overline{x} - r$. The polynomial φ is of degree $p^n + 1$ and has accordingly at most $p^n + 1$ roots over $\mathrm{GF}(p^{2n})$. Since $r \neq 0$, it follows that 0 is not a root of φ. Hence, every image of the map

$$\begin{aligned} \mathrm{GF}(p^{2n})\backslash\{0\} &\longrightarrow GF(p^n)\backslash\{0\}, \\ x &\longmapsto x\overline{x} = \|x\| \end{aligned}$$

occurs at most $p^n + 1$ times. But by the pigeonhole principle, we find that every image occurs not only at most $p^n + 1$ times, but exactly $p^n + 1$ times (figure 3.6). This means that φ has precisely $p^n + 1$ roots. Consequently, the equation $(z-c)\overline{(z-c)} = r$ has $p^n + 1$ solutions over $\mathrm{GF}(p^{2n})$.

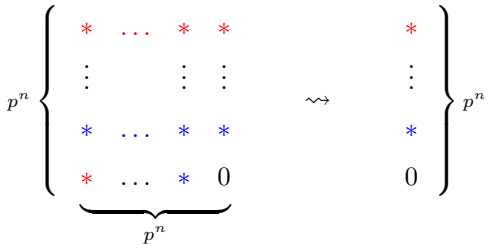


FIGURE 3.6: Pigeonhole principle.

(b) Let $x = \overline{a}z \in \mathrm{GF}(p^{2n})$. Then the equation $\overline{a}z + a\overline{z} = b$ gets

$$x + \overline{x} = b, \quad \text{where } b \in \mathrm{GF}(p^n).$$

Now let $\psi(x) = x + \overline{x} - b$. The polynomial ψ is of degree p^n and has thus at most p^n roots over $\mathrm{GF}(p^{2n})$. Hence, every image of the map

$$\begin{aligned} \mathrm{GF}(p^{2n}) &\longrightarrow GF(p^n), \\ x &\longmapsto x + \overline{x} = \mathrm{Tr}(x) \end{aligned}$$

occurs at most p^n times. The pigeonhole principle implies now in this case that every image occurs exactly p^n times. This means that ψ has precisely p^n roots, and thus, $\overline{a}z + a\overline{z} = b$ has p^n solutions over $\mathrm{GF}(p^{2n})$.

□

Since the point ∞ is added to the solution set of the equation $\overline{a}z + a\overline{z} = b$, we obtain with proposition 3.3.3 the following result.

Corollary 3.3.4. Every block is incident with exactly $p^n + 1$ points.

We will now prove that the system $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ as defined in (3.3)–(3.5) is a Möbius plane of order p^n. By proving axiom (A1), we will also obtain a recipe to explicitly find the unique block passing through three given points. Moreover, in order to prove axiom (A2), we will introduce Möbius transformations, which are crucial automorphisms of $\mathcal{M}_{p^n}$. We follow the proof of [Hun18].

Theorem 3.3.5. The incidence structure $\mathcal{M}_{p^n} = (\mathbb{P}, \mathbb{B}, \mathbb{I})$ is a Möbius plane.

Proof. We need to verify that the axioms (A1)–(A3) are true. Then it follows together with corollary 3.3.4 that the incidence structure $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ is a Möbius plane of order p^n.

Verification of axiom (A1): Let $Z_1, Z_2, Z_3 \in \mathbb{P}$ be three different points. We need to show that there is exactly one block $g \in \mathbb{B}$ that is incident with Z_1, Z_2, and Z_3. For this, we distinguish between two cases: first, the case where $\infty \in \{Z_1, Z_2, Z_3\}$; second, the case where $\infty \notin \{Z_1, Z_2, Z_3\}$.

(i) Assume, without loss of generality, that $Z_3 = \infty$ and $Z_1, Z_2 \in \mathrm{GF}(p^{2n})$. Then, since $\infty \in g$, it follows that $g = \mathcal{B}^2_{(a,b)}$, where $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$ and $b \in \mathrm{GF}(p^n)$ need to be determined. This means that Z_1 and Z_2 have to satisfy the equation $\overline{a}z + a\overline{z} = b$, and therefore, we consider the following system of equations:

$$\begin{pmatrix} z & \overline{z} & 1 \\ Z_1 & \overline{Z_1} & 1 \\ Z_2 & \overline{Z_2} & 1 \end{pmatrix} \begin{pmatrix} \overline{a} \\ a \\ -b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This system has a nontrivial solution if and only if the determinant of the coefficient matrix is 0 (cf. [Det86], theorem 2.5.4). Hence, we can make the approach

$$0 = \det \begin{pmatrix} z & \overline{z} & 1 \\ Z_1 & \overline{Z_1} & 1 \\ Z_2 & \overline{Z_2} & 1 \end{pmatrix}. \tag{3.6}$$

By using the Laplace expansion along the first row, we can write equation (3.6) as

$$\begin{aligned} & z(\overline{Z_1} - \overline{Z_2}) - \overline{z}(Z_1 - Z_2) + (Z_1\overline{Z_2} - \overline{Z_1}Z_2) = 0 \\ \iff \quad & z(\overline{Z_1} - \overline{Z_2}) + \overline{z}(Z_2 - Z_1) = -(Z_1\overline{Z_2} - \overline{Z_1}Z_2). \end{aligned} \tag{3.7}$$

Equation (3.7) is not yet of the form $\overline{a}z + a\overline{z} = b$. To achieve this, we divide both sides of equation (3.7) by $r - \overline{r}$ for some arbitrary $r \in \mathrm{GF}(p^{2n})\backslash\mathrm{GF}(p^n)$ (for which it holds that $r \neq \overline{r}$ by observation 2.1.19). Then we get

$$z \cdot \frac{\overline{Z_1} - \overline{Z_2}}{r - \overline{r}} + \overline{z} \cdot \frac{Z_2 - Z_1}{r - \overline{r}} = -\frac{Z_1\overline{Z_2} - \overline{Z_1}Z_2}{r - \overline{r}}. \tag{3.8}$$

Claim. Equation (3.8) is of the form $\overline{a}z + a\overline{z} = b$ with $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$ and $b \in \mathrm{GF}(p^n)$.

Proof of Claim: Let

$$a = \frac{Z_2 - Z_1}{r - \overline{r}} \quad \text{and} \quad b = -\frac{Z_1\overline{Z_2} - \overline{Z_1}Z_2}{r - \overline{r}}. \tag{3.9}$$

Then

$$\overline{a} = \frac{\overline{Z_2} - \overline{Z_1}}{\overline{r} - r} = \frac{\overline{Z_1} - \overline{Z_2}}{r - \overline{r}},$$

and thus, equation (3.8) is of the form $\overline{a}z + a\overline{z} = b$. Obviously, it holds that $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$, as Z_1 and Z_2 are different.

Moreover, since

$$\overline{b} = -\frac{\overline{Z_1}Z_2 - Z_1\overline{Z_2}}{\overline{r} - r} = -\frac{Z_1\overline{Z_2} - \overline{Z_1}Z_2}{r - \overline{r}} = b,$$

it follows from observation 2.1.19 that b is an element of $\mathrm{GF}(p^n)$. ■

Consequently, the line $g = \mathcal{B}^2_{(a,b)}$ with a and b as defined in (3.9) is by construction the unique block passing through Z_1, Z_2, and ∞.

(ii) Now we assume that $Z_1, Z_2, Z_3 \in \mathrm{GF}(p^{2n})$. Let

$$D = \det \begin{pmatrix} Z_1 & \overline{Z_1} & 1 \\ Z_2 & \overline{Z_2} & 1 \\ Z_3 & \overline{Z_3} & 1 \end{pmatrix}.$$

If $D = 0$, then g is a line and we can determine g as in case (i). Thus, we assume now that $D \neq 0$. Then $g = \mathcal{B}^1_{(c,r)}$, where $c \in \mathrm{GF}(p^{2n})$ and $r \in \mathrm{GF}(p^n)\backslash\{0\}$ need to be determined. This means that Z_1, Z_2, and Z_3 have to satisfy the equation $(z-c)\overline{(z-c)} = r$. Since

$$(z-c)\overline{(z-c)} = r \iff \|z\| - \overline{c}z - c\overline{z} + \|c\| = r,$$

we consider the system of equations given by

$$\begin{pmatrix} \|z\| & z & \overline{z} & 1 \\ \|Z_1\| & Z_1 & \overline{Z_1} & 1 \\ \|Z_2\| & Z_2 & \overline{Z_2} & 1 \\ \|Z_3\| & Z_3 & \overline{Z_3} & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -\overline{c} \\ -c \\ \|c\| - r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

As before, this system has a nontrivial solution if and only if the determinant of the coefficient matrix is 0. Hence, we can make the approach

$$0 = \det \begin{pmatrix} \|z\| & z & \overline{z} & 1 \\ \|Z_1\| & Z_1 & \overline{Z_1} & 1 \\ \|Z_2\| & Z_2 & \overline{Z_2} & 1 \\ \|Z_3\| & Z_3 & \overline{Z_3} & 1 \end{pmatrix}. \tag{3.10}$$

Using the Laplace expansion along the first row, equation (3.10) can be written as

$$0 = \|z\|\, D - z \det \begin{pmatrix} \|Z_1\| & \overline{Z_1} & 1 \\ \|Z_2\| & \overline{Z_2} & 1 \\ \|Z_3\| & \overline{Z_3} & 1 \end{pmatrix} + \overline{z} \det \begin{pmatrix} \|Z_1\| & Z_1 & 1 \\ \|Z_2\| & Z_2 & 1 \\ \|Z_3\| & Z_3 & 1 \end{pmatrix} - \det \begin{pmatrix} \|Z_1\| & Z_1 & \overline{Z_1} \\ \|Z_2\| & Z_2 & \overline{Z_1} \\ \|Z_3\| & Z_3 & \overline{Z_1} \end{pmatrix}. \quad (3.11)$$

Equation (3.11) is not yet of the form $\|z\| - \overline{c}z - c\overline{z} + \|c\| = r$. For this, we divide equation (3.11) by D (which is possible, as $D \neq 0$ by assumption). Then we get

$$\|z\| - \frac{z}{D} \det \begin{pmatrix} \|Z_1\| & \overline{Z_1} & 1 \\ \|Z_2\| & \overline{Z_2} & 1 \\ \|Z_3\| & \overline{Z_3} & 1 \end{pmatrix} - \overline{z}\Big(-\frac{1}{D}\Big) \det \begin{pmatrix} \|Z_1\| & Z_1 & 1 \\ \|Z_2\| & Z_2 & 1 \\ \|Z_3\| & Z_3 & 1 \end{pmatrix} = \frac{1}{D} \det \begin{pmatrix} \|Z_1\| & Z_1 & \overline{Z_1} \\ \|Z_2\| & Z_2 & \overline{Z_1} \\ \|Z_3\| & Z_3 & \overline{Z_1} \end{pmatrix}. \quad (3.12)$$

Claim. Equation (3.12) is of the form $\|z\| - \overline{c}z - c\overline{z} + \|c\| = r$ with $c \in \mathrm{GF}(p^{2n})$ and $r \in \mathrm{GF}(p^n)\backslash\{0\}$.

Proof of Claim: Let

$$c = -\frac{1}{D} \det \begin{pmatrix} \|Z_1\| & Z_1 & 1 \\ \|Z_2\| & Z_2 & 1 \\ \|Z_3\| & Z_3 & 1 \end{pmatrix} \quad \text{and} \quad r = \|c\| + \frac{1}{D} \det \begin{pmatrix} \|Z_1\| & Z_1 & \overline{Z_1} \\ \|Z_2\| & Z_2 & \overline{Z_2} \\ \|Z_3\| & Z_3 & \overline{Z_3} \end{pmatrix}. \quad (3.13)$$

Observe that

$$\overline{D} = \det \begin{pmatrix} \overline{Z_1} & Z_1 & 1 \\ \overline{Z_2} & Z_2 & 1 \\ \overline{Z_3} & Z_3 & 1 \end{pmatrix} = -\det \begin{pmatrix} Z_1 & \overline{Z_1} & 1 \\ Z_2 & \overline{Z_2} & 1 \\ Z_3 & \overline{Z_3} & 1 \end{pmatrix} = -D, \quad (3.14)$$

since the interchange of any two columns of a matrix changes the sign of its determinant.

Then

$$\overline{c} = -\frac{1}{\overline{D}} \det \begin{pmatrix} \|Z_1\| & \overline{Z_1} & 1 \\ \|Z_2\| & \overline{Z_2} & 1 \\ \|Z_3\| & \overline{Z_3} & 1 \end{pmatrix} = \frac{1}{D} \det \begin{pmatrix} \|Z_1\| & \overline{Z_1} & 1 \\ \|Z_2\| & \overline{Z_2} & 1 \\ \|Z_3\| & \overline{Z_3} & 1 \end{pmatrix},$$

and thus, equation (3.12) is of the form $\|z\| - \overline{c}z - c\overline{z} + \|c\| = r$. Obviously, it holds that $c \in \mathrm{GF}(p^{2n})$. Moreover, since

$$\overline{r} = \|c\| - \frac{1}{D} \det \begin{pmatrix} \|Z_1\| & \overline{Z_1} & Z_1 \\ \|Z_2\| & \overline{Z_2} & Z_2 \\ \|Z_3\| & \overline{Z_3} & Z_3 \end{pmatrix} = \|c\| + \frac{1}{D} \det \begin{pmatrix} \|Z_1\| & Z_1 & \overline{Z_1} \\ \|Z_2\| & Z_2 & \overline{Z_2} \\ \|Z_3\| & Z_3 & \overline{Z_3} \end{pmatrix} = r,$$

it follows from observation 2.1.19 that $r \in \mathrm{GF}(p^n)$. We are left to show that $r \neq 0$. For this, we use that Z_1 lies on g, which means that

$$\underbrace{\left(Z_1 D + \det \begin{pmatrix} \|Z_1\| & Z_1 & 1 \\ \|Z_2\| & Z_2 & 1 \\ \|Z_3\| & Z_3 & 1 \end{pmatrix} \right)}_{\text{Term (1)}} \cdot \underbrace{\left(\overline{Z_1} D - \det \begin{pmatrix} \|Z_1\| & \overline{Z_1} & 1 \\ \|Z_2\| & \overline{Z_2} & 1 \\ \|Z_3\| & \overline{Z_3} & 1 \end{pmatrix} \right)}_{\text{Term (2)}} = rD^2. \tag{3.15}$$

Term (1) of equation (3.15) can be simplified as follows:

$$\begin{aligned} \text{Term (1)} &= \det \begin{pmatrix} Z_1 & \|Z_1\| & 1 \\ Z_2 & Z_1\overline{Z_2} & 1 \\ Z_3 & Z_1\overline{Z_3} & 1 \end{pmatrix} + \det \begin{pmatrix} \|Z_1\| & Z_1 & 1 \\ \|Z_2\| & Z_2 & 1 \\ \|Z_3\| & Z_3 & 1 \end{pmatrix} \\ &= -\|Z_1\|(Z_2 - Z_3) + Z_1\overline{Z_2}(Z_1 - Z_3) - Z_1\overline{Z_3}(Z_1 - Z_2) \\ &\qquad + \|Z_1\|(Z_2 - Z_3) - \|Z_2\|(Z_1 - Z_3) + \|Z_3\|(Z_1 - Z_2) \\ &= (Z_1 - Z_2)(\|Z_3\| - Z_1\overline{Z_3}) + (Z_1 - Z_3)(Z_1\overline{Z_2} - \|Z_2\|) \\ &= (Z_1 - Z_2)\overline{Z_3}(Z_3 - Z_1) + (Z_1 - Z_3)\overline{Z_2}(Z_1 - Z_2) \\ &= (Z_1 - Z_2)(Z_1 - Z_3)(\overline{Z_2} - \overline{Z_3}). \end{aligned}$$

Similarly, we obtain for term (2) of equation (3.15) that the following holds:

$$\text{Term (2)} = (\overline{Z_1} - \overline{Z_2})(\overline{Z_1} - \overline{Z_3})(Z_3 - Z_2).$$

Therefore, equation (3.15) can be written as

$$(Z_1 - Z_2)(Z_1 - Z_3)(\overline{Z_2} - \overline{Z_3})(\overline{Z_1} - \overline{Z_2})(\overline{Z_1} - \overline{Z_3})(Z_3 - Z_2) = rD^2. \tag{3.16}$$

Now since Z_1, Z_2, and Z_3 are distinct, it follows that the left hand side of equation (3.16) is not 0. As we assumed that $D \neq 0$, we thus conclude that $r \neq 0$. ■

Consequently, the circle $g = \mathcal{B}^1_{(c,r)}$ with c and r as defined in (3.13) is by construction the unique block passing through Z_1, Z_2, and Z_3 (on the assumption that Z_1, Z_2, and Z_3 do not lie on a common line).

Verification of axiom (A2): Let $g \in \mathbb{B}$, and let $P, Q \in \mathbb{P}$ with $P \,\mathrm{I}\, g$ and $\neg(Q \,\mathrm{I}\, g)$. We need to show that there is a unique block $h \in \mathbb{B}$ such that $g \cap h = \{P\}$ and $Q \,\mathrm{I}\, h$. To achieve this, we distinguish between two cases, namely whether or not $P = \infty$.

(i) Assume that $P = \infty$, and let $g = \mathcal{B}^2_{(a_g,b_g)}$. Then, since $\infty \in h$, it follows that $h = \mathcal{B}^2_{(a,b)}$, where $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$ and $b \in \mathrm{GF}(p^n)$ need to be determined. The condition $Q \,\mathrm{I}\, h$ immediately implies that

$$b = \overline{a}Q + a\overline{Q}$$

and since $b = \overline{a}Q + a\overline{Q} = \mathrm{Tr}(\overline{a}Q)$, it holds by corollary 2.1.20 that $b \in \mathrm{GF}(p^n)$. In order to determine a, we use the condition that $h \cap g = \{\infty\}$, which means that the system of equations given by

$$\begin{pmatrix} \overline{a_g} & a_g \\ \overline{a} & a \end{pmatrix} \begin{pmatrix} z \\ \overline{z} \end{pmatrix} = \begin{pmatrix} b_g \\ \overline{a}Q + a\overline{Q} \end{pmatrix} \tag{3.17}$$

has no solution over $\mathrm{GF}(p^{2n})$. This is the case if and only if its coefficient matrix is singular (cf. [Det86], theorem 2.5.5). Thus

$$\det \begin{pmatrix} \overline{a_g} & a_g \\ \overline{a} & a \end{pmatrix} = \overline{a_g}a - a_g\overline{a} \stackrel{!}{=} 0. \tag{3.18}$$

Hence, for $h = \mathcal{B}^2_{(a,b)}$ with $a := a_g$ and $b := \overline{a_g}Q + a_g\overline{Q}$ it holds that $Q \,\mathrm{I}\, h$ and $h \cap g = \{\infty\}$. This is indeed the only possible choice for h, since for $a \neq a_g$ it follows that

$$\begin{aligned} & \overline{a}z + a\overline{z} = \overline{a}Q + a\overline{Q} \\ \stackrel{(a_g \neq 0)}{\Longleftrightarrow} \quad & (a_g\overline{a})\overline{a_g}z + (\overline{a_g}a)a_g\overline{z} = (a_g\overline{a})\overline{a_g}Q + (\overline{a_g}a)a_g\overline{Q} \\ \stackrel{(3.18)}{\Longleftrightarrow} \quad & (a_g\overline{a})\overline{a_g}z + (a_g\overline{a})a_g\overline{z} = (a_g\overline{a})\overline{a_g}Q + (a_g\overline{a})a_g\overline{Q} \\ \stackrel{(a \neq 0 \neq a_g)}{\Longleftrightarrow} \quad & \overline{a_g}z + a_g\overline{z} = \overline{a_g}Q + a_g\overline{Q}. \end{aligned}$$

(ii) Now assume that $P \neq \infty$. Our goal is to use an incident preserving transformation that maps P to the point ∞, as we are then again in case (i). For this, consider the

following map:

$$\mu_P \colon \mathbb{P} \longrightarrow \mathbb{P}, \quad z \longmapsto z' := \begin{cases} \frac{1}{z-P} & \text{if } z \neq P, z \neq \infty, \\ \infty & \text{if } z = P, \\ 0 & \text{if } z = \infty. \end{cases} \tag{3.19}$$

Claim 3.3.6. The map μ_P is an incident preserving transformation.

Proof of Claim:

- *μ_P is bijective:* Let $x, y \in \mathbb{P}$ and suppose that $x' = y'$. If $x' = y' = \infty$, then it follows by definition of μ_P that $x = y = P$. Likewise, if $x' = y' = 0$, then $x = y = \infty$. For $x' \in \mathbb{P} \setminus \{0, \infty\}$ it holds that:

$$x' = y' \iff \frac{1}{x-P} = \frac{1}{y-P} \iff y - P = x - P \iff x = y.$$

  Hence, in every case, $x' = y'$ implies that $x = y$, which means that μ_P is injective. As the set $\mathbb{P}$ is finite, it follows that μ_P is surjective as well.

- *μ_P is incident preserving:* We need to show that the images of the points on a block lie again on a block.

  (a) We consider first a line $\mathcal{B}^2_{(a,b)} \in \mathbb{B}$. Then it holds for $z \in \mathcal{B}^2_{(a,b)}$ and $z \notin \{P, \infty\}$ that

$$\begin{aligned} & 0 = \overline{a}z + a\overline{z} - b \\ \iff \quad & 0 = a(\overline{z} - \overline{P}) + \overline{a}(z - P) + (\overline{a}P + a\overline{P} - b) \\ \iff \quad & 0 = \frac{a}{z-P} + \frac{\overline{a}}{\overline{z}-\overline{P}} + \frac{\overline{a}P + a\overline{P} - b}{(z-P)(\overline{z}-\overline{P})} \\ \iff \quad & 0 = az' + \overline{az'} + z'\overline{z'} \underbrace{(\overline{a}P + a\overline{P} - b)}_{\text{Term (1)}}. \end{aligned} \tag{3.20}$$

  Firstly, if $P \in \mathcal{B}^2_{(a,b)}$, then term (1) of equation (3.20) is 0, and thus, the images of $z \in \mathcal{B}^2_{(a,b)} \setminus \{P, \infty\}$ satisfy the equation

$$az' + \overline{az'} = 0. \tag{3.21}$$

  But equation (3.21) corresponds to the line $\mathcal{B}^2_{(\overline{a},0)}$, since $a \in \mathrm{GF}(p^{2n}) \setminus \{0\}$. Moreover, $P' = \infty \in \mathcal{B}^2_{(\overline{a},0)}$ and $\infty' = 0 \in \mathcal{B}^2_{(\overline{a},0)}$. Therefore, if $P \in \mathcal{B}^2_{(a,b)}$, then μ_P maps the points on the line $\mathcal{B}^2_{(a,b)}$ to the line $\mathcal{B}^2_{(\overline{a},0)}$.
  Secondly, if $P \notin \mathcal{B}^2_{(a,b)}$, then term (1) is not 0. Thus, we can divide both sides

of equation (3.20) by term (1). Then the images of $z \in \mathcal{B}^2_{(a,b)} \backslash \{\infty\}$ satisfy

$$z'\overline{z'} + \frac{\overline{az'}}{\overline{a}P + a\overline{P} - b} + \frac{az'}{\overline{a}P + a\overline{P} - b} = 0. \tag{3.22}$$

Now let

$$c = -\frac{\overline{a}}{\overline{a}P + a\overline{P} - b} \quad \text{and} \quad r = \|c\|. \tag{3.23}$$

Since $b \in \mathrm{GF}(p^n)$, it follows that $\overline{c} = -\frac{a}{\overline{a}P + a\overline{P} - b}$. Thus, equation (3.22) can be written as

$$(z' - c)(\overline{z' - c}) = r. \tag{3.24}$$

Obviously, $c \in \mathrm{GF}(p^{2n})$. Moreover, from corollary 2.1.20 we know that $r \in \mathrm{GF}(p^n)$, and since $a \neq 0$, it holds that $r \neq 0$. Thus, equation (3.24) corresponds to the circle $\mathcal{B}^1_{(c,r)}$. Furthermore, $\infty' = 0 \in \mathcal{B}^1_{(c,r)}$. Therefore, if $P \notin \mathcal{B}^2_{(a,b)}$, then μ_P maps the points on the line $\mathcal{B}^2_{(a,b)}$ to the circle $\mathcal{B}^1_{(c,r)}$ with c and r as defined in (3.23).

(b) Now let $\mathcal{B}^1_{(c,r)} \in \mathbb{B}$. Then it holds for $z \in \mathcal{B}^1_{(c,r)}$ and $z \notin \{P, \infty\}$ that

$$\begin{aligned} & 0 = (z - c)(\overline{z} - \overline{c}) - r \\ \iff \quad & 0 = 1 + z'(P - c) + \overline{z'}(\overline{P} - \overline{c}) + z'\overline{z'} \underbrace{\big((P - c)(\overline{P} - \overline{c}) - r\big)}_{\text{Term (1)}} = 0. \end{aligned} \tag{3.25}$$

Analogously as in (a), one may verify that the following holds:

- If $P \in \mathcal{B}^1_{(c,r)}$, then term (1) of equation (3.25) is 0. In this case, μ_P maps the points on the circle $\mathcal{B}^1_{(c,r)}$ to the line $\mathcal{B}^2_{(\overline{P-c},-1)}$.
- If $P \notin \mathcal{B}^1_{(c,r)}$, then term (1) of equation (3.25) is not 0. In this case, μ_P maps the points on the circle $\mathcal{B}^1_{(c,r)}$ to the circle $\mathcal{B}^1_{(c^\star,r^\star)}$, where $c^\star := \frac{1}{r+c-P}$ and $r^\star := \|c^\star\|$.

■

Verification of axiom (A3): We need to show that there exist four points that are not all incident with the same block. For this, let $R \in \mathrm{GF}(p^{2n}) \backslash \mathrm{GF}(p^n)$ (for which it holds that $R \neq \overline{R}$, $R \neq 0$, and $R \neq 1$). Then

$$\det \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ R & \overline{R} & 1 \end{pmatrix} = \overline{R} - R \neq 0,$$

which means that the points $0, 1$, and R determine a circle. Since the point ∞ is only incident with lines, it follows that $0, 1, R$, and ∞ are four different points that do not lie on a common block. Moreover, we know from corollary 3.3.4 that every block is incident with at least one point.

We conclude that the axioms (A1)–(A3) hold true, which means that $\mathcal{M}_{p^n}$ is indeed a Möbius plane. □

The incident preserving transformation μ_P that we used to prove axiom (A2) in $\mathcal{M}_{p^n}$ (q.v. (3.19)) is an example of a Möbius transformation. These are automorphisms of $\mathcal{M}_{p^n}$ and are defined as follows (cf. [HK15]).

Definition 3.3.7. Let $a, b, c, d \in \mathrm{GF}(p^{2n})$ such that $ad - bc \neq 0$. The map μ defined by

$$\mu\colon \mathbb{P} \longrightarrow \mathbb{P}, \quad z \longmapsto z' := \begin{cases} \frac{az+b}{cz+d} & \text{if } z \neq \infty, cz + d \neq 0, \\ \infty & \text{if } z \neq \infty, cz + d = 0, \\ \frac{a}{c} & \text{if } z = \infty, c \neq 0, \\ \infty & \text{if } z = \infty, c = 0 \end{cases}$$

is called a *Möbius transformation* of $\mathcal{M}_{p^n}$.

Möbius transformations act three times sharply transitive on $\mathbb{P}$, that is to say that there is a unique Möbius transformation mapping any three points to any other three points (cf. [Dem68], section 6.4). Since axiom (A1) implies that every block is determined by three points, it follows that there is a unique Möbius transformation mapping any block to any other block. Furthermore, Möbius transformations preserve incidences, and thus, disjoint blocks are mapped to disjoint blocks, tangent blocks to tangent blocks, and intersecting blocks to intersecting blocks.
We especially take advantage of the fact that Möbius transformations allow us to convert lines into circles and vice versa, which is what we used to verify axiom (A2) in $\mathcal{M}_{p^n}$.

The proof of axiom (A1) in $\mathcal{M}_{p^n}$ also reveals a further result, since the rearrangement of the equations (3.6) and (3.10) immediately imply the following lemma.

Lemma 3.3.8. (a) Let $g \in \mathbb{B}$ be a line, and let $Z_1, Z_2 \in \mathrm{GF}(p^{2n})$ be two different points. If $Z_1 \,\mathrm{I}\, g$ and $Z_2 \,\mathrm{I}\, g$, then

$$g = \{z \in \mathrm{GF}(p^{2n}) \mid (Z_1 - z)(\overline{Z_2} - \overline{z}) = (\overline{Z_1} - \overline{z})(Z_2 - z)\} \cup \{\infty\}.$$

(b) Let $g \in \mathbb{B}$ be a circle, and let $Z_1, Z_2, Z_3 \in \mathrm{GF}(p^{2n})$ be three different points. If $Z_1 \,\mathrm{I}\, g$, $Z_2 \,\mathrm{I}\, g$, and $Z_3 \,\mathrm{I}\, g$, then the points on g are precisely the solutions of the equation

$$(Z_1 - Z_3)(Z_2 - z)(\overline{Z_1} - \overline{z})(\overline{Z_2} - \overline{Z_3}) = (\overline{Z_1} - \overline{Z_3})(\overline{Z_2} - \overline{z})(Z_1 - z)(Z_2 - Z_3)$$

over $\mathrm{GF}(p^{2n})$.

From lemma 3.3.8, we can now deduce the following property (cf. [Hun18]).

Proposition 3.3.9. (i) Three different points $Z_1, Z_2, Z_3 \in \mathrm{GF}(p^{2n})$ lie on a common line if and only if

$$\frac{Z_1 - Z_2}{Z_1 - Z_3} \in \mathrm{GF}(p^n).$$

(ii) Four different points $Z_1, Z_2, Z_3, Z_4 \in \mathrm{GF}(p^{2n})$ lie on a common circle if and only if

$$\frac{(Z_1 - Z_3)\cdot(Z_2 - Z_4)}{(Z_1 - Z_4)\cdot(Z_2 - Z_3)} \in \mathrm{GF}(p^n) \quad \text{and} \quad \frac{Z_1 - Z_2}{Z_1 - Z_3} \notin \mathrm{GF}(p^n).$$

Proof. (i) From axiom (A1), it follows that there exists a unique block $g \in \mathbb{B}$ passing through Z_2, Z_3, and ∞. Since $\infty \in g$, we know that g is a line. Now lemma 3.3.8 (a) implies that $Z_1 \in g$ if and only if

$$(Z_2 - Z_1)(\overline{Z_3} - \overline{Z_1}) = (\overline{Z_2} - \overline{Z_1})(Z_3 - Z_1). \tag{3.26}$$

As the points Z_1, Z_2, and Z_3 are distinct, we can rearrange equation (3.26) as

$$\begin{aligned} &\frac{Z_1 - Z_2}{Z_1 - Z_3} = \frac{\overline{Z_1} - \overline{Z_2}}{\overline{Z_1} - \overline{Z_3}} \\ \iff \quad &\frac{Z_1 - Z_2}{Z_1 - Z_3} = \overline{\left(\frac{Z_1 - Z_2}{Z_1 - Z_3}\right)}. \end{aligned}$$

Then the result follows immediately from observation 2.1.19.

(ii) From axiom (A1), it follows that there exists a unique block $g \in \mathbb{B}$ passing through Z_1, Z_2, and Z_3. Case (i) implies that g is a circle if and only if

$$\frac{Z_1 - Z_2}{Z_1 - Z_3} \notin \mathrm{GF}(p^n).$$

Now it follows from lemma 3.3.8 (b) that $Z_4 \in g$ if and only if

$$\begin{aligned} (Z_1 - Z_3)(Z_2 - Z_4)(\overline{Z_1} - \overline{Z_4})(\overline{Z_2} - \overline{Z_3}) = \\ (\overline{Z_1} - \overline{Z_3})(\overline{Z_2} - \overline{Z_4})(Z_1 - Z_4)(Z_2 - Z_3). \end{aligned} \tag{3.27}$$

Since the points Z_1, Z_2, Z_3, and Z_4 are different, we can rearrange equation (3.27) as

$$\frac{(Z_1 - Z_3)\cdot(Z_2 - Z_4)}{(Z_1 - Z_4)\cdot(Z_2 - Z_3)} = \overline{\left(\frac{(Z_1 - Z_3)\cdot(Z_2 - Z_4)}{(Z_1 - Z_4)\cdot(Z_2 - Z_3)}\right)}.$$

Then the desired result follows from observation 2.1.19.

□

Observe that if Z_1, Z_2, Z_3, and Z_4 lie on a common line, then proposition 3.3.9 (i) implies that

$$\frac{Z_1 - Z_3}{Z_1 - Z_4}, \frac{Z_2 - Z_4}{Z_2 - Z_3} \in \mathrm{GF}(p^n).$$

As $\mathrm{GF}(p^n)$ is a subfield of $\mathrm{GF}(p^{2n})$ (q.v. theorem 2.1.5) and therefore closed under multiplication, it follows that

$$\frac{Z_1 - Z_3}{Z_1 - Z_4} \cdot \frac{Z_2 - Z_4}{Z_2 - Z_3} \in \mathrm{GF}(p^n).$$

This means, that proposition 3.3.9 also implies the following result.

Corollary 3.3.10. Four different points $Z_1, Z_2, Z_3, Z_4 \in \mathrm{GF}(p^{2n})$ lie on a common block if and only if

$$\frac{(Z_1 - Z_3) \cdot (Z_2 - Z_4)}{(Z_1 - Z_4) \cdot (Z_2 - Z_3)} \in \mathrm{GF}(p^n).$$

Definition 3.3.11. Let $Z_1, Z_2, Z_3, Z_4 \in \mathrm{GF}(p^{2n})$ be four different points. The term

$$[Z_1, Z_2; Z_3, Z_4] := \frac{(Z_1 - Z_3) \cdot (Z_2 - Z_4)}{(Z_1 - Z_4) \cdot (Z_2 - Z_3)}$$

is called *cross-ratio*, which provides information whether the points Z_1, Z_2, Z_3, and Z_4 lie on a common block or not.

Remark 3.3.12. Once again, we can draw a connection with the classical Möbius plane: Let $Z_1, Z_2, Z_3, Z_4 \in \mathbb{C}$ be four different points. If it holds that

$$\frac{(Z_1 - Z_3) \cdot (Z_2 - Z_4)}{(Z_1 - Z_4) \cdot (Z_2 - Z_3)} \in \mathbb{R},$$

then the points Z_1, Z_2, Z_3, and Z_4 lie on one common block (cf. [Sch79], chapter 5).

With corollary 3.3.10, we have now a powerful tool at hand to proof Miquel's theorem (q.v. theorem 3.2.1) in $\mathcal{M}_{p^n}$.

Theorem 3.3.13. The Möbius plane $\mathcal{M}_{p^n} = (\mathbb{P}, \mathbb{B}, \mathbb{I})$ is Miquelian.

Remark 3.3.14. We consider in Miquel's theorem groups of four points on a block. Therefore, we need at least four points on each block, which means that the order of a Miquelian Möbius plane has to be at least 3.

Proof. Let $P_1, \ldots, P_8 \in \mathbb{P}$ be eight different points such that

$$P_1 \in \overrightarrow{P_2\, P_3\, P_4}, \quad P_3 \in \overrightarrow{P_4\, P_5\, P_6},$$
$$P_5 \in \overrightarrow{P_6\, P_7\, P_8}, \quad P_7 \in \overrightarrow{P_8\, P_1\, P_2}, \quad \text{and} \quad P_1 \in \overrightarrow{P_3\, P_5\, P_7},$$

as shown in figure 3.4. We need to prove that P_2, P_4, P_6, and P_8 lie on a common block as well. First, we assume that $P_1, \dots, P_8 \in \mathrm{GF}(p^{2n})$. Then corollary 3.3.10 implies that

$$[P_1, P_4; P_3, P_2],\ [P_5, P_4; P_6, P_3],\ [P_5, P_8; P_7, P_6],\\ [P_1, P_8; P_2, P_7],\ [P_1, P_5; P_7, P_3] \in \mathrm{GF}(p^n).$$

The product of all of the above cross-ratios can be simplified as follows:

$$\begin{aligned}
&[P_1, P_4; P_3, P_2] \cdot [P_5, P_4; P_6, P_3] \cdot [P_5, P_8; P_7, P_6] \cdot [P_1, P_8; P_2, P_7] \cdot [P_1, P_5; P_7, P_3] \\
&= \frac{(P_1 - P_3)(P_4 - P_2)}{(P_1 - P_2)(P_4 - P_3)} \cdot \frac{(P_5 - P_6)(P_4 - P_3)}{(P_5 - P_3)(P_4 - P_6)} \cdot \frac{(P_5 - P_7)(P_8 - P_6)}{(P_5 - P_6)(P_8 - P_7)} \cdot \\
&\quad \cdot \frac{(P_1 - P_2)(P_8 - P_7)}{(P_1 - P_7)(P_8 - P_2)} \cdot \frac{(P_1 - P_7)(P_5 - P_3)}{(P_1 - P_3)(P_5 - P_7)} \\
&= \frac{(P_4 - P_2)(P_8 - P_6)}{(P_4 - P_6)(P_8 - P_2)} \\
&= [P_4, P_8; P_2, P_6].
\end{aligned}$$

Now, since $\mathrm{GF}(p^n)$ is a field and therefore closed under multiplication, it follows that

$$[P_4, P_8; P_2, P_6] \in \mathrm{GF}(p^n).$$

With corollary 3.3.10, we conclude that P_2, P_4, P_6, and P_8 lie on a common block. Second, we consider the case where $\infty \in \{P_1, \dots, P_8\}$. Since the order of $\mathcal{M}_{p^n}$ is at least 3 (q.v. remark 3.3.14), it follows that $\mathrm{card}(\mathbb{P}) = p^{2n} + 1 \geq 3^2 + 1 = 10$. Therefore, it is always possible to choose a point $P \in \mathbb{P} \setminus \{P_1, \dots, P_8\}$. Then consider the Möbius transformation μ_P as defined in (3.19). We proved that μ_P is an incident preserving bijection that maps the point P to ∞ (q.v. claim 3.3.6). Thus, applying the map μ_P leads us again to the case where $P_1', \dots, P_8' \in \mathrm{GF}(p^{2n})$, and the desired result follows. □

3.3.2 Intersection Points of Two Blocks

Before we can properly deal with circle theorems in Miquelian Möbius planes, we also need to address the question of whether two given blocks are disjoint, tangent, or intersecting. Of course, one can straightforwardly list all points on each block and thereby identify intersection points of two blocks. In fact, we will afterwards use the latter method with the help of a programming language when we consider the plane $\mathcal{M}_{11}$. But for the sake of completeness, we state now a formula for this matter (cf. [HV18]).

Proposition 3.3.15. Consider a Miquelian Möbius plane of order p^n, where $p \neq 2$.

(i) Let $\mathcal{B}^2_{(a_1,b_1)}$ and $\mathcal{B}^2_{(a_2,b_2)}$ be two different lines.

- If $a_1\overline{a_2} - \overline{a_1}a_2 = 0$, then the lines are tangent at ∞.
- If $a_1\overline{a_2} - \overline{a_1}a_2 \neq 0$, then the lines intersect at ∞ and $z_0 = \frac{a_1 b_2 - a_2 b_1}{a_1\overline{a_2} - \overline{a_1}a_2}$.

(ii) Let $\mathcal{B}^1_{(c_1,r_1)}$ and $\mathcal{B}^1_{(c_2,r_2)}$ be two different circles, and let

$$D = (r_2 - r_1 - \|c\|)^2 - 4\,\|c\|\,r_1 \quad \text{for } c := c_2 - c_1.$$

- If $D \neq 0$ is a square in $\mathrm{GF}(p^n)$, then the circles are disjoint.
- If $D = 0$, then the circles are tangent at $z_0 = \frac{\|c\|+r_1-r_2}{2\overline{c}} + c_1$.
- If $D \neq 0$ is a nonsquare in $\mathrm{GF}(p^n)$, then the circles intersect at $z_{1,2} = \frac{(\|c\|+r_1-r_2)\pm\sqrt{D}}{2\overline{c}} + c_1$.

(iii) Let $\mathcal{B}^1_{(c,r)}$ and $\mathcal{B}^2_{(a,b)}$ be two different blocks, and let

$$D = b_0^2 - 4\,\|a\|\,r \quad \text{for } b_0 := b - \overline{a}c - a\overline{c}.$$

- If $D \neq 0$ is a square in $\mathrm{GF}(p^n)$, then the blocks are disjoint.
- If $D = 0$, then the blocks are tangent at $z_0 = \frac{b_0}{2\overline{a}} + c$.
- If $D \neq 0$ is a nonsquare in $\mathrm{GF}(p^n)$, then the blocks intersect at $z_{1,2} = \frac{b_0\pm\sqrt{D}}{2\overline{a}} + c$.

Proof. (i) The equations of the lines $\mathcal{B}^2_{(a_1,b_1)}$ and $\mathcal{B}^2_{(a_2,b_2)}$ define the system of equations

$$\begin{cases} \overline{a_1}z + a_1\overline{z} = b_1, \\ \overline{a_2}z + a_2\overline{z} = b_2, \end{cases}$$

where $a_1, a_2 \in \mathrm{GF}(p^{2n})\backslash\{0\}$ and $b_1, b_2 \in \mathrm{GF}(p^n)$. Since $a_1 \neq 0 \neq a_2$, we can multiply the first equation by $\frac{a_2}{a_1}$ and then subtract the resulting equation from the second equation in the above system. Then we get

$$\begin{aligned} & z\Big(\overline{a_2} - \frac{\overline{a_1}a_2}{a_1}\Big) = b_2 - \frac{a_2 b_1}{a_1} \\ \iff \quad & z(a_1\overline{a_2} - \overline{a_1}a_2) = a_1 b_2 - a_2 b_1. \end{aligned} \tag{3.28}$$

We already saw that $\mathcal{B}^2_{(a_1,b_1)} \cap \mathcal{B}^2_{(a_2,b_2)} = \{\infty\}$ if and only if $a_1\overline{a_2} = \overline{a_1}a_2$ (q.v. equations (3.17) and (3.18)). If $a_1\overline{a_2} \neq \overline{a_1}a_2$, then we can divide equation (3.28) by $a_1\overline{a_2} - \overline{a_1}a_2$ and the result follows.

(ii) The equations of the circles $\mathcal{B}^1_{(c_1,r_1)}$ and $\mathcal{B}^1_{(c_2,r_2)}$ are given by

$$(z - c_1)(\overline{z} - \overline{c_1}) = r_1 \quad \text{and} \quad (z - c_2)(\overline{z} - \overline{c_2}) = r_2, \tag{3.29}$$

respectively, where $c_1, c_2 \in \mathrm{GF}(p^{2n})$ and $r_1, r_2 \in \mathrm{GF}(p^n)\backslash\{0\}$.

Let $x = z - c_1$ and $c = c_2 - c_1$. With this, the equations in (3.29) define the following system of equations:

$$\begin{cases} x\overline{x} = r_1, \\ (x-c)(\overline{x}-\overline{c}) = r_2. \end{cases} \tag{3.30}$$

As $r_1 \neq 0$, it follows that $x \neq 0$. Thus, we can multiply the second equation of the system (3.30) by x and then replace all instances of $x\overline{x}$ by r_1. Then we get

$$\overline{c}x^2 + (r_2 - r_1 - \|c\|)x + r_1 c = 0, \tag{3.31}$$

which is a quadratic equation in x. By assumption, the characteristic of the field $\mathrm{GF}(p^{2n})$ is not 2 (i.e. p is odd), hence we can use the quadratic formula and find that the solutions of equation (3.31) are

$$x_{1,2} = \frac{(\|c\| + r_1 - r_2) \pm \sqrt{D}}{2\overline{c}} \quad \text{for } D := (r_2 - r_1 - \|c\|)^2 - 4\,\|c\|\, r_1.$$

Observe that we may assume that $c \neq 0$: if $c = c_2 - c_1 = 0$, then it follows that $r_1 \neq r_2$, since the two circles are different. In this case, the circles clearly do not intersect. Notice that the case $c = 0$ is covered in the proposition, since $D = (r_2 - r_1)^2$ is a square in $\mathrm{GF}(p^n)$, which leads to the conclusion that the circles are disjoint.

However, since $r_1, r_2, \|c\| \in \mathrm{GF}(p^n)$, it follows that D is an element of $\mathrm{GF}(p^n)$. Consequently, x_1 and x_2 always exist (q.v. lemma 2.1.22). Therefore, we need to check whether x_1 and x_2 indeed satisfy the equations of the system (3.30). For this, we distinguish between two cases: first, the case where either D is a nonsquare in $\mathrm{GF}(p^n)$ or $D = 0$; second, the case where $D \neq 0$ is a square in $\mathrm{GF}(p^n)$.

- Suppose that D is a nonsquare in $\mathrm{GF}(p^n)$ or $D = 0$. Using lemma 2.1.23 (ii), we find the following: For $j \in \{1, 2\}$ it holds that

$$\begin{aligned} x_j\overline{x_j} &= \frac{\Big((\|c\| + r_1 - r_2) \pm \sqrt{D}\Big)\Big((\|c\| + r_1 - r_2) \mp \sqrt{D}\Big)}{4\,\|c\|} \\ &= \frac{(\|c\| + r_1 - r_2)^2 - D}{4\,\|c\|} \\ &= \frac{4\,\|c\|\, r_1}{4\,\|c\|} \\ &= r_1. \end{aligned}$$

  Analogously, one may verify that also $(x_j - c)(\overline{x_j} - \overline{c}) = r_2$ holds, which means that x_1 and x_2 indeed satisfy both equations in the system (3.30). Consequently, if D is a nonsquare in $\mathrm{GF}(p^n)$, then $\mathcal{B}^1_{(c_1,r_1)}$ and $\mathcal{B}^1_{(c_2,r_2)}$ intersect at

$$z_{1,2} = x_{1,2} + c_1 = \frac{(\|c\| + r_1 - r_2) \pm \sqrt{D}}{2\overline{c}} + c_1.$$

If $D = 0$, then $\mathcal{B}^1_{(c_1,r_1)}$ and $\mathcal{B}^1_{(c_2,r_2)}$ are tangent at $z = \frac{\|c\|+r_1-r_2}{2\overline{c}} + c_1$.

- Suppose that $D \neq 0$ is a square in $\mathrm{GF}(p^n)$. Using lemma 2.1.23 (i), we find the following: For $j \in \{1, 2\}$ it holds that

$$\begin{aligned} x_j\overline{x_j} &= \frac{\Big((\|c\| + r_1 - r_2) \pm \sqrt{D}\Big)^2}{4\,\|c\|} \\ &= \frac{(\|c\| + r_1 - r_2)^2 \pm 2\sqrt{D}(\|c\| + r_1 - r_2) + D}{4\,\|c\|} \\ &= \frac{\big((\|c\| + r_1 - r_2)^2 - D\big) + \Big(2D \pm 2\sqrt{D}(\|c\| + r_1 - r_2)\Big)}{4\,\|c\|} \\ &= r_1 + \frac{D \pm \sqrt{D}(\|c\| + r_1 - r_2)}{2\,\|c\|}. \end{aligned}$$

Observe that

$$\begin{aligned} \frac{D \pm \sqrt{D}(\|c\| + r_1 - r_2)}{2\,\|c\|} = 0 &\iff \sqrt{D}\Big(\sqrt{D} \pm (\|c\| + r_1 - r_2)\Big) = 0 \\ &\overset{(D\neq 0)}{\iff} \sqrt{D} \pm (\|c\| + r_1 - r_2) = 0 \\ &\iff D = (\|c\| + r_1 - r_2)^2 \\ &\iff 4\,\|c\|\, r_1 = 0. \end{aligned}$$

However, since p is odd and $c \neq 0 \neq r_1$, it follows that $4\,\|c\|\, r_1 \neq 0$. Therefore, the system (3.30) has no solution if $D \neq 0$ is a square in $\mathrm{GF}(p^n)$. Consequently, the blocks $\mathcal{B}^1_{(c_1,r_1)}$ and $\mathcal{B}^1_{(c_2,r_2)}$ are disjoint.

(iii) The equations of the blocks $\mathcal{B}^1_{(c,r)}$ and $\mathcal{B}^2_{(a,b)}$ are given by

$$(z - c)(\overline{z} - \overline{c}) = r \quad \text{and} \quad \overline{a}z + a\overline{z} = b, \tag{3.32}$$

respectively, where $c \in \mathrm{GF}(p^{2n})$, $r \in \mathrm{GF}(p^n)\backslash\{0\}$, $a \in \mathrm{GF}(p^{2n})\backslash\{0\}$, and $b \in \mathrm{GF}(p^n)$. Let $x = z - c$ and $b_0 = b - \overline{a}c - a\overline{c}$. With this, the equations in (3.32) define the following system of equations:

$$\begin{cases} x\overline{x} = r, \\ \overline{a}x + a\overline{x} = b_0. \end{cases} \tag{3.33}$$

Since $x \neq 0$, we can multiply the second equation of the system (3.33) by x and then replace all instances of $\overline{x}$ by $\frac{r}{x}$. Then we get the following quadratic equation in x:

$$\overline{a}x^2 - b_0x + ar = 0. \tag{3.34}$$

Thus, the solutions of equation (3.34) are given by

$$x_{1,2} = \frac{b_0 \pm \sqrt{D}}{2\overline{a}} \quad \text{for } D := b_0^2 - 4\,\|a\|\,r.$$

However, also in this case it holds that D is an element of $\mathrm{GF}(p^n)$. Therefore, x_1 and x_2 always exist, but are not necessarily solutions of the system (3.33). As before, we distinguish between two cases:

- Assume that D is a nonsquare in $\mathrm{GF}(p^n)$ or $D = 0$. Using lemma 2.1.23 (ii), we find the following: For $j \in \{1, 2\}$ it holds that

  $$x_j\overline{x_j} = \frac{\left(b_0 \pm \sqrt{D}\right)\left(b_0 \mp \sqrt{D}\right)}{4\,\|a\|} = \frac{b_0^2 - D}{4\,\|a\|} = \frac{4\,\|a\|\,r}{4\,\|a\|} = r$$

  and

  $$\overline{a}x_j + a\overline{x_j} = \frac{b_0 \pm \sqrt{D}}{2} + \frac{b_0 \mp \sqrt{D}}{2} = b_0.$$

  Thus, x_1 and x_2 satisfy both equations in the system (3.33). Consequently, if D is a nonsquare in $\mathrm{GF}(p^n)$, then $\mathcal{B}^1_{(c,r)}$ and $\mathcal{B}^2_{(a,b)}$ intersect at

  $$z_{1,2} = x_{1,2} + c = \frac{b_0 \pm \sqrt{D}}{2\overline{a}} + c.$$

  If $D = 0$, then $\mathcal{B}^1_{(c,r)}$ and $\mathcal{B}^2_{(a,b)}$ are tangent at $z = \frac{b_0}{2\overline{a}} + c$.

- Assume that $D \neq 0$ is a square in $\mathrm{GF}(p^n)$. Using lemma 2.1.23 (i), we find the following: For $j \in \{1, 2\}$ it holds that

  $$\begin{aligned} x_j\overline{x_j} &= \frac{\left(b_0 \pm \sqrt{D}\right)^2}{4\,\|a\|} = \frac{b_0^2 \pm 2b_0\sqrt{D} + D}{4\,\|a\|} = \frac{\left(b_0^2 - D\right) + \left(2D \pm 2b_0\sqrt{D}\right)}{4\,\|a\|} \\ &= r + \frac{D \pm b_0\sqrt{D}}{2\,\|a\|}. \end{aligned}$$

  Observe that

  $$\begin{aligned} \frac{D \pm b_0\sqrt{D}}{2\,\|a\|} = 0 &\overset{(D\neq 0)}{\iff} \sqrt{D} \pm b_0 = 0 \\ &\iff D = b_0^2 \\ &\iff 4\,\|a\|\,r = 0. \end{aligned}$$

  However, since p is odd and $a \neq 0 \neq r$, it follows that $4\,\|a\|\,r \neq 0$. Therefore, the system (3.33) has no solution if $D \neq 0$ is a square in $\mathrm{GF}(p^n)$. Consequently, the blocks $\mathcal{B}^1_{(c,r)}$ and $\mathcal{B}^2_{(a,b)}$ are disjoint.

□

3.3.3 The Plane $\mathcal{M}_{11}$

We complete this chapter with the explicit construction of the Miquelian Möbius plane of order 11, which we will afterwards use again to introduce the five circles theorem.

The plane $\mathcal{M}_{11}$ may be constructed over the pair of finite fields GF(11) and GF(11^2). In example 2.1.4, we constructed the field GF(11^2) using the irreducible polynomial $\varphi(x) = x^2 + 1$. Now, $\mathcal{M}_{11}$ is defined by

$$\begin{aligned}
&\mathbb{P} := \mathrm{GF}(11^2) \cup \{\infty\}, \infty \notin \mathrm{GF}(11^2),\\
&\mathbb{B} := \left\{ \{z \in \mathrm{GF}(11^2) \mid \overline{a}z + a\overline{z} = b\} \cup \{\infty\} \,\middle|\, a \in \mathrm{GF}(11^2)\backslash\{0\}, b \in \mathrm{GF}(11) \right\}\\
&\qquad \cup \left\{ \{z \in \mathrm{GF}(11^2) \mid (z-c)\overline{(z-c)} = r\} \,\middle|\, c \in \mathrm{GF}(11^2), r \in \mathrm{GF}(11)\backslash\{0\} \right\}, \text{ and}\\
&\mathbb{I} \subseteq \mathbb{P} \times \mathbb{B} : \; P \,\mathrm{I}\, g \;:\Longleftrightarrow\; P \in g,
\end{aligned}$$

where $\overline{z} = z^{11}$.

This plane consists of $11^2 + 1 = 122$ points and a total of $11(11^2 + 1) = 1342$ blocks comprising $\frac{11^2-1}{11-1} \cdot 11 = 132$ lines and $11^2(11-1) = 1210$ circles (q.v. observation 3.3.1). Moreover, each block is incident with exactly 12 points (q.v. corollary 3.3.4).

We saw how to find a block passing through three given points (q.v. lemma 3.3.8) and how to check whether four given points lie on a common block or not (q.v. corollary 3.3.10). Furthermore, we discussed in section 3.3.2 how to compute the intersection points of two blocks wherever they exist. As the calculations in $\mathcal{M}_{11}$ are rather extensive by hand, we use now the programming language **R**. We implemented the addition and multiplication tables of the field GF(p^{2n}) and defined functions for all the mentioned computations. The code is provided in appendix A.

Now, let us consider the circle $\mathcal{B}^1_{(0,1)}$ and the line $\mathcal{B}^2_{(1,0)}$. The points on these blocks have to satisfy the equations $z\overline{z} = 1$ and $z + \overline{z} = 0$, respectively. Solving these equations yields that

$$\begin{aligned}
\mathcal{B}^1_{(0,1)} = \{&1,\ 10,\ x,\ 3x+5,\ 3x+6,\ 5x+3,\\
&5x+8,\ 6x+3,\ 6x+8,\ 8x+5,\ 8x+6,\ 10x\},
\end{aligned} \tag{3.35}$$

$$\mathcal{B}^2_{(1,0)} = \{0,\ x,\ 2x,\ 3x,\ 4x,\ 5x,\ 6x,\ 7x,\ 8x,\ 9x,\ 10x,\ \infty\}. \tag{3.36}$$

Remark 3.3.16. We shall point out that the points on the circle $\mathcal{B}^1_{(c,1)}$ may also be determined by applying the Möbius transformation $\mu(z) = z - c$ to each element of $\mathcal{B}^1_{(0,1)}$. Similarly, the points on the line $\mathcal{B}^2_{(a,0)}$ are determined by applying the Möbius transformation $\mu(z) = \overline{a}z$ to each element of $\mathcal{B}^2_{(1,0)}$.

The circle $\mathcal{B}^1_{(0,1)}$ will play a crucial role in the following chapter, so let us consider this circle in more detail. One way to determine the distribution of the points on $\mathcal{B}^1_{(0,1)}$ is the following: As for circles in the Euclidean plane, we may consider 0 as the center of the circle $\mathcal{B}^1_{(0,1)} : (z-0)(\overline{z} - \overline{0}) = r$. By identifying the line through the center 0

and the point $1 \in \mathcal{B}^1_{(0,1)}$, and then the second intersection point of this line and the circle $\mathcal{B}^1_{(0,1)}$, we find that 1 and 10 are "opposite" points on the circle. Following

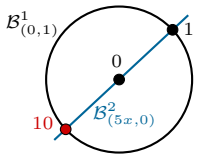


FIGURE 3.7: Opposite point of 1 on $\mathcal{B}^1_{(0,1)}$ in $\mathcal{M}_{11}$.

this idea, we may identify which points on $\mathcal{B}^1_{(0,1)}$ are opposite to each other:

1	10
x	$10x$
$3x+5$	$8x+6$
$3x+6$	$8x+5$
$5x+3$	$6x+8$
$5x+8$	$6x+3$

TABLE 3.1: Opposite points on $\mathcal{B}^1_{(0,1)}$ in $\mathcal{M}_{11}$.

Notice that the opposite point of $P \in \mathcal{B}^1_{(0,1)}$ is $-P$. Next, we consider all circles that have center 1 or 10 and determine the points where these circles intersect $\mathcal{B}^1_{(0,1)}$:

r	$\mathcal{B}^1_{(1,r)} \cap \mathcal{B}^1_{(0,1)}$	$\mathcal{B}^1_{(10,r)} \cap \mathcal{B}^1_{(0,1)}$
1	$\{3x+6,\ 8x+6\}$	$\{3x+5,\ 8x+5\}$
2	$\{x,\ 10x\}$	$\{x,\ 10x\}$
3	$\{3x+5,\ 8x+5\}$	$\{3x+6,\ 8x+6\}$
4	$\{10\}$	$\{1\}$
5	$\varnothing$	$\varnothing$
6	$\varnothing$	$\varnothing$
7	$\{5x+3,\ 6x+3\}$	$\{5x+8,\ 6x+8\}$
8	$\{5x+8,\ 6x+8\}$	$\{5x+3,\ 6x+3\}$
9	$\varnothing$	$\varnothing$
10	$\varnothing$	$\varnothing$

With this, we obtain the distribution of the points on $\mathcal{B}^1_{(0,1)}$ (figure 3.8).

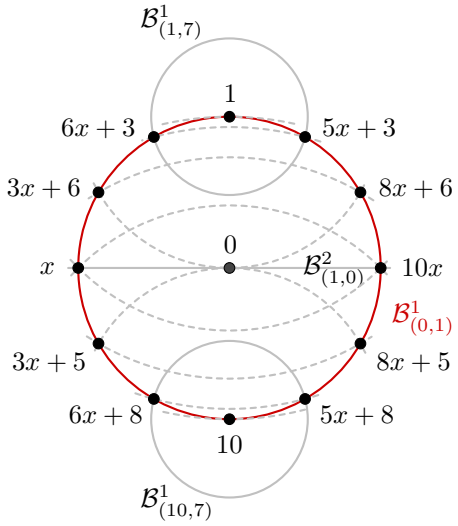


FIGURE 3.8: Distribution of points on $\mathcal{B}^1_{(0,1)}$ in $\mathcal{M}_{11}$.

Convention. From now on, we will refer to $\mathcal{B}^1_{(0,1)}$ as the *unit circle* in Miquelian Möbius planes $\mathcal{M}_{p^n}$. Moreover, we call c the *center* of $\mathcal{B}^1_{(c,r)}$.

Chapter 4

Circle Theorems in Finite Miquelian Möbius Planes

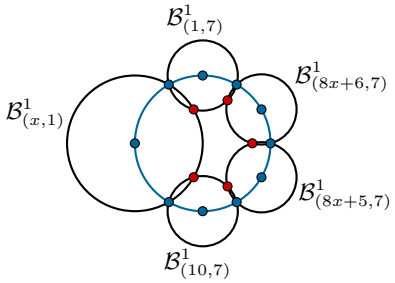
We constructed and examined Miquelian Möbius planes of prime power order in chapter 3. With this, we are now prepared to study the five circles theorem and Miquel's pentagon theorem in these planes. The latter two theorems can both be verified in an elementary way in the Euclidean plane (q.v. chapter 1). However, as an incidence structure, a Möbius plane does not involve concepts such as length, angle, continuity, and betweenness, but only incidence. Hence, the theorems cannot be proved in the same way.

In section 4.1, we first verify the five circles theorem in the Miquelian Möbius plane of order 11 by using visualizations and our implementation in **R** for the computations (q.v. appendix A). Then we go over to the general case, meaning that we prove the five circles theorem in $\mathcal{M}_{p^n}$, where p is a prime and n a positive integer. In section 4.2, we prove Miquel's pentagon theorem in $\mathcal{M}_{p^n}$ in an algebraic manner.

4.1 The Five Circles Theorem

4.1.1 Verification in $\mathcal{M}_{11}$

Let us now have a closer look at the Miquelian Möbius plane of order 11, which we constructed in section 3.3.3. We consider again the unit circle $\mathcal{B}^1_{(0,1)}$ (q.v. figure 3.8) along with the five circles $\mathcal{B}^1_{(1,7)}$, $\mathcal{B}^1_{(8x+6,7)}$, $\mathcal{B}^1_{(8x+5,7)}$, $\mathcal{B}^1_{(10,7)}$, and $\mathcal{B}^1_{(x,1)}$.



The latter five circles are chosen such that they all have its center on the unit circle and such that they intersect "chainwise" at two points with one of them lying on the unit circle. These intersection points are the following:

$$\begin{aligned}
\mathcal{B}^1_{(1,7)} \cap \mathcal{B}^1_{(8x+6,7)} &= \{5x+3, 3x+4\}, & \mathcal{B}^1_{(8x+6,7)} \cap \mathcal{B}^1_{(8x+5,7)} &= \{10x, 6x\},\\
\mathcal{B}^1_{(8x+5,7)} \cap \mathcal{B}^1_{(10,7)} &= \{5x+8, 3x+7\}, & \mathcal{B}^1_{(10,7)} \cap \mathcal{B}^1_{(x,1)} &= \{6x+8, 9x+5\},\\
\mathcal{B}^1_{(x,1)} \cap \mathcal{B}^1_{(1,7)} &= \{6x+3, 9x+6\},
\end{aligned}$$

where $5x+3$, $10x$, $5x+8$, $6x+8$, $6x+3 \in \mathcal{B}^1_{(0,1)}$. For each two "adjacent" intersection points that do not lie on the unit circle, we determine now the unique line passing through them:

$$\begin{aligned}
3x+4,\ 6x \in \mathcal{B}^2_{(2x+7,2)}, \qquad & 6x,\ 3x+7 \in \mathcal{B}^2_{(9x+7,9)},\\
3x+7,\ 9x+5 \in \mathcal{B}^2_{(x+3,4)}, \qquad & 9x+5,\ 9x+6 \in \mathcal{B}^2_{(5x,2)},\\
9x+6,\ 3x+4 \in \mathcal{B}^2_{(10x+3,7)}. &
\end{aligned}$$

Remarkably, it holds now that the intersection point of every pair of these five lines lies again on one of the five circles with its center on the unit circle:

$$\begin{aligned}
\mathcal{B}^2_{(2x+7,2)} \cap \mathcal{B}^2_{(x+3,4)} &= \{8\} \subseteq \mathcal{B}^1_{(8x+5,7)}, & \mathcal{B}^2_{(9x+7,9)} \cap \mathcal{B}^2_{(5x,2)} &= \{9x+4\} \subseteq \mathcal{B}^1_{(10,7)},\\
\mathcal{B}^2_{(x+3,4)} \cap \mathcal{B}^2_{(10x+3,7)} &= \{2x\} \subseteq \mathcal{B}^1_{(x,1)}, & \mathcal{B}^2_{(5x,2)} \cap \mathcal{B}^2_{(2x+7,2)} &= \{9x+7\} \subseteq \mathcal{B}^1_{(1,7)},\\
\mathcal{B}^2_{(10x+3,7)} \cap \mathcal{B}^2_{(9x+7,9)} &= \{3\} \subseteq \mathcal{B}^1_{(8x+6,7)}.
\end{aligned}$$

And this is exactly what the five circles theorem tells us (figure 4.1).

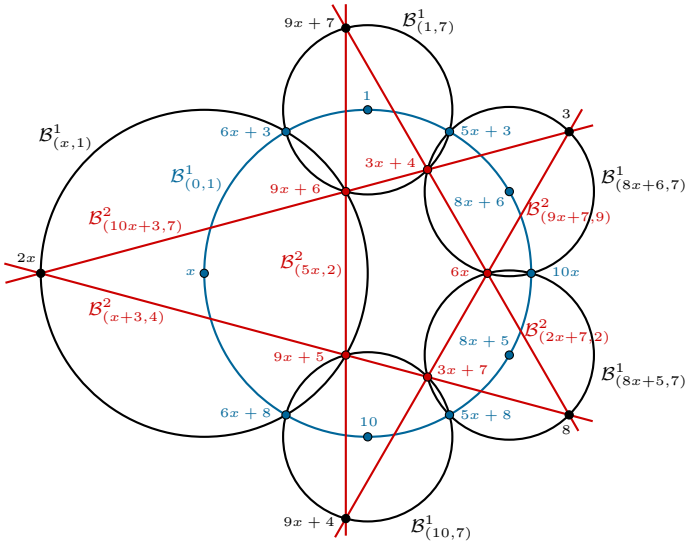
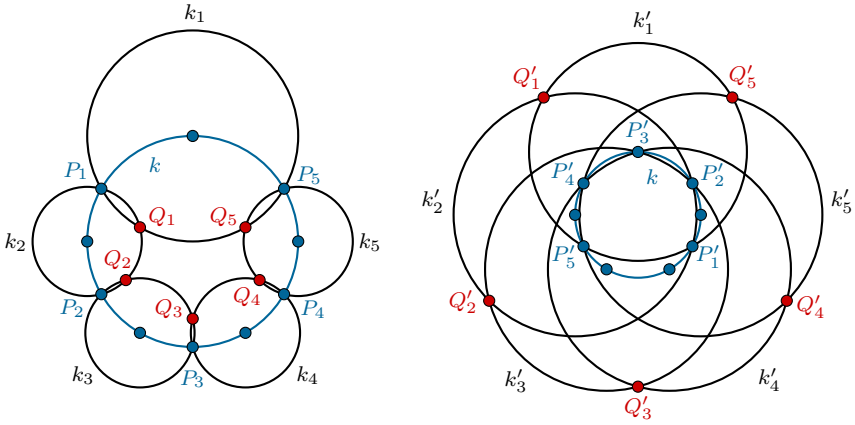


FIGURE 4.1: Example of the five circles theorem in $\mathcal{M}_{11}$.

Now we aim to consider each family of six circles $k, k_1, \ldots, k_5$ in $\mathcal{M}_{11}$ with the property that $k_1, \ldots, k_5$ have its center on k and such that $k_i \cap k_{i+1} = \{P_i, Q_i\}$ with $P_i \in k$ for $i \in \{1, \ldots, 5\}$ as shown in figure 4.2, case (i).

Remark 4.1.1. Be aware that there exists another family of five circles $k'_1, \ldots, k'_5$ such that k_i and k'_i have the same center (lying on k) and also $k'_i \cap k'_{i+1} = \{P'_i, Q'_i\}$ with $P'_i \in k$ as shown in figure 4.2, case (ii). But the five circles theorem does not hold true in this case. For now, since we are working in the concrete plane $\mathcal{M}_{11}$, we distinguish between a chainwise set-up (case (i)) and a non-chainwise set-up (case (ii)) by using visualizations. In section 4.1.2, we will give more explicit conditions to distinguish the two cases without the use of visualizations.



Case (i): chainwise set-up. Case (ii): non-chainwise set-up.

FIGURE 4.2: On the condition of the five circles theorem.

We mentioned in section 3.3.1 that there is a unique Möbius transformation mapping any block to any other block. Consequently, we may assume without loss of generality that k is the unit circle. We know that there are exactly twelve points on k, of which ten are involved in the five circles theorem. This results a priori in $\binom{12}{10} = 66$ possible choices for the family of circles $k_1, \ldots, k_5$. However, these circles have to intersect chainwise. From figure 3.8 and by direct computation, we find the following:

- A circle with center $T_i \in \mathcal{B}^1_{(0,1)}$ that passes through the adjacent points of T_i, say $T_{i-1}, T_{i+1} \in \mathcal{B}^1_{(0,1)}$, is given by $\mathcal{B}^1_{(T_i,7)}$. In particular, $r = 7$.
- A circle with center $T_i \in \mathcal{B}^1_{(0,1)}$ that passes through the points $T_{i-2}, T_{i+2} \in \mathcal{B}^1_{(0,1)}$ is given by $\mathcal{B}^1_{(T_i,1)}$. In particular, $r = 1$.

Now, choosing for $k_1, \ldots, k_5$ only circles with $r = 7$ results in six circles (figure 4.3 (a)), which is not what we need. Furthermore, if we choose a circle with $r \notin \{1, 7\}$, then we end up with at most four circles, which is again not of the desired form (figure

4.3 (c)). Evidently, the only suitable possibility is to choose one circle with $r = 1$ and four circles with $r = 7$ (figure 4.3 (b)). We have twelve possibilities for the choice of $\mathcal{B}^1_{(T_i,1)}$, namely the twelve points on the unit circle for T_i. But once we chose $\mathcal{B}^1_{(T_i,1)}$, the other four circles are already uniquely determined. Consequently, we have twelve possible choices for the family of circles $k_1, \ldots, k_5$.

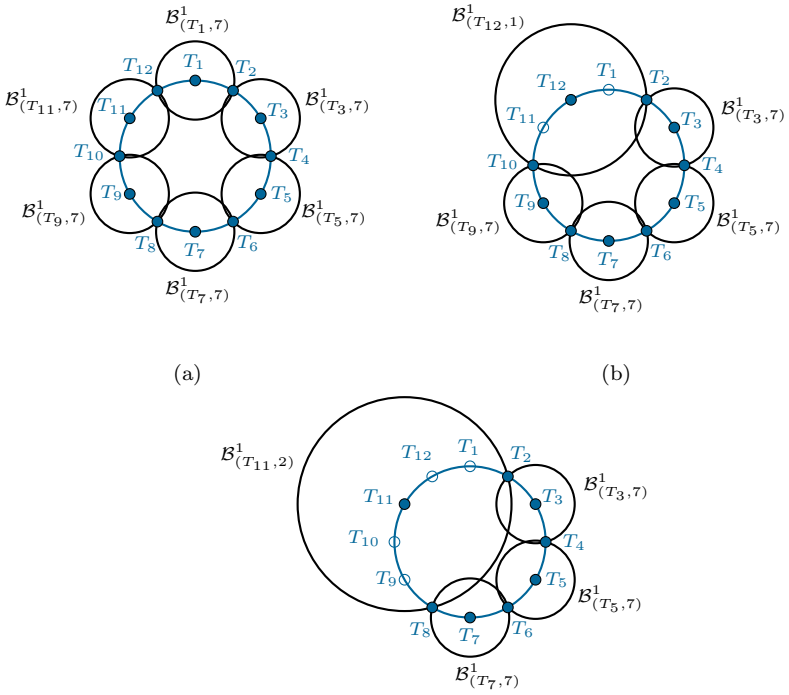


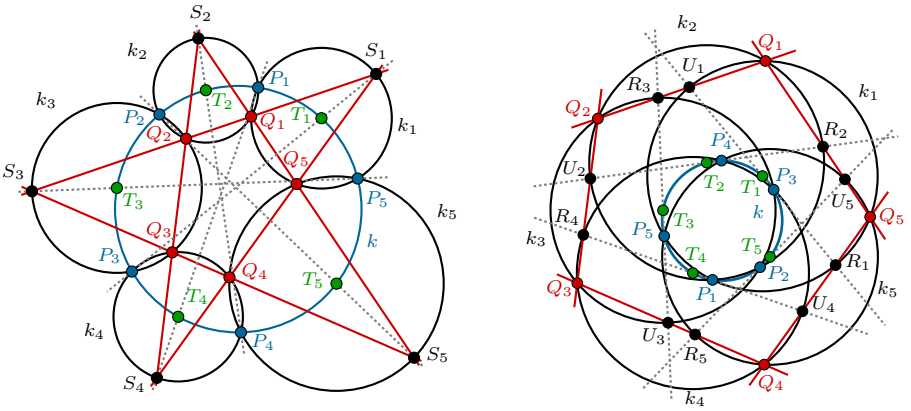
FIGURE 4.3: Possibilities in $\mathcal{M}_{11}$.

By direct computation one verifies that the five circles theorem holds true for all of these twelve suitable possibilities for the circles $k, k_1, \ldots, k_5$ with $k = \mathcal{B}^1_{(0,1)}$. This shows that the five circles theorem is indeed true in the Miquelian Möbius plane of order 11.

4.1.2 The General Case

As the five circles theorem is satisfied in $\mathcal{M}_{11}$, it already seems promising that the theorem holds true in every Miquelian Möbius plane of prime power order. Let us now state the theorem in $\mathcal{M}_{p^n}$.

Theorem 4.1.2. Let $T_1, \dots, T_5$ be five different points on a circle k. Then there are two families of five circles $k_1, \dots, k_5$, where T_i is the center of k_i and such that k_i and k_{i+1} intersect at P_i on k and Q_i for each $i \in \{1, \dots, 5\}$. In one family the three blocks $\overrightarrow{T_i\, P_{i+2}\, \infty}$, $\overrightarrow{Q_i\, Q_{i+1}\, \infty}$, and $\overrightarrow{Q_{i+3}\, Q_{i+4}\, \infty}$ meet in a point S_i on k_i, while in the other family the blocks $\overrightarrow{T_i\, P_{i+2}\, \infty}$ and $\overrightarrow{Q_i\, Q_{i+1}\, \infty}$ meet in U_i on k_i and the blocks $\overrightarrow{T_i\, P_{i+2}\, \infty}$ and $\overrightarrow{Q_{i+3}\, Q_{i+4}\, \infty}$ meet in $R_i \neq U_i$ on k_i.



Family (i) Family (ii)

FIGURE 4.4: The five circles theorem in $\mathcal{M}_{p^n}$.

Remark 4.1.3. The case of family (i) in figure 4.4 represents what is commonly understood by the five circles theorem and is thus more interesting than the case of family (ii). We distinguish here between these two families since the absence of concepts as length, angle, and betweenness in Miquelian Möbius planes prevents us from properly using notions like chainwise intersection or adjacent points.

Remark 4.1.4. Throughout this section the subscripts are always taken modulo 5.

Proof. Let $k \in \mathbb{B}$, and let $T_1, \dots, T_5 \in \mathbb{P}$ be five different points on k. There exists a unique Möbius transformation that maps the circle k to the unit circle $\mathcal{B}^1_{(0,1)}\colon z\overline{z} = 1$. Therefore, we may assume without loss of generality that k is the unit circle. Our first goal is to find every family consisting of five circles $k_1, \dots, k_5$ with the property that $k_i \cap k_{i+1} = \{P_i, Q_i\}$ for $P_i \in k$ and $Q_i \in \mathbb{P}$ and such that T_i is the center of k_i

for each $i \in \{1, \dots, 5\}$. To achieve this, we introduce the following map:

$$\begin{aligned} \varphi_T \colon k &\longrightarrow k, \\ z &\longmapsto z' := T^2\,\overline{z} \end{aligned}$$

for $T \in k$. Observe that the image of every point $z \in k$ indeed lies on k, since

$$z'\overline{z'} = T^2\,\overline{z} \cdot \overline{T^2\,\overline{z}} = T\,\overline{T} \cdot T\overline{T} \cdot \overline{z}z = 1,$$

as T and z lie on $k = \mathcal{B}^1_{(0,1)}$, which means that $T\overline{T} = z\overline{z} = 1$.

Claim 1. The map φ_T corresponds to the reflection at $g := \overleftrightarrow{0\,T\,\infty}$.

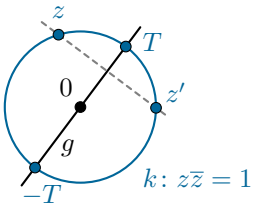


FIGURE 4.5: The map φ_T.

Proof of claim 1:

- First, we show that $\pm T \in k \cap g$ are fixed points:

  $$\varphi_T(\pm T) = \pm T^2\,\overline{T} = \pm T \cdot T\,\overline{T} = \pm T,$$

  since $T \in k$.

- Second, we verify that φ_T is an involution:

  $$\varphi_T \circ \varphi_T(z) = T^2\,\overline{T^2\,\overline{z}} = T\,\overline{T} \cdot T\overline{T} \cdot z = z.$$

■

Now, we can use the map φ_T to express the points $P_1, \dots, P_5$ in terms of the points $T_1, \dots, T_5$:

Claim 2. Given five different circles $k_1, \dots, k_5$, where $T_i \in k$ is the center of k_i and such that k_i and k_{i+1} intersect at $P_i \in k$ and Q_i for each $i \in \{1, \dots, 5\}$, then there are two possibilities for P_i, namely

$$P_i = \pm\, T_i\, T_{i+1}\, \overline{T_{i+2}}\, T_{i+3}\, \overline{T_{i+4}}.$$

Proof of claim 2: We use the map φ_T for each $T \in \{T_1, \dots, T_5\} \subseteq k$ (figure 4.6). Since $P_i \in k$ and $P_i \in k_i \cap k_{i+1}$ for all $i \in \{1, \dots, 5\}$, we subsequently find that

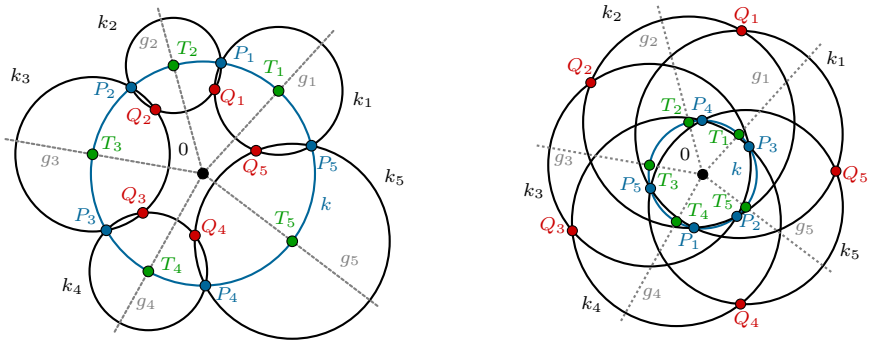
$$P_1 = \varphi_{T_1}(P_5) = T_1^2\,\overline{P_5}, \tag{4.1}$$

$$P_2 = \varphi_{T_2}(P_1) = T_2^2\,\overline{P_1} = T_2^2\,\overline{T_1^2\,\overline{P_5}} = \overline{T_1^2}\,T_2^2\,P_5, \tag{4.2}$$

$$P_3 = \varphi_{T_3}(P_2) = T_3^2\,\overline{P_2} = T_3^2\,\overline{\overline{T_1^2}\,T_2^2\,P_5} = T_1^2\,\overline{T_2^2}\,T_3^2\,\overline{P_5}, \tag{4.3}$$

$$P_4 = \varphi_{T_4}(P_3) = T_4^2\,\overline{P_3} = T_4^2\,\overline{T_1^2\,\overline{T_2^2}\,T_3^2\,\overline{P_5}} = \overline{T_1^2}\,T_2^2\,\overline{T_3^2}\,T_4^2\,P_5, \tag{4.4}$$

$$P_5 = \varphi_{T_5}(P_4) = T_5^2\,\overline{P_4} = T_5^2\,\overline{\overline{T_1^2}\,T_2^2\,\overline{T_3^2}\,T_4^2\,P_5} = T_1^2\,\overline{T_2^2}\,T_3^2\,\overline{T_4^2}\,T_5^2\,\overline{P_5}. \tag{4.5}$$



Family (i) Family (ii)

FIGURE 4.6

Multiplying equation (4.5) by P_5 results in the following quadratic equation in P_5:

$$P_5^2 = (T_1\,\overline{T_2}\,T_3\overline{T_4}\,T_5)^2\,\underbrace{\overline{P_5}P_5}_{=1}.$$

Consequently, it follows that

$$P_5 = \pm\,T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5.$$

Now, we replace P_5 by $\pm\,T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5$ in (4.1)–(4.4). Then we obtain the points $P_1, \dots, P_5$ written in terms of the centers $T_1, \dots, T_5$. As we have two solutions for

P_5, we also obtain two sets of distinct points $P_1, \dots, P_5$:

$$\begin{aligned}
P_1 &= T_1^2\,\overline{P_5} = \pm\, T_1^2\,\overline{T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5} = \pm\, T_1\,T_2\,\overline{T_3}\,T_4\,\overline{T_5},\\
P_2 &= \overline{T_1^2}\,T_2^2\,P_5 = \pm\,\overline{T_1^2}\,T_2^2\,T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5 = \pm\,\overline{T_1}\,T_2\,T_3\,\overline{T_4}\,T_5,\\
P_3 &= T_1^2\,\overline{T_2^2}\,T_3^2\,\overline{P_5} = \pm\, T_1^2\,\overline{T_2^2}\,T_3^2\,\overline{T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5} = \pm\, T_1\,\overline{T_2}\,T_3\,T_4\,\overline{T_5},\\
P_4 &= \overline{T_1^2}\,T_2^2\,\overline{T_3^2}\,T_4^2\,P_5 = \pm\,\overline{T_1^2}\,T_2^2\,\overline{T_3^2}\,T_4^2\,T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5 = \pm\,\overline{T_1}\,T_2\,\overline{T_3}\,T_4\,T_5,\\
P_5 &= \pm\, T_1\,\overline{T_2}\,T_3\,\overline{T_4}\,T_5.
\end{aligned}$$

Hence, the points $P_1, \dots, P_5$ are given by

$$P_i = \pm\, T_i\,T_{i+1}\,\overline{T_{i+2}}\,T_{i+3}\,\overline{T_{i+4}} \quad \text{for } i \in \{1, \dots, 5\}.$$

These points all lie indeed on k, since

$$P_i\,\overline{P_i} = (\pm\, T_i\,T_{i+1}\,\overline{T_{i+2}}\,T_{i+3}\,\overline{T_{i+4}})(\overline{\pm\, T_i\,T_{i+1}\,\overline{T_{i+2}}\,T_{i+3}\,\overline{T_{i+4}}}) = 1,$$

as $T_1, \dots, T_5 \in k$. Moreover, it holds that $P_{i-1}, P_i \in k_i$ for all $i \in \{1, \dots, 5\}$, since

$$\begin{aligned}
(P_{i-1} - T_i)(\overline{P_{i-1}} - \overline{T_i}) &= P_{i-1}\,\overline{P_{i-1}} - T_i\,\overline{P_{i-1}} - \overline{T_i}\,P_{i-1} + \underbrace{T_i\,\overline{T_i}}_{=1}\\
&= T_i\,\overline{T_i}\,P_{i-1}\,\overline{P_{i-1}} - T_i\,\overline{P_{i-1}} - \overline{T_i}\,P_{i-1} + 1\\
&= (T_i\,\overline{P_{i-1}} - 1)(\overline{T_i}\,P_{i-1} - 1)\\
&= T_i\,\overline{T_i}\,(T_i\,\overline{P_{i-1}} - 1)(\overline{T_i}\,P_{i-1} - 1)\\
&= (T_i^2\,\overline{P_{i-1}} - T_i)(\overline{T_i}^2\,P_{i-1} - \overline{T_i})\\
&= (T_i^2\,\overline{P_{i-1}} - T_i)(\overline{T_i^2\,\overline{P_{i-1}}} - \overline{T_i})\\
&= (P_i - T_i)(\overline{P_i} - \overline{T_i}),
\end{aligned}$$

where we used that $P_i = \varphi_{T_i}(P_{i-1}) = T_i^2\,\overline{P_{i-1}}$. Thus, P_{i-1} is a solution of the equation

$$(z - T_i)(\overline{z} - \overline{T_i}) = (P_i - T_i)(\overline{P_i} - \overline{T_i}),$$

which corresponds to the circle k_i with center T_i and $P_i \in k$. ■

Conversely, this means that there are two families of five circles $k_1, \dots, k_5$, where $T_i \in k$ is the center of k_i and $k_i \cap k_{i+1} = \{P_i, Q_i\}$ with $P_i \in k$ for each $i \in \{1, \dots, 5\}$. Now, we can also write the points $Q_1, \dots, Q_5$ in terms of the centers $T_1, \dots, T_5$:

Claim 3. The points $Q_1, \dots, Q_5$ may be expressed in the following way:

$$Q_i = T_i + T_{i+1} - \overline{P_i}\,T_i\,T_{i+1} \quad \text{for } i \in \{1, \dots, 5\}.$$

Proof of claim 3: Since $Q_i \in k_i \cap k_{i+1}$ for all $i \in \{1, \dots, 5\}$, we consider the system defined by the equations of k_i and k_{i+1}:

$$\begin{cases} (z - T_i)(\overline{z} - \overline{T_i}) = (P_i - T_i)(\overline{P_i} - \overline{T_i}), \\ (z - T_{i+1})(\overline{z} - \overline{T_{i+1}}) = (P_i - T_{i+1})(\overline{P_i} - \overline{T_{i+1}}), \end{cases} \tag{4.6}$$

where we used that $P_i \in k_i \cap k_{i+1}$. Subtracting the second equation from the first equation in system (4.6) yields that

$$\begin{aligned} & - z\,\overline{T_i} + z\,\overline{T_{i+1}} - \overline{z}\,T_i + \overline{z}\,T_{i+1} = -P_i\,\overline{T_i} + P_i\,\overline{T_{i+1}} - \overline{P_i}\,T_i + \overline{P_i}\,T_{i+1} \\ \iff \quad & z(\overline{T_{i+1}} - \overline{T_i}) + \overline{z}(T_{i+1} - T_i) = P_i\,(\overline{T_{i+1}} - \overline{T_i}) + \overline{P_i}\,(T_{i+1} - T_i) \\ \iff \quad & (z - P_i)(\overline{T_{i+1}} - \overline{T_i}) = (\overline{z} - \overline{P_i})(T_i - T_{i+1}) \\ \iff \quad & \overline{z} = \overline{P_i} + \frac{(z - P_i)(\overline{T_{i+1}} - \overline{T_i})}{T_i - T_{i+1}} \end{aligned} \tag{4.7}$$

Now, we replace $\overline{z}$ in the first equation of system (4.6) by the expression in (4.7):

$$\begin{aligned} & (z - T_i)\Big(\overline{P_i} - \overline{T_i} + \frac{(z - P_i)(\overline{T_{i+1}} - \overline{T_i})}{T_i - T_{i+1}}\Big) = (P_i - T_i)(\overline{P_i} - \overline{T_i}) \\ \iff \quad & (\overline{P_i} - \overline{T_i})(T_i - T_{i+1})(z - T_i - P_i + T_i) + (z - T_i)(z - P_i)(\overline{T_{i+1}} - \overline{T_i}) = 0 \\ \iff \quad & (z - P_i)\Big((\overline{P_i} - \overline{T_i})(T_i - T_{i+1}) + (z - T_i)(\overline{T_{i+1}} - \overline{T_i})\Big) = 0 \\ \iff \quad & (z - P_i)\Big(\overline{P_i}\,(T_i - T_{i+1}) - 1 + \overline{T_i}\,T_{i+1} + z(\overline{T_{i+1}} - \overline{T_i}) - T_i\,\overline{T_{i+1}} + 1\Big) = 0 \\ \iff \quad & z = P_i \quad \vee \quad z = \frac{T_i\,\overline{T_{i+1}} - \overline{T_i}\,T_{i+1} + \overline{P_i}\,(T_{i+1} - T_i)}{\overline{T_{i+1}} - \overline{T_i}}. \end{aligned}$$

Thus, since $k_i \cap k_{i+1} = \{P_i, Q_i\}$, it follows that

$$Q_i = \frac{T_i\,\overline{T_{i+1}} - \overline{T_i}\,T_{i+1} + \overline{P_i}(T_{i+1} - T_i)}{\overline{T_{i+1}} - \overline{T_i}}.$$

By using that $T_1, \dots, T_5 \in k$ and $0 \notin k$, we can further reduce the expression for Q_i:

$$\begin{aligned} Q_i &= \frac{T_i^2 - T_{i+1}^2 + \overline{P_i}\,T_i\,T_{i+1}(T_{i+1} - T_i)}{T_i - T_{i+1}} \\ &= T_i + T_{i+1} - \overline{P_i}\,T_i\,T_{i+1}. \end{aligned}$$

■

Our next goal is to find the properties of the lines joining the intersection points Q_i and Q_{i+1} for $i \in \{1, \dots, 5\}$. For this, we need to distinguish between the two families of circles $k_1, \dots, k_5$.

- *Family (i):* Consider the five circles $k_1, \dots, k_5$, where $T_i \in k$ is the center of k_i and $k_i \cap k_{i+1} = \{P_i, Q_i\}$ for each $i \in \{1, \dots, 5\}$ with

$$P_i = -T_i\, T_{i+1}\, \overline{T_{i+2}}\, T_{i+3}\, \overline{T_{i+4}} \quad \text{and} \quad Q_i = T_i + T_{i+1} - \overline{P_i}\, T_i\, T_{i+1}. \tag{4.8}$$

Inserting the expression of P_i in the expression of Q_i yields that

$$\begin{aligned} Q_i &= T_i + T_{i+1} + \overline{T_i\, T_{i+1}\, \overline{T_{i+2}}\, T_{i+3}\, \overline{T_{i+4}}}\, T_i\, T_{i+1} \\ &= T_i + T_{i+1} + T_{i+2}\, \overline{T_{i+3}}\, T_{i+4}. \end{aligned} \tag{4.9}$$

We need to show that the three blocks $\overrightarrow{T_i\, P_{i+2}\, \infty}$, $\overrightarrow{Q_i\, Q_{i+1}\, \infty}$, and $\overrightarrow{Q_{i+3}\, Q_{i+4}\, \infty}$ meet in a point S_i on k_i for each $i \in \{1, \dots, 5\}$. So, let h_{i+1} be the line through the points Q_i and Q_{i+1}, and let l_{i+1} be the line through the points T_i and P_{i+2} for every $i \in \{1, \dots, 5\}$. From lemma 3.3.8 (a) it follows that

$$\begin{aligned} h_{i+1} &= \{z \in \mathrm{GF}(p^{2n}) \mid (Q_i - z)(\overline{Q_{i+1}} - \overline{z}) = (\overline{Q_i} - \overline{z})(Q_{i+1} - z)\} \cup \{\infty\}, \\ l_{i+1} &= \{z \in \mathrm{GF}(p^{2n}) \mid (T_i - z)(\overline{P_{i+2}} - \overline{z}) = (\overline{T_i} - \overline{z})(P_{i+2} - z)\} \cup \{\infty\}. \end{aligned}$$

Of course, the lines h_{i+1}, h_{i+4}, and l_{i+1} meet in ∞, but ∞ is not on the circle k_i. First, we verify that the lines h_{i+1}, h_{i+4}, and l_{i+1} meet in a point other than ∞:

Claim 4. For each $i \in \{1, \dots, 5\}$ the lines h_{i+1}, h_{i+4}, and l_{i+1} meet in

$$S_i = T_i \left(\frac{T_{i+2}}{T_{i+1}} + \frac{T_{i+3}}{T_{i+4}} + 1 \right). \tag{4.10}$$

Proof of claim 4: The equations of the lines h_{i+1} and h_{i+4} define the following system of equations:

$$\begin{cases} (Q_i - z)(\overline{Q_{i+1}} - \overline{z}) = (\overline{Q_i} - \overline{z})(Q_{i+1} - z), \\ (Q_{i+3} - z)(\overline{Q_{i+4}} - \overline{z}) = (\overline{Q_{i+3}} - \overline{z})(Q_{i+4} - z). \end{cases} \tag{4.11}$$

We solve both equation in system (4.11) for $\overline{z}$. For the first equation we get

$$\begin{aligned} & (Q_i - z)(\overline{Q_{i+1}} - \overline{z}) = (\overline{Q_i} - \overline{z})(Q_{i+1} - z) \\ \iff\ & (Q_i - z)\, \overline{Q_{i+1}} - (Q_i - z)\overline{z} = \overline{Q_i}\, (Q_{i+1} - z) - \overline{z}(Q_{i+1} - z) \\ \iff\ & \overline{z}(Q_{i+1} - Q_i) = \overline{Q_i}\, Q_{i+1} - Q_i\, \overline{Q_{i+1}} + z(\overline{Q_{i+1}} - \overline{Q_i}) \\ \iff\ & \overline{z} = \frac{\overline{Q_i}\, Q_{i+1} - Q_i\, \overline{Q_{i+1}} + z(\overline{Q_{i+1}} - \overline{Q_i})}{Q_{i+1} - Q_i}. \end{aligned}$$

By symmetry, we get for the second equation

$$\overline{z} = \frac{\overline{Q_{i+3}}\,Q_{i+4} - Q_{i+3}\,\overline{Q_{i+4}} + z(\overline{Q_{i+4}} - \overline{Q_{i+3}})}{Q_{i+4} - Q_{i+3}}.$$

Thus, system (4.11) reduces to

$$\frac{\overline{Q_i}\,Q_{i+1} - Q_i\,\overline{Q_{i+1}} + z(\overline{Q_{i+1}} - \overline{Q_i})}{Q_{i+1} - Q_i} = \frac{\overline{Q_{i+3}}\,Q_{i+4} - Q_{i+3}\,\overline{Q_{i+4}} + z(\overline{Q_{i+4}} - \overline{Q_{i+3}})}{Q_{i+4} - Q_{i+3}}.$$

By solving the latter equation for z, we find the intersection point S_i of h_{i+1} and h_{i+4}:

$$S_i = \frac{(Q_{i+1} - Q_i)(\overline{Q_{i+3}}\,Q_{i+4} - Q_{i+3}\,\overline{Q_{i+4}}) - (Q_{i+4} - Q_{i+3})(\overline{Q_i}\,Q_{i+1} - Q_i\,\overline{Q_{i+1}})}{(\overline{Q_{i+1}} - \overline{Q_i})(Q_{i+4} - Q_{i+3}) - (\overline{Q_{i+4}} - \overline{Q_{i+3}})(Q_{i+1} - Q_i)}.$$

To further reduce the expression of S_i, we insert the expression of the points Q_i, Q_{i+1}, Q_{i+3}, and Q_{i+4} defined in (4.9). Although this calculation is straightforward, it gets very long. Therefore, we use *Wolfram Mathematica*, which is a symbolic mathematical computation program (q.v. appendix B.1):

```
In[10]:= Si = Simplify[ ((Qi+1 - Qi) * (Conjugate[Qi+3] * Qi+4 - Qi+3 * Conjugate[Qi+4]) - (Qi+4 - Qi+3) * (Conjugate[Qi] * Qi+1 - Qi * Conjugate[Qi+1])) / ((Conjugate[Qi+1] - Conjugate[Qi]) (Qi+4 - Qi+3) - (Conjugate[Qi+4] - Conjugate[Qi+3]) (Qi+1 - Qi)) ]
```

$$\text{Out[10]= } T_i \left(1 + \frac{T_{2+i}}{T_{1+i}} + \frac{T_{3+i}}{T_{4+i}}\right)$$

So, $S_i = T_i\left(\frac{T_{i+2}}{T_{i+1}} + \frac{T_{i+3}}{T_{i+4}} + 1\right)$. Next, we need to verify that S_i also satisfies the equation of l_{i+1}, namely that it holds

$$(T_i - S_i)(\overline{P_{i+2}} - \overline{S_i}) = (\overline{T_i} - \overline{S_i})(P_{i+2} - S_i). \tag{4.12}$$

By inserting the expressions of P_i and S_i as defined in (4.8) and (4.10), respectively, and using that $\overline{T_i} = \frac{1}{T_i}$ for $T_i \in k$, the left hand side of equation (4.12) gets

$$\left(T_i - T_i\left(\frac{T_{i+2}}{T_{i+1}} + \frac{T_{i+3}}{T_{i+4}} + 1\right)\right)\left(-\overline{T_i}\,T_{i+1}\,\overline{T_{i+2}}\,\overline{T_{i+3}}\,T_{i+4} - \overline{T_i}\left(\frac{T_{i+1}}{T_{i+2}} + \frac{T_{i+4}}{T_{i+3}} + 1\right)\right)$$

Factoring out $T_i\,\overline{T_i}$ then yields

$$\begin{aligned}
&\left(\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}\right)\left(\frac{T_{i+1}\,T_{i+4}}{T_{i+2}\,T_{i+3}}+\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}+1\right)\\
&=\left(\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}\right)\left(\frac{T_{i+1}\,T_{i+4}}{T_{i+2}\,T_{i+3}}+1\right)+\left(\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}\right)\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}\right)\\
&=\frac{T_{i+2}T_{i+4}+T_{i+1}T_{i+3}}{T_{i+2}\,T_{i+3}}\cdot\frac{T_{i+1}T_{i+4}+T_{i+2}T_{i+3}}{T_{i+1}\,T_{i+4}}+\left(\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}\right)\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}\right)\\
&=\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}\right)\left(\frac{T_{i+2}\,T_{i+3}}{T_{i+1}\,T_{i+4}}+1\right)+\left(\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}\right)\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}\right)\\
&=\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}\right)\left(\frac{T_{i+2}\,T_{i+3}}{T_{i+1}\,T_{i+4}}+\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}+1\right),
\end{aligned}$$

which is the same as the right hand side of equation (4.12), since

$$\begin{aligned}
&\left(\overline{T_i}-\overline{T_i}\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}+1\right)\right)\left(-T_i\,\overline{T_{i+1}}\,T_{i+2}\,T_{i+3}\,\overline{T_{i+4}}-T_i\left(\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}+1\right)\right)\\
&=\left(\frac{T_{i+1}}{T_{i+2}}+\frac{T_{i+4}}{T_{i+3}}\right)\left(\frac{T_{i+2}\,T_{i+3}}{T_{i+1}\,T_{i+4}}+\frac{T_{i+2}}{T_{i+1}}+\frac{T_{i+3}}{T_{i+4}}+1\right).
\end{aligned}$$

Hence, S_i lies on h_{i+1}, h_{i+4}, and l_{i+1}. ■

Finally, we need to show that the point S_i lies on k_i.

Claim 5. The three lines l_{i+1}, h_{i+1}, and h_{i+4} meet in S_i on k_i for each $i \in \{1,\dots,5\}$.

Proof of claim 5: The points P_{i-1}, P_i, and Q_i lie on the circle k_i for each $i \in \{1,\dots,5\}$. One way to show that S_i lies as well on k_i is therefore to verify that the points P_{i-1}, P_i, Q_i, and S_i are on one common block. This is the case if and only if

$$\det\begin{pmatrix} S_i\,\overline{S_i} & S_i & \overline{S_i} & 1\\ Q_i\,\overline{Q_i} & Q_i & \overline{Q_i} & 1\\ P_{i-1}\,\overline{P_{i-1}} & P_{i-1} & \overline{P_{i-1}} & 1\\ P_i\,\overline{P_i} & P_i & \overline{P_i} & 1 \end{pmatrix}=0.$$

As P_{i-1} and P_i lie on k, it follows that $P_{i-1}\,\overline{P_{i-1}} = P_i\,\overline{P_i} = 1$. Nevertheless, inserting the expressions of S_i, Q_i, P_i, and P_{i-1} as defined in (4.10), (4.9), and (4.8), respectively, the expression of this determinant gets very long. Therefore, we use again *Mathematica* for this computation (q.v. appendix B.1):

```
In[14]:= Simplify[Det[{{Si * Conjugate[Si], Si, Conjugate[Si], 1}, {Qi * Conjugate[Qi], Qi, Conjugate[Qi], 1}, {1, Pi-1, 1/Pi-1, 1},
          {1, Pi, 1/Pi, 1}}]]
Out[14]= 0
```

Hence, the point S_i indeed lies on k_i. ■

Altogether, we found that in family (i) (figure 4.4) the three blocks $\overrightarrow{T_i\,P_{i+2}\,\infty}$, $\overrightarrow{Q_i\,Q_{i+1}\,\infty}$, and $\overrightarrow{Q_{i+3}\,Q_{i+4}\,\infty}$ meet in a point S_i on k_i for each $i \in \{1,\dots,5\}$.

- *Family (ii):* Consider the five circles $k_1,\dots,k_5$, where $T_i \in k$ is the center of k_i and $k_i \cap k_{i+1} = \{P_i, Q_i\}$ for each $i \in \{1,\dots,5\}$ with

$$P_i = T_i\,T_{i+1}\,\overline{T_{i+2}}\,T_{i+3}\,\overline{T_{i+4}} \quad \text{and} \quad Q_i = T_i + T_{i+1} - \overline{P_i}\,T_i\,T_{i+1}. \tag{4.13}$$

Inserting the expression of P_i in the expression of Q_i yields that

$$\begin{aligned} Q_i &= T_i + T_{i+1} - \overline{T_i\,T_{i+1}\,\overline{T_{i+2}}\,T_{i+3}\,\overline{T_{i+4}}}\,T_i\,T_{i+1} \\ &= T_i + T_{i+1} - T_{i+2}\,\overline{T_{i+3}}\,T_{i+4}. \end{aligned}$$

In this case, we need to show that the blocks $l_{i+1} = \overrightarrow{T_i\,P_{i+2}\,\infty}$ and $h_{i+1} = \overrightarrow{Q_i\,Q_{i+1}\,\infty}$ meet in U_i on k_i and the blocks l_{i+1} and h_{i+4} meet in $R_i \neq U_i$ on k_i for each $i \in \{1,\dots,5\}$.

Claim 6. For each $i \in \{1,\dots,5\}$ the lines h_{i+1} and l_{i+1} meet in

$$U_i = T_i\left(\frac{T_{i+2}}{T_{i+1}} - \frac{T_{i+3}}{T_{i+4}} + 1\right) \tag{4.14}$$

and the lines h_{i+4} and l_{i+1} meet in

$$R_i = T_i\left(\frac{T_{i+3}}{T_{i+4}} - \frac{T_{i+2}}{T_{i+1}} + 1\right). \tag{4.15}$$

Proof of claim 6: First, we determine the intersection point of h_{i+1} and l_{i+1} other than ∞. For this, we consider the following system of equations:

$$\begin{cases} (Q_i - z)(\overline{Q_{i+1}} - \overline{z}) = (\overline{Q_i} - \overline{z})(Q_{i+1} - z), \\ (T_i - z)(\overline{P_{i+2}} - \overline{z}) = (\overline{T_i} - \overline{z})(P_{i+2} - z). \end{cases} \tag{4.16}$$

Symmetrical to the solution S_i of system (4.11), the solution of system (4.16) is

$$U_i = \frac{(Q_{i+1} - Q_i)(\overline{T_i}\, P_{i+2} - T_i\, \overline{P_{i+2}}) - (P_{i+2} - T_i)(\overline{Q_i}\, Q_{i+1} - Q_i\, \overline{Q_{i+1}})}{(\overline{Q_{i+1}} - \overline{Q_i})(P_{i+2} - T_i) - (\overline{P_{i+2}} - \overline{T_i})(Q_{i+1} - Q_i)}.$$

We insert the expressions of the points Q_i, Q_{i+1}, and P_{i+2} as defined in (4.13) for which we use again *Mathematica* (q.v. appendix B.1):

```
In[13]:= Ui = Simplify[((Qi+1 - Qi) * (1/Ti * Pi+2 - Ti * 1/Pi+2) - (Pi+2 - Ti) * (Conjugate[Qi] * Qi+1 - Qi * Conjugate[Qi+1])) /
          ((Conjugate[Qi+1] - Conjugate[Qi]) (Pi+2 - Ti) - (1/Pi+2 - 1/Ti) (Qi+1 - Qi))]
Out[13]= Ti (1 + T2+i/T1+i - T3+i/T4+i)
```

So, $U_i = T_i \left(\frac{T_{i+2}}{T_{i+1}} - \frac{T_{i+3}}{T_{i+4}} + 1\right)$. Second, we determine the intersection point of h_{i+4} and l_{i+1} other than ∞. Thus, we consider the following system of equations:

$$\begin{cases} (Q_{i+3} - z)(\overline{Q_{i+4}} - \overline{z}) = (\overline{Q_{i+3}} - \overline{z})(Q_{i+4} - z), \\ (T_i - z)(\overline{P_{i+2}} - \overline{z}) = (\overline{T_i} - \overline{z})(P_{i+2} - z). \end{cases} \tag{4.17}$$

By symmetry it follows that the solution of system (4.17) is

$$R_i = \frac{(Q_{i+4} - Q_{i+3})(\overline{T_i}\, P_{i+2} - T_i\, \overline{P_{i+2}}) - (P_{i+2} - T_i)(\overline{Q_{i+3}}\, Q_{i+4} - Q_{i+3}\, \overline{Q_{i+4}})}{(\overline{Q_{i+4}} - \overline{Q_{i+3}})(P_{i+2} - T_i) - (\overline{P_{i+2}} - \overline{T_i})(Q_{i+4} - Q_{i+3})}.$$

Inserting the expressions of Q_{i+3}, Q_{i+4}, and P_{i+2} as defined in (4.13), we obtain the following with *Mathematica* (q.v. appendix B.1):

```
In[15]:= Ri =
          Simplify[((Qi+4 - Qi+3) * (1/Ti * Pi+2 - Ti * 1/Pi+2) - (Pi+2 - Ti) * (Conjugate[Qi+3] * Qi+4 - Qi+3 * Conjugate[Qi+4])) /
          ((Conjugate[Qi+4] - Conjugate[Qi+3]) (Pi+2 - Ti) - (1/Pi+2 - 1/Ti) (Qi+4 - Qi+3))]
Out[15]= Ti (1 - T2+i/T1+i + T3+i/T4+i)
```

So, $R_i = T_i \left(\frac{T_{i+3}}{T_{i+4}} - \frac{T_{i+2}}{T_{i+1}} + 1\right)$. ■

Claim 7. The points U_i and R_i are different and lie both on k_i for each $i \in \{1, \ldots, 5\}$.

Proof of claim 7: Suppose by contradiction that $U_i = R_i$. Then

$$\begin{aligned}
& T_i\left(\frac{T_{i+2}}{T_{i+1}} - \frac{T_{i+3}}{T_{i+4}} + 1\right) = T_i\left(\frac{T_{i+3}}{T_{i+4}} - \frac{T_{i+2}}{T_{i+1}} + 1\right) \\
\overset{T_i \neq 0}{\Longleftrightarrow} \quad & \frac{T_{i+2}}{T_{i+1}} - \frac{T_{i+3}}{T_{i+4}} = \frac{T_{i+3}}{T_{i+4}} - \frac{T_{i+2}}{T_{i+1}} \\
\Longleftrightarrow \quad & T_{i+2}\,T_{i+4} = T_{i+3}\,T_{i+1} \\
\Longleftrightarrow \quad & \overline{T_{i+1}}\,T_{i+2}\,\overline{T_{i+3}}\,T_{i+4} = 1 \\
\Longleftrightarrow \quad & T_i\,\overline{T_{i+1}}\,T_{i+2}\,\overline{T_{i+3}}\,T_{i+4} = T_i.
\end{aligned}$$

Consequently,

$$P_{i+4} = T_i\,\overline{T_{i+1}}\,T_{i+2}\,\overline{T_{i+3}}\,T_{i+4} = T_i.$$

On the one hand, it holds that $P_{i+4}, P_i \in k_i$, where $T_i = P_{i+4}$ is the center of k_i. But on the other hand, since $P_i \neq P_{i+4} = T_i$, it follows that $P_{i+4} \notin k_i$, which results in a contradiction. Therefore, $U_i \neq R_i$ for all $i \in \{1, \ldots, 5\}$.

In order to show that U_i and R_i both lie on k_i, we verify first that the points U_i, R_i, P_i, and P_{i-1} are on one block, which is the case if and only if

$$\det\begin{pmatrix} U_i\,\overline{U_i} & U_i & \overline{U_i} & 1 \\ R_i\,\overline{R_i} & R_i & \overline{R_i} & 1 \\ 1 & P_{i-1} & \overline{P_{i-1}} & 1 \\ 1 & P_i & \overline{P_i} & 1 \end{pmatrix} = 0.$$

We insert the expressions of U_i, R_i, P_{i-1}, and P_i as defined in (4.14), (4.15), and (4.13), respectively, and obtain the desired result with *Mathematica* (q.v. appendix B.1):

```
In[17]:= Simplify[Det[{{Ui * Conjugate[Ui], Ui, Conjugate[Ui], 1}, {Ri * Conjugate[Ri], Ri, Conjugate[Ri], 1}, {1, Pi-1, 1/Pi-1, 1}, {1, Pi, 1/Pi, 1}}]]
Out[17]= 0
```

Now, it is sufficient to verify that P_{i-1}, P_i, Q_i, and U_i lie on one common block, which is the case if and only if

$$\det \begin{pmatrix} U_i\,\overline{U_i} & U_i & \overline{U_i} & 1 \\ Q_i\,\overline{Q_i} & Q_i & \overline{Q_i} & 1 \\ 1 & P_{i-1} & \overline{P_{i-1}} & 1 \\ 1 & P_i & \overline{P_i} & 1 \end{pmatrix} = 0.$$

Indeed, with the expressions of P_{i-1}, P_i, Q_i, and U_i as defined in (4.13) and (4.14), respectively, *Mathematica* (q.v. appendix B.1) gives us the desired result:

```
In[18]:= Simplify[Det[{{Ui * Conjugate[Ui], Ui, Conjugate[Ui], 1}, {Qi * Conjugate[Qi], Qi, Conjugate[Qi], 1}, {1, Pi-1, 1/Pi-1, 1}, {1, Pi, 1/Pi, 1}}]]
Out[18]= 0
```

Hence, the distinct points U_i and R_i lie on k_i for each $i \in \{1, \dots, 5\}$. ■

By claim 6 and 7 it follows in particular that in contrast to family (i) it holds in family (ii) that the lines h_{i+1}, h_{i+4}, and l_{i+1} only meet in ∞.

Altogether, we found that in family (ii) (figure 4.4) the blocks $\overrightarrow{T_i\,P_{i+2}\,\infty}$ and $\overrightarrow{Q_i\,Q_{i+1}\,\infty}$ meet in U_i on k_i and the blocks $\overrightarrow{T_i\,P_{i+2}\,\infty}$ and $\overrightarrow{Q_{i+3}\,Q_{i+4}\,\infty}$ meet in $R_i \neq U_i$ on k_i for each $i \in \{1, \dots, 5\}$.

□

4.2 Miquel's Pentagon Theorem

The five circles theorem starts with a circle k and a family of circles $k_1, \dots, k_5$ that have their center on k and intersect "chainwise" at two points with one of them on k. Joining the second intersection points then results in a "star polygon" with its five vertices one upon each of the circles $k_1, \dots, k_5$. Miquel's pentagon theorem now goes the other way round, meaning that we start with a "star polygon" and end up with a family of circles $k_1, \dots, k_5$ that intersect on a common sixth circle k. In Euclidean geometry, the theorem thus starts with a convex *pentagon* and considers the intersections of its extended sides, which explains the name of the theorem. For finite Miquelian Möbius planes, we adapt Miquel's pentagon theorem in the following way.

Theorem 4.2.1. Let $h_1, \dots, h_5$ be five different blocks that are all incident with a point I and such that any three of them only meet in I. Let Q_i be the second intersection point of h_i and h_{i+1}, and let S_i be the second intersection point of h_{i+1} and

h_{i+4} for each $i \in \{1, \dots, 5\}$. Then the blocks $\overrightarrow{Q_i\, Q_{i+4}\, S_i}$ and $\overrightarrow{Q_i\, Q_{i+1}\, S_{i+1}}$ intersect at a second point P_i for each $i \in \{1, \dots, 5\}$ and the so determined points $P_1, \dots, P_5$ all lie on one common block.

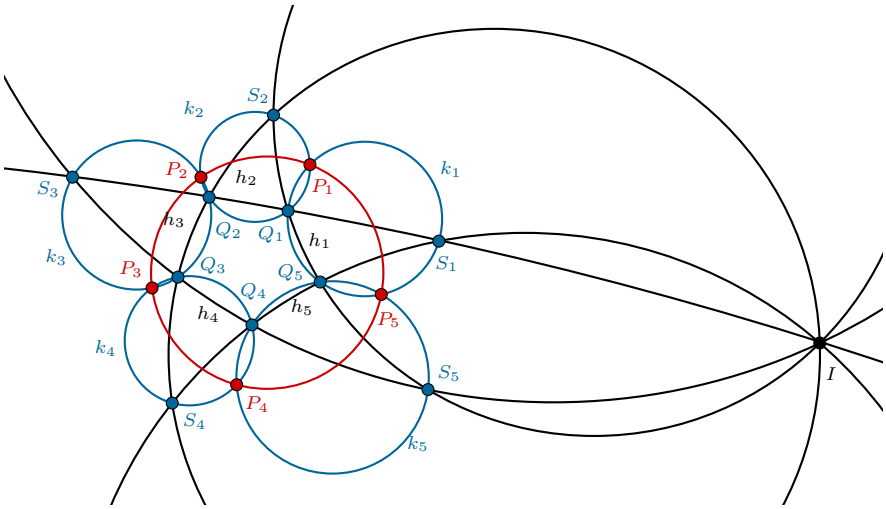


FIGURE 4.7: Miquel's pentagon theorem.

Proof. The Möbius transformation μ_I as defined in (3.19) maps the point I to the point ∞. Therefore, we may assume without loss of generality that I is the point ∞. Thus, let $h_1, \dots, h_5$ be five lines, and let $Q_i \neq \infty$ be the intersection point of h_i and h_{i+1} for each $i \in \{1, \dots, 5\}$. Then $Q_i, Q_{i+4} \in h_i$. By lemma 3.3.8 (a) we can now write the lines $h_1, \dots, h_5$ as

$$h_i = \{z \in \mathrm{GF}(p^{2n}) \mid (Q_{i+4} - z)(\overline{Q_i} - \overline{z}) = (\overline{Q_{i+4}} - \overline{z})(Q_i - z)\} \cup \{\infty\}. \tag{4.18}$$

Let $S_i \neq \infty$ be the intersection point of h_{i+1} and h_{i+4} for each $i \in \{1, \dots, 5\}$. First, we express S_i in terms of $Q_1, \dots, Q_5$. To do so, we solve the following system given by the equations of h_{i+1} and h_{i+4} in (4.18):

$$\begin{cases} (Q_i - z)(\overline{Q_{i+1}} - \overline{z}) = (\overline{Q_i} - \overline{z})(Q_{i+1} - z) \\ (Q_{i+3} - z)(\overline{Q_{i+4}} - \overline{z}) = (\overline{Q_{i+3}} - \overline{z})(Q_{i+4} - z) \end{cases}$$

As for system (4.11), the solution of this system of equations is

$$S_i = \frac{(Q_{i+1} - Q_i)(\overline{Q_{i+3}}\, Q_{i+4} - Q_{i+3}\, \overline{Q_{i+4}}) - (Q_{i+4} - Q_{i+3})(\overline{Q_i}\, Q_{i+1} - Q_i\, \overline{Q_{i+1}})}{(\overline{Q_{i+1}} - \overline{Q_i})(Q_{i+4} - Q_{i+3}) - (\overline{Q_{i+4}} - \overline{Q_{i+3}})(Q_{i+1} - Q_i)}. \tag{4.19}$$

Second, we determine the circles $\overrightarrow{Q_i\, Q_{i+4}\, S_i}$ for each $i \in \{1, \dots, 5\}$ and express their intersection points in terms of $Q_1, \dots, Q_5$. For this, observe that the points

$Q_1, \dots, Q_5, S_1, \dots, S_5$ are different, since any three of the lines $h_1, \dots, h_5$ only meet in ∞. Therefore, since also $S_i \neq \infty \neq Q_i$, there exists a unique circle k_i passing through the points S_i, Q_i, and Q_{i+4} for each $i \in \{1, \dots, 5\}$. By lemma 3.3.8 (b) the equation of k_i is

$$(S_i - Q_{i+4})(Q_i - z)(\overline{S_i} - \overline{z})(\overline{Q_i} - \overline{Q_{i+4}}) = (\overline{S_i} - \overline{Q_{i+4}})(\overline{Q_i} - \overline{z})(S_i - z)(Q_i - Q_{i+4}).$$

Then the circles k_i and k_{i+1} intersect by construction at Q_i. For their second intersection point we consider the system given by the equations of k_i and k_{i+1}, namely

$$\begin{cases} \frac{(Q_i - z)(\overline{S_i} - \overline{z})}{(\overline{S_i} - \overline{Q_{i+4}})(Q_i - Q_{i+4})} = \frac{(\overline{Q_i} - \overline{z})(S_i - z)}{(S_i - Q_{i+4})(\overline{Q_i} - \overline{Q_{i+4}})} \\ \frac{(Q_{i+1} - z)(\overline{S_{i+1}} - \overline{z})}{(\overline{S_{i+1}} - \overline{Q_i})(Q_{i+1} - Q_i)} = \frac{(\overline{Q_{i+1}} - \overline{z})(S_{i+1} - z)}{(S_{i+1} - Q_i)(\overline{Q_{i+1}} - \overline{Q_i})} \end{cases} \tag{4.20}$$

We solve both equation in system (4.20) for $\overline{z}$. For the first equation we find

$$\overline{z} = \frac{\overline{Q_i}(S_i - z)(\overline{S_i} - \overline{Q_{i+4}})(Q_i - Q_{i+4}) - \overline{S_i}(Q_i - z)(S_i - Q_{i+4})(\overline{Q_i} - \overline{Q_{i+4}})}{(S_i - z)(\overline{S_i} - \overline{Q_{i+4}})(Q_i - Q_{i+4}) - (Q_i - z)(S_i - Q_{i+4})(\overline{Q_i} - \overline{Q_{i+4}})}$$

and for the second equation

$$\overline{z} = \frac{\overline{Q_{i+1}}(S_{i+1} - z)(\overline{S_{i+1}} - \overline{Q_i})(Q_{i+1} - Q_i) - \overline{S_{i+1}}(Q_{i+1} - z)(S_{i+1} - Q_i)(\overline{Q_{i+1}} - \overline{Q_i})}{(S_{i+1} - z)(\overline{S_{i+1}} - \overline{Q_i})(Q_{i+1} - Q_i) - (Q_{i+1} - z)(S_{i+1} - Q_i)(\overline{Q_{i+1}} - \overline{Q_i})}.$$

Now, we use again *Mathematica*, as the calculations are very large (q.v. appendix B.2). First, we replace S_i in the latter two equations with the expression found in (4.19). Then, by equalizing the right hand side of these two equations and solving for z, we obtain two solutions. One of the solutions is of course Q_i. The other solution is the second intersection point P_i of k_i and k_{i+1}:

$$\begin{aligned} P_i = \Big[& (Q_{i+4} - Q_{i+3})\Big(Q_{i+1}\,\overline{Q_{i+2}}(Q_{i+4} - Q_i) - \overline{Q_{i+1}}(Q_{i+1}\,Q_{i+4} - Q_i\,Q_{i+2})\Big) \\ & + (Q_{i+1} - Q_{i+2})\Big(\overline{Q_{i+3}}\,Q_{i+4}(Q_i - Q_{i+1}) + \overline{Q_{i+4}}(Q_{i+1}\,Q_{i+4} - Q_i\,Q_{i+3})\Big)\Big] \\ & \Big/ \Big[(Q_{i+1} - Q_{i+2})\Big(\overline{Q_{i+3}}(Q_i - Q_{i+1}) + \overline{Q_{i+4}}(Q_{i+4} - Q_i + Q_{i+1} - Q_{i+3}\Big) \\ & + (Q_{i+4} - Q_{i+3})\Big(\overline{Q_{i+2}}(Q_{i+4} - Q_i) + \overline{Q_{i+1}}(Q_{i+4} - Q_i + Q_{i+1} - Q_{i+2})\Big)\Big] \end{aligned} \tag{4.21}$$

Finally, we verify that the points $P_1, \dots, P_5$ lie on a common block. For this, we use the cross-ratio (q.v. definition 3.3.11). The cross-ratio of the points P_1, P_2, P_3, and P_4 is

$$[P_1, P_2; P_3, P_4] = \frac{(P_1 - P_3)(P_2 - P_4)}{(P_1 - P_4)(P_3 - P_3)}.$$

Inserting the expression of P_i found in (4.21), we obtain with *Mathematica* (q.v. appendix B.2) that $[P_1, P_2; P_3, P_4]$ may be written the following way:

```
In[54]:= cr1 = Simplify[ ((P1 - P3) (P2 - P4)) / ((P1 - P4) (P2 - P3)) ]
```

$$\text{Out[54]=}\quad \frac{\left(\overline{Q_5}\,(Q_2 - Q_4) + \overline{Q_2}\,(Q_4 - Q_5) + \overline{Q_4}\,(-Q_2 + Q_5)\right)\left(\overline{Q_5}\,(-Q_1 + Q_3) + \overline{Q_3}\,(Q_1 - Q_5) + \overline{Q_1}\,(-Q_3 + Q_5)\right)}{\left(\overline{Q_5}\,(Q_1 - Q_4) + \overline{Q_1}\,(Q_4 - Q_5) + \overline{Q_4}\,(-Q_1 + Q_5)\right)\left(\overline{Q_5}\,(-Q_2 + Q_3) + \overline{Q_3}\,(Q_2 - Q_5) + \overline{Q_2}\,(-Q_3 + Q_5)\right)}$$

In particular, the numerator and the denominator of the cross-ratio are both expressed as a product. By rearranging the terms of the first factor in the numerator, we obtain the following:

$$\begin{aligned}
&\overline{Q_5}(Q_2 - Q_4) + \overline{Q_2}(Q_4 - Q_5) + \overline{Q_4}(Q_5 - Q_2) \\
&\qquad = Q_2\,\overline{Q_5} - Q_4\,\overline{Q_5} + \overline{Q_2}\,Q_4 - \overline{Q_2}\,Q_5 + \overline{Q_4}\,Q_5 - Q_2\,\overline{Q_4} \\
&\qquad = \overline{Q_2}\,Q_4 - \overline{\overline{Q_2}\,Q_4} + Q_2\,\overline{Q_5} - \overline{Q_2}\,\overline{Q_5} + \overline{Q_4}\,Q_5 - \overline{\overline{Q_4}\,Q_5} \\
&\qquad = \underbrace{\left(\overline{Q_2}\,Q_4 + Q_2\,\overline{Q_5} + \overline{Q_4}\,Q_5\right)}_{=:u_1} - \overline{\left(\overline{Q_2}\,Q_4 + Q_2\,\overline{Q_5} + \overline{Q_4}\,Q_5\right)} \\
&\qquad = u_1 - \overline{u_1}.
\end{aligned}$$

Thus, by symmetry, the cross-ratio of the points P_1, P_2, P_3, and P_4 is of the form

$$\frac{(u_1 - \overline{u_1})(u_2 - \overline{u_2})}{(u_3 - \overline{u_3})(u_4 - \overline{u_4})}.$$

Now observe that

$$\begin{aligned}
(u_j - \overline{u_j})(u_k - \overline{u_k}) &= (u_j u_k + \overline{u_j u_k}) - (\overline{u_j} u_k + \overline{\overline{u_j} u_k}) \\
&= \mathrm{Tr}(u_j u_k) + \mathrm{Tr}(\overline{u_j} u_k).
\end{aligned}$$

Consequently, it follows from corollary 2.1.20 that

$$(u_j - \overline{u_j})(u_k - \overline{u_k}) \in \mathrm{GF}(p^n),$$

and therefore,

$$[P_1, P_2; P_3, P_4] \in \mathrm{GF}(p^n).$$

Hence, it follows from corollary 3.3.10 that P_1, P_2, P_3, and P_4 lie on a common block. By symmetry, it holds that P_2, P_3, P_4, and P_5 lie on one block as well, and consequently, the points $P_1, \ldots, P_5$ are all on a common block. □

Remark 4.2.2. Notice that in contrast to the five circles theorem the centers of the five circles $k_1, \ldots, k_5$ are not necessarily on a block. This is also the main reason why

we stated the five circles theorems using the notions of lines and circles instead of blocks, as we cannot talk about centers of lines.

Remark 4.2.3. There is an algebraic proof of Miquel's pentagon theorem in Euclidean geometry as well (cf. [LXZ05]). However, without the use of the cross-ratio, the proof is more difficult and very different from our proof in $\mathcal{M}_{p^n}$.

Chapter 5

A Connection to Clifford's Circle Theorems

In this chapter, we move away from our concrete construction of finite Miquelian Möbius planes. We only stick with the axioms (A1)–(A3) of a Möbius plane and add Miquel's theorem (q.v. theorem 3.2.1) as axiom (A4) to our set of axioms and go from there. As introduced in section 3.2, an incidence structure $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ that satisfies the axioms (A1)–(A4) is called Miquelian Möbius plane. Of course, what follows from the axioms (A1)–(A4) is necessarily true in finite Miquelian Möbius planes since they are a model for this axiomatic system. However, for example the classical Möbius plane is also a model for this system as we mentioned in section 3.2. Thus, by using only the axioms (A1)–(A4), we obtain more general results.

More precisely, we consider now an incidence structure $(\mathbb{P}, \mathbb{B}, \mathbb{I})$ that satisfies the following set of axioms:

(A1) For any three different points $P, Q, R \in \mathbb{P}$, there exists a unique block $g \in \mathbb{B}$ such that $P \,\mathrm{I}\, g$, $Q \,\mathrm{I}\, g$, and $R \,\mathrm{I}\, g$.

(A2) For any block $g \in \mathbb{B}$ and any two points $P, Q \in \mathbb{P}$ with $P \,\mathrm{I}\, g$ and $\neg(Q \,\mathrm{I}\, g)$, there exists a unique block $h \in \mathbb{B}$ such that

$$P \,\mathrm{I}\, h,\ Q \,\mathrm{I}\, h,\ \text{and } \forall R \in \mathbb{P},\ R \neq P : R \,\mathrm{I}\, g \implies \neg(R \,\mathrm{I}\, h).$$

(A3) There are four different points $P, Q, R, S \in \mathbb{P}$ that are not all incident with one block. Moreover, every block is incident with at least one point.

(A4) Let $P_1, \ldots, P_8 \in \mathbb{P}$ be eight different points. If it holds that

$$P_1 \in \overrightarrow{P_2\,P_3\,P_4}, \quad P_3 \in \overrightarrow{P_4\,P_5\,P_6},$$
$$P_5 \in \overrightarrow{P_6\,P_7\,P_8}, \quad P_7 \in \overrightarrow{P_8\,P_1\,P_2}, \quad \text{and} \quad P_1 \in \overrightarrow{P_3\,P_5\,P_7},$$

then the points P_2, P_4, P_6, and P_8 lie on a common block as well.

In section 5.1, we consider Clifford's first and second circle theorems and show that they follow from the axioms (A1)-(A4). Then, in section 5.2, we look at the connection between the latter two theorems, Steiner's quadrilateral theorem, and Miquel's pentagon theorem. Lastly, in section 5.3, we end with a summary diagram including all the circle theorems we considered.

5.1 Clifford's First and Second Circle Theorems

Let us now consider Clifford's first and second circle theorems adapted from [Cox61] and show their validity in Miquelian Möbius planes.

Theorem 5.1.1 (Clifford's First Circle Theorem)**.** Let k_1, k_2, k_3, and k_4 be four distinct blocks through a point I and otherwise in general position. Let P_{ij} be the second intersection point of k_i and k_j for each $i, j \in \{1, \dots, 4\}$ with $i < j$, and let k_{ijl} denote the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \dots, 4\}$. Then the four blocks $k_{123}, k_{124}, k_{134}$, and k_{234} meet in a point P_{1234}.

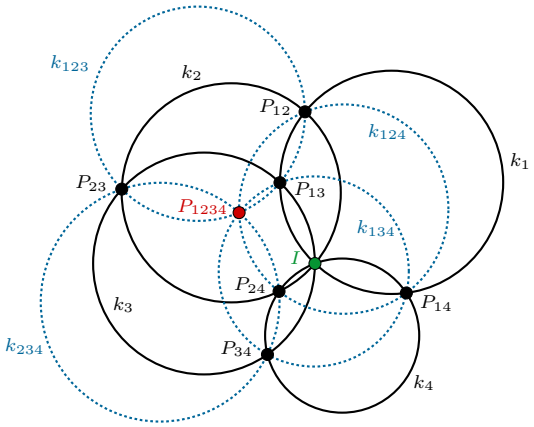


FIGURE 5.1: Clifford's first circle theorem.

Proof. First, we consider the five blocks $k_1, k_{123}, k_{134}, k_2$, and k_4. Let Q be the second intersection point of k_{123} and k_{134}. Then it holds that

$$P_{13}, Q, P_{12}, P_{23} \in k_{123}, \quad P_{12}, P_{23}, I, P_{24} \in k_2,$$
$$I, P_{24}, P_{14}, P_{34} \in k_4, \quad P_{14}, P_{34}, P_{13}, Q \in k_{134}, \quad \text{and} \quad P_{13}, P_{12}, I, P_{14} \in k_1.$$

Now axiom (A4) implies that the points Q, P_{23}, P_{24}, and P_{34} lie on a common block. Since $P_{23}, P_{24}, P_{34} \in k_{234}$, it follows from axiom (A1) that $Q \in k_{234}$.

Second, consider the five blocks $k_1, k_{123}, k_{234}, k_3$, and k_4. It holds that

$$P_{23}, Q, P_{13}, P_{12} \in k_{123}, \quad P_{13}, P_{12}, I, P_{14} \in k_1,$$
$$I, P_{14}, P_{34}, P_{24} \in k_4, \quad P_{34}, P_{24}, P_{23}, Q \in k_{234}, \quad \text{and} \quad P_{23}, P_{13}, I, P_{34} \in k_3.$$

Thus, axiom (A4) implies that the points Q, P_{12}, P_{14}, and P_{24} lie on a common block. Since $P_{12}, P_{14}, P_{24} \in k_{124}$, it follows from axiom (A1) that $Q \in k_{124}$.
Consequently, the blocks $k_{123}, k_{124}, k_{134}$, and k_{234} all pass through $Q =: P_{1234}$. □

Clifford's first circle theorem is commonly stated with four blocks $k_1, \dots, k_4$ passing through a common point I that are otherwise *in general position*, meaning that there are $\binom{4}{2} = 6$ additional points where exactly two of the four blocks intersect. However, the theorem still holds true if some of the blocks among $k_1, \dots, k_4$ are tangent at I. Let us consider the case in which the blocks $k_1, \dots, k_4$ determine precisely five additional points where exactly two of the four blocks intersect.

Lemma 5.1.2. Let k_1, k_2, k_3, and k_4 be four distinct blocks through a common point P_{12}, in which k_1 and k_2 are tangent, and otherwise in general position. Let P_{ij} be the second intersection point of each non-tangent blocks k_i and k_j for $i, j \in \{1, \dots, 4\}$ with $i < j$, and let k_{ijl} denote the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \dots, 4\}$. Then the four blocks $k_{123}, k_{124}, k_{134}$, and k_{234} meet in P_{34}.

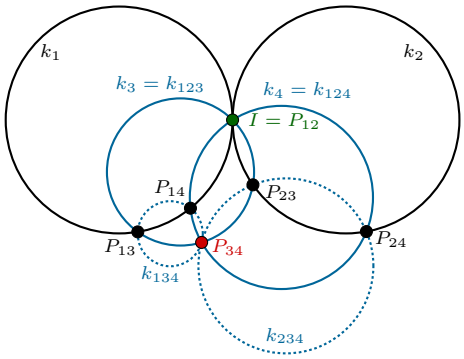


FIGURE 5.2: Clifford's first circle theorem with $k_1 \cap k_2 = \{I\}$.

Proof. First, we consider the blocks k_{123} and k_{124}. Since

$$P_{13}, P_{23} \in k_3 \quad \text{and} \quad \{P_{12}\} = k_1 \cap k_2 \cap k_3 \cap k_4 \subseteq k_3,$$

it follows from axiom (A1) that $k_{123} = k_3$. Similarly, as

$$P_{14}, P_{24} \in k_4 \quad \text{and} \quad \{P_{12}\} = k_1 \cap k_2 \cap k_3 \cap k_4 \subseteq k_4,$$

axiom (A1) implies that $k_{124} = k_4$. But $k_3 \cap k_4 = \{P_{34}\}$, and consequently, it holds that $P_{34} \in k_{123}$ and $P_{34} \in k_{124}$. Moreover, it holds by construction that $P_{34} \in k_{134}$ and $P_{34} \in k_{234}$. Hence, the blocks $k_{123}, k_{124}, k_{134}$, and k_{234} meet in P_{34}. □

Remark 5.1.3. (i) If the blocks $k_1, \ldots, k_4$ in Clifford's first circle theorem define only four additional points where exactly two of the four blocks intersect, then the theorem is still true, as the blocks through the intersection points are precisely the blocks $k_1, \ldots, k_4$, which meet in I.

Proof. Assume that $k_1 \cap k_2 = \{P_{12}\}$ and $k_3 \cap k_4 = \{P_{34}\}$, where $P_{12} = P_{34} = I$. Since $P_{13}, P_{23} \in k_3$ and $P_{12} = I \in k_3$, it follows from axiom (A1) that $k_{123} = k_3$. Analogously, it follows that $k_{124} = k_4, k_{134} = k_1$, and $k_{234} = k_2$. Hence, $k_{123} \cap k_{124} \cap k_{134} \cap k_{234} = \{I\}$. □

(ii) If the blocks $k_1, \ldots, k_4$ in Clifford's first circle theorem define less than four additional points where exactly two of the four blocks intersect, then some blocks through the intersection points of $k_1, \ldots, k_4$ are not uniquely determined. However, they still intersect at I.

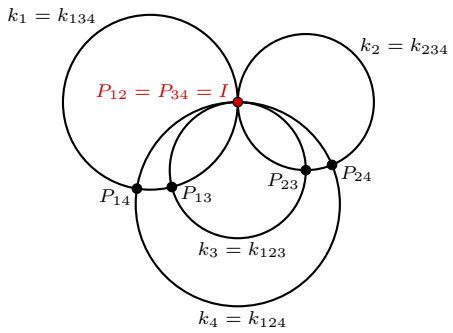


FIGURE 5.3: Clifford's first circle theorem with $k_1 \cap k_2 = k_3 \cap k_4 = \{I\}$.

Let us now consider Clifford's second circle theorem, which builds on the first theorem and gives a further result.

Theorem 5.1.4 (Clifford's Second Circle Theorem)**.** Let k_1, k_2, k_3, k_4, and k_5 be five distinct blocks through a point I and otherwise in general position. Let P_{ij} be the second intersection point of k_i and k_j for each $i, j \in \{1, \ldots, 5\}$ with $i < j$, and let k_{ijl} denote the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \ldots, 5\}$. Then the five points P_{ijlm} with $i < j < l < m \in \{1, \ldots, 5\}$ determined by Clifford's first circle theorem all lie on a common block.

Proof. Clifford's first circle theorem implies the following:

- $k_{123} \cap k_{124} \cap k_{134} \cap k_{234} = \{P_{1234}\}$,
- $k_{123} \cap k_{125} \cap k_{135} \cap k_{235} = \{P_{1235}\}$,
- $k_{124} \cap k_{125} \cap k_{145} \cap k_{245} = \{P_{1245}\}$,
- $k_{134} \cap k_{135} \cap k_{145} \cap k_{345} = \{P_{1345}\}$,
- $k_{234} \cap k_{235} \cap k_{245} \cap k_{345} = \{P_{2345}\}$.

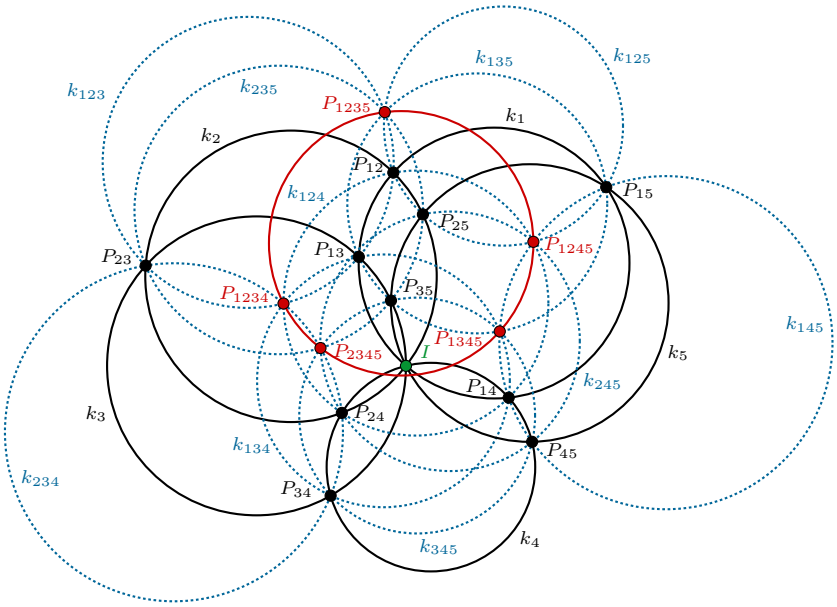


FIGURE 5.4: Clifford's second circle theorem.

We need to show that these points P_{ijlm} for $i < j < l < m \in \{1, \dots, 5\}$ all lie on one block. For this, we consider first the five blocks $k_1, k_{124}, k_{125}, k_{134}$, and k_{135}. It holds that

$$\begin{aligned} &P_{12}, P_{1245}, P_{14}, P_{1234} \in k_{124}, \quad P_{14}, P_{1234}, P_{13}, P_{1345} \in k_{134}, \\ &P_{13}, P_{1345}, P_{15}, P_{1235} \in k_{135}, \quad P_{15}, P_{1235}, P_{12}, P_{1245} \in k_{125}, \quad \text{and} \\ &P_{12}, P_{14}, P_{13}, P_{15} \in k_1. \end{aligned}$$

Thus, it follows from axiom (A4) that $P_{1245}, P_{1234}, P_{1345}$, and P_{1235} are on a common block. Second, we consider the five blocks $k_{124}, k_{134}, k_{245}, k_{345}$, and k_4. It holds that

$$\begin{aligned} &P_{24}, P_{1245}, P_{14}, P_{1234} \in k_{124}, \quad P_{14}, P_{1234}, P_{34}, P_{1345} \in k_{134}, \\ &P_{34}, P_{1345}, P_{45}, P_{2345} \in k_{345}, \quad P_{45}, P_{2345}, P_{24}, P_{1245} \in k_{245}, \quad \text{and} \\ &P_{24}, P_{14}, P_{34}, P_{45} \in k_4. \end{aligned}$$

Now, axiom (A4) implies that also $P_{1245}, P_{1234}, P_{1345}$, and P_{2345} lie on a common block. Consequently, it follows from axiom (A1) that $P_{1234}, P_{1235}, P_{1245}, P_{1345}$, and P_{2345} all lie on one block. □

Also Clifford's second circle theorem is commonly stated with five blocks $k_1, \dots, k_5$ passing through a common point I that are otherwise *in general position*, meaning that there are $\binom{5}{2} = 10$ additional points where exactly two of the five blocks intersect.

Let us now consider the cases where some of the blocks among $k_1, \dots, k_5$ are tangent at I. First, the case in which the blocks $k_1, \dots, k_5$ determine precisely nine additional points where exactly two of the five blocks intersect.

Lemma 5.1.5. Let $k_1, \dots, k_5$ be five distinct blocks through a common point P_{12}, in which k_1 and k_2 are tangent, and otherwise in general position. Let P_{ij} be the second intersection point of each non-tangent blocks k_i and k_j for $i, j \in \{1, \dots, 5\}$ with $i < j$, and let k_{ijl} denote the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \dots, 5\}$. Then the five points P_{ijlm} with $i < j < l < m \in \{1, \dots, 5\}$ all lie on the block k_{345}.

Proof. Lemma 5.1.2 implies that

- $\{P_{1234}\} = k_{123} \cap k_{124} \cap k_{134} \cap k_{234} = \{P_{34}\}$,
- $\{P_{1235}\} = k_{123} \cap k_{125} \cap k_{135} \cap k_{235} = \{P_{35}\}$,
- $\{P_{1245}\} = k_{124} \cap k_{125} \cap k_{145} \cap k_{245} = \{P_{45}\}$.

Thus, P_{1234}, P_{1235}, and P_{1245} lie on k_{345}, as k_{345} is the block through P_{34}, P_{35}, and P_{45}. Clifford's first circle theorem implies that

- $\{P_{1345}\} = k_{134} \cap k_{135} \cap k_{145} \cap k_{345} \subseteq k_{345}$,
- $\{P_{2345}\} = k_{234} \cap k_{235} \cap k_{245} \cap k_{345} \subseteq k_{345}$.

Hence, the points $P_{1234}, P_{1235}, P_{1245}, P_{1345}$, and P_{2345} all lie on k_{345}. □

Second, we consider the case in which the blocks $k_1, \dots, k_5$ determine precisely eight additional points where exactly two of the five blocks intersect.

Lemma 5.1.6. Let $k_1, \dots, k_5$ be five distinct blocks through a common point I such that precisely two pairs of these blocks are tangent at I, say k_1 and k_2 are tangent at P_{12}, and k_3 and k_4 are tangent at P_{34}, where $I = P_{12} = P_{34}$. Let P_{ij} be the second intersection point of each non-tangent blocks k_i and k_j for $i, j \in \{1, \dots, 5\}$ with $i < j$, and let k_{ijl} denote the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \dots, 5\}$. Then the five points P_{ijlm} with $i < j < l < m \in \{1, \dots, 5\}$ all lie on the block k_5.

Proof. Lemma 5.1.2 implies that

- $\{P_{1235}\} = k_{123} \cap k_{125} \cap k_{135} \cap k_{235} = \{P_{35}\}$,
- $\{P_{1245}\} = k_{124} \cap k_{125} \cap k_{145} \cap k_{245} = \{P_{45}\}$,
- $\{P_{1345}\} = k_{134} \cap k_{135} \cap k_{145} \cap k_{345} = \{P_{15}\}$,
- $\{P_{2345}\} = k_{234} \cap k_{235} \cap k_{245} \cap k_{345} = \{P_{25}\}$.

As the points P_{15}, P_{25}, P_{35}, and P_{45} lie by construction on k_5, it holds that P_{1235}, P_{1245}, $P_{1345}, P_{2345} \in k_5$. Moreover, remark 5.1.3 (i) implies that $\{P_{1234}\} = k_{123} \cap k_{124} \cap k_{134} \cap k_{234} = \{I\} \subseteq k_5$. Hence, the points $P_{1234}, P_{1235}, P_{1245}, P_{1345}$, and P_{2345} all lie on k_5. □

Remark 5.1.7. (i) If the blocks $k_1, \ldots, k_5$ in Clifford's second circle theorem define only seven additional points where exactly two of the five blocks intersect, then the theorem is still true.

Proof. Assume that $k_1 \cap k_2 = \{P_{12}\}$, $k_1 \cap k_3 = \{P_{13}\}$, and $k_2 \cap k_3 = \{P_{23}\}$, where $P_{12} = P_{13} = P_{23} = I$. Lemma 5.1.2 implies that $P_{1245} = P_{1345} = P_{2345} = P_{45}$ and remark 5.1.3 (ii) that $P_{1234} = P_{1235} = I$. By axiom (A1) the theorem is thus for this case trivially true. □

- (ii) If the blocks $k_1, \ldots, k_5$ in Clifford's second circle theorem define less than seven additional points where exactly two of the five blocks intersect, then $P_{1234} = P_{1235} = P_{1245} = P_{1345} = P_{2345} = I$. Thus, also in this case the theorem is trivially true.

5.2 Miquel-Clifford Configurations

When Clifford published a synthetic proof of Miquel's pentagon theorem in the Euclidean plane, he obtained the following series of propositions, which is according to its development often associated with the names of Miquel and Clifford (cf. p.51 in [Cli82]):

(P1) Given *three* lines, a circle may be drawn through their intersections.

(P2) Given *four* lines, the four circles so determined meet in a point.

(P3) Given *five* lines, the five points so found lie on a circle.

(P4) Given *six* lines, the six circles so determined meet in a point.

And the chain continues in this way, with the closure taking place alternately on a point or on a circle.

In this series of propositions, (P2) corresponds to Steiner's quadrilateral theorem and (P3) to Miquel's pentagon theorem. Moreover, replacing the n straight lines by concurrent circles leads to Clifford's circle theorems, which we considered in section 5.1 (cf. [Rao38]). Evidently, as lines and circles are merged to a set of blocks in Möbius planes, there is a strong connection between Steiner's quadrilateral theorem, Miquel's pentagon theorem, and Clifford's first and second circle theorems, which we consider in the following.

5.2.1 Steiner's Quadrilateral Theorem

Steiner's quadrilateral theorem is a direct consequence of Miquel's theorem and may be proved analogously in Miquelian Möbius planes as in the Euclidean plane (cf. [Var18]). We will now state the theorem similar to its version in Euclidean geometry (with an additional point ∞ on every line) and show that it follows directly from Clifford's first circle theorem.

Theorem 5.2.1. Let h_1, h_2, h_3, and h_4 be four distinct blocks that are all incident with ∞ and such that any three of them only meet in ∞. Let P_{ij} be the second

intersection point of the blocks h_i and h_j for each $i \in \{1, \dots, 4\}$ with $i < j$, and let k_{ijl} denote the block passing through the points P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \dots, 4\}$. Then the blocks $k_{123}, k_{124}, k_{134}$, and k_{234} meet in a point Q.

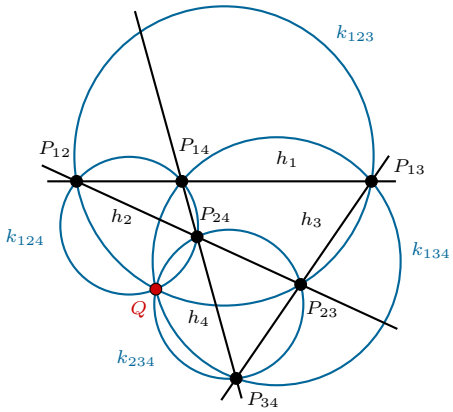


FIGURE 5.5: Steiner's quadrilateral theorem.

Proof. Consider the case where $I = \infty$ in Clifford's first circle theorem. Then, we immediately see that the theorems state exactly the same. □

Thus Clifford's first circle theorem is more general than Steiner's quadrilateral theorem. However, the one-point completion of the Euclidean plane leads to the same statement. Moreover, as we may use Möbius transformations, it follows that Steiner's quadrilateral theorem and Clifford's first circle theorem are equivalent in Miquelian Möbius planes.

Remark 5.2.2. If some of the blocks among $h_1, \dots, h_4$ in Steiner's quadrilateral theorem are tangent at ∞, then the theorem is still true, as we generalized Clifford's first circle theorem in section 5.1.

5.2.2 Miquel's Pentagon Theorem

We already considered Miquel's pentagon theorem in section 4.1.2. We provide now a different proof for this theorem using only Clifford's first and second circle theorems. Without loss of generality, we choose now $I = \infty$ in Miquel's pentagon theorem (q.v. theorem 4.2.1) to make the connection to its version in the Euclidean plane and adapt the notation slightly.

Theorem 5.2.3. Let $h_1, \dots, h_5$ be five distinct blocks that are all incident with ∞ and such that any three of them only meet in ∞. Let P_{ij} be the second intersection point of h_i and h_j for each $i, j \in \{1, \dots, 5\}$ with $i < j$, and let k_{ijl} be the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \dots, 5\}$. Then the blocks k_{124} and k_{134}, the blocks k_{134} and k_{135}, the blocks k_{135} and k_{235}, the blocks k_{235} and k_{245}, and the

blocks k_{245} and k_{124} each intersect at a second point and these five points all lie on one block.

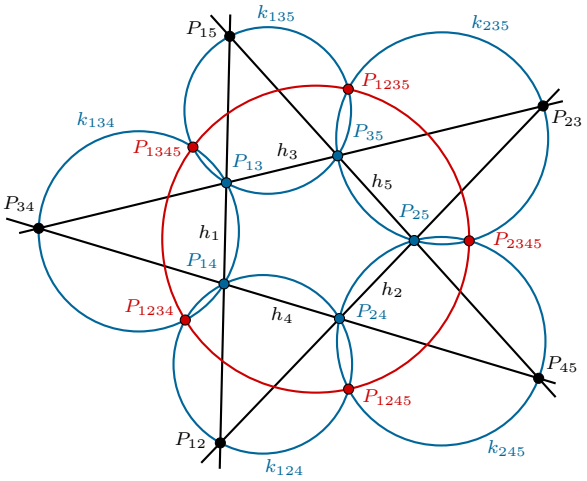


FIGURE 5.6: Miquel's pentagon theorem.

Proof. Consider any four of the five distinct blocks $h_1, \ldots, h_5$, say we discard h_5 and consider h_1, h_2, h_3, and h_4. These four blocks determine $\binom{4}{2} = 6$ intersection points $P_{ij} \neq \infty$, where $i, j \in \{1, 2, 3, 4\}$ with $i < j$. Now, consider the $\binom{4}{3} = 4$ blocks k_{ijl} through P_{ij}, P_{il}, and P_{jl}, where $i < j < l \in \{1, 2, 3, 4\}$, namely $k_{123}, k_{124}, k_{134}$, and k_{234}. Then, Clifford's first circle theorem implies that the latter four blocks meet in a point P_{1234}. In particular, it holds that

$$k_{124} \cap k_{134} = \{P_{14}, P_{1234}\}.$$

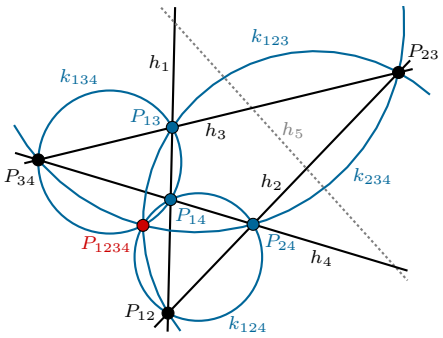


FIGURE 5.7: Geometric proof of Miquel's pentagon theorem.

Discarding h_4, h_3, h_2, and h_1 successively yields analogously as before that

- $k_{135} \cap k_{235} = \{P_{35}, P_{1235}\}$,
- $k_{124} \cap k_{245} = \{P_{24}, P_{1245}\}$,
- $k_{134} \cap k_{135} = \{P_{13}, P_{1345}\}$,
- $k_{235} \cap k_{245} = \{P_{25}, P_{2345}\}$.

Now Clifford's second circle theorem immediately implies that these points P_{1234}, P_{1235}, P_{1245}, P_{1345}, and P_{2345} all lie on a common block. □

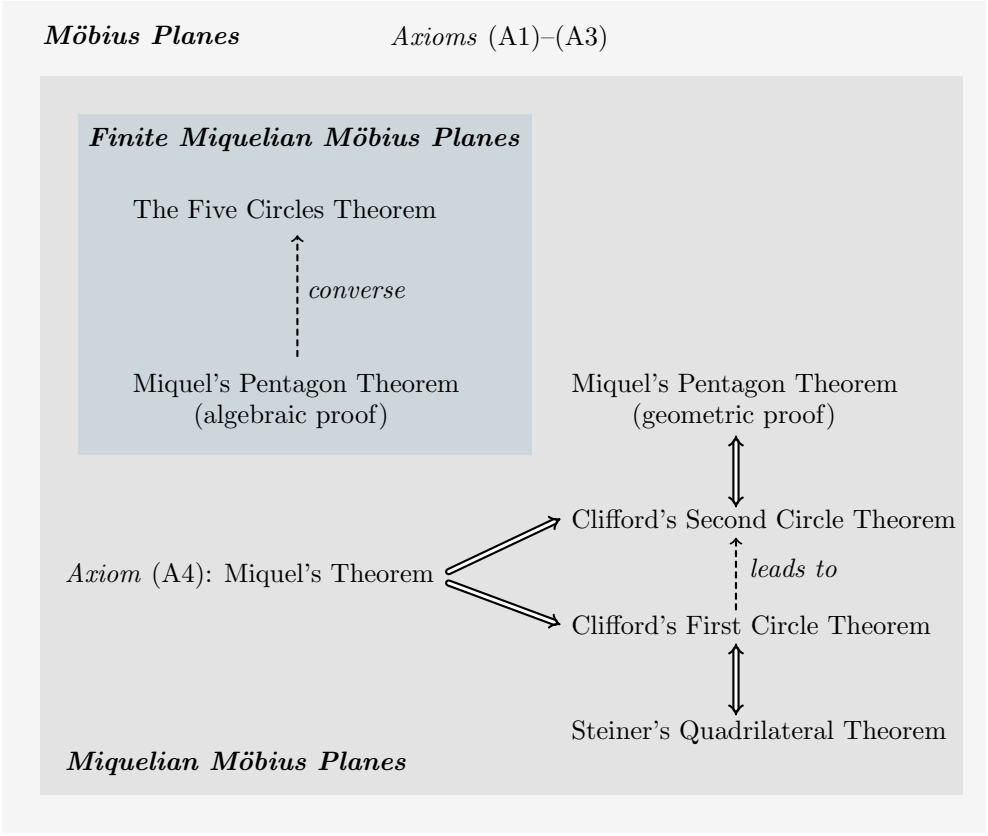
Since Clifford's second circle theorem and Miquel's pentagon both state that the points $P_{1234}, P_{1235}, P_{1245}, P_{1345}$, and P_{2345} are on one block, of course Miquel's pentagon theorem implies as well Clifford's second circle theorem. Consequently, these two theorems are indeed equivalent in Miquelian Möbius planes.

Remark 5.2.4. If some of the blocks among $h_1, \ldots, h_5$ in Miquel's pentagon theorem are tangent at ∞, then the theorem is still true, as we generalized Clifford's first and second circle theorems in section 5.1.

Remark 5.2.5. By replacing ∞ with some arbitrary point $I \in \mathbb{P}$ in the previous proof, we obtain in particular a geometric proof of Miquel's pentagon theorem in Miquelian Möbius planes.

5.3 Summary Diagram

We conclude now with a diagram that involves all the circle theorems we considered.



We introduced Möbius planes as an incidence structure in which the axioms (A1)–(A3) are satisfied. Axioms (A1) postulates that any three points define a unique block, which ensures that any two different blocks are either disjoint, tangent, or intersecting. Axiom (A2) guarantees that if two different blocks touch a third block at the same point, then these two blocks touch at this point as well (i.e. there is no second intersection point). And finally, the richness axiom (A3). If we add Miquel's theorem as axiom (A4) to the set of axioms, then we obtain Miquelian Möbius planes.

First, we gave a concrete construction of Miquelian Möbius planes of prime power order. This allowed us to prove Miquel's pentagon theorem and its converse, namely the five circles theorem, in finite Miquelian Möbius planes.

Using only the axioms (A1)–(A4), we proved that Clifford's first and second circle theorems hold true. The latter two theorems in turn show the validity of Steiner's quadrilateral theorem and Miquel's pentagon theorem in Miquelian Möbius planes.

Appendix A

Code for Calculations in $\mathcal{M}_{11}$

In section 3.3.3, we saw the construction of the Miquelian Möbius plane of order 11. In order to prove the five circles theorem in arbitrary finite Miquelian Möbius planes, we started by verifying the theorem in the concrete plane $\mathcal{M}_{11}$ (q.v. section 4.1.1). As the computations are rather extensive by hand, the calculations were made with the code below, which provides addition and multiplication tables for GF(11^2) and some functions concerning blocks in $\mathcal{M}_{11}$. However, we like to point out, that the goal of this code was not efficiency.

We now provide an implementation in **R** (written in RStudio Version 1.3.1093 for macOS):

```
# install.packages("polynom")
# install.packages("dplyr")
library(polynom)
library(dplyr)
x <- polynomial()

# We first create a matrix "elts" with the elements of GF(11^2) and
    assign an index to each element:
elts <- matrix(NA,ncol=4,nrow=121)
elts <- data.frame(elts)
colnames(elts) <- c("Index","Polynomial","m","a")
elts$Index <- 0:120
elts$Polynomial[1:11] <- paste0("0*x+",0:10)
elts$m[1:11] <- 0
elts$a[1:11] <- 0:10
m <- 1
a <- 0
for (k in 12:121) {
   elts$Polynomial[k] <- paste0(m,"*x+",a)
   elts$m[k] <- m
   elts$a[k] <- a
   if (a == 10) {
     a <- 0
     m <- floor((k - 2)/10)
   } else {
     a <- a + 1
  }
}
View(elts)
```

```
# Now we create the addition and multiplication tables "MxA" and "
    MxAmult" in GF(11^2):
MxA <- matrix(NA,nrow=121,ncol=121,
              dimnames=list(as.character(0:120),as.character(0:120)))
MxAmult <- matrix(NA,nrow=121,ncol=121,
                  dimnames=list(as.character(0:120),
                                as.character(0:120)))
for (i in 1:nrow(MxA)) {
  for (j in 1:ncol(MxA)) {
    mij <- (elts$m[elts$Index==(i-1)]+elts$m[elts$Index==(j-1)]) %% 11
    aij <- (elts$a[elts$Index==(i-1)]+elts$a[elts$Index==(j-1)]) %% 11
    MxA[i,j] <- paste0(mij,"*x+",aij)
    Polynomiali <- elts$m[elts$Index == (i-1)]*x+elts$a[elts$Index==(i
    -1)]
    Polynomialj <- elts$m[elts$Index == (j-1)]*x+elts$a[elts$Index==(j
    -1)]
    Polynomialmult <- ((Polynomiali*Polynomialj) %% (x^2+1))
    Polynomialmod11 <- paste0(ifelse(is.na(Polynomialmult[2] %% 11),
                                     0,Polynomialmult[2] %% 11),
                              "*","x+",
                               Polynomialmult[1] %% 11)
    MxAmult[i,j] <-  Polynomialmod11
  }
}
View(MxA)
View(MxAmult)

# Now the addition and multiplication tables "B" and "Bmult" in GF(11^2)
     with the indices:
B <- matrix(NA,nrow=121,ncol=121,
            dimnames=list(as.character(0:120),as.character(0:120)))
Bmult <- matrix(NA,nrow=121,ncol=121,
                dimnames=list(as.character(0:120),
                              as.character(0:120)))
for (i in 1:nrow(B)) {
  for (j in 1:ncol(B)) {
    B[i,j] <- elts$Index[elts$Polynomial==MxA[elts$Index==as.character(i
    -1),
                                              elts$Index==as.character(j
    -1)]]
    Bmult[i,j] <- elts$Index[elts$Polynomial==
                               MxAmult[elts$Index==as.character(i-1),
                                       elts$Index==as.character(j-1)]]
  }
}
View(B)
# isSymmetric(B)
View(Bmult)
# isSymmetric(Bmult)

# We define a function to get the polynomial of an index:
polyn <- function(i) {
  pIndex <- elts$Polynomial[elts$Index==i]
  return(pIndex)
}

# We define a function to get the index of a polynomial "mi*x+ai":
indexz <- function(mi,ai) {
```

```
  v1 <- elts$Index[elts$m==mi]
  v2 <- elts$Index[elts$a==ai]
  ppoly <- intersect(v1,v2)
  return(ppoly)
 }

# We define a function to calculate the product of the indices i and j:
multij <- function(i,j) {
  P <- Bmult[i+1,j+1]
  return(P)
}

# Function to calculate the sum of the indices i and j:
addij <- function(i,j) {
  P <- B[i+1,j+1]
  return(P)
}

# We define a function to calculate the conjugate elements,
# then we add them to the matrix "elts":
getconjIndex<- function(idx) {
  conjidx <- Bmult[idx+1,idx+1]
  for (k in 3:11) {
    conjidx <- Bmult[conjidx+1,idx+1]
  }
  return(conjidx)
}
elts$IndexConj <- sapply(elts$Index,getconjIndex)

# We also add the trace and the norm to the matrix "elts":
elts$Trace <- mapply(function(i,j) B[i+1,j+1],elts$Index,elts$IndexConj)
elts$Norm <- mapply(function(i,j) Bmult[i+1,j+1],elts$Index,elts$
    IndexConj)

# Function to calculate the norm of an index:
norm <- function(z) {
  n <- elts[z+1,7]
  return(n)
}

# Function to calculate the division of the index i by the index j:
divij <- function(i,j) {
  z <- which(Bmult[j+1,]==i)-1
  return(as.integer(z))
}

# Function to subtract the index j from the index i:
subij <- function(i,j) {
  z <- which(B[j+1,]==i)-1
  return(as.integer(z))
}

# Function for the multiplicative inverse of an index:
invmult <- function(z) {
  inv <- which(Bmult[z+1,]==1)-1
  return(as.integer(inv))
}
```

```
# Function for the additive inverse of an index:
invadd <- function(z) {
  inv <- which(B[z+1,]==1)-1
  return(as.integer(inv))
}

# Function to compute the square root of an index:
sqrroot <- function(z) {
  sr <- which(diag(Bmult)==z)-1
  return(as.integer(sr))
}

# Function to compute the solutions of the equation "z + conj(z) = b":
equnit2add <- function(bi) {
  return(subset(elts,Trace==bi,select=c(Index,Polynomial,Trace)))
}

# Function to compute the solutions of the equation "z * conj(z) = r":
equnit1mult <- function(ri) {
  return(subset(elts,Norm==ri,select=c(Index,Polynomial,Norm)))
}

# We use the points on B^1_(0,r) to calculate the points on B^1_(c,r)
# (Moebius transformation):
Moebeqmultcr<- function(ci,ri) {
  LM <- subset(elts,Norm==ri,select=c(Index,Polynomial,Norm))
  L <- LM[,1]
  for (i in 1:12){
    L[i] = B[L[i]+1,ci+1]
  }
  return(sort(L))
}

# We use the points on B^2_(1,b) to calculate the points on B^2_(a,b)
# (Moebius transformation):
Moebeqaddab <- function(ai,bi) {
  LM <- subset(elts,Trace==bi,select=c(Index,Polynomial,Trace))
  L <- LM[,1]
  for (i in 1:11){
    L[i] = divij(L[i],getconjIndex(ai))
  }
  return(sort(L))
}

# Function for the intersection points of two circles B^1_(c1,r1), B^1_(
    c2,r2):
intpointsB1<- function(c1,r1,c2,r2) {
  Ip <- intersect(Moebeqmultcr(c1,r1),Moebeqmultcr(c2,r2))
  print(polyn(Ip[1]))
  print(polyn(Ip[2]))
  return(as.integer(Ip))
}

# Function for the intersection points of two blocks B^1_(c1,r1), B^2_(
    a2,b2):
intpointsB12 <- function(c1,r1,a2,b2) {
  Ip <- intersect(Moebeqmultcr(c1,r1),Moebeqaddab(a2,b2))
  return(as.integer(Ip))
```

```
}

# Function for the intersection points of two lines B^2_(a1,b1), B^2_(a2
    ,b2):
intpointsB2 <- function(a1,b1,a2,b2) {
  Ip <- intersect(Moebeqaddab(a1,b1),Moebeqaddab(a2,b2))
  return(as.integer(Ip))
}

# Find the line through the points P1,P2
# (i.e. find a,b in a*conj(z) + conj(a)*z = b):
lineP1P2 <- function(P1,P2) {
  a <- subij(0,divij(subij(P1,P2),22))
  b <- subij(0,divij(subij(multij(P1,getconjIndex(P2)),
                                  multij(getconjIndex(P1),P2)),22))
  print("B^2_(a,c): a*conj(z)+conj(a)*z=b")
  print(paste0("a = ",a))
  print(paste0("conj(a) = ",getconjIndex(a)))
  print(paste0("b = ",b))
}

# Find the circle through the points P1,P2,P3
# (i.e. find c,r in (z-c)*(conj(z)-conj(c))=r):
# First, we check whether P1,P2,P3 are on a line, which is the case if
    and only if D=0.
isline <- function(P1,P2,P3) {
  D1 <- subij(subij(multij(P2,getconjIndex(P3)),
                          multij(getconjIndex(P2),P3)),
                  multij(P1,getconjIndex(P3)))
  D2 <- subij(addij(multij(getconjIndex(P1),P3),
                          multij(P1,getconjIndex(P2))),
                  multij(getconjIndex(P1),P2))
  D0 <- addij(D1,D2)
  (D0==0)
}
circleP1P2P3 <- function(P1,P2,P3) {
  if (isTRUE(isline(P1,P2,P3))) {
    print("Line")
    return(lineP1P2(P1,P2))
  }
  else {
    D1 <- subij(subij(multij(P2,getconjIndex(P3)),
                            multij(getconjIndex(P2),P3)),
                    multij(P1,getconjIndex(P3)))
    D2 <- subij(addij(multij(getconjIndex(P1),P3),
                            multij(P1,getconjIndex(P2))),
                    multij(getconjIndex(P1),P2))
    D0 <- addij(D1,D2)
    C1 <- subij(subij(multij(norm(P2),P3),multij(P2,norm(P3))),
                    multij(norm(P1),P3))
    C2 <- subij(addij(multij(P1,norm(P3)),multij(norm(P1),P2)),
                    multij(P1,norm(P2)))
    C0 <- addij(C1,C2)
    G1 <- addij(multij(multij(norm(P1),P2),getconjIndex(P3)),
                    multij(multij(P1,getconjIndex(P2)),norm(P3)))
    G2 <- subij(multij(multij(norm(P2),P3),getconjIndex(P1)),
                    multij(multij(P2,getconjIndex(P1)),norm(P3)))
    G3 <- addij(multij(multij(norm(P1),P3),getconjIndex(P2)),
```

```
                    multij(multij(P1,getconjIndex(P3)),norm(P2)))
    G <- subij(addij(G1,G2),G3)
    c0 <- divij(C0,subij(0,D0))
    r <- addij(divij(G,D0),norm(c0))
    print("B^1_(c,r): (z-c)*(conj(z)-conj(c))=r")
    print(paste0("c = ",c0))
    print(paste0("conj(c) = ",getconjIndex(c0)))
    print(paste0("r = ",r))
  }
}

# Find the circle with center c through the point P (i.e. find r):
circlecP <- function(c0,P) {
  r <- multij(subij(P,c0),subij(getconjIndex(P),getconjIndex(c0)))
  return(r)
}

# Check if four points are on a block using the cross-ratio [P1,P2;P3,P4
    ]:
# (If the cross-ratio is an element of GF(11), then P1,P2,P3,P4 lie on a
     common block)
crossratio <- function(P1,P2,P3,P4) {
  cr <- multij(divij(subij(P3,P1),subij(P3,P2)),
                 divij(subij(P4,P2),subij(P4,P1)))
  print(paste0("cross ratio = ",cr))
  if (cr < 11) {
    print("The four points lie on a common block.")
  }
  else {
    print("The four points do not lie on a common block.")
  }
}
```

Appendix B

Computations in Mathematica

B.1 The Five Circles Theorem

In section 4.1.2, we proved the five circles theorem in Miquelian Möbius planes of prime power order. The proof involves some calculations that are straightforward but very large. Therefore, we used the symbolic mathematical computation program *Wolfram Mathematica*. For the sake of completeness, we provide now the entire code in *Mathematica* (Version 12.2.0.0 for macOS).

First, the code used for family (i):

```
In[1]:= SetOptions[EvaluationNotebook[], Background → RGBColor[0.95, 0.95, 0.96]]
        Qi = Ti + Ti+1 + Ti+2 * 1/Ti+3 * Ti+4;
        Qi+1 = Ti+1 + Ti+2 + Ti+3 * 1/Ti+4 * Ti;
        Qi+3 = Ti+3 + Ti+4 + Ti * 1/Ti+1 * Ti+2;
        Qi+4 = Ti+4 + Ti + Ti+1 * 1/Ti+2 * Ti+3;
        Q̄i = 1/Ti + 1/Ti+1 + Ti+3/(Ti+2 * Ti+4);
        Q̄i+1 = 1/Ti+1 + 1/Ti+2 + Ti+4/(Ti+3 * Ti);
        Q̄i+3 = 1/Ti+3 + 1/Ti+4 + Ti+1/(Ti * Ti+2);
        Q̄i+4 = 1/Ti+4 + 1/Ti + Ti+2/(Ti+1 * Ti+3);

In[10]:= Si = Simplify[ ((Qi+1 - Qi) * (Q̄i+3 * Qi+4 - Qi+3 * Q̄i+4) - (Qi+4 - Qi+3) * (Q̄i * Qi+1 - Qi * Q̄i+1)) / ((Q̄i+1 - Q̄i) (Qi+4 - Qi+3) - (Q̄i+4 - Q̄i+3) (Qi+1 - Qi)) ]

Out[10]= Ti (1 + T2+i/T1+i + T3+i/T4+i)
```

```
In[11]:= S_i = 1/T_i * (T_{i+1}/T_{i+2} + T_{i+4}/T_{i+3} + 1);
         P_{i-1} = -T_i * 1/T_{i+1} * T_{i+2} * 1/T_{i+3} * T_{i+4};
         P_i = -T_i * T_{i+1} * 1/T_{i+2} * T_{i+3} * 1/T_{i+4};

In[14]:= Simplify[Det[{{S_i * S_i, S_i, S_i, 1}, {Q_i * Q_i, Q_i, Q_i, 1}, {1, P_{i-1}, 1/P_{i-1}, 1},
           {1, P_i, 1/P_i, 1}}]]

Out[14]= 0
```

Second, the code used for family (ii):

```
In[1]:= SetOptions[EvaluationNotebook[], Background → RGBColor[0.95, 0.95, 0.96]]
        Q_i = T_i + T_{i+1} - T_{i+2} * 1/T_{i+3} * T_{i+4};
        Q_{i+1} = T_{i+1} + T_{i+2} - T_{i+3} * 1/T_{i+4} * T_i;
        Q_{i+3} = T_{i+3} + T_{i+4} - T_i * 1/T_{i+1} * T_{i+2};
        Q_{i+4} = T_{i+4} + T_i - T_{i+1} * 1/T_{i+2} * T_{i+3};
        Q_i = 1/T_i + 1/T_{i+1} - T_{i+3}/(T_{i+2} * T_{i+4});
        Q_{i+1} = 1/T_{i+1} + 1/T_{i+2} - T_{i+4}/(T_{i+3} * T_i);
        Q_{i+3} = 1/T_{i+3} + 1/T_{i+4} - T_{i+1}/(T_i * T_{i+2});
        Q_{i+4} = 1/T_{i+4} + 1/T_i - T_{i+2}/(T_{i+1} * T_{i+3});
        P_{i-1} = T_i * 1/T_{i+1} * T_{i+2} * 1/T_{i+3} * T_{i+4};
        P_i = T_i * T_{i+1} * 1/T_{i+2} * T_{i+3} * 1/T_{i+4};
        P_{i+2} = T_{i+2} * T_{i+3} * 1/T_{i+4} * T_i * 1/T_{i+1};

In[13]:= U_i = Simplify[((Q_{i+1} - Q_i) * (1/T_i * P_{i+2} - T_i * 1/P_{i+2}) - (P_{i+2} - T_i) * (Q_i * Q_{i+1} - Q_i * Q_{i+1})) /
           ((Q_{i+1} - Q_i) (P_{i+2} - T_i) - (1/P_{i+2} - 1/T_i) (Q_{i+1} - Q_i))]

Out[13]= T_i (1 + T_{2+i}/T_{1+i} - T_{3+i}/T_{4+i})
```

```
In[14]:= $\overline{U_i} = \frac{1}{T_i}\left(1 + \frac{T_{i+1}}{T_{i+2}} - \frac{T_{i+4}}{T_{i+3}}\right)$

Out[14]= $\frac{1 + \frac{T_{1+i}}{T_{2+i}} - \frac{T_{4+i}}{T_{3+i}}}{T_i}$

In[15]:= R_i =
  Simplify[((Q_{i+4} - Q_{i+3}) * (1/T_i * P_{i+2} - T_i * 1/P_{i+2}) - (P_{i+2} - T_i) * (Conj[Q_{i+3}] * Q_{i+4} - Q_{i+3} * Conj[Q_{i+4}]))/
    ((Conj[Q_{i+4}] - Conj[Q_{i+3}]) (P_{i+2} - T_i) - (1/P_{i+2} - 1/T_i) (Q_{i+4} - Q_{i+3}))]

Out[15]= $T_i\left(1 - \frac{T_{2+i}}{T_{1+i}} + \frac{T_{3+i}}{T_{4+i}}\right)$

In[16]:= $\overline{R_i} = \frac{1}{T_i}\left(1 - \frac{T_{i+1}}{T_{i+2}} + \frac{T_{i+4}}{T_{i+3}}\right)$

Out[16]= $\frac{1 - \frac{T_{1+i}}{T_{2+i}} + \frac{T_{4+i}}{T_{3+i}}}{T_i}$

In[17]:= Simplify[Det[{{U_i * Conj[U_i], U_i, Conj[U_i], 1}, {R_i * Conj[R_i], R_i, Conj[R_i], 1}, {1, P_{i-1}, 1/P_{i-1}, 1},
    {1, P_i, 1/P_i, 1}}]]

Out[17]= 0
```

B.2 Miquel's Pentagon Theorem

In section 4.2, we proved Miquel's pentagon theorem in Miquelian Möbius planes of prime power order by using the cross-ratio. Again, some of the calculations are elementary but very extensive. Therefore, we used also in this case *Mathematica*. Here, we provide the code used to justify our calculations made in the proof.

```
In[1]:= SetOptions[EvaluationNotebook[], Background → RGBColor[0.95, 0.95, 0.96]]
  (*First we calculate the lines h_i passing though Q_i and Q_{i+4}*)
  h_1 = Solve[Det[{{z, Conj[z], 1}, {Q_1, Conj[Q_1], 1}, {Q_5, Conj[Q_5], 1}}] == 0, Conj[z]];
  h_2 = Solve[Det[{{z, Conj[z], 1}, {Q_1, Conj[Q_1], 1}, {Q_2, Conj[Q_2], 1}}] == 0, Conj[z]];
  h_3 = Solve[Det[{{z, Conj[z], 1}, {Q_2, Conj[Q_2], 1}, {Q_3, Conj[Q_3], 1}}] == 0, Conj[z]];
  h_4 = Solve[Det[{{z, Conj[z], 1}, {Q_3, Conj[Q_3], 1}, {Q_4, Conj[Q_4], 1}}] == 0, Conj[z]];
  h_5 = Solve[Det[{{z, Conj[z], 1}, {Q_4, Conj[Q_4], 1}, {Q_5, Conj[Q_5], 1}}] == 0, Conj[z]];
  h_1 = Simplify[Conj[z] /. h_1[[1]]];
  h_2 = Simplify[Conj[z] /. h_2[[1]]];
  h_3 = Simplify[Conj[z] /. h_3[[1]]];
  h_4 = Simplify[Conj[z] /. h_4[[1]]];
  h_5 = Simplify[Conj[z] /. h_5[[1]]];
```

```
In[12]:= (*Next we calculate the intersection point of h_{i+1} and h_{i+4}*)
S1 = Solve[h2 == h5, z];
S2 = Solve[h1 == h3, z];
S3 = Solve[h2 == h4, z];
S4 = Solve[h3 == h5, z];
S5 = Solve[h4 == h1, z];
S1 = Simplify[z /. S1[[1]]] (*we only display S1*)
S2 = Simplify[z /. S2[[1]]];
S3 = Simplify[z /. S3[[1]]];
S4 = Simplify[z /. S4[[1]]];
S5 = Simplify[z /. S5[[1]]];
```

Out[17]=
$$\frac{\overline{Q_5}\,(Q_1-Q_2)\,Q_4+\overline{Q_1}\,Q_2\,Q_4-\overline{Q_4}\,Q_1\,Q_5-\overline{Q_1}\,Q_2\,Q_5+\overline{Q_4}\,Q_2\,Q_5+\overline{Q_2}\,Q_1\,(-Q_4+Q_5)}{\overline{Q_5}\,(Q_1-Q_2)+\overline{Q_4}\,(-Q_1+Q_2)+\left(\overline{Q_1}-\overline{Q_2}\right)\,(Q_4-Q_5)}$$

```
In[22]:= (*Now we compute the conjugate S_i of S_i*)
S1 = S1 /. {Q1 → s1, Q2 → s2, Q3 → s3, Q4 → s4, Q5 → s5, Conjugate[Q1] → t1, Conjugate[Q2] → t2,
    Conjugate[Q3] → t3, Conjugate[Q4] → t4, Conjugate[Q5] → t5};
Conjugate[S1] = S1 /. {s1 → Conjugate[Q1], s2 → Conjugate[Q2], s3 → Conjugate[Q3], s4 → Conjugate[Q4], s5 → Conjugate[Q5], t1 → Q1, t2 → Q2, t3 → Q3,
    t4 → Q4, t5 → Q5};
S2 = S2 /. {Q1 → s1, Q2 → s2, Q3 → s3, Q4 → s4, Q5 → s5, Conjugate[Q1] → t1, Conjugate[Q2] → t2, Conjugate[Q3] → t3,
    Conjugate[Q4] → t4, Conjugate[Q5] → t5};
Conjugate[S2] = S2 /. {s1 → Conjugate[Q1], s2 → Conjugate[Q2], s3 → Conjugate[Q3], s4 → Conjugate[Q4], s5 → Conjugate[Q5], t1 → Q1, t2 → Q2, t3 → Q3,
    t4 → Q4, t5 → Q5};
S3 = S3 /. {Q1 → s1, Q2 → s2, Q3 → s3, Q4 → s4, Q5 → s5, Conjugate[Q1] → t1, Conjugate[Q2] → t2, Conjugate[Q3] → t3,
    Conjugate[Q4] → t4, Conjugate[Q5] → t5};
Conjugate[S3] = S3 /. {s1 → Conjugate[Q1], s2 → Conjugate[Q2], s3 → Conjugate[Q3], s4 → Conjugate[Q4], s5 → Conjugate[Q5], t1 → Q1, t2 → Q2, t3 → Q3,
    t4 → Q4, t5 → Q5};
S4 = S4 /. {Q1 → s1, Q2 → s2, Q3 → s3, Q4 → s4, Q5 → s5, Conjugate[Q1] → t1, Conjugate[Q2] → t2, Conjugate[Q3] → t3,
    Conjugate[Q4] → t4, Conjugate[Q5] → t5};
Conjugate[S4] = S4 /. {s1 → Conjugate[Q1], s2 → Conjugate[Q2], s3 → Conjugate[Q3], s4 → Conjugate[Q4], s5 → Conjugate[Q5], t1 → Q1, t2 → Q2, t3 → Q3,
    t4 → Q4, t5 → Q5};
S5 = S5 /. {Q1 → s1, Q2 → s2, Q3 → s3, Q4 → s4, Q5 → s5, Conjugate[Q1] → t1, Conjugate[Q2] → t2, Conjugate[Q3] → t3,
    Conjugate[Q4] → t4, Conjugate[Q5] → t5};
Conjugate[S5] = S5 /. {s1 → Conjugate[Q1], s2 → Conjugate[Q2], s3 → Conjugate[Q3], s4 → Conjugate[Q4], s5 → Conjugate[Q5], t1 → Q1, t2 → Q2, t3 → Q3,
    t4 → Q4, t5 → Q5};
Clear[S1, S2, S3, S4, S5]
```

```
In[33]:= (*We compute the circle k_i passing though S_i, Q_i, and Q_{i+4}*)
k1 =
  Solve[
   Det[{{z * Conjugate[z], z, Conjugate[z], 1}, {Q1 * Conjugate[Q1], Q1, Conjugate[Q1], 1}, {Q5 * Conjugate[Q5], Q5, Conjugate[Q5], 1},
      {S1 * Conjugate[S1], S1, Conjugate[S1], 1}}] == 0, Conjugate[z]];
```

```
k2 =
  Solve[
   Det[{{z * z̄, z, z̄, 1}, {Q1 * Q̄1, Q1, Q̄1, 1}, {Q2 * Q̄2, Q2, Q̄2, 1},
      {S2 * S̄2, S2, S̄2, 1}}] == 0, z̄];
k3 =
  Solve[
   Det[{{z * z̄, z, z̄, 1}, {Q2 * Q̄2, Q2, Q̄2, 1}, {Q3 * Q̄3, Q3, Q̄3, 1},
      {S3 * S̄3, S3, S̄3, 1}}] == 0, z̄];
k4 =
  Solve[
   Det[{{z * z̄, z, z̄, 1}, {Q3 * Q̄3, Q3, Q̄3, 1}, {Q4 * Q̄4, Q4, Q̄4, 1},
      {S4 * S̄4, S4, S̄4, 1}}] == 0, z̄];
k5 =
  Solve[
   Det[{{z * z̄, z, z̄, 1}, {Q4 * Q̄4, Q4, Q̄4, 1}, {Q5 * Q̄5, Q5, Q̄5, 1},
      {S5 * S̄5, S5, S̄5, 1}}] == 0, z̄];
k1 = Simplify[z̄ /. k1[[1]]];
k2 = Simplify[z̄ /. k2[[1]]];
k3 = Simplify[z̄ /. k3[[1]]];
k4 = Simplify[z̄ /. k4[[1]]];
k5 = Simplify[z̄ /. k5[[1]]];
```

In[43]:=
```
(*ki and ki+1 intersect at Qi and at a second point Pi. Now we compute Pi*)
z1 = Solve[k1 == k2, z] (*we obtain two solutions*)
z2 = Solve[k2 == k3, z];
z3 = Solve[k3 == k4, z];
z4 = Solve[k4 == k5, z];
z5 = Solve[k5 == k1, z];
P1 = Simplify[z /. z1[[2]]];
P2 = Simplify[z /. z2[[2]]] (*each second solution is Pi, we only display P2*)
P3 = Simplify[z /. z3[[2]]];
P4 = Simplify[z /. z4[[2]]];
P5 = Simplify[z /. z5[[2]]];
```

Out[43]=
$$\Big\{\{z \to Q_1\},$$
$$\Big\{z \to \big(\overline{Q_3}\, Q_1\, Q_2\, Q_4 - \overline{Q_5}\, Q_1\, Q_2\, Q_4 - \overline{Q_2}\, Q_1\, Q_3\, Q_4 + \overline{Q_5}\, Q_1\, Q_3\, Q_4 - \overline{Q_3}\, Q_1\, Q_2\, Q_5 + \overline{Q_4}\, Q_1\, Q_2\, Q_5 - \overline{Q_4}\, Q_2^2\, Q_5 + \overline{Q_5}\, Q_2^2\, Q_5 + \overline{Q_2}\, Q_1\, Q_3\, Q_5 - \overline{Q_4}\, Q_1\, Q_3\, Q_5 + \overline{Q_4}\, Q_2\, Q_3\, Q_5 - \overline{Q_5}\, Q_2\, Q_3\, Q_5 + \overline{Q_2}\, Q_2\, Q_4\, Q_5 - \overline{Q_3}\, Q_2\, Q_4\, Q_5 - \overline{Q_2}\, Q_2\, Q_5^2 + \overline{Q_3}\, Q_2\, Q_5^2\big) \Big/$$
$$\big(\overline{Q_4}\, Q_1\, Q_2 - \overline{Q_5}\, Q_1\, Q_2 - \overline{Q_4}\, Q_2^2 + \overline{Q_5}\, Q_2^2 - \overline{Q_4}\, Q_1\, Q_3 + \overline{Q_5}\, Q_1\, Q_3 + \overline{Q_4}\, Q_2\, Q_3 - \overline{Q_5}\, Q_2\, Q_3 - \overline{Q_2}\, Q_1\, Q_4 + \overline{Q_3}\, Q_1\, Q_4 + \overline{Q_2}\, Q_2\, Q_4 - \overline{Q_5}\, Q_2\, Q_4 - \overline{Q_2}\, Q_3\, Q_4 + \overline{Q_5}\, Q_3\, Q_4 + \overline{Q_2}\, Q_1\, Q_5 - \overline{Q_3}\, Q_1\, Q_5 - \overline{Q_2}\, Q_2\, Q_5 + \overline{Q_5}\, Q_2\, Q_5 + \overline{Q_2}\, Q_3\, Q_5 - \overline{Q_5}\, Q_3\, Q_5 + \overline{Q_2}\, Q_4\, Q_5 - \overline{Q_3}\, Q_4\, Q_5 - \overline{Q_2}\, Q_5^2 + \overline{Q_3}\, Q_5^2\big)\Big\}\Big\}$$

Out[49]=
$$\left(\overline{Q_4}\,(Q_1-Q_2)\,Q_3\,(Q_1-Q_5)-\overline{Q_3}\,(Q_1\,Q_3-Q_2\,Q_4)\,(Q_1-Q_5)+(Q_3-Q_4)\left(\overline{Q_5}\,Q_1\,(Q_2-Q_3)+\overline{Q_1}\,(Q_1\,Q_3-Q_2\,Q_5)\right)\right)\Big/\left((Q_3-Q_4)\left(\overline{Q_5}\,(Q_2-Q_3)+\overline{Q_1}\,(Q_1-Q_2+Q_3-Q_5)\right)+\overline{Q_4}\,(Q_1-Q_2)\,(Q_1-Q_5)-\overline{Q_3}\,(Q_1-Q_2+Q_3-Q_4)\,(Q_1-Q_5)\right)$$

In[53]:=
```
(*Finally, we compute the cross-ratio of the points P1,...,P4*)
```

In[54]:=
```
cr1 = Simplify[ (P1 - P3) (P2 - P4) / (P1 - P4) (P2 - P3) ]
```

Out[54]=
$$\frac{\left(\overline{Q_5}\,(Q_2-Q_4)+\overline{Q_2}\,(Q_4-Q_5)+\overline{Q_4}\,(-Q_2+Q_5)\right)\left(\overline{Q_5}\,(-Q_1+Q_3)+\overline{Q_3}\,(Q_1-Q_5)+\overline{Q_1}\,(-Q_3+Q_5)\right)}{\left(\overline{Q_5}\,(Q_1-Q_4)+\overline{Q_1}\,(Q_4-Q_5)+\overline{Q_4}\,(-Q_1+Q_5)\right)\left(\overline{Q_5}\,(-Q_2+Q_3)+\overline{Q_3}\,(Q_2-Q_5)+\overline{Q_2}\,(-Q_3+Q_5)\right)}$$

In[55]:=
```
(*And also the cross-ratio of the points P2,...,P5*)
cr2 = Simplify[ (P2 - P4) (P3 - P5) / (P2 - P5) (P3 - P4) ]
```

Out[55]=
$$\frac{\left(\overline{Q_4}\,(-Q_1+Q_2)+\overline{Q_2}\,(Q_1-Q_4)+\overline{Q_1}\,(-Q_2+Q_4)\right)\left(\overline{Q_5}\,(-Q_1+Q_3)+\overline{Q_3}\,(Q_1-Q_5)+\overline{Q_1}\,(-Q_3+Q_5)\right)}{\left(\overline{Q_4}\,(-Q_1+Q_3)+\overline{Q_3}\,(Q_1-Q_4)+\overline{Q_1}\,(-Q_3+Q_4)\right)\left(\overline{Q_5}\,(-Q_1+Q_2)+\overline{Q_2}\,(Q_1-Q_5)+\overline{Q_1}\,(-Q_2+Q_5)\right)}$$

Appendix C

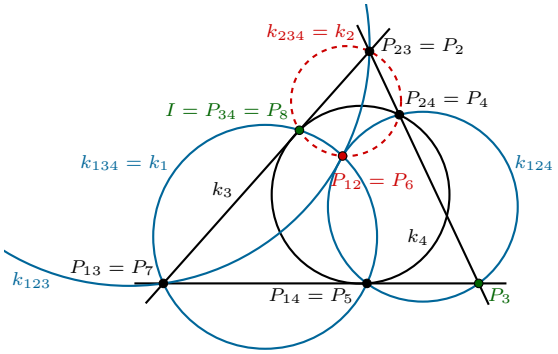
An Open Question

The axiomatic definition of Miquelian Möbius planes involves four axioms: the three axioms of a Möbius plane and Miquel's theorem (q.v. theorem 3.2.1) as the fourth axiom. We saw in section 5.1 that these four axioms imply Clifford's first and second circle theorems. A question which is at present still open is whether Clifford's circle theorems in turn also imply Miquel's theorem. If this were the case, then we could characterize Miquelian Möbius planes using the axioms of the Möbius plane and Clifford's circle theorems.

Observe that Miquel's theorem yields an $8_3 6_4$ point and block configuration, meaning that there are eight points, six blocks, three blocks through each point, and four points on each block. Clifford's first circle theorem on the other side yields a self-dual 8_4 point and block configuration (cf. [Dor88]). An idea to prove Miquel's theorem from Clifford's first circle theorem is therefore to introduce another block such that four blocks pass through some points, which enables us to apply Clifford's first circle theorem. Consider the following attempt:

Let $P_1, \ldots, P_8 \in \mathbb{P}$ be eight different points such that

$$P_1 \in \overrightarrow{P_2\,P_3\,P_4}, \quad P_3 \in \overrightarrow{P_4\,P_5\,P_6},$$
$$P_5 \in \overrightarrow{P_6\,P_7\,P_8}, \quad P_7 \in \overrightarrow{P_8\,P_1\,P_2}, \quad \text{and} \quad P_1 \in \overrightarrow{P_3\,P_5\,P_7}.$$



Let $k_1 = \overrightarrow{P_5\,P_7\,P_8}$, $k_2 = \overrightarrow{P_2\,P_4\,P_8}$, $k_3 = \overrightarrow{P_2\,P_7\,P_8}$, and $k_4 = \overrightarrow{P_4\,P_5\,P_8}$. Then the blocks k_1, k_2, k_3, and k_4 all pass through P_8. Thus, we aim to apply Clifford's first circle theorem (q.v. theorem 5.1.1) for $I := P_8$. Although the blocks k_3 and k_4 are not necessarily tangent at P_8, we may discard a possible second intersection point and consider them as tangent blocks in order to apply the generalized version of Clifford's first circle theorem, namely lemma 5.1.2. Thus, let P_{12} be the intersection point of k_1 and k_2. The intersection points of k_i and k_j for $i, j \in \{1, \ldots, 4\}$ are the following points:

$$\begin{aligned} &P_2 = P_{23}, \quad P_4 = P_{24}, \quad P_5 = P_{14}, \\ &P_7 = P_{13}, \quad P_8 = P_{34}. \end{aligned}$$

Let k_{ijl} denote the block through P_{ij}, P_{il}, and P_{jl} for $i < j < l \in \{1, \ldots, 4\}$. Then lemma 5.1.2 implies that the blocks $k_{123}, k_{124}, k_{134}$, and k_{234} meet in P_{12}. Now, *if* P_3 lies on k_{124}, then it follows that $P_{12} = P_6$, which means that P_6 lies indeed on k_2. Consequently, it would hold that $P_2 \in \overrightarrow{P_4\,P_6\,P_8}$. However, it requires another idea to ensure that the point P_3 is on k_{124}, as this is here not necessarily the case.

Bibliography

[Ale12] Gerhard Wanner Alexander Ostermann. *Geometry by Its History*. Undergraduate Texts in Mathematics. Springer, Berlin, Heidelberg, 2012. DOI: https://doi.org/10.1007/978-3-642-29163-0.

[Ben73] Walter Benz. *Vorlesungen über Geometrie der Algebren. Geometrien von Möbius, Laguerre-Lie, Minkowski in einheitlicher und grundlagengeometrischer Behandlung*. Grundlehren der mathematischen Wissenschaften Bd. 197. Berlin Heidelberg: Springer, 1973. DOI: 10.1007/978-3-642-88670-6.

[Che70] Yi Chen. "Der Satz von Miquel in der Möbiusebene". In: *Mathematische Annalen* 186 (1970), pp. 81–100. DOI: 10.1007/BF01350684.

[Cli82] William K. Clifford. "Synthetic Proof of Miquel's Theorem". In: *Mathematical Papers* (1882), pp. 38–54. URL: https://archive.org/details/mathematicalpap00smitgoog/page/n133/mode/2up.

[Cox61] Harold S. M. Coxeter. *Introduction to Geometry. Second Edition*. Wiley Classics Library, 1961. ISBN: 0471504580.

[Dan16] Tobias Dantzig. "Elementary Proof of a Theorem Due to F. Morley". In: *The American Mathematical Monthly* 23.7 (1916), pp. 246–248. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2973889.

[Dem68] Peter Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete Bd. 44. Berlin: Berlin Heidelberg, 1968. DOI: 10.1007/978-3-642-62012-6.

[Det86] John W. Dettman. *Introduction to Linear Algebra and Differential Equations*. New York: Dover, 1986. ISBN: 0486651916.

[Dor88] Harold L. Dorwart. "Point and Circle Configurations; a New Theorem". In: *Mathematics Magazine* 61.4 (1988), pp. 253–259. ISSN: 0025570X, 19300980. URL: http://www.jstor.org/stable/2689362.

[Har04] Erich Hartmann. "Planar Circle Geometries: an Introduction to Moebius–, Laguerre– and Minkowski–planes". Lecture Notes. Department of Mathematics, Darmstadt University of Technology, 2004. URL: http://www2.mathematik.tu-darmstadt.de/~ehartmann/circlegeom.pdf.

[HK15] Norbert Hungerbühler and Katharina Kusejko. *Steiner's Porism in finite Miquelian Möbius planes*. 2015. arXiv: 1507.01377 [math.CO].

[Hun17] Norbert Hungerbühler. "Endliche Geometrien I". Lecture Notes. ETH Zürich, 2017.

[Hun18] Norbert Hungerbühler. "Endliche Geometrien II". Lecture Notes. ETH Zürich, 2018.

[HV18] Norbert Hungerbühler and Gideon Villiger. *Exotic Steiner Chains in Miquelian Möbius Planes*. 2018. arXiv: 1811.06201 [math.CO].

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. 2nd ed. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1996. DOI: 10.1017/CBO9780511525926.

[LXZ05] Hongbo Li, Ronghua Xu, and Ning Zhang. "On Miquel's Five-Circle Theorem". In: *Computer Algebra and Geometric Algebra with Applications*. Springer Berlin Heidelberg, 2005, pp. 217–228. ISBN: 978-3-540-32119-4.

[Miq36] Auguste Miquel. "Théorèmes de Géométrie". In: *Journal de mathématiques pures et appliquées* 3 ser.1 (1836), pp. 485–487. URL: https://archive.org/details/s1journaldemat03liou/page/486/mode/2up.

[Moo94] Eliakim H. Moore. "A Doubly-Infinite System of Simple Groups". In: *Bulletin of the New York Mathematical Society* 3 (1893/94), pp. 73–79. URL: http://eudml.org/doc/186523.

[Mor07] Frank Morley. "On Reflexive Geometry". In: *Transactions of the American Mathematical Society* 8.1 (1907), pp. 14–24. ISSN: 00029947. URL: http://www.jstor.org/stable/1986231.

[Neu08] Max Neunhöffer. "MT 5826 Finite Fields". Lecture Notes. University of St Andrews, 2007/08. URL: http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2012/ff2012.pdf.

[Rao38] A. Rao. "On the Miquel-Clifford Configuration". In: *Proceedings of the Indian Academy of Sciences - Section A* 7 (1938), pp. 68–74. DOI: 10.1007/BF03045381.

[Sch79] Hans Schwerdtfeger. *Geometry of Complex Numbers. circle geometry, Moebius transformation, non-euclidean geometry*. Dover, 1979. ISBN: 0486638308.

[Ste28] Jakob Steiner. "Questions proposées. Théorème sur le quadrilatère complet". In: *Annales de mathématiques pures et appliquées* 18 (1827/28), pp. 302–304. URL: www.numdam.org/item/AMPA_1827-1828__18__302_0/.

[Var18] Anderson R. Vargas. *The generalization of Miquel's theorem*. 2018. arXiv: 1812.04175 [math.HO].

[WS35] B. L. van der Waerden and L. J. Smid. "Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie". In: *Mathematische Annalen* 110 (1935), pp. 753–776. DOI: 10.1007/BF01448057.